Cibercrimen: Tendencias y desafíos actuales

Coordinadores:

Marina Mínguez Rosique
David Gallego Arribas

Derecho Penal
y Procesal Penal

BOE

CIBERCRIMEN: TENDENCIAS Y DESAFÍOS ACTUALES

COLECCIÓN DE DERECHO PENAL Y PROCESAL PENAL

CIBERCRIMEN: TENDENCIAS Y DESAFÍOS ACTUALES

MARINA MÍNGUEZ ROSIQUE
DAVID GALLEGO ARRIBAS
(Coordinadores)

COLECCIÓN DERECHO PENAL Y PROCESAL PENAL 25

AGENCIA ESTATAL BOLETÍN OFICIAL DEL ESTADO
MADRID, 2025

Primera edición: abril de 2025.

En la página web de la Agencia Estatal Boletín Oficial del Estado, www.boe.es, apartado de *publicaciones,* se incluyen las instrucciones para envío de originales, normas para su presentación y modelo de solicitud de publicación en esta colección que el autor deberá cumplimentar.

La AEBOE no se solidariza con las opiniones sostenidas por los autores de los originales publicados.

https://cpage.mpr.gob.es

NIPO: 144-25-038-8 (edición en papel)
144-25-039-3 (edición en línea, PDF)
144-25-040-6 (edición en línea, ePUB)
ISBN: 978-84-340-3058-9
Depósito legal: M-9574-2025

IMPRENTA NACIONAL DE LA AGENCIA ESTATAL
BOLETÍN OFICIAL DEL ESTADO
Avenida de Manoteras, 54. 28050 Madrid

ÍNDICE

PRÓLOGO

I

El seminario anual de Derecho penal de la Universidad Autónoma de Madrid celebró con éxito su sexta edición los días 22 y 23 de junio de 2023, continuando con la tradición de ofrecer un espacio académico de alto nivel para el análisis y la reflexión sobre temas relevantes en el ámbito del Derecho penal. Este evento se desarrolló siguiendo el formato y el enfoque establecido en sus cinco ediciones anteriores, consolidándose así como un evento fijo en el calendario en el que abordar desde una perspectiva crítica y actualizada los desafíos penales actuales. Precisamente sobre desafíos y actualidad versó esta sexta edición, cuyo tema central fue «Cibercrimen: tendencias y desafíos actuales».

La razón que motivó la elección de este tema no fue sino el vasto abanico de problemas jurídico-penales que plantea, no exentos de complejidad. Y es que, en un mundo cada vez más globalizado y conectado, las tecnologías digitales han transformado todos los aspectos de nuestra vida cotidiana, abriendo nuevas posibilidades en ámbitos tan diversos como la comunicación, la economía, la educación o la cultura. Sin embargo, junto a estas oportunidades, también han surgido riesgos y amenazas que desafían los marcos legales tradicionales. Así, el fenómeno del cibercrimen, en su creciente e imparable expansión, nos ha mostrado la necesidad de enfrentarnos no sólo a nuevas formas delictivas que afectan a diversos bienes jurídicos, sino, también, de hacerlo en un nuevo escenario: un espacio digital, interconectado y globalizado al que se puede acceder desde cualquier lugar del planeta, y en el que el anonimato se configura como un elemento clave que dificulta la trazabilidad y la perseguibilidad de los ataques (que, a mayor abundamiento, pueden llevarse a cabo de manera

instantánea y escalar rápidamente, afectando a multitud de personas en cuestión de segundos).

Durante las dos jornadas que ocupó el seminario, tuvimos la suerte de contar con las ponencias de los/as profesores/as Fernando Miró Llinares (Universidad Miguel Hernández), Fátima Flores Mendoza (Universidad de La Laguna), Ángeles Jareño Leal (Universitat de València-Estudi General) e Ivan Salvadori (Università di Verona), así como con la exposición de las comunicaciones finalistas, que corrieron a cargo de Carlos Trincado Castán (entonces investigador predoctoral de la Universidad del País Vasco y, en la actualidad, Profesor Ayudante en la Universidad de la Laguna) y Mario Santisteban Galarza (investigador predoctoral en la Universidad del País Vasco). Queremos agradecerles a todos/as ellos/as su participación en el seminario, tanto por sus presentaciones como por su participación en el interesante debate que las mismas suscitaron, y, en especial, a los/as Profs. Flores Mendoza, Jareño Leal, Salvadori y Trincado Castán el haber cumplido con el compromiso de enviar sus contribuciones para esta obra colectiva que ahora se publica.

II

El primero de los trabajos, titulado «El lugar de comisión de los ciberdelitos transnacionales. Nuevos desafíos para su persecución» es obra de la profesora Flores Mendoza. En él se aborda cómo el fenómeno de los ciberdelitos, impulsado por la naturaleza descentralizada y global de Internet, presenta un desafío significativo para el Derecho penal, en la medida en la que permite la ejecución de hechos que trascienden de una determinada frontera espacial. El ciberespacio, caracterizado por su naturaleza transnacional, ha transformado las dinámicas tradicionales de la comunicación y la jurisdicción en el ámbito de delitos que abarcan desde el acceso no autorizado a información y fraudes, hasta la difusión de contenidos prohibidos, como la pornografía infantil y los mensajes de odio.

La Profa. Flores Mendoza resalta cómo, a pesar del carácter transnacional de la cibercriminalidad, la posibilidad de su enjuiciamiento queda condicionada al cumplimiento de determinados principios contenidos en las distintas legislaciones penales nacionales que limitan la capacidad jurisdiccional de los Estados. Así, se examina cómo el principio de territorialidad, unido a la teoría de la ubicuidad, puede acabar produciendo dos consecuencias diametralmente opuestas: la impunidad o una concurrencia masiva de jurisdicciones.

En relación con el debate sobre la impunidad, la autora destaca la relevancia que ha cobrado en los delitos de contenido, también conocidos como

delitos de difusión o de expresión, donde la doctrina, especialmente la alemana, ha señalado que muchas conductas delictivas, como las injurias, el acoso o la incitación al odio, pueden quedar sin sanción si se difunden desde un país que no las penalice. Estos delitos, caracterizados como de mera actividad, se cometen sin necesidad de un resultado material, complicando la determinación del lugar de comisión y la jurisdicción aplicable. A pesar de que se pueden invocar principios de extraterritorialidad para su enjuiciamiento, la dificultad de cumplir con exigencias como la doble incriminación pueden llevar a vacíos legales.

Sin embargo, como una suerte de otra cara de la misma moneda, la propia estructura de comisión estos ciberdelitos, que dependen de la difusión de información a múltiples receptores, sugiere que, en realidad, suelen existir varios lugares de comisión. Internet, a menudo descrito como una autopista de información sin límites, provoca que el ciberdelito se manifieste sin restricción geográfica, lo que implica que las conductas delictivas de difusión pueden ser consideradas cometidas en todos los países desde donde se emite la información y en aquellos donde es recibida. Este fenómeno da lugar a una multilocalización física que se opone a la deslocalización virtual, evidenciando la universalización de los delitos en el ciberespacio.

Esto, que limitaría la posibilidad de impunidad, incrementaría el riesgo de concurrencia o colisión entre distintas jurisdicciones nacionales, debido al efecto de la aplicación combinada del principio de territorialidad y la teoría de la ubicuidad. Como en el supuesto anterior, este conflicto jurisdiccional es especialmente problemático en el contexto de los delitos de mera comunicación, lo que acaba generando un riesgo evidente de transgredir el principio de *non bis in idem*.

Ante esto, la autora señala cómo la doctrina alemana ha propuesto restricciones a la aplicación de la legislación penal para evitar que los distintos Estados asuman un rol de vigilancia en el ciberespacio, exigiendo el cumplimiento de condiciones adicionales como, por ejemplo, la nacionalidad del autor o de la víctima. En cualquier caso, a nivel internacional, no existen reglas claras para resolver esta concurrencia, como lo evidencian, por ejemplo, los convenios contra la delincuencia organizada y cibercriminalidad, que no proporcionan criterios de preferencia en la jurisdicción.

Ante la dificultad de establecer una justicia penal internacional efectiva para los ciberdelitos, la Profa. Flores Mendoza acaba concluyendo que la solución a corto plazo radica en fortalecer la colaboración internacional en ámbitos legislativos, judiciales y policiales, con el objetivo de combatir eficazmente esta forma de delincuencia y evitar la impunidad, así como la posible

vulneración de los principios de justicia. Mientras se avanza en este sentido, es crucial mejorar el control y la supervisión de Internet para abordar los riesgos asociados a la cibercriminalidad.

III

El segundo trabajo que el lector podrá encontrar es el de la Profa. Jareño Leal, titulado «El delito de acoso en el ámbito digital del artículo 172 ter.5 del Código Penal. Con una referencia especial a los casos de *deepfake* sexual». En este, la autora lleva a cabo un análisis de la nueva conducta delictiva –introducida por la Ley Orgánica 10/2022, de garantía integral de la libertad sexual– consistente en la creación de perfiles falsos o anuncios en redes sociales mediante el uso de la imagen de la víctima sin su consentimiento, generando situaciones de acoso, hostigamiento o humillación.

La Profa. Jareño Leal evidencia cómo la necesidad de tipificar expresamente dicha conducta en el artículo 172 ter.5 CP surge de las dificultades que algunos tribunales encontraban para encajar determinadas conductas de «acoso digital» en el artículo 172 ter.1 CP –como tipo básico de acoso–, en la medida en la que este último exige una reiteración sistemática de la conducta. Así, en alguna ocasión, la conducta consistente en la publicación de un anuncio con datos personales de la víctima en una página web de contactos sexuales –ofreciendo esos servicios a cambio de un precio– fue considerada atípica por la ausencia de reiteración del acto.

Como destaca la autora, la nueva modalidad de acoso introducida en el artículo 172 ter.5 CP acaba con el problema anterior, pues permite sancionar la creación de perfiles falsos sin necesidad de reiteración, reconociendo el impacto que incluso una única acción puede tener sobre la libertad y dignidad de la víctima, especialmente en contextos digitales. Asimismo, la autora evidencia otras diferencias con lo previsto en el artículo 172 ter.1 CP. En primer lugar, en el artículo 172 ter.5 CP, el acoso u hostigamiento es realizado por terceras personas, no por quien crea el perfil falso, esto es, el sujeto activo del delito. De igual manera, tampoco sería necesario demostrar una alteración de la vida cotidiana, como exige el acoso del artículo 172 ter.1 CP. De igual modo, el nuevo tipo penal contempla la «humillación» como un posible resultado, incluso si no se produce acoso, lo que genera un problema de desproporción punitiva al equiparar conductas de diferente gravedad bajo la misma sanción.

Estas características reflejan, a juicio de la autora, la complejidad del nuevo delito y la necesidad de un equilibrio interpretativo para su correcta aplicación. Así, por ejemplo, propone que, en virtud del principio de interven-

ción mínima, se consideren atípicos aquellos casos en los que el acoso no se materializa ni la conducta contiene elementos humillantes, evitando así una aplicación desproporcionada.

De igual modo, la Profa. Jareño Leal examina las posibles relaciones concursales del nuevo artículo 172 ter.5 CP, especialmente en aquellos casos en los existe una reiteración de la conducta y se genera una alteración en la vida cotidiana de la víctima. En este punto, la autora alerta de que la pena prevista para el artículo 172 ter.5 CP es más leve que la prevista en el artículo 172 ter.1 CP. Por ello, para evitar una suerte de desproporción por defecto, sería preferible aplicar el artículo 172 ter.1 CP cuando la conducta sea reiterada, afecte la vida cotidiana de la víctima y se utilice la imagen de esta de manera insistente.

Además, en la contribución también se evidencia que existen supuestos que no están plenamente cubiertos por el artículo 172 ter.5 CP, como la creación de un perfil falso utilizando los datos de contacto, pero no la imagen de la víctima, que ocasione acoso o hostigamiento. En estos casos, la conducta no encaja en ninguna de las modalidades de acoso del artículo 172 ter CP, dejando como única opción recurrir al delito de injurias con publicidad (artículo 208 CP), que ofrece una respuesta penal menos severa.

Por último, en la parte final del trabajo, la Profa. Jareño Leal aborda la potencial subsunción bajo el artículo 172 ter.5 CP de los supuestos de *deepfake*, en los que a partir de inteligencia artificial u otros programas se crean imágenes hiperrealistas de personas. Considera la autora que, en la medida en la que el artículo 172 ter.5 CP no protege únicamente el contenido moral del derecho a la imagen, la creación de imágenes simuladas, cuando sean utilizadas para acosar o humillar a una persona, pueden subsumirse dentro del tipo. La elaboración de un *deepfake* en contextos sexuales puede llevar al mismo nivel de acoso, humillación y daño psíquico que una imagen auténtica, especialmente si se acompaña de datos personales que facilitan la identificación de la víctima. En cualquier caso, de cara al futuro será crucial modificar la legislación para abordar estas conductas y garantizar una protección adecuada para las víctimas.

IV

En tercer lugar, se publica el trabajo del Prof. Salvadori titulado «Cibercrimen y uso ilícito de la inteligencia artificial: retos y desafíos del Derecho penal». En este, el autor aborda de modo comparativo la evolución que ha seguido la legislación jurídico-penal europea, italiana y española, consecuencia de la irrupción de las tecnologías de la información en el desarrollo de actividades delictivas.

Lo que al principio se percibía como una simple adaptación de delitos tradicionales a un nuevo entorno –lo que se conoce como «vino viejo en botellas nuevas»– pronto reveló una realidad más compleja: los nuevos medios informáticos no solo ofrecían nuevas formas de delinquir, sino que también creaban nuevos objetos y bienes jurídicos que requerían una protección distinta –«vino nuevo en botellas nuevas»–.

El rápido avance de las tecnologías, especialmente con la llegada de Internet, desbordó las capacidades de los sistemas legales tradicionales, que intentaron infructuosamente encajar estos nuevos crímenes dentro de marcos normativos preexistentes. Sin embargo, la sofisticación y alcance de estos delitos, junto con la falta de respuestas jurídicas adecuadas, dejaron en evidencia la necesidad de reformas profundas.

Frente a este desafío, el autor analiza cómo países como Italia y España iniciaron un proceso de reformas –muchas de ellas impulsadas por la necesidad de alinearse con las directivas europeas– en sus legislaciones penales, creando nuevos tipos delictivos para abordar la nueva delincuencia de manera específica. En ambos casos, los legisladores optaron por no crear leyes especiales ni agrupar los delitos cibernéticos en categorías autónomas, sino, más bien, por integrar estas nuevas figuras dentro de los delitos tradicionales, lo que, según la opinión del Prof. Salvadori, ha llevado a resultados normativos no siempre satisfactorios.

Sin embargo, como el autor también resalta, en pleno siglo XXI, la irrupción de la inteligencia artificial ha dado un giro aún más radical al panorama criminal. Una de las innovaciones más transformadoras de nuestra era, también presenta riesgos significativos. Los delitos cometidos mediante inteligencia artificial plantean cuestiones que van más allá de lo conocido, generando incertidumbres jurídicas y nuevos retos para los sistemas penales. Así, aunque la IA aún no ha alcanzado un nivel de autonomía que la convierta en un sujeto potencialmente responsable en el ámbito del Derecho penal, su impacto ya está reconfigurando el panorama de la ciberseguridad.

Uno de los ejemplos más alarmantes empleados por el autor es el *spear phishing*, una forma avanzada de engaño donde los atacantes, utilizando inteligencia artificial y técnicas como el *deepfake*, logran recrear imágenes, voces o identidades de personas de confianza para engañar a sus víctimas y obtener datos sensibles. Los casos de suplantación de identidad se han vuelto tan realistas que incluso altos ejecutivos han sido manipulados para realizar transferencias millonarias basadas en videoconferencias falsas.

El Prof. Salvadori analiza cómo el marco legal actual en países como Italia y España intenta lidiar con estos nuevos desafíos, aunque con diferencias

significativas. En Italia, el Código Penal contempla sanciones específicas para quienes, mediante engaño, suplantan identidades con fines de lucro o daño. En España, sin embargo, el castigo para la suplantación de identidad digital es menos claro, lo que puede llegar a dificultar la persecución de estos delitos en el entorno *online*. En cualquier caso, concluye que una correcta interpretación *lege lata* de los distintos preceptos penales es suficiente a efectos de evitar vacíos normativos que impidan el castigo de aquellos que empleen este tipo de tecnología en sus actividades delictivas.

V

Por último, pero desde luego no menos importante, se publica una de las comunicaciones seleccionadas, en concreto, la del Prof. Trincado Castán, titulada «La protección penal de la historia clínica digital». En ella, el autor aborda el delito de descubrimiento y revelación de secretos en el ámbito sanitario, destacando como el propio avance de la digitalización incrementa los riesgos de accesos no autorizados a datos personales y sensibles (principalmente, por empleados de las instituciones que gestionan dichos datos).

El Prof. Trincado Castán destaca como, si bien el artículo 197.2 del Código Penal castiga específicamente estas conductas, su redacción y contenido genera diversos problemas. Por un lado, presenta ambigüedades al describir acciones similares, pero sin resultar clara la exigencia o no de un perjuicio respecto de cada una de ellas. Por otro lado, en la medida en la que los datos de salud son considerados especialmente sensibles, el acceso a ellos sin autorización puede acarrear penas especialmente graves y elevadas, sobre todo si quien comete la infracción es un funcionario. Esto plantea dilemas sobre la proporcionalidad de las penas, y sobre si determinadas infracciones, como los accesos por curiosidad, deben quedar abarcadas por el Derecho penal (y, si es así, si deben llevar asociada pena de prisión) o si, en virtud del principio de *ultima ratio*, bastaría con la intervención del Derecho administrativo. En este sentido, el autor acaba concluyendo que una reforma legal que aclare estos puntos parece necesaria para una mejor aplicación de la ley y un tratamiento más justo de estos delitos.

Marina Mínguez Rosique y David Gallego Arribas

Coordinadores

EL LUGAR DE COMISIÓN DE LOS CIBERDELITOS TRANSNACIONALES. NUEVOS DESAFÍOS PARA SU PERSECUCIÓN

Fátima Flores Mendoza*

I. INTERNET AL SERVICIO DE LA COMISIÓN DE DELITOS TRANSNACIONALES

De Internet se ha dicho que constituye una autopista de la información y comunicación de masas libre y universal en la que no existen fronteras espaciales o temporales [1].

No es de extrañar entonces el elevado número de ciberdelitos transnacionales que, utilizando como medio comisivo la red de redes, hacen notar sus efectos más allá de las fronteras del Estado en el que se lleva a cabo la actividad delictiva [2]. En este trabajo se partirá por tanto de un concepto amplio de ciberdelitos, entendidos como aquellos que se ejecutan en el ciberespacio [3], ya

* Profesora Titular de Derecho penal, Universidad de La Laguna.

[1] Romeo Casabona, C. M., *Los delitos de descubrimiento y revelación de secretos,* Valencia (Tirant lo Blanch), 2004, p. 60.

[2] Para la definición de delito transnacional podemos partir de la recogida en el art. 3.2 del Convenio contra la Delincuencia Organizada Transnacional de la ONU, aprobado por la resolución 55/25 de la Asamblea General, de 15 de noviembre de 2000: *«A los efectos del párrafo 1 del presente artículo, el delito será de carácter transnacional si: a) Se comete en más de un Estado; b) Se comete dentro de un solo Estado, pero una parte sustancial de su preparación, planificación, dirección o control se realiza en otro Estado; c) Se comete dentro de un solo Estado, pero entraña la participación de un grupo delictivo organizado que realiza actividades delictivas en más de un Estado; o d) Se comete en un solo Estado, pero tiene efectos sustanciales en otro Estado»*. A pesar de que el convenio se ocupa de la delincuencia organizada transnacional relacionándola con diversas formas de criminalidad como el terrorismo, tráfico de seres humanos, de armas, drogas, etc., curiosamente, no la relaciona con la delincuencia económica, a salvo del blanqueo de capitales, ni con la ciberdelincuencia.

[3] Así, Miró Llinares, F., *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio,* Madrid (Marcial Pons), 2012, pp. 43 y ss.

sean delitos que tengan por objetivo la Red, delitos específicos de la propia Red, y que por tanto solo pueden ejecutarse en el ciberespacio, o simplemente delitos que se cometen en el ciberespacio.

Entre los delitos más frecuentes cometidos a través de Internet se encuentran no solo las conductas de sabotaje contra las infraestructuras, sistemas y datos informáticos mediante el uso de la Red, sino también los accesos no autorizados a información ajena o interceptación de las comunicaciones (espionaje), gran diversidad de fraudes, piratería, o la difusión de determinados contenidos: de pornografía infantil, incitación al odio, a la violencia y a la discriminación en redes sociales, de adoctrinamiento y captación terrorista, además de los cada vez más frecuentes de acosos, injurias, amenazas, etc.

Esta nueva tecnología de la era digital permite obtener, procesar y transmitir de forma automatizada grandes cantidades de información en tiempo real desde casi cualquier punto del mundo a todo el planeta (ciberespacio). Funciona simultáneamente como medio de publicación y de comunicación de carácter descentralizado y está orientada por la libertad de información y comunicación, donde el usuario puede ser a la vez emisor y receptor [4].

Estas características exclusivas de amplitud y diversidad de contenidos, automatismo, interactividad, multiubicación, universalización de uso, alcance global o internacional y descentralización constituyen su gran potencial, pero también el origen de la vulnerabilidad del sistema, convirtiéndolo en un poderosísimo instrumento técnico al servicio del crimen.

Esto es así, fundamentalmente, por las dificultades para controlar las comunicaciones e información que circula por la red, la potencialidad multiplicadora o amplificadora de sus efectos (contenidos, programas malignos, facilidad de réplica de los ataques), la posibilidad de actuación clandestina y la existencia de paraísos informáticos, representando todo ello verdaderos obstáculos para el descubrimiento y persecución de los delitos cometidos a través de ella [5]. Así, tanto el colosal número de usuarios como de la información, la frecuencia de accesos y su carácter descentralizado, dificultan el control de las comunicaciones y la información que circula a través de Internet. Asimismo, la posibilidad de acceder a la red de forma anónima o a través de identidad falsa, desde cualquier terminal o servidor del ciberespacio en cualquier momento y cambiar unos y otros con total facilidad, de ocultar la comisión del

[4] Sobre estas características, vid. más ampliamente el estudio de Morón Lerma, E., *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la red,* Pamplona (Aranzadi), 2002, pp. 114 y ss.

[5] Romeo Casabona, C. M., «De los delitos informáticos al Cibercrimen», en Romeo Casabona, C. M., (coord.), *El Cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales,* Granada (Comares), 2006, pp. 2 y ss.

delito o dificultar su rastreo, de ampliar sus efectos gracias, entre otras características, a su alcance global o internacional y automatismo, favorecen la comisión de delitos al tiempo que dificultan su persecución [6].

Ante este panorama, los Estados se han visto obligados, además de a mejorar y ampliar sus sistemas de seguridad frente a estas amenazas, a perfeccionar su sistema de justicia penal, adaptando los tipos penales o creando nuevas figuras delictivas a esta nueva realidad [7], pero también abordando los problemas a los que conduce esta delincuencia de carácter transfronterizo, como son el establecimiento de las bases de la responsabilidad penal de los intermediarios de Internet y la determinación de la jurisdicción aplicable y, con ella, la del lugar de comisión del delito. De esta última, considerada como una de las cuestiones centrales de los ciberdelitos [8] y a la que ha prestado especial atención la doctrina alemana [9], me ocuparé en este trabajo.

II. LA DETERMINACIÓN DE LA LEY PENAL APLICABLE EN EL ESPACIO PARA LOS CIBERDELITOS

A pesar del marcado carácter internacional o transnacional de la cibercriminalidad, la ley penal aplicable a la misma no posee un carácter internacional, sino nacional, dada la complejidad técnica para justificar la existencia de un sistema penal internacional, pero fundamentalmente por la reserva de los Estados a ceder parte de su soberanía [10].

Se plantea entonces un problema de determinación de la ley penal aplicable en el espacio, que debe abordarse de acuerdo con las normas nacionales de determinación de la jurisdicción. Esta cuestión es resuelta mayoritariamente en el Derecho penal contemporáneo a través del principio de territorialidad, que conduce a la aplicación de la ley penal de los Estados en los que tiene lugar

---

[6] Romeo Casabona, C. M., 2006, pp. 3 y 10.

[7] Romeo Casabona, C. M., 2006, p. 10.

[8] Como así lo ha considerado Fischer, T., *Strafgesetzbuch mit Nebengesetzen,* München (C. H. Beck), 2018, § 9 Rd 5.

[9] Entre otros, Eser, A., «Internet und internationales Strafrecht», en Leipold, D., (Hrsg.), *Rechtsfragen des Internet und der Informationsgesellschaft,* Heidelberg (Müller), 2002, pp. 303 y ss.; Weigend, T., «Unbegrenzte Freiheit oder grenzlose Strafbarkeit im Internet?», en Hochloch, G., (Hrsg.), *Recht und Internet,* Baden-Baden (Nomos), 2001, pp. 85 y ss.; Sieber, U., «Internationales Strafrecht im Internet. Das Territorialitätsprinzip der §§ 3, 9 StGB im globalen Cyberspace», *Neue Juristische Wochenschrift,* núm. 29, 1999, pp. 2065 y ss.; Hilgendorf, E., «Überlegungen zur strafrechtlichen Interpretation des Ubiquitätsprinzip im Zeitalter des Internet», *Neue Juristische Wochenschrift,* núm. 29, 1997, pp. 1873 y ss.

[10] Como así apunta Flores Prada, I., «Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia», *Revista Electrónica de Ciencia Penal y Criminología,* núm. 17, 2015, p. 20.

la comisión del delito. Este principio se complementa con otros de carácter supletorio, que extienden la jurisdicción de los Estados más allá de sus fronteras y del alcance de su soberanía. Son los llamados principios de extraterritorialidad: personalidad activa, personalidad pasiva, protección de intereses nacionales, justicia universal (protección de intereses internacionales o de interés para la comunidad internacional) y justicia supletoria.

Conforme al principio de territorialidad, de aplicación preferente en las legislaciones de nuestro entorno [11], la determinación de los lugares de comisión de este grupo de delitos transnacionales, como en el resto, deberá resolverse de acuerdo con la teoría de la ubicuidad, mayoritaria en derecho comparado [12] y exigida por la Unión Europea en diversas directivas en materia penal [13], a fin de evitar lagunas de punibilidad.

En nuestro ordenamiento jurídico, el principio de territorialidad se encuentra regulado en el art. 23. 1 de la Ley Orgánica del Poder Judicial. Sin embargo, ni este precepto, ni ningún otro de la Ley Orgánica del Poder Judicial, de la Ley de Enjuiciamiento Criminal o del Código Penal, establece cuál es el lugar de comisión del delito, a diferencia de otras legislaciones de nuestro entorno, o de alguno de nuestros antecedentes legislativos [14].

Para resolver esta cuestión, históricamente se han propuesto tres soluciones. La de la teoría de la acción, que entiende que el delito se considera cometido allí donde haya tenido lugar toda o parte de la acción. La de la teoría del resultado, que propone que el lugar de comisión del delito será el lugar en el que se produzca su resultado. Y la de la teoría de la unidad o ubicuidad, que defiende que el delito se entenderá cometido tanto en el lugar en el que se lleve a cabo toda o parte de la acción, como en el lugar en el que se produzca su

---

[11] Así, García Sánchez, B., *Límites a la ley penal en el espacio,* Barcelona (Atelier), 2004, p. 24.

[12] Sánchez García de Paz, I. / Blanco Cordero, I., «Problemas de derecho penal internacional en la persecución de delitos cometidos a través de Internet», *Actualidad Penal,* núm. 7, 2002, p. 169; Mata y Martín, R., *Delincuencia informática y Derecho Penal,* Madrid (Edisofer), 2001, p. 146.

[13] Como entre otras, Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, sobre los ataques a los sistemas de información (art. 12.1 a); 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 (art. 12.1); Directiva UE 2017/1371 del Parlamento Europeo y del Consejo, de 5 de julio de 2017, sobre la lucha contra el fraude que afecta a los intereses financieros de la Unión a través del Derecho penal (art. 11.1 a); Directiva 2017/541 UE del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo (art. 19.1 a); Directiva 2011/92 UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil (art. 17.1 a); Decisión Marco 2008/913 JAI, de 28 de noviembre de 2008 relativa a la lucha contra determinadas formas y manifestaciones de racismo y xenofobia mediante el Derecho penal (art. 9.1 a). En todas ellas se establece que los Estados tendrán jurisdicción para enjuiciar tales conductas cuando se hayan cometido *«total o parcialmente en su territorio»*.

[14] Al respecto, García Sánchez, B., 2004, p. 68.

resultado. Esta última es la defendida mayoritariamente por la doctrina y jurisprudencia en nuestro país [15].

De acuerdo con la teoría de la unidad o ubicuidad y de la clasificación de los delitos en atención a si cuentan o no con un resultado, se defiende mayoritariamente que los delitos de mera actividad se entenderán cometidos en el lugar o lugares en los que se lleve a cabo la acción, mientras que los delitos de resultado, material o de peligro concreto, se considerarán cometidos tanto en el lugar o lugares en los que se realice la acción como en el lugar o lugares en los que se produzca el resultado. Para esta teoría constituye lugar de comisión del delito todo aquel en el que haya tenido lugar total o parcialmente el delito; esto es, bastaría que la acción, una parte de ella o tan solo el resultado tuviese lugar en el territorio sometido a la soberanía de un Estado para ejercitar la jurisdicción conforme al principio de territorialidad.

Tradicionalmente, el lugar de comisión del delito ha sido uno, dada la escasa frecuencia de los delitos a distancia, esto es, aquéllos en los que acción y resultado concurren en lugares diferentes [16], o de aquéllos otros en los que la acción se desarrolla en sitios diferentes. Sin embargo, en los ciberdelitos, el número de delitos a distancia ha aumentado considerablemente, siendo gran parte de ellos delitos transnacionales. Consecuentemente, en tales supuestos el delito se entenderá cometido, como mínimo, en dos lugares, en dos Estados, siendo aplicables la ley penal de cada uno de ellos. Sin perjuicio de la concurrencia de un mayor número de jurisdicciones de acuerdo con los principios de extraterritorialidad como los de personalidad activa, personalidad pasiva, protección de intereses o justicia universal. Ante esta realidad, nos enfrentaremos en la mayoría de las ocasiones a un problema de concurrencia de jurisdicciones que, de no resolverse adecuadamente, podría dar lugar a una vulneración del *ne bis in idem*. Pero, por otro lado, tampoco se puede descartar de forma absoluta la impunidad de estos delitos, a pesar de su carácter transnacional. Comencemos por esta última cuestión.

III. ¿ES POSIBLE LA IMPUNIDAD DE LOS CIBERDELITOS TRANSNACIONALES?

Esta posibilidad de impunidad ha sido planteada especialmente por la doctrina alemana en relación con los denominados delitos de contenido

[15] Por todos, García Sánchez, B., 2004, pp. 68 y ss.

[16] Como los de los conocidos ejemplos del paquete postal que contiene una bomba que estalla en un lugar diferente a aquél en el que se elaboró, o el del veneno que causa la muerte de una persona en un lugar diferente a aquél en el que el asesino lo introdujo en su comida.

(Inhaltsdelikte) [17], o también conocidos como delitos de difusión *(Verbreitungsdelikte),* de expresión o declaración (*Äußerungsdelikte*) [18] o incluso de comunicación *(Komuniktionsdelikte)* [19].

También por parte de nuestra doctrina se han empleado algunas de estas denominaciones. Hasta ahora, la más común ha sido la de delitos de expresión, referida a todas aquellas conductas que pueden entrar en conflicto con la libertad de expresión, como las injurias y calumnias, las vejaciones, la incitación al odio y al terrorismo, e incluso las amenazas [20]. Y ello a pesar de que también se venía utilizando para designar a aquellas figuras delictivas en las que existe discordancia entre lo que el sujeto activo sabe o conoce y aquello que declara (falso testimonio, calumnias) [21]. No obstante, la más frecuente entre los ciberdelitos es la de delitos de contenido [22]. Y, en mi opinión, es la más adecuada debido a su amplitud, pues abarca no solo a todos los delitos de expresión, declaración u opinión, sino también a muchos otros que no responden a esta denominación, como las conductas de acoso, piratería intelectual e industrial, fraude publicitario, e incluso las de amenaza [23].

Estos son mayoritariamente delitos de mera actividad, en los que el tipo de lo injusto no requiere de la producción de un resultado, material o de peligro, sobre el objeto material [24]. Por tanto, en ellos no contamos con un lugar de producción del resultado, tan solo con el lugar de comisión de la acción [25]. De

---

[17] Eser, A., 2002, p. 312.

[18] Así, Fischer, T., 2018, § 9, Rd 5a.

[19] Así, Bremer, K., *Strafbare Internet-Inhalte in internationaler Hinsicht. Ist der Nationalstaat wirklich überholt?,* Frankfurt am Main (Peter Lang), 2001, p. 53.

[20] Así, la STS 846/2015, de 30 de diciembre (FJ 1.º). En relación con las injurias, vid. el ATS de 17 de enero de 2006. También, respecto de las amenazas, Quintero Olivares, G, «Delitos contra la libertad», en Quintero Olivares, G. (dir.), *Comentarios a la Parte Especial del Derecho Penal,* 9.ª ed., Cizur Menor (Aranzadi/Thomson Reuters), 2011, p. 208. En relación con las conductas de enaltecimiento y apología del terrorismo, Cuerda Arnau, M. L., «Delitos contra el orden público», en González Cussac, J. L. (coord.), *Derecho Penal. Parte Especial,* 8.ª ed., Valencia (Tirant lo Blanch), 2023, pp. 919 y ss.

[21] Al respecto, Cerezo Mir, J., *Curso de Derecho Penal Español. Parte General. II,* 6.ª ed., Madrid (Tecnos), 2004, p. 123.

[22] Así, Barrio Andrés, M., *Ciberdelitos. Amenazas criminales del ciberespacio,* Madrid (Reus), 2017, p. 59, para el que, bajo el término delitos de contenidos, se encuentran aquellos que persiguen no solo la difusión o distribución, sino también la creación de contenidos ilegales (p. 100); Miró Llinares, F., 2012, p. 100; y, ya antes, Romeo Casabona, C. M., 2006, p. 4.

[23] Si bien doctrina y jurisprudencia las ha clasificado como delitos de expresión, no siempre las amenazas pueden entrar en conflicto con la libertad de expresión. Por ejemplo, en los supuestos de anuncio de un mal constitutivo de delito.

[24] Asimismo, muchas de estas conductas, al menos las correspondientes figuras del Código Penal alemán, también se corresponden con las categorías de delitos de peligro abstracto o abstracto-concreto. Al respecto, Kappel, J., *Das Ubiquitätsprinzip im Internet. Wie weit reicht das deutsche Strafrecht?,* Hamburg (Dr. Kovač), 2007, pp. 118 y 130.

[25] Así, Fischer, T., 2018, § 9, Rd 5c y 6, a pesar de que un sector de la doctrina defiende que también en estos podemos contar con un lugar de producción del resultado. Sobre estas posiciones, vid. Fischer, 2018, § 9, Rd 8 y 8a.

acuerdo con el principio de territorialidad y la teoría de la ubicuidad, tan solo los Estados en los que se haya ejecutado total o parcialmente la acción típica tendrían jurisdicción para su persecución, por lo que se ha planteado la posibilidad de que tales conductas puedan quedar impunes si la difusión o distribución de los contenidos se llevase a cabo desde un Estado que no la castigase (paraíso penal de Internet) o no tuviese interés en perseguirla [26, 27]. Especialmente ha preocupado esta cuestión en Alemania debido a que la difusión de contenidos en la Red se reconduce a un reducido número de acciones que limitan el alcance del lugar de comisión del delito [28]. Pero el mismo riesgo podría darse en los delitos de resultado que no llegaran a consumarse y que, por tanto, solo pudiesen perseguirse en grado de tentativa.

Para evitar esta posible impunidad de acuerdo con el principio de territorialidad, podría recurrirse a la aplicación extraterritorial de la ley penal nacional a través de los principios de personalidad activa, personalidad pasiva, principio de protección (de intereses nacionales), principio de justicia universal, principio de justicia supletoria, etc. No obstante, tampoco ellos eliminarían el riesgo, dado que están sujetos a una serie de condiciones y requisitos como la doble incriminación, difícil de superar si no se cuenta con la necesaria armonización internacional y se mantienen los paraísos penales de Internet, la relación tasada de delitos, la necesidad de denuncia, etc. [29]. A ellos habría de sumarse los límites de la extradición y entrega de los responsables (doble incriminación, prescripción, no entrega de nacionales, etc.). Pero, en mi opinión, tal riesgo es mínimo, dado que este grupo de delitos cuenta con múltiples lugares de comisión, posiblemente tantos o más que los concurrentes en un ciberdelito de resultado.

Y ello es así, en primer lugar, por la propia estructura y características de este grupo de delitos, basada en la difusión de contenidos. De acuerdo con la descripción típica de todas estas figuras, cuya acción consiste en difundir, divulgar, distribuir, revelar, ceder, comunicar públicamente, poner a disposición, etc., se requiere que la información emitida sea o bien recibida y, en su caso, comprendida por múltiples receptores, o, al menos, que se permita tal posibilidad. Esto supondría que el lugar de comisión de la acción sería tanto aquel en

---

[26] Entre nosotros, Romeo Casabona, C. M., 2006, p. 37; Sánchez García de Paz, I. / Blanco Cordero, I., *Actualidad Penal,* núm. 7, 2002, p. 168.

[27] Por todos, Sieber, U., *Neue Juristische Wochenschrift,* núm. 29, 1999, p. 2067.

[28] En efecto, si bien el Código Penal alemán cuenta con acciones equivalentes a las del nuestro, las aplicables a las conductas cometidas a través de la Red se reconducen básicamente a la de puesta a disposición pública *(öffentlich zugänglich machen),* dado que las comunicaciones electrónicas, según la opinión dominante, estarían excluidas de los tipos de difusión *(verbreiten),* como se verá más abajo.

[29] Sobre estos principios, García Sánchez, B., 2004.

el que se produjese la emisión, como todos los lugares donde se llevase a cabo la recepción múltiple, esto es, donde se encontrasen los receptores reales o, en su caso, potenciales [30]. Ello se debe a su condición de delitos de comunicación, cuya acción típica no se consuma con la mera exteriorización del mensaje o contenido a comunicar. Por tanto, este tipo de figuras, a pesar de constituir delitos de mera actividad, contarían con múltiples lugares de comisión de la acción, y, consecuentemente, del delito; al menos, un lugar de emisión y múltiples lugares de recepción, todos aquellos donde haya llegado la información o contenido emitido [31].

Así se mantiene por parte de la doctrina española al tratar la consumación de los delitos de difusión de contenidos [32] y exigir que el contenido, ilícito o no (pornografía, contenidos de odio, injuriosos, publicidad incierta, secretos, anuncio del mal, etc.), llegue a conocimiento de una multitud de personas, en unos casos, o, al menos, de un único individuo, en otros [33]. Y ello con independencia de que este elemento forme parte de la acción o constituya el resultado típico y de que en los tipos de difusión o divulgación se exija que el mensaje llegue a conocimiento de uno o múltiples receptores. En efecto, si bien existe consenso sobre la consumación, se discute tanto la consideración de delitos de mera actividad de muchos de estos tipos [34], como el alcance de la difusión y

---

[30] También así, Werle, G. / Jessberger, F., «Ort der Tat», en Weigend, T. / Dannecker, G. / Werle, G. (Hrsg.), *Leipziger Kommentar. StGB,* 12 Auf., Berlin (De Gruyter), 2011, § 9, Rd 82 y s. En cambio, cuando la transmisión del contenido se realiza a través de una mera puesta a disposición *(Zugänglichmachen)* y no de difusión *(Verbreitung),* tanto el Tribunal Supremo alemán como parte de la doctrina alemana consideran que a través de esta acción típica tan solo contaríamos con un lugar de la acción, aquel desde el que se introduce en la Red el contenido, con el consiguiente problema de impunidad ya comentado. Vid. la BGHSt 47,60 (2001), que, en un caso de pornografía infantil a través de Internet, señala que la puesta a disposición tan solo requiere que los contenidos estén disponibles en la Red y puedan ser percibidos por terceros, sin necesidad de que los usuarios accedan al mismo. Y, de forma más contundente, Werle, G./ Jessberger, F., 2011, § 9, Rd 84.

[31] Así también, Eser, A., «Ort der Tat», en Schönke, A. / Schröder, H., *Strafgesetzbuch Kommentar,* 29 Auf., München (C. H. Beck), 2014, § 9, Rd 7c, considerando que el lugar desde el que se descarga o accede a un contenido es lugar de comisión de la acción *(Tätigkeitsort)* y no del resultado *(Erfolgsort).*

[32] Pues son escasos los trabajos que se ocupan del lugar de comisión de los ciberdelitos de contenido.

[33] Sobre esta cuestión, más ampliamente, Flores Mendoza, F., «Análisis del lugar de comisión de los ciberdelitos de contenido ¿Impunidad o universalización del delito?», *Cuadernos de Política Criminal,* núm. 128, 2019, p. 136 y ss.

[34] Mayoritariamente todos los tipos de lo injusto señalados se consideran delitos de mera actividad. Así, respecto de las amenazas, Cuerda Arnau, M. L., «Delitos contra la libertad (II)», en González Cussac, J. L. (coord.) *Derecho Penal. Parte Especial,* 8.ª ed., Valencia, (Tirant lo Blanch), 2023, p. 185, quien señala que esta es también la posición mayoritaria de la jurisprudencia. En relación con los delitos contra la intimidad, Romeo Casabona, C. M., «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en Díez Ripollés, J. L. / Romeo Casabona, C. M. (eds.), *Comentarios al Código Penal. Parte Especial II,* Valencia (Tirant lo Blanch), 2004, p. 781. De la misma opinión, para las injurias y calumnias, Quintero Olivares, G. / Morales Prats, F., «Delitos contra el honor», en Quintero Olivares, G. (dir.), *Comentarios a la Parte Especial del Derecho Penal,* 9.ª ed., Cizur Menor (Aranzadi/Thomson Reuters), 2011, p. 534.

divulgación respecto de la revelación [35]. Pero, la consideración como delitos de resultado de muchas de estas figuras [36], en nada obstaculizaría la concurrencia de múltiples lugares de comisión del delito, que ahora se presentarían como lugares del resultado. Y, por otro lado, aunque el tipo de lo injusto no exigiera contar con múltiples lugares de recepción, nada lo impediría y, en cualquier caso, precisaría al menos de dos lugares de comisión, el de la emisión y el de la recepción.

En segundo lugar, lo que determina decisivamente que este tipo de conductas cuenten con múltiples lugares de comisión es su condición de ciberdelitos, esto es, la utilización de Internet como instrumento de transmisión de la información. Las cualidades técnicas de este medio de comunicación ofrecen una mayor potencialidad de divulgación de los contenidos frente a los tradicionales (prensa, radio o televisión), especialmente cuando se recurre a sus específicos modelos de publicación abiertos (páginas electrónicas/web, redes sociales) [37]. Y ello con independencia de que la acción típica de estas figuras delictivas consista en una mera cesión o en una revelación que requiera tan solo un único punto de recepción.

Por todo ello, difícilmente se podrían plantear problemas de impunidad en relación con este tipo de conductas. En el supuesto de que el contenido (ilícito) fuese emitido desde un Estado que no persiguiese su difusión (por ej. pseudopornografía, publicidad falsa) o no tuviese interés en hacerlo (por ej. en relación con contenidos homófobos), la conducta se entendería igualmente ejecutada en todos aquellos otros Estados receptores del contenido, en los que sí sería punible su distribución.

---

[35] En el ámbito de los delitos contra la intimidad, vid. Bolea Bardón, C., «Delitos contra la intimidad», en Corcoy Bidasolo, M. (dir.) *Manual de Derecho Penal. Parte Especial I,* 3.ª ed., Valencia (Tirant lo Blanch), 2023, p. 348, señalando que la doctrina y jurisprudencia mayoritaria de nuestro país exigen un mayor alcance de publicidad para la difusión frente a la revelación o cesión. Considerando indiferente que la información se transmita a una o más personas, Romeo Casabona, C. M., «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en Romeo Casabona, C. M. / Sola Reche, E. / Boldova Pasamar, M. A. (coords.), *Derecho Penal. Parte Especial,* 3.ª ed., Granada (Comares), 2023, p. 325.

[36] Así, frente a la doctrina y jurisprudencia mayoritaria, un sector mantiene que estos delitos son de resultado. Así, por ejemplo, respecto de las amenazas, Díez Ripollés, J. L., «De las amenazas», en Díez Ripollés, J. L. / Gracia Martín, L. / Laurenzo Copello, P. (eds.), *Comentarios al Código Penal. Parte Especial I,* Valencia (Tirant lo Blanch), 1997, p. 782; en relación con la difusión de secretos y datos personales y familiares, Rueda Martín, M. A., *La nueva protección de la vida privada y de los sistemas de información en el Código Penal,* Barcelona (Atelier), 2018, pp. 135 y ss.; para las injurias y calumnias, Laurenzo Copello, P., «Delitos contra el honor», en Díez Ripollés, J. L. / Romeo Casabona, C. M. (eds.), *Comentarios al Código Penal. Parte Especial II,* Valencia (Tirant lo Blanch), 2004, pp. 963, 1010 y ss. y 1033.

[37] Y, en menor medida, cuando se emplea como medio de comunicación cerrada (mensajería instantánea, correo electrónico, chat, etc.).

Consecuentemente, para su persecución bastaría entonces con la aplicación del principio de territorialidad de acuerdo con la teoría de la ubicuidad, no siendo necesario recurrir a los principios subsidiarios de extraterritorialidad, que tendrían un alcance más limitado, dadas sus exigencias, ya comentadas, de doble incriminación (principio de personalidad activa), vinculación del hecho con el Estado que pretende ejercer la jurisdicción (principio de justicia universal), o la reducción a un catálogo más o menos tasado de delitos (principio de protección de intereses o de justicia universal). Pero, en todo caso, los problemas de persecución no estarían excluidos, pues habría que contar con la extradición o entrega de los responsables, que no siempre es fácil de conseguir debido a sus respectivos límites (doble incriminación, prescripción, no entrega de nacionales, etc.) y a los criterios políticos que operan en estas figuras.

No lo ha entendido así la doctrina alemana, para la que esta cuestión sigue siendo un tema de discusión [38]. En el Código Penal alemán las acciones equivalentes también serían las de difundir *(verbreiten),* declarar *(äußern),* publicar *(öffentlichen)* o hacer accesible *(zugänglich machen)* [39]. Sin embargo, la aplicable a las conductas cometidas a través de la Red será básicamente la puesta a disposición pública *(öffentlich zugänglich machen),* dado que las comunicaciones electrónicas, según la opinión dominante, estarían excluidas de los tipos de difusión de documentos, que exigen la transmisión física o material de aquellos, no siendo suficiente la mera comunicación del contenido [40]. De acuerdo con esta interpretación, los tipos de lo injusto construidos a partir de esta acción, delitos de mera actividad y de peligro abstracto básicamente [41], se consumarían con el mero hecho de hacer accesible a terceros el contenido. De esta forma, el lugar de comisión del delito sería tan solo el de la emisión, no así los lugares de recepción del contenido (reales o, incluso, potenciales) [42], no pudiendo configurarse como delitos a distancia [43]. Consecuentemente, el lugar de comisión se reduciría a uno, en el peor de los casos, incrementándose considerablemente los supuestos de impunidad en muchas conductas.

---

[38] Vid., entre otros, FISCHER, T., 2018, § 9, Rd 5; WERLE, G. / JESSBERGER, F., 2011, § 9, Rd 73.

[39] KAPPEL, J., 2007, p. 113.

[40] Así, SIEBER, U., «Strafrechtliche Verantwortung für den Datenverkehr in internationalen Computernetzen (2)», *Juristen Zeitung,* núm. 51, 1996, p. 495.

[41] Vid., por todos, CORNILS, K., «Die territorialen Grenzen der Strafrecht und Internet», en HOCHLOCH, G. (Hrsg.), *Recht und Internet,* Baden-Baden (Nomos), 2001, p. 76.

[42] Así, RÖMER, N., *Verbreitungs- und Äußerungsdelikte im Internet,* Frankfurt am Main (Peter Lang), 2000, pp. 93 y ss.

[43] KIENLE, M., *Internationales Strafchrecth und Straftaten in Internet. Zum Erfordenis der Einschränkung des Ubiquitätsprinzips des § 9 Abs. 1 Var. 3 StGB,* Konstanz (Hartung-Gorre), 1998, pp. 68 y ss.

Es por ello que la doctrina, a fin de evitar lagunas de punibilidad en la comunicación de contenidos publicados en el extranjero, pero accesibles desde Alemania (ej. pornografía, mensajes de odio, etc.), propone ampliar el lugar de comisión del delito, bien a través del lugar de comisión de la acción, bien del lugar de producción del resultado, ofreciendo diversas soluciones que van desde considerar lugar de comisión del delito aquel en el que se sitúa el servidor en el que están alojados los contenidos, a la de mantener que también los delitos de peligro abstracto cuentan con un lugar de producción del resultado, pasando por aquella otra que considera que este no se corresponde con aquel en el que tiene lugar el resultado del tipo de lo injusto *(Tatbestanderfolg),* sino con aquel otro en el que se produce cualquier efecto o consecuencia de la acción *(Tathandlungserfolg)* [44].

De acuerdo con la propuesta ya expuesta, tales soluciones me parecen innecesarias cuando no distorsionadoras [45], pues suponen la modificación de conceptos y estructuras consolidadas, como la definición del lugar del resultado propio de la teoría de la ubicuidad, o la posición de que los delitos de mera actividad y de peligro abstracto no precisan de resultado típico. Además de que, paradójicamente, la búsqueda de soluciones a la impunidad mediante criterios de extensión del lugar de comisión del delito ha tenido como consecuencia la ampliación de la vigencia ley penal nacional a todos los delitos de difusión cometidos en el ciberespacio, lo que tampoco ha convencido a la doctrina alemana, que ha visto la necesidad de restringir esta ampliación a través de criterios de diverso tipo, que comentaré más abajo.

Pero, por otro lado, este instrumento de comunicación plantea nuevas cuestiones de difícil solución, hasta ahora inexistentes entre los delitos transnacionales. En efecto, por un lado, introduce una doble realidad que, en mi opinión, surge con los ciberdelitos y, especialmente, con los de contenido: la universalización del delito como consecuencia de su multilocalización [46], con la consiguiente intensificación de la aplicación de las leyes penales nacionales [47].

Todo ello es resultado de las particularidades o caracteres intrínsecos de este medio de comunicación y del espacio en el que se proyecta, el ciberespacio, que supone una modificación de las coordenadas espacio-tiempo frente al

---

[44] De las diferentes propuestas da cuenta Fischer, T., 2018, § 9, Rd 5; Kappel, J., 2007, pp. 108 y ss.

[45] También críticamente Eser, A., 2002, pp. 318 y ss.

[46] Universalización entendida, de acuerdo con la cuarta acepción del Diccionario de la Real Academia Española, como acción de hacer algo universal, que se extiende por todos los países.

[47] Se trataría de una especie de *hiperactividad,* de admitirse este término en este sentido.

espacio físico [48]. De Internet se ha dicho que constituye una autopista de la información y comunicación de masas libre y universal en la que no existen fronteras espaciales o temporales [49]. Y, por lo que a este trabajo interesa, la ausencia de fronteras espaciales supone contar con un espacio virtual de carácter transnacional, en su relación con el espacio geográfico [50]. Por tanto, si el ciberespacio no tiene fronteras espaciales, el ciberdelito tampoco las tiene.

Consecuentemente, y tal y como se ha señalado, de acuerdo con el principio de territorialidad, la teoría de la ubicuidad, la acción típica propia de los delitos de difusión y, especialmente, las características del medio de comunicación, tales conductas deben entenderse cometidas en todos aquellos Estados desde los que se haya emitido la información, pero también en todos aquellos en los que esta haya sido recibida o, en su caso, desde los que sea accesible. Siendo así, el lugar de comisión de las conductas de difusión de contenidos a través de la Red podría alcanzar teóricamente a todo el mundo geográfico (del primero al tercer mundo) [51]. Es por ello que se produce un fenómeno de multilocalización desde una perspectiva física o geográfica, sin perjuicio de que en el plano virtual pueda hablarse de una deslocalización [52], pues aquí no se produce una traslación del lugar de comisión del delito, sino que este se ejecuta en múltiples lugares físicos, de ahí su internacionalización o universalización [53]. Por la misma razón, tampoco se puede hablar de *Deterritorialisierung,* en referencia a la ley penal nacional [54], pues no se produce una expansión de la misma o universalización respecto del espacio físico o geográfico, al no tener lugar

---

[48] Vid., más ampliamente, Miró Llinares, F., 2012, pp. 145 y ss.

[49] Romeo Casabona, C. M., 2004, p. 60. Estas notas de universalidad y libertad constituyen caracteres extrínsecos del ciberespacio que Miró Llinares, F., 2012, pp. 152 y ss., desarrolla en el siguiente sentido. Universalidad, entendida como generalización o popularización, al menos teóricamente, pues la realidad política y económica de algunos estados implican restricciones en su utilización. Y libertad, comprensiva de los siguientes aspectos: como realidad desregulada, descentralizada, neutral o sin censuras, dinámica o en constante mutación.

[50] Lo configura como un carácter intrínseco básico del ciberespacio, Miró Llinares, F., 2012, pp. 153 y ss.

[51] Lo que no ha sucedido hasta ahora con el resto de los medios de comunicación de masas como la prensa, la radio o la televisión, salvo que se trate de televisión o radio por satélite. Pero incluso en estos casos, aunque la información pudiese llegar técnicamente a todo el planeta, lo cierto es que su uso no presenta la misma relevancia que la que tiene actualmente Internet. A pesar de que como advierte Miró Llinares, F., 2012, p. 153, este tampoco presenta un alcance universal en el sentido de su popularización, dadas las limitaciones políticas y económicas existente en determinados Estados.

[52] Así, Miró Llinares, F., 2012, p. 111, al tratar la difusión de pornografía infantil.

[53] En este grupo de delitos lo único que se traslada o transmite es la información, los contenidos, pero no el delito. Críticamente con este resultado, Werle, G. / Jessberger, F., «Ort der Tat», en Weigend, T. / G. Dannecker, G. / Werle, G. (Hrsgs.), *Leipziger Kommentar. StGB,* 12 Auf., Berlin (De Gruyter), 2011, § 9, Rd 91.

[54] Así, Eser, A., 2014, § 9, Rd 7.

una aplicación extraterritorial de la misma [55], sino, como he señalado, una especie de *hiperactividad* o aumento de su aplicación, debido a las características de la realidad sobre la que actúa la criminalidad en el ciberespacio. Y, paradójicamente, este incremento se debe a la aplicación del principio de territorialidad sin limitaciones a un grupo de delitos [56], y no como consecuencia del principio de justicia universal, que, de acuerdo con su carácter extraterritorial, sí supone la expansión de la jurisdicción de un Estado más allá del territorio sometido a su soberanía, al menos por lo que respecta a nuestra legislación y para el catálogo de delitos más o menos tasado al que tradicionalmente se ha vinculado [57].

A fin de evitar las situaciones descritas de multilocalización y consecuente intensificación de la actividad de las leyes penales nacionales, pero también la tentación de los Estados de convertirse en guardianes del ciberespacio, cuando no obligación por aplicación del principio de legalidad, la doctrina alemana ha ofrecido diversas soluciones de restricción a la aplicación de la ley penal nacional [58], sin que por el momento exista consenso al respecto [59]. Estas limitaciones, que precisarían de la correspondiente previsión legislativa, van desde exigir que el autor dirija dolosamente su conducta contra el Estado que pretende ejercer la jurisdicción conforme a la teoría de la ubicuidad (criterio de restricción subjetivo) [60], a establecer vínculos de conexión objetivos, algunos de los cuales recuerdan a los límites propios de los principios de extraterritorialidad, como la nacionalidad del responsable o de la víctima, el tipo de contenido, el idioma en el que estos se publican [61], el modelo de comunicación *(push-technology)* [62], bien exigiendo la doble incriminación de la conducta o

---

[55] En contra de lo defendido por Fischer, T., 2018, § 9, Rd 5c, para el que sí puede hablarse de una aplicación universal de las leyes penales nacionales.

[56] Aunque claramente condicionados al uso de un concreto medio de comunicación: Internet.

[57] Vid. el art. 23.4 de la Ley Orgánica del Poder Judicial hasta las reformas operadas por las Leyes 1/2009, de 3 de marzo, y 1/2014, de 13 de marzo, que redujeron considerablemente el alcance de este principio, hasta el momento ilimitado de acuerdo con su tenor literal.

[58] Sobre las mismas vid, entre otros, Kappel, J., 2007, pp. 141 y ss.; Kienle, M., 1998, pp. 159 y ss.

[59] Eser, A., 2014, § 9, Rd 7.

[60] Sin embargo, esta propuesta no sería viable dado que el lugar de comisión del delito no forma parte del tipo de lo injusto de las figuras delictivas, no debiendo ser abarcadas por el dolo. Así, Romeo Casabona, C. M., 2006, p. 35.

[61] El idioma no resulta adecuado, dado que el lenguaje de la Red es básicamente el inglés y, también, porque supondría dejar la jurisdicción de tales conductas al mundo anglosajón. De forma similar, Hilgendorf, E. / Frank, T. / Valerius, B., *Computer- und Internetstrafrecht. Ein Grundiss,* Berlin (Springer), 2005, p. 72.

[62] De la misma forma, tampoco parece convincente reducir la aplicación de la ley penal al hecho, a veces irreflexivo por parte del autor, de difundir los contenidos a través de modelos de comunicación dirigida y/o cerrada (correos electrónicos, mensajería instantánea, etc.), propio de las *push-technology,* en lugar de modelos abiertos *(pull-technology),* en los que el contenido se pone a disposición en la Red, y que requieren que el usuario se descargue la información (bitácoras o blogs).

recurriendo, finalmente, a criterios de oportunidad o subsidiariedad, que, en la práctica, entiendo que son los que se están imponiendo en todos los Estados.

IV. DE LA NECESARIA COLABORACIÓN INTERNACIONAL PARA RESOLVER LA CONCURRENCIA DE JURISDICCIONES

Por otro lado, la cibercriminalidad lleva aparejada otro problema, en esta ocasión propio de los delitos transnacionales, pero de mayor incidencia entre los ciberdelitos, cual es la concurrencia de múltiples jurisdicciones nacionales competentes para el enjuiciamiento de los ciberdelitos, en atención no solo al principio de territorialidad, sino también de acuerdo con los de extraterritorialidad. Especialmente problemática podría ser esta cuestión en relación con los ciberdelitos de comunicación, teniendo en cuenta su carácter universal (multilocalización). Ante este panorama, el conflicto jurisdiccional entre los Estados no será imposible [63]. En tales supuestos, el problema estará entonces en establecer qué ley penal nacional sería la aplicable o qué Estado tendría la competencia preferente para castigar estas conductas a fin de evitar la prohibición del *non bis in idem* [64].

En el orden internacional no existe ninguna regla para resolver la concurrencia de leyes penales nacionales en la lucha contra la delincuencia transnacional [65], ni parece que sea posible conseguirlo a corto plazo, o, con carácter general, en supuestos con notas de internacionalidad o extranjería en atención a la nacionalidad o residencia de los responsables, los sujetos pasivos, o el interés de terceros estados, etc. Así, el mencionado Convenio contra la Delincuencia Organizada Transnacional plantea el problema en su art. 15.5, pero no establece ningún criterio de preferencia [66]. En el mismo sentido se plantea la cuestión en el art. 22.5 del Convenio sobre Cibercriminalidad del Consejo de

---

[63] Apuntando también la ineludible existencia de conflictos jurisdiccionales, Barrio Andrés, M., 2017, pp. 44 y ss.

[64] En el mismo sentido, García Sánchez, B., 2004, p. 65.

[65] En el ámbito interno, el Tribunal Supremo en el Acuerdo de Pleno no jurisdiccional de 2 de marzo de 2005 establece el criterio de la prioridad temporal: «El delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales será en principio competente para la instrucción de la causa».

[66] Art. 15.5: «Si un Estado Parte que ejerce su jurisdicción con arreglo a los párrafos 1 o 2 del presente artículo ha recibido notificación, o tomado conocimiento por otro conducto, de que otro u otros Estados Parte están realizando una investigación, un proceso o una actuación judicial respecto de los mismos hechos, las autoridades competentes de esos Estados Parte se consultarán, según proceda, a fin de coordinar sus medidas».

Europa, de 23 de noviembre de 2001 [67]. Tampoco lo hacía la Decisión Marco del Consejo de la Unión Europea, de 25 de febrero 2005, relativa a los ataques contra los sistemas de información, más allá de reconocer la prioridad del principio de territorialidad frente al de personalidad activa [68], y la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, que la sustituye, ni siquiera plantea esta cuestión en su art. 12. La razón puede estar en que para la doctrina la solución pasa por el acuerdo entre los Estados [69].

Ante tal situación no resultará imposible, por tanto, que una determinada conducta pueda ser enjuiciada y, en su caso, castigada por más de un Estado, dado que la prohibición del *non bis in idem,* a pesar de su reconocimiento internacional [70], no forma parte del derecho interno de todos los Estados, ni está regulado de la misma forma en los que sí lo reconocen [71].

Por ello, y dada la dificultad para lograr, incluso a largo plazo, una justicia penal internacional para los ciberdelitos, que posiblemente no se logre en determinados temas y con determinados Estados [72], la solución a corto plazo necesariamente debe conducir a la ampliación, mejora e intensificación de la colaboración internacional en materia legislativa, judicial y policial. Esta coo-

---

[67] Art. 22.5: «Cuando varios Estados reivindiquen una competencia respecto a una infracción descrita en el presente Convenio, los Estados implicados se reunirán, cuando ello sea oportuno, a fin de decidir cuál de ellos está en mejores condiciones para ejercer la persecución».

[68] Art. 10.4: «Cuando una infracción sea competencia de más de un Estado miembro y cualquiera de estos Estados pueda legítimamente iniciar acciones judiciales por los mismos hechos, los Estados miembros de que se trate colaborarán para decidir cuál de ellos iniciará acciones judiciales contra los autores de la infracción, con el objetivo de centralizar, en la medida de lo posible, dichas acciones en un solo Estado miembro. Con este fin, los Estados miembros podrán recurrir a cualquier órgano o mecanismo creado en el marco de la Unión Europea para facilitar la cooperación entre sus autoridades judiciales y la coordinación de sus actuaciones. Se podrán tener en cuenta los siguientes criterios por orden consecutivo: el Estado miembro en cuyo territorio se hayan cometido las infracciones de acuerdo con los apartados 1, letra a), y 2; el Estado miembro del que sea nacional el autor; el Estado miembro en el que se haya encontrado al autor».

[69] Sobre esta cuestión, Vogel, J., «Principio de legalidad, territorialidad y competencia judicial», en Tiedemann, K. (dir.) *Eurodelitos. El Derecho Penal económico en la Unión Europea,* Cuenca (Universidad Castilla-La Mancha), 2004, p. 34, que señala la falta de regulación al respecto y la dificultad de establecer criterios aceptados por todos los estados. Frente a una solución vertical, como podría ser, por ejemplo, aquella impuesta por el Tribunal de Justicia de la Unión Europea, considera más adecuada una solución horizontal de consenso entre los diferentes Estados implicados en el conflicto. Para favorecer este acuerdo, Flores Prada, I., *Revista Electrónica de Ciencia Penal y Criminología,* núm. 17, 2015, pp. 30 y ss. apunta varios criterios para determinar la jurisdicción preferente.

[70] Está reconocido en el art. 14.7 del Pacto Internacional de Derechos Civiles y Políticos de 1966. A nivel europeo en el art. 7 del Convenio Europeo de Derechos Humanos y de las Libertades Fundamentales de 1950 y en el art. 50 de la Carta de Derechos de la Unión Europea de 2007.

[71] De la misma opinión, U. Sieber, U. / Cornils, K. (Hrsg.), *Nationales Strafrecht in rechtsvergleichender Darstellung. Allgemeiner Teil.* Band. 2, Berlin (Duncker & Humblot), 2008.

[72] Schwarzeneger, C., «Der räumliche Geltungsbereich des Strafrechts im Internet», en *Schweizerische Zeitschrift für Strafrecht,* núm. 118, 2000, p. 129; Flores Prada, I., *Revista Electrónica de Ciencia Penal y Criminología,* núm 17, 2015, p. 20.

peración debe tener como objetivos prioritarios la lucha eficaz contra este tipo de delincuencia, evitando tanto la impunidad como la posible vulneración del principio *ne bis in idem,* tanto los conflictos de jurisdicción o competencia como la expansión de la ley penal de estados que pretendan actuar como guardianes del mundo [73]. Pero hasta que éste se produzca, es conveniente que la cooperación policial y judicial internacional se refuerce y se mejore la actividad de control y supervisión de Internet [74].

[73] Así, Romeo Casabona, C. M., 2004, p. 62; Sieber, U., *Neue Juristische Wochenschrift,* núm. 29, 1999, pp. 272 y ss.

[74] Schwarzeneger, C., «Der räumliche Geltungsbereich des Strafrechts im Internet», en *Schweizerische Zeitschrift für Strafrecht,* núm. 118, 2000, p. 129.

EL DELITO DE ACOSO EN EL ÁMBITO DIGITAL DEL ART. 172 TER.5 DEL CÓDIGO PENAL. CON UNA REFERENCIA ESPECIAL A LOS CASOS DE *DEEPFAKE SEXUAL*

Ángeles Jareño Leal*

I. EL DELITO DE ACOSO EN EL ÁMBITO DIGITAL

La Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual, introdujo el párrafo 5 del art. 172 ter CP, regulando una nueva forma de acoso junto al delito de coacciones («El que, 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, será castigado con pena de prisión de tres meses a un año o multa de seis a doce meses. Si la víctima del delito es un menor o una persona con discapacidad, se aplicará la mitad superior de la condena») [1]. En la exposición de motivos no se proporcionan argumentos para la exégesis del precepto, que se fundamenta en una genérica razón de «violencia sexual cometida en el ámbito digital». De manera que parece obedecer a la finalidad de proporcionar la máxima cobertura en dicho contexto, tipificando conductas que, pese a no ser las más frecuentes, sí han planteado problemas de encuadre típico cuando se han producido. El hecho de que el legislador haya creado una nueva figura, en lugar de adicionar estas conductas al acoso ya existente en el art. 172 ter.1 CP,

* Catedrática de Derecho penal. Universidad de Valencia. Trabajo realizado dentro del grupo de investigación: *Los límites del ius puniendi y su aplicación a los delitos y las penas* (IUSPEN) GIUV2023-576.

[1] La redacción actual del inciso final del precepto, referido a la víctima menor o persona con discapacidad, proviene de la reforma efectuada por la Ley Orgánica 1/2023, de 28 de febrero.

conduce a la conclusión de que existe una voluntad de marcar distancia. Quizás se deba al deseo de encuadrar este tipo en un contexto sexual, en sintonía con la Ley que la introdujo (de «garantía integral de la libertad sexual»), aunque de la redacción del precepto no puede desprenderse una delimitación de tal naturaleza, pudiendo afirmarse que otras conductas que no la tengan también tendrán encaje típico en el párrafo 5. En todo caso, ha quedado abierta la puerta al concurso con el tipo descrito en el 172 ter.1.3.ª CP («Mediante el uso indebido de sus *datos personales,* adquiera productos o mercancías, o contrate servicios, o *haga que terceras personas se pongan en contacto con ella»).*

Aunque el nuevo delito ha sido tipificado a continuación de las conductas de acoso coactivo del art. 172 ter.1 CP, el bien jurídico no es totalmente coincidente con éste, al exigirse determinados resultados que tienen que ver también con otros bienes como el honor («humillación», acercando este delito al de injurias); junto, naturalmente, a la libertad de obrar y decidir («acoso», «hostigamiento»). Así, también queda abierta la vía para apreciar el concurso con los delitos contra el honor o contra la intimidad, en su caso, como señala el propio art. 172 ter.3 CP («Las penas previstas en este artículo se impondrán sin perjuicio de las que pudieran corresponder a los delitos en que se hubieran concretado los actos de acoso»). Además, sobre el art. 172 ter.1 CP se discute si se produce la lesión de la libertad de decidir o de obrar; pero, en mi opinión, ambas pueden resultar indistintamente laceradas, sin que ello perturbe la interpretación de los requisitos típicos de dicho precepto, como puede comprobarse analizando los casos que resuelve la jurisprudencia [2].

II. ¿ERA NECESARIO INTRODUCIR EN EL CÓDIGO PENAL LA NUEVA MODALIDAD DE ACOSO?

Para entender la necesidad de introducir el nuevo delito hay que comprobar la efectividad que haya podido tener el delito de acoso ya existente en el art. 172 ter.1 CP con respecto a las conductas que ahora se protegen específicamente, a la vista de la dificultad que existía para encajarlas en los diferentes numerales del citado precepto.

Antes de la reforma 10/2022, la jurisprudencia había venido incluyendo los casos de acoso en el ámbito digital, en ocasiones, dentro de dicho art. 172 ter.1 CP, pese a la existencia de determinadas dificultades típicas, las cuales ponía muy

[2] De otra opinión, Matallín Evangelio, A., «Delito de acoso», en González Cussac, J. L. (dir.), *Comentarios a la Reforma del Código Penal de 2015*, 2.ª ed., Valencia (Tirant lo Blanch), 2015, p. 577.

bien de manifiesto la SAP Granada 55/2021, de 18 de febrero, que rechazó la aplicación de dicho precepto para el caso de una mujer que, por venganza, insertó un anuncio con la foto y número de teléfono de otra en una página *web* de contactos sexuales, ofreciendo determinados servicios a cambio de precio, debiendo soportar esta última numerosas llamadas solicitando contacto. Para la Sala no existía en este caso un delito de acoso del art. 172 ter.1.3.º CP por no darse la reiteración sistemática y prolongada en el tiempo de la conducta que requiere dicho precepto («(…) el que acose a una persona llevando a cabo de forma insistente y reiterada (…) mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella»), ya que, en el caso enjuiciado, un solo acto era el que había producido el «efecto complejo» de que la víctima recibiese numerosas llamadas de terceros. Por eso, el Tribunal calificó los hechos como delito de injurias de los arts. 208, 209 y 211 CP (a mi juicio correctamente), ya que no se había tratado de una «simple molestia por tener que contestar a las comunicaciones de los interesados, sino de poner en entredicho una cuestión tan íntima como es la del ejercicio sexual en todas sus facetas (cómo, cuándo y con quién), que afecta no sólo a la propia estimación sino a la consideración social de un bien personal tan íntimo».

Sin embargo, no era ésta la línea de trabajo habitual en la jurisprudencia antes de la reforma 10/2022, que se decantaba por acoger en el acoso del art. 172 ter.1 CP los casos que ahora integran el nuevo delito del párrafo 5. A título de ejemplo, pueden citarse la SAP Granada, de 27 de febrero, que, sin cuestionar el obstáculo típico que señala la sentencia anteriormente citada, sí que condenó por el delito de acoso del art. 172 ter.1 CP en un caso en que el sujeto también abrió un perfil en una red social a nombre de su expareja, publicando su fotografía y teléfono, solicitando citas con terceras personas, si bien aquí el autor perpetró los mismos hechos en dos ocasiones; la SAP Granada 88/2018, de 27 de febrero, condenando por el art. 172 ter.2 CP, sin especificar qué numeral del párrafo 1 concurría, al hombre que creó un perfil, con la fotos y teléfono de la expareja, en una página de contactos; la SAP Cádiz 397/2021, de 2 de diciembre, condenando por acoso al hombre que publicó un anuncio en una página *web* de contactos con fotografías de su expareja exhibiendo zonas íntimas del cuerpo, acompañadas de su correo electrónico y teléfono, ofreciendo servicios sexuales a cambio de determinado precio (en este caso en concurso con el delito del art. 197.7 CP, por difundir la imagen íntima sin consentimiento de la titular); la SAP Madrid 429/2019, de 11 de julio, condenando también por el acoso del art. 172 ter.1 CP al sujeto que elaboró perfiles falsos de otro, con su fotografía, en páginas *web* de contacto sexual; aunque en este caso

dicha conducta quedó diluida por el juzgador dentro de otras que se habían producido en los hechos, y que se incardinaban propiamente en dicho precepto. Así que se trata de decisiones judiciales en las que, tanto si la conducta típica llevada a cabo con medios digitales se ha producido de forma aislada, como cuando ha tenido lugar junto a otros actos físicos de acoso, ha sido incardinada en el art. 172 ter.1 CP de forma indiscriminada.

Por el contrario, en otras ocasiones, la jurisprudencia anterior a la reforma 10/2022 daba prioridad en esta clase de comportamientos a la utilización no consentida de datos personales de un tercero (teléfono, mail, fotografía), para sancionar así el acoso en el ámbito digital por el delito contra la intimidad del art. 197.2 CP («Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado»). Así ocurre en la SAP Barcelona 309/2020, de 1 de julio, cuando una mujer utiliza las fotos de otra (extraídas de *facebook* y *whatsapp),* y sus datos de contacto, para abrir un anuncio ofreciendo servicios sexuales; y de forma similar en la SAP Guadalajara 166/2019, de 14 de octubre.

A partir de esta situación jurisprudencial quedaba planteada la necesidad, o no, de introducir el nuevo modelo de acoso del artículo 172 ter.5 CP. El obstáculo principal para incardinar el acoso en el ámbito digital en las conductas mencionadas en el numeral 3.º del artículo 172 ter.1 CP es la exigencia típica de reiteración de la conducta de este último precepto. Mientras tanto, en el acoso recientemente introducido se tipifica la mera creación de un perfil o anuncio falso con la intención de producir determinados efectos en el sujeto pasivo; con lo que una sola conducta del sujeto activo basta para consumar el tipo penal. Desde luego es innegable que la creación de un único perfil falso con connotación sexual (o no) puede alterar la libertad de decidir o de obrar del sujeto pasivo, o de lesionar su dignidad.

III. DIFERENTES POSIBILIDADES CONCURSALES: ESBOZOS PARA UNA POLÉMICA

1. **Diferencias y similitudes entre las dos modalidades de acoso del art. 172 ter del Código Penal**

Aparte del hecho evidente de que la nueva modalidad de acoso del art. 172 ter.5 CP requiere el uso específico de «la imagen» como objeto del delito,

existen dos características propias que distancian esta clase de acoso del que ya existe desde el año 2015 en el art. 172 ter.1 CP: en primer lugar, en el tipo del párrafo 5, el acoso u hostigamiento es realizado por terceras personas, no por quien ha creado el perfil falso; y, en segundo lugar, no es necesario constatar como resultado del delito la alteración de la vida cotidiana. Veamos estas características típicas del nuevo delito.

A) En el tipo del art. 172 ter.5 del Código Penal el acoso u hostigamiento no es producido por el autor del delito, sino por terceras personas

Una característica fundamental para distinguir las dos modalidades recogidas en el art. 172 ter CP es que en el párrafo 5 la conducta material de acoso u hostigamiento no se lleva a cabo por el que es castigado como autor del delito, sino por terceras personas *(«ocasionándole* a la misma situación de acoso, hostigamiento…»). Así, sin necesidad de realizar más que una única acción (abrir un perfil o un anuncio falsos utilizando la imagen de una persona), la víctima sufre intentos de contacto por parte de terceros, siendo la suma de tales intentos la que ocasiona el acoso u hostigamiento que señala el precepto. Por el contrario, en la modalidad del art. 172 ter.1 CP, el mismo autor del delito es quien lleva personalmente a cabo las reiteradas conductas que alteran el normal desarrollo de la vida cotidiana de la víctima (excepción hecha del segundo inciso de la circunstancia 3.ª del art. 172 ter.1 CP: «…o haga que terceras personas se pongan en contacto con ella»). Por eso, doctrina y jurisprudencia exigen una repetición de *actos suficientes* a dichos efectos [3].

Pero debemos tener presente que el tipo del artículo 172 ter.5 CP también habla de «humillación», y esto implica un resultado diferente en relación con el «acoso u hostigamiento», y permite incardinar en el precepto la conducta consistente en crear un perfil que no da lugar al acoso, pero sí tiene un contenido humillante (supuesto éste en el que sí puede afirmarse que el resultado es producido por el propio autor del delito). Tal posibilidad típica implica que

[3] STS 324/2017, de 8 de mayo: «(…) vocación de persistencia o una intencionalidad, latente o explícita, de sistematizar o enraizar una conducta intrusiva sistemática (persecución, reiteración de llamadas...) capaz de perturbar los hábitos, costumbres, rutinas o forma de vida de la víctima (…) [*L*]a persistencia insistente de esas intrusiones nutre el desvalor del resultado hasta rebasar el ámbito de lo simplemente molesto y reclamar la respuesta penal que el legislador ha previsto (…) [*o*]bligar a la víctima a modificar su forma de vida acorralada por un acoso sistemático sin visos de cesar» (FJ 4.º). Si bien, y en sentido contrario a la doctrina que se acaba de transcribir, también se han incluido en el art. 172 ter.1 CP casos con en los que sólo ha existido una llamada de teléfono y dos mensajes de *whatsapp:* SAP Granada 121/2022, de 15 de marzo.

este precepto está parificando conductas de *resultado material* («ocasionándole a la misma una situación de acoso, hostigamiento») con otras que no lo son (la «humillación»). Siendo esto así, parece claro que existe desproporción punitiva, al estar ambas modalidades abarcadas por la misma pena, equiparándose la conducta de crear un perfil falso con una connotación humillante, con aquella otra en la que, además de crear el perfil falso, la víctima ha sufrido intentos de contacto. También se iguala valorativamente lo que puede ser la tentativa del delito (el autor crea el perfil humillante con la intención de que la víctima sufra hostigamiento de terceros, pero esto no llega a producirse porque el perfil es retirado a tiempo), con la consumación del propio tipo (además de crear el perfil falso la víctima sufre los intentos de contacto). Así que es evidente que no estamos ante la redacción más acertada, lo cual hace necesario buscar un equilibrio valorativo por vía interpretativa, o con la propia aplicación de la pena, que oscila entre prisión o multa.

Por otro lado, nótese que la humillación se presenta como un posible resultado, y no como un grado que cualifique el acoso u hostigamiento. De la misma forma que hacen las modalidades de acoso del art. 173.1, párrafos tercero y cuarto CP, cuando hablan de «actos hostiles *o* humillantes»: así, en el acoso laboral del artículo 173.1, párrafo tercero CP («Con la misma pena serán castigados los que, en el ámbito de cualquier relación laboral o funcionarial y prevaliéndose de su relación de superioridad, realicen contra otro de forma reiterada actos hostiles *o humillantes* que, sin llegar a constituir trato degradante, supongan grave acoso contra la víctima»). Y en el acoso inmobiliario del párrafo cuarto de este precepto («Se impondrá también la misma pena al que de forma reiterada lleve a cabo actos hostiles *o humillantes* que, sin llegar a constituir trato degradante, tengan por objeto impedir el legítimo disfrute de la vivienda»)[4]. Por el contrario, en el acoso «callejero» del art. 173.4, párrafo segundo CP, el término se convierte en adjetivo («…expresiones, comportamientos o proposiciones de carácter sexual que creen en la víctima una situación *objetivamente humillante…»).* Sin detenerme ahora en analizar las razones del legislador en cada caso, sí debe constatarse la diferente repercusión en materia de concursos. En el caso que nos ocupa, el acoso en el ámbito digital del artículo 172 ter.5 CP, creo que es difícil hablar de concurso con el delito

[4] También en el caso del acoso sexual se introduce el resultado «humillante» en el artículo 184 CP («El que solicitare favores de naturaleza sexual para sí o para un tercero, en el ámbito de una relación laboral, docente, de prestación de servicios o análoga, continuada o habitual, y con tal comportamiento provocare a la víctima una situación objetiva y gravemente intimidatoria, hostil *o humillante*…»). De tal forma que también aquí podemos encontrar modalidades de acoso sexual que produzcan diferentes resultados: intimidación, hostilidad o humillación.

contra la integridad moral del artículo 173 1 CP, pues este último requiere un nivel de cosificación de la persona que me parece complicado con la utilización de la imagen. Sobre esta cuestión volveré más adelante.

B) La alteración normal del desarrollo de la vida cotidiana no se exige en la modalidad de acoso del art. 172 ter.5 del Código Penal

Una de las cosas que llama la atención en la jurisprudencia existente sobre el delito de acoso más antiguo, el del art. 172 ter.1 CP, es que, pese a reconocerse que es un delito de resultado, no se ha aplicado el tipo en su modalidad de tentativa, como podría ocurrir cuando el autor despliega un número de actos insuficientes, por su cuantía o por su entidad, para alterar el normal desarrollo de la vida cotidiana de la víctima [5]. Por el contrario, se declara la atipicidad de la conducta cuando los actos realizados no alcanzan entidad suficiente para producir dicho resultado [6]. Pero, en mi opinión, cuando no llega a constatarse ningún cambio en los hábitos cotidianos de la persona afectada, pese a haber desplegado el autor comportamientos de acoso, nada obsta a la aplicación de la tentativa del delito del art. 172 ter.1 CP; sin que ello quiera decir que propongo aquí un mayor despliegue típico del precepto, pues me parece encomiable que la jurisprudencia se mueva con cautela en este terreno, en el que se impone la necesidad de la mínima intervención penal. Aunque siempre hay excepciones, los Tribunales parecen esforzarse en no extender más allá de lo necesario la aplicación del tipo penal (véase la sentencia del Pleno del Tribunal Supremo 324/2017, de 8 de mayo [7]). Con tal práctica están participando de las

[5] A título de ejemplo, exigen la alteración de la vida cotidiana como resultado del delito la STS 344/2020, de 25 de junio, la SAP Barcelona, 604/2020, de 17 de noviembre, la SAP Barcelona 121/2019, de 7 de febrero («se está ante un delito de resultado en la medida en que se exige que las referidas conductas causen directamente una limitación trascendente en alguno de los aspectos integrantes de la liberad de obrar el sujeto pasivo, ya sea en la capacidad de decidir, ya en la capacidad de actuar según lo decidido» (FJ 4.º); SAP Madrid 456/2022, de 8 de septiembre y SAP Madrid 869/2022, de 22 de diciembre.

[6] Como ocurre, por ejemplo, en la STS 324/2017, de 8 de mayo, en la SAP Madrid 221/2019, de 1 de abril, en la SAP Lugo 122/2017, de 28 de junio, y en la SAP Granada 121/2022, de 15 de marzo, (según la Sala, en este último caso sólo había tenido lugar una molestia «generadora de inseguridad»).

[7] FJ 4.º: «Son hechos que, vistos conjuntamente, suponen algo más que la suma de cuatro incidencias, pero que no alcanzan el relieve suficiente, especialmente por no haberse dilatado como resultado del delito en el tiempo, para considerarlos idóneos o con capacidad para alterar gravemente la vida ordinaria de la víctima… Se exige implícitamente una cierta prolongación en el tiempo; o, al menos, que quede patente, que sea apreciable, esa voluntad de perseverar en esas acciones intrusivas, que no se perciban como algo puramente episódico o coyuntural, pues en ese caso no serían idóneas para alterar las costumbres cotidianas de la víctima… El tipo no exige planificación, pero sí una metódica secuencia de acciones que obligan a la víctima, como única vía de escapatoria, a variar, sus hábitos cotidianos. Para valorar esa idoneidad de la acción secuenciada para alterar los hábitos cotidianos de la víctima hay que atender al

críticas doctrinales que suscitó esta modalidad de acoso introducida con la reforma penal 1/2015, de 30 de marzo, al recelar de un tipo penal que parecía sancionar la producción de simples molestias o situaciones incómodas. Sin embargo, y sin que sirva de precedente, el tiempo parece haber dado la razón al legislador, ya que se constatan en los tribunales hechos de notable gravedad para la libertad de decisión y de obrar (y también para la salud síquica) [8].

Sin embargo, el reciente delito del art. 172 ter.5 CP no queda supeditado a la necesidad de alteración del normal desarrollo de la vida cotidiana de la víctima, con respecto a lo cual nada dice el tipo penal. Desde luego lo normal es que al acosar u hostigar a una persona se acabe alterando el desarrollo de su vida cotidiana; pero, aunque esto último no llegue a producirse, también queda consumado el tipo penal. Cabe plantearse, sin embargo, la calificación de aquellos casos en que el resultado de acoso u hostigamiento no llega a producirse, pese a ser la intención del autor, y tampoco existe un contenido humillante del anuncio o perfil. No sería un supuesto muy frecuente si interpretamos este tipo penal dentro de un contexto sexual (que parece ser el que quería darle la Ley orgánica de garantía integral de la libertad sexual que lo introdujo); pero, como vengo sosteniendo, creo que la letra del precepto no lo ha reducido a una interpretación de estas características. Por eso, en el caso apuntado habría que hacer una interpretación acorde con el acoso del art. 172 ter.1 CP, con respecto al que no se aplica la tentativa (principio de intervención mínima), siendo lo más adecuado entender que la conducta señalada ahora también es atípica a efectos del art. 172 ter.5 CP.

Por otro lado, en esta nueva modalidad de acoso no se va a suscitar un problema que se ha descrito en relación con el acoso recogido en el art. 172 ter.1 CP, con respecto al cual se critica que el resultado del delito pueda quedar a merced del sujeto pasivo, que según su capacidad de perturbación alterará, o no, sus hábitos de conducta, sentimiento que puede variar de una persona a otra, aunque la intensidad de los actos de acoso sea la misma. En mi opinión, en dicho precepto no debe bastar, para apreciar el tipo, atender exclusivamente a las manifestaciones de la propia víctima sobre sus sentimientos ante el comportamiento hostigador, pues, tal y como ocurre en el delito de amenazas (con respecto al resultado de que la víctima se sienta intimidada realmente para

estándar del «hombre medio», aunque matizado por las circunstancias concretas de la víctima (vulnerabilidad, fragilidad psíquica,...) que no pueden ser totalmente orilladas».

[8] Jareño Leal, Á., «Delitos contra la libertad (3): las coacciones», en Boix Reig, J. (dir.), *Derecho penal. Parte especial, Vol. I,* 2.ª ed., Madrid (Iustel), 2016, p. 282: «Este tipo de conductas comportan un riesgo serio para la salud síquica de la víctima si se prolongan durante cierto período de tiempo…de ahí que también el «peligro» existente para dicha salud deba considerarse como objeto indirecto de protección del delito».

entender consumado el tipo), la mayor o menor resistencia emocional de ésta no es en exclusiva lo que debe motivar la aparición del delito, aunque por supuesto esta circunstancia debe ser valorada a tales efectos [9]. Por tanto, una mezcla de criterios objetivos y subjetivos es lo que permitirá concluir que la conducta es lo suficientemente intensa como para alterar de forma grave la vida cotidiana de una persona (hay que recordar que, en su redacción original, el precepto decía «altere gravemente…»). Así que, mientras el art. 172 ter.1 CP es tajante exigiendo un determinado resultado típico de alteración del normal desarrollo de la vida cotidiana de la víctima, en el acoso del art. 172 ter.5 CP el resultado es objetivamente evaluable por el juzgador, pues se trata de constatar sólo la existencia de los actos de acoso, sin que los sentimientos del sujeto pasivo sean determinantes a estos efectos.

2. ¿Concurso de normas entre ambas modalidades de acoso del art. 172 ter del Código Penal?

Pese a que, aparentemente, existen claras diferencias típicas entre las dos modalidades de acoso del art. 172 ter CP, siendo la fundamental que el artículo 172 ter.5 CP *no exige* una reiteración de comportamientos ni la alteración de la vida cotidiana de la víctima (además de que debe realizarse utilizando la imagen de una persona), lo cierto es que este precepto *no excluye* la concurrencia de dichas circunstancias y efectos, por lo que no puede descartarse la posibilidad del concurso de normas entre ambas modalidades del art. 172 ter CP. Desde luego no parece posible que el legislador haya sido ajeno a esta posibilidad concursal, pero, probablemente, desde su perspectiva la solución es clara, teniendo en cuenta la connotación sexual que, seguramente, quiso otorgar al acoso en el ámbito digital del artículo 172 ter.5 CP, a tenor de la Ley que lo introdujo. Pero, como he señalado antes, la letra del precepto no cierra su aplicación a casos de dicha naturaleza; y, además, si se entendiera que en esta modalidad de acoso deben incluirse siempre tales supuestos, se produciría la paradoja de que, a tenor de la pena prevista, serían sancionados los casos de naturaleza sexual, y de géne-

[9] Jareño Leal, Á., 2016, p. 282; Torres Roig, M., *El delito de acoso del artículo 172 ter del Código penal,* Valencia (Tirant lo Blanch), 2024, p. 334, propone una modificación que, siguiendo el modelo alemán, exija la idoneidad objetiva del comportamiento que da lugar a que la persona modifique sus costumbres, valorando objetivamente la conducta desplegada por el autor para concluir sobre su «idoneidad» para alterar la vida de una persona independientemente de que, en el caso concreto, haya llegado o no a producirse dicha alteración, bastando con la capacidad de las acciones realizadas para lograr dicho fin.

Sobre la forma de resolver esta cuestión en el delito de amenazas: Jareño Leal, Á., *Las amenazas y el chantaje en el Código penal de 1995,* Valencia (Tirant lo Blanch), 1997, pp. 20 y ss.

ro, más levemente que si se tipifican en el art. 172 ter.1 CP, lo cual no cuadra muy bien con la tónica del legislador de agravar la pena para esta clase de sucesos. El hecho de que el acoso del art. 172 ter.5 CP tenga una pena más leve puede deberse a que no requiere para su consumación la reiteración de conductas.

Partiendo de las afirmaciones anteriores, puede decirse que la posibilidad del concurso de normas queda abierta entre la nueva modalidad de acoso y, en concreto, la del art. 172 ter.1 CP, numeral 3, que no excluye utilizar la imagen de una persona, y es la única de dicho precepto que admite la producción del acoso por parte de terceras personas («Mediante el uso indebido de sus datos personales …o haga que terceras personas se pongan en contacto con ella»). A estos efectos no es determinante recurrir a una supuesta relación de especialidad del artículo 172 ter.5 CP basada en su naturaleza sexual, pues la creación de un perfil falso (utilizando, o no, la imagen), sin tal connotación sexual, también puede producir acoso y humillación: por ejemplo, fingiendo que la persona sostiene una ideología violentamente racista, que presume de realizar determinados delitos, que suscribe opiniones disparatadas o ridículas, que la hacen parecer trastornada, etc. [10] Así que los criterios de solución son otros:

a) Por descontado, lo primero a tener en cuenta es que para llegar al acoso del art. 173 ter.1 CP es necesario una reiteración de conductas que alteren la vida cotidiana de la víctima. Sumando esta exigencia al hecho de que la pena establecida en esta modalidad de acoso es más elevada que la señalada en el párrafo 5, puede concluirse que este precepto debe aplicarse preferentemente cuando se utilice la imagen de una persona para crear perfiles falsos con una connotación sexual, si ello se hace de forma repetida e insistente. De lo contrario, calificando tales casos con el nuevo delito de acoso (al priorizar su naturaleza sexual y el uso de la imagen), resultarían castigados más levemente, lo cual, como ya he señalado, no encaja bien con la habitual política criminal de agravar los atentados de características sexuales o de género.

b) Sin embargo, el mismo supuesto que se acaba de mencionar, pero sin utilizar la imagen de la persona afectada, es decir, creando perfiles falsos de forma reiterada e insistente, ya tengan, o no, una connotación sexual, es evidente que debe reconducirse, necesariamente, al acoso del artículo 172 ter.1 CP, ya que la redacción típica del acoso del art. 172 ter.5 CP expulsa las conductas en las que no se utilice como objeto material la imagen de la víctima.

[10] Por otro lado, la referencia que contiene el artículo 172 ter.5 CP al resultado de «humillación» no condiciona restrictivamente la interpretación de los términos acoso y hostigamiento, a efectos de considerarlos típicos solo cuando comporten un atentado contra la dignidad de la persona, lo que podría alegrase, también, como base para el criterio de la especialidad.

c) Por otro lado, deben llevarse al acoso del artículo 172 ter.5 CP aquellos casos en los que se utiliza la imagen de una persona para crear un único perfil o anuncio falso, que ocasione acoso, hostigamiento o humillación a la víctima, cuando no se hace de forma reiterada e insistente; ya tenga dicho perfil, o no, una naturaleza sexual. Esta conducta no cabe en el acoso del art. 172 ter.1 CP, que exige reiteración de comportamientos.

d) Por último, hay que resaltar que carece de respuesta jurídica, en cualquier apartado del artículo 172 ter CP, la creación de un único perfil o anuncio falso sin utilizar la imagen de una persona, pero sí sus datos de contacto, cuando dicho perfil tenga naturaleza sexual, aunque dé lugar a una situación de acoso u hostigamiento para la víctima. Este supuesto no puede entrar en el acoso del párrafo 1 porque se trata de una sola conducta y no de una reiteración de conductas. Y tampoco cabe en el acoso del párrafo 5 porque no se utiliza la imagen para crear dicho perfil. Para estos casos sólo queda la posible calificación de los hechos como delito de injurias con publicidad.

La falta de solución para este último caso evidencia ciertas incongruencias en la tipificación resultante del art. 172 ter CP, al no cubrir la creación de un único perfil, sin utilizar la imagen de la persona, pero sí su identidad (nombre, mail, teléfono, dirección), que es insertado en páginas de contactos sexuales. La posibilidad de acudir entonces al delito de injurias de los artículos 208 y 209 CP resuelve parcialmente el problema, pero con una respuesta penológica de diferente proporción a las establecidas en los dos delitos de acoso del artículo 197 ter CP [11].

Debe destacarse que siguen quedando en un limbo jurídico determinados comportamientos similares a los anteriores, pero que no persiguen ninguno de los resultados previstos en los párrafos 1 y 5 del art. 172 ter CP, y tampoco encajan en el delito de injurias. Tal ocurre con los hechos descritos en la SAP Zaragoza 191/2022, 6 de junio, en los que una mujer abre una cuenta en una

[11] A un supuesto de estas características se refería la STS 344/2020, de 25 de junio, ratificando el castigo por injurias graves con publicidad, señalando que: «Insertar en páginas de periódicos digitales, dedicados al anuncio de bienes y servicios, contactos de tipo sexual por una persona ajena al propio anunciante, sin su consentimiento, es decir, incluyendo como prestadora de servicios sexuales gratuitos, y sobre la base de una avidez rayana con la ninfomanía, a una tercera persona desconocedora del anuncio, nos parece un clarísimo ejemplo de una acción desarrollada en descrédito y humillación de su persona. No se trata de una simple molestia por tener que contestar a las comunicaciones de los interesados, sino de poner en entredicho una cuestión tan íntima como es la del ejercicio sexual en todas sus facetas (cómo, cuándo o con quien) que afecta no sólo a la propia estimación sino a la consideración social de un bien personal tan íntimo»; añadiendo que «quien imputa falsa y voluntariamente a una mujer ese estilo de sexualidad exagerada no lo hace de manera simplemente descriptiva o sin adoptar postura o juicio de valor, sino todo lo contrario, con intención de que las molestias que reciba de los clientes la humillen» (FJ 5.º).

red social, utilizando la fotografía y el mail de otra, para hacerse pasar por ella y emitir determinados comentarios injuriosos hacia terceras personas. Aunque aquí puede verificarse una parte del tipo del art. 172 ter. 5 CP (abrir una cuenta en una red social utilizando la imagen de otra persona), no se hace con la intención de crear una «situación de acoso, hostigamiento o humillación». Queda el recurso de la jurisdicción civil, con la Ley 1/1982, de protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen, que, en su artículo séptimo, apartado 6, considera una intromisión ilegítima en el ámbito de protección de dicha Ley: «La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o *de naturaleza análoga»* (aunque no está exento de problemas encajar aquí la conducta citada) [12].

3. **El resultado de «humillación» en el art. 172 ter.5 del Código Penal y el concurso con el delito de injurias**

Como se ha señalado más arriba, el artículo 172 ter.5 CP contiene una referencia a la humillación del sujeto pasivo que abre una puerta a interpretar este precepto con connotaciones que van más allá de lo que tiene que ver con conductas de acoso u hostigamiento, porque, en principio, no todo acoso tiene que comportar una lesión a la dignidad de la persona. Por ejemplo, no es humillante la modalidad descrita en el acoso del art. 172 ter.1.2.ª CP, que consiste en intentar contactar con la víctima por medio de reiteradas llamadas telefónicas, *whatsapps, mails,* etc.

El artículo 172 ter.5 CP establece resultados diferentes e, incluso, alternativos: así, por una parte, es posible utilizar la imagen para crear el perfil o anuncio falso dando lugar al acoso u hostigamiento de terceros; y también es posible que dicho resultado no tenga lugar y, sin embargo, el perfil o anuncio falsos tengan una connotación claramente humillante para la víctima, de tal forma que el autor lo haya creado solo con este objetivo, y no tanto con el de que terceras personas se pongan en contacto con ella. Pese a que el precepto está dentro de los delitos de coacciones, donde lo fundamental es lesionar la libertad de obrar de la persona, pero no su honor, lo cierto es que, intencionadamente, o no, el tipo ha quedado redactado admitiendo resultados de diferen-

[12] Además, es posible solicitar a la Agencia Nacional de Protección de Datos la retirada de los datos personales difundidos sin consentimiento del titular, cuando tal resultado no se haya logrado a través de los canales especialmente previstos por el prestador de los servicios concretos.

te naturaleza, dejando abierta la puerta al concurso con el delito de injurias. Desde mi punto de vista, dependiendo de cómo se planteen los hechos, podrá hablarse de *concurso de normas* o de *concurso de delitos* entre ambos:

a) En el caso de que el perfil o anuncio falso produzca acoso, hostigamiento y humillación al sujeto pasivo, creo que puede hablarse de un *concurso de delitos* con las injurias del art. 208 (y art. 209 CP), ya que, por sí sólo, el art. 172 ter.5 CP no cubriría todo el contenido de injusto propio de los diferentes resultados. De lo contrario, resultaría sancionada con la misma repuesta la conducta de quien solo ocasiona acoso u hostigamiento, pero no humillación, con aquella que además de lo anterior lesiona la dignidad de la persona.

b) Por otro lado, si la creación de dicho perfil o anuncio falso sólo ha ocasionado humillación (y no ha dado lugar a un acoso por parte de terceros), creo que existe un *concurso de normas* entre este delito y las injurias de los artículos 208 y 209 CP. En este caso, en mi opinión, debe aplicarse la regla de la especialidad a favor del acoso art. 172 ter.5 CP, en la medida en que este precepto lesiona la dignidad de una persona utilizando, en concreto, su imagen. En definitiva, la creación del perfil o anuncio falsos en el ámbito digital, utilizando la imagen de otro con el fin de humillarle, debe sancionarse como forma de acoso, extrayendo esta tipología del delito de injurias. Fuera ésta, o no, la intención del legislador es, en mi opinión, una conclusión inevitable, al haberse introducido en el art. 172 ter.5 CP un resultado con un componente atentatorio contra la dignidad de la persona.

A tenor de esta última conclusión, cabe preguntarse por qué el legislador ha introducido las dos modalidades de acoso del artículo 172 ter CP en el grupo de los delitos de coacciones y, sin embargo, otras modalidades, como el acoso laboral, el de impedir el legítimo disfrute de la vivienda, o el callejero, se llevaron, en su momento, a los delitos contra la integridad moral del artículo 173.1, párrafos segundo y tercero, y art. 173.4, párrafo segundo CP. Pareciera que con ello se deja abierta la puerta al concurso de delitos entre las formas de acoso del artículo 172 ter CP y el delito contra la integridad moral del artículo 173.1 CP. Pero tal opción me parece difícil de aceptar, dados los términos utilizados en el art. 172 ter CP, en el que la descripción de las conductas no da pie, en principio, a resultados que atenten contra la integridad moral de la víctima con la intensidad que requiere el art. 173.1 CP. Más bien, como he señalado más arriba, nos encontramos antes ofensas a la dignidad, propias del delito de injurias. Tal y como se describe el delito contra la integridad moral del art. 173.1 CP, en éste se trata de intervenir en la esfera corporal de la víctima con el fin de

lograr su sumisión, o de obligarla a realizar determinadas conductas [13]; o de causarle padecimientos físicos, y psíquicos o morales, al tratarla al margen de la consideración y respeto que merece el ser humano por el solo hecho de serlo, siendo tal persona cosificada e instrumentalizada en manos de un sujeto que abusa de su superioridad permanente o temporal [14]. Por ello, aunque el resultado sea humillante, el nivel que requiere el delito contra la integridad moral es difícil de alcanzar con la utilización de una imagen para abrir anuncios o perfiles falsos.

4. Concurso entre el delito de acoso del art. 172 ter.5 y los delitos contra la intimidad de los arts. 197.1 y 197.7 del Código Penal

Como es evidente, la circunstancia que más individualidad confiere al tipo del 172 ter.5 CP es la referencia concreta a la imagen como objeto material del delito, lo que lleva, inevitablemente, a la necesidad de conceptualizarla, pues existe la posibilidad concursal entre este acoso y los delitos contra la intimidad de los arts. 197.1 y 197.7 CP, que también contienen una referencia expresa a la protección de la imagen.

Debe aclararse antes que en el delito de acoso puede haberse utilizado la figura completa de una persona o solo la representación de su rostro, pero, al contrario de lo que ocurre en el artículo 197.1 CP, no se protege la intimidad, sino la libertad de decisión y de obrar, además de, en ocasiones, el honor (como ya se ha señalado). Es decir, que el derecho a la imagen íntima no es el objeto central de protección en el art. 172 ter.5 CP, sino que su utilización sería el instrumento para conseguir los fines de acosar, hostigar o humillar, que señala el precepto. Por eso, la imagen a la que se refiere este último tipo penal admite una configuración más amplia que la propia de los delitos contra la intimidad, y su delimitación es menos exigente que en aquellos, sin perjuicio de que pueda darse la coincidencia en determinadas ocasiones que más abajo se citarán.

Por el contrario, en el art. 197.1 CP se protege el derecho a la imagen reconocido en el artículo 18.1 de la Constitución, que también acoge los derechos fundamentales a la intimidad y el honor (señalando el precepto penal: «El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consen-

[13] Cuerda Arnau, M. L., «Torturas y otros delitos contra la integridad moral. Trata de seres humanos», en González Cussac, J. L. (coord.), *Derecho penal. Parte especial,* Valencia (Tirant lo Blanch), 2023, p. 204.

[14] De la Mata Barranco, N. y Pérez Machío, A. I., «El concepto de trato degradante en el delito contra la integridad moral del artículo 173.1 del Código Penal», *Revista penal,* núm. 15, 2005, p. 42.

timiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de 1 a 4 años y multa de 12 a 24 meses»). El Tribunal Constitucional ha definido el derecho a la imagen como un derecho de la personalidad, que deriva de la dignidad humana y protege la dimensión moral de las personas. Tal derecho abarca la facultad de decidir la información gráfica formada por los rasgos físicos que puede tener difusión pública, y la facultad de impedir la captación, reproducción o publicación por parte de cualquier persona no autorizada [15].

La protección que otorga el art. 197.1 CP entra en juego cuando se capta y/o reproduce sin consentimiento *la imagen íntima;* pues cuando el contenido de ésta es neutro, la jurisdicción adecuada para responder a la injerencia es la de carácter civil, a tenor de la Ley 1/1982 de protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Además, la imagen íntima protegida en el artículo 197.1 CP es la que se ha obtenido de forma subrepticia, es decir, superando las barreras defensivas puestas por su titular, ya que a tal conclusión obliga la letra del precepto, cuando habla de *interceptar telecomunicaciones o utilizar artificios técnicos* de escucha, transmisión y grabación del sonido o la imagen [16]. En definitiva, en el delito contra la intimidad es protegido el derecho a la imagen por sí mismo, en su aspecto moral, relacionado con la dignidad de la persona (art. 18.1 de la Constitución). Exigencia que no existe para la imagen a la que se refiere el artículo 172 ter.5 CP. De hecho, la casuística de este delito pone de manifiesto que lo más frecuente es que el autor la consiga en formato digital, extrayéndola de las redes sociales; o bien que, en el caso de relaciones sentimentales rotas, la posea porque la captó con el consentimiento de su titular.

Pero, a pesar de que no existe necesariamente coincidencia entre el objeto protegido en ambos delitos, la identidad puede producirse cuando la conducta del acoso del artículo 172 ter.5 CP se lleva a cabo utilizando imágenes íntimas que han sido obtenidas de forma subrepticia, en cuyo caso aparece, también aquí, la posibilidad concursal con el art. 197.1 CP; o cuando la imagen íntima se ha obtenido con el consentimiento del titular, en cuyo caso el concurso será con el art. 197.7 CP («Será castigado con una pena de prisión de

[15] Entre otras, y citando sentencias separadas en el tiempo: STC 81/2001, 26 de marzo y STC 27/2020, de 24 de febrero.

[16] Jareño Leal, Á., *Intimidad e imagen: los límites de la protección penal,* Madrid (Iustel), 2008, p. 23.

3 meses a 1 año o multa de 6 a 12 meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiere obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona») [17].

Especialmente complejos de resolver son los casos en que se crea el perfil o anuncio falso utilizando *la imagen íntima* de una persona, obtenida de forma subrepticia –art. 197.1 CP–; o a disposición del autor porque la captó con su consentimiento –art. 197.7 CP–. Pues en tales hechos nos encontramos con la posibilidad de una triple respuesta: el delito de acoso, el delito contra la intimidad y el delito de injurias si el contenido es también humillante.

a) De entrada, podemos excluir el delito de injurias frente a los otros dos citados, porque en ellos se hace expresa mención a la utilización concreta de la imagen como objeto material y, en definitiva, es el único objeto del delito (arts. 172 ter.5 y 197.1, o 197.7 CP). Hay que tener también presente que el artículo 197.3 CP prevé una agravación de las penas cuando se difunden revelan o ceden a terceros las imágenes (prisión de 2 a 5 años), la cual cubre el resultado humillante que la difusión de la intimidad puede producir.

b) En el caso de que se haya obtenido de forma subrepticia la imagen íntima de una persona para abrir un perfil o anuncio falso en páginas sexuales, con el objeto de que sufra el acoso de terceros, en realidad se está llevando a cabo la conducta descrita en el artículo 197.1 CP como medio para conseguir

[17] Me sumo a la opinión de quienes entienden que la letra del precepto solo incluye como autor del delito al que ha captado la imagen que después difunde él mismo. Así, Tomás-Valiente Lanuza, C., «Del descubrimiento y revelación de secretos», en Gómez Tomillo, M. (dir.), *Comentarios prácticos al Código penal, Vol. II,* Navarra (Aranzadi), 2015, p. 671. Sobre la polémica existente es de gran interés la STS 699/2022, de 11 de julio, por los dos votos particulares que discrepan de la doctrina seguida por el Tribunal Supremo, el cual suele mantener que la conducta de quien *recibe* la imagen de la propia víctima, y la difunde, también está comprendida en el tipo penal. En este mismo sentido, Colás Turégano, A., «Nuevas conductas delictivas contra la intimidad: (arts. 197, 197 bis y 197 ter)», en González Cussac, J. L. (dir.), *Comentarios a la Reforma del Código Penal de 2015,* 2.ª ed., Valencia (Tirant lo Blanch), 2015, p. 668; Rueda Martín, M. A., *La nueva protección de la vida privada y de los sistemas de información en el Código penal,* Barcelona (Atelier), 2018, p. 166; Juanatey Dorado, C., «Intimidad y revelación no consentida de imágenes o grabaciones audiovisuales (art. 197.7 CP)», en Gómez Martín, V. *et al* (dirs.), *Un modelo integral de Derecho penal. Libro homenaje a la profesora Mirentxu Corcoy Bidasolo, Vol. II,* Madrid (BOE), 2022, p. 1229; Lloria García, P., «La difusión tecnológica de imágenes íntimas sin consentimiento como manifestación de violencia de género», en Fernández Teruelo, J. / García Amez, P. / Fernández-Rivera González, P. (coords.), *Nuevas formas de prevención y respuesta jurídico-social frente a la violencia de género,* Navarra (Aranzadi), 2022, p. 1991. La introducción del párrafo segundo en el art. 197.7 (Ley Orgánica 10/22, de 6 de septiembre) afecta a terceros ajenos a la captación u obtención de la imagen, que continúan con su difusión. Ver una crítica a dicho párrafo en Juanatey Dorado, C., «Revelación no consentida de imágenes o grabaciones audiovisuales obtenidas con consentimiento (artículo 197.7 Código Penal», *Diario La ley,* núm. 10366, 11 de octubre de 2023.

el resultado de acoso u hostigamiento previsto en el art. 172 ter.5 CP. Y, puesto que hablamos de bienes jurídicos distintos (intimidad y libertad de decidir y de obrar), parece lógico acudir aquí al concurso medial de delitos entre ambos preceptos. En definitiva, el autor de los hechos puede reunir tanto el dolo de lesionar la intimidad como el de cercenar la libertad de decidir o de obrar de la víctima. Si bien hay que plantear si debe aplicarse la agravación del 197.3 CP, referida a la difusión o revelación de la imagen, o si, por el contrario, utilizar este numeral junto al acoso del 172 ter.5 CP constituye un *bis in idem* (solución por la que me decanto), ya que, de suyo, los perfiles o anuncios creados en el ámbito digital tienen siempre dimensión pública.

c) Por lo que se refiere a la posibilidad concursal con el artículo 197.7 CP, cuando la imagen íntima utilizada para crear el perfil o anuncio falsos se ha obtenido con anuencia del titular, la solución es la misma que la que se acaba de describir, es decir, la de aplicar el concurso medial entre dicho tipo penal y el art. 172 ter.5 CP. Preceptos estos dos que, casualmente o no, prevén la misma pena (prisión de 3 meses a 1 año o multa de 6 a 12 meses).

d) Por último, en aquellos casos en que la imagen utilizada para crear el perfil o anuncio falsos no tiene carácter íntimo, por ejemplo, porque se reproduce solo el rostro, el único precepto aplicable debe ser el acoso del artículo 172 ter.5 CP.

IV. EL *DEEPFAKE SEXUAL* Y EL ACOSO DEL ART. 172 TER.5 DEL CÓDIGO PENAL

Como se ha puesto de manifiesto, el contenido moral del derecho a la imagen no es lo que protege el artículo 172 ter.5 CP, y, en la medida en que se persigue acosar o humillar a una persona, puede lograrse dicho fin con la utilización de una *imagen simulada,* que la represente de forma casi idéntica. Por tanto, también cabe en el precepto la utilización de una imagen elaborada *con inteligencia artificial,* en concreto, la utilización de un *deepfake (sexual),* cuando la imagen utilizada para crear un perfil falso o un anuncio es una simulación construida a partir del rostro de una persona, normalmente introducido en un contexto sexual, obtenido de fotografías captadas o extraídas de las redes sociales; al añadir a dicha imagen los datos personales de la víctima, como su dirección y teléfono, haciendo posible su identificación, puede lograrse un resultado acosador de la misma intensidad que en el caso de tratarse de la imagen auténtica.

Las imágenes elaboradas con inteligencia artificial están consiguiendo –cada vez más– reproducir con verosimilitud las que son reales, y los terceros pueden no reconocer la falsedad [18]. En este sentido, creo que no es relevante a efectos del precepto que aquí estamos estudiando el hecho de que los demás piensen que se trata de la imagen auténtica o, por el contrario, tengan conciencia de que están contemplando una simulación. Como digo, cuando la reproducción falsa del rostro o de la figura se acompaña de datos personales que permiten identificar a la persona, de forma indubitada, el resultado del delito de acoso que ahora analizamos puede producirse igualmente. Porque lo determinante es que los demás piensen que el perfil o el anuncio son realizados por el titular de la imagen (a la que se añaden los datos personales), lo cual generará intentos de contacto si se trata de páginas de contenido sexual. Por tanto, a estos efectos no es necesario que la imagen sea auténtica, sino que «se identifique» a la persona, con el fin de que sufra acoso u hostigamiento [19]. Lo cierto es que ni siquiera sería necesario utilizar la imagen para lograr que una persona sea acosada, bastando con proporcionar en el perfil falso su número de teléfono, o su dirección. Pese a lo cual el legislador se ha empeñado en incluir sólo tal imagen en la redacción del art. 172 ter.5 CP, con lo que la creación de un perfil sin utilizar una fotografía, aunque se proporcione mediante otros datos la identidad de una persona, no cabe en este tipo penal. Y, como también se ha argumentado más arriba, tampoco cabe en la modalidad de acoso del artículo 172 ter.1 CP si no existe una reiteración de conductas.

En conclusión, puede tipificarse en el tipo penal del art. 172 ter.5 CP tanto la utilización de la reproducción de la imagen auténtica como la de una imagen simulada con inteligencia artificial, pues también con esta última puede producirse acoso o humillación para la víctima, y también puede lesionarse su libertad de obrar o de decidir. En este sentido, tampoco es determinante que el *deepfake,* en sí mismo, tenga un contenido sexual.

---

[18] El uso de herramientas para crear imágenes artificiales se ha generalizado a partir de su fácil acceso. Dicho de forma muy superficial, se trata de técnicas de *machine learning* o *deep learning,* consistentes en la utilización de algoritmos que aprenden de los patrones de las imágenes reales, para intercambiar el rostro de las personas o para recrear imágenes falsas.

[19] Para dicha identificación sirve cualquier imagen, auténtica o no. De hecho, hasta podría servir una caricatura, si fuera acompañada de los datos de identificación de la persona; aunque este último caso es evidente que no cabe en el tipo del artículo 172 ter.5 CP, porque en este sentido es muy expresivo con la necesidad del objeto material del delito.

V. OTRAS POSIBILIDADES DE CALIFICACIÓN DE LOS CASOS DE ELABORACIÓN Y DIFUSIÓN DEL *DEEPFAKE SEXUAL*

Siguiendo con las reflexiones sobre la elaboración y distribución de imágenes generadas con inteligencia artificial, en concreto por lo que se refiere a los casos de *deepfake sexual,* además de poder incardinarse dentro del acoso en el ámbito digital, existen otras posibles respuestas para una práctica que se expande cada día más. En primer lugar, la más evidente: puede tratarse de un delito de injurias de los artículos 208 y 209 CP. En estos momentos ésta es la opción principal, porque debe descartarse calificar la elaboración y difusión de tales imágenes como delitos contra la intimidad del artículo 197.1 CP, puesto que éste no es el bien que resulta lesionado, y, desde mi punto de vista, tampoco pueden calificarse estos hechos como delitos contra la integridad moral del artículo 173.1 CP. Veamos cada una de estas afirmaciones por separado.

A) La calificación de la elaboración y difusión del *deepfake sexual* como un delito de injurias me parece actualmente la solución más plausible, sin perjuicio de que, de *lege ferenda,* otras soluciones puedan ser punitivamente más proporcionadas. Los casos más frecuentes son aquellos en los que la reproducción del rostro (o la figura) de una persona, extraída normalmente de las redes sociales o de otros medios audiovisuales, se inserta en un contexto pornográfico y se distribuye en páginas *web* de estas características. Evidentemente las conductas más frecuentes se están produciendo en relación con personajes públicos, pero no sólo. Normalmente se trata de comportamientos con fines crematísticos por parte de los titulares de las páginas *web;* pero también los hay que se llevan a cabo con fines de mero divertimento, escarnio, burla, o a modo de venganza. El fácil acceso a las herramientas que permiten la elaboración de imágenes con la técnica *deepfake* está haciendo que determinado público, especialmente joven, utilice estas transformaciones digitales como forma de diversión. Nada que objetar a los casos en que esto se hace con consentimiento de todos los implicados; pero el problema empieza cuando ello no es así, y se difunden tales imágenes falsas en las redes sociales u otros medios audiovisuales sin consentimiento del titular, aunque pueda hacerse con un simple ánimo jocoso, produciéndose un resultado expansivo que carece de control y multiplica la humillación de la persona afectada. En tales casos, creo que se dan los requisitos para aplicar el delito de injurias graves del artículo 208 CP, y del artículo 209 CP por la difusión pública de tales contenidos.

La recientemente aprobada Ley de inteligencia artificial por el Parlamento Europeo, el 13 de febrero de 2024, prevé determinadas reglas de transparen-

cia que intentan certificar y avisar a terceros de los contenidos generados con inteligencia artificial [20]. En el caso del *deepfake* deberá insertarse una suerte de aviso para el consumidor que visiona la imagen falsa, de forma que sea advertido de que ha sido generada con inteligencia artificial. A tales efectos, el art. 3.60) define como «ultrafalsificación» el «contenido de imagen, audio o vídeo generado o manipulado por una IA (inteligencia artificial) que se asemeja a personas, objetos, lugares u otras entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos». Y en su art. 50.4 se establece el deber de transparencia, al señalar que: «Los responsables del despliegue de un sistema de IA que genere o manipule imágenes o contenidos de audio o vídeo que constituyan una «ultrafalsificación» harán público que estos contenidos o imágenes han sido generados o manipulados de manera artificial. Esta obligación no se aplicará cuando la ley autorice su uso para para detectar, prevenir, investigar o enjuiciar infracciones penales…». Si bien se añade que dicho deber deja de existir «cuando el contenido forme parte de una obra o programa manifiestamente creativos, satíricos, artísticos o de ficción, las obligaciones de transparencia establecidas en el presente apartado se limitarán a la obligación de hacer pública la existencia de dicho contenido generado o manipulado artificialmente de una manera adecuada que no dificulte la exhibición o el disfrute de la obra».

Podría pensarse que la obligación de transparencia resuelve el problema de la lesión al honor en estos casos, pero, desde mi punto de vista, ello no es así. El parecido logrado con una imagen elaborada con inteligencia artificial es tan absoluto con la imagen real, que el efecto humillante que puede producir para su titular es el mismo. Cuando la normativa nacional adapte en el futuro las obligaciones que establece la Ley de inteligencia artificial, en principio los consumidores de un *deepfake sexual* conocerán desde el mismo momento del visionado que lo que miran no se corresponde con la imagen auténtica de la persona titular en cuestión [21]. Pero subsiste el problema de que la imagen falsa ha sido generada sin consentimiento del titular, y está insertada en un determinado contexto sexual, que a la persona en cuestión puede resultarle humillante. La obligación de transparencia que vendrá impuesta por la Ley de inteligencia artificial puede desplazar el problema al conflicto entre la libertad de expresión

[20] Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión [COM (2021) 0206 – C9-0146/2021 – 2021/0106 (COD)].

[21] Art. 50.5 de la Ley: «La información a que se refieren los apartados 1 a 4 se facilitará a las personas físicas de que se trate de manera clara y distinguible a más tardar con ocasión de la primera interacción o exposición. La información se ajustará a los requisitos de accesibilidad aplicables».

y el derecho al honor, y en tal caso habrá que manejar los parámetros constitucionales clásicos para resolver la inclinación del peso de la balanza a favor de un derecho u otro; pero la clave está en el contenido humillante del contexto en el que se inserta la imagen de la persona en cuestión. Por eso, en los casos del *deepfake sexual* que se inserta en páginas *web* de contenido pornográfico, creo que el equilibrio debe resolverse a favor del derecho al honor (recordemos que, en todo caso, será la propia persona afectada la que decida interponer o no la querella, valorando el atentado a su autoestima) [22]. En definitiva, desde mi punto de vista, las cosas no cambiarán mucho a efectos del delito de injurias con la nueva Ley, pues, aunque el consumidor sepa que no se trata de la imagen real de una persona, la absoluta similitud con ésta permite la mofa, el escarnio, la venganza o la diversión a su costa, máxime teniendo en cuenta que la posibilidad de difusión es infinita y escapa a cualquier control.

Por otro lado, con la difusión de un *deepfake sexual* también es posible la causación de unas lesiones psíquicas a la víctima (art. 147 CP), pues la divulgación en las redes, por ejemplo, puede producirle angustia, temor, deseo de aislamiento social o depresión, cosa que ocurre fácilmente cuando se trata, especialmente, de víctimas menores de edad. Y, por descontado, no hay que descartar la existencia de los delitos de amenazas básicas o condicionales (art. 169 CP), cuando se intimida al titular de la imagen falsa con la mera amenaza de su difusión; o poniendo una condición para no hacerlo (por ejemplo, solicitando dinero).

B) Debe descartarse que exista un delito contra la intimidad del artículo 197.1 CP en los casos de elaboración y difusión del *deepfake sexual*. Este último precepto protege, como se ha señalado más arriba, el aspecto moral del derecho a la imagen recogido en el artículo 18.1 de la Constitución. Por tanto, se refiere a la imagen que reproduce los rasgos auténticos de una perso-

[22] La propia Ley deja la puerta abierta al conflicto con las diferentes facetas de la libertad de expresión o artística (Considerando 134): «El cumplimiento de esta obligación de transparencia no debe interpretarse como un indicador de que la utilización del sistema o de su información de salida obstaculiza el derecho a la libertad de expresión y el derecho a la libertad de las artes y de las ciencias, garantizados por la Carta, en particular cuando el contenido forme parte de una obra o programa manifiestamente creativos, satíricos, artísticos o de ficción, con sujeción a unas garantías adecuadas para los derechos y libertades de terceros. En tales casos, la obligación de transparencia en relación con las ultrafalsificaciones establecida en el presente Reglamento se limita a revelar la existencia de tales contenidos generados o manipulados de una manera adecuada que no obstaculice la presentación y el disfrute de la obra, también su explotación y uso normales, al tiempo que se conservan la utilidad y la calidad de la obra. Además, también conviene prever una obligación de divulgación similar en relación con el texto generado o manipulado por una IA en la medida en que se publique con el fin de informar al público sobre asuntos de interés público, a menos que el contenido generado por la IA haya sido sometido a un proceso de revisión humana o de control editorial y que una persona física o jurídica ejerza la responsabilidad editorial de la publicación del contenido».

na en un contexto de intimidad, y que ha sido captada de forma subrepticia; es decir, protege *la representación de la verdad*. Sin embargo, tales connotaciones no se dan cuando dicha imagen se ha elaborado con inteligencia artificial, por la conexión que tiene el art. 197.1 CP con la dignidad, tal y como se deduce de la jurisprudencia del Tribunal Constitucional relacionada con el derecho recogido en el artículo 18.1 de la Constitución, al señalar que se protege la esfera moral relacionada con la dignidad humana, y la garantía de un ámbito privado libre de intromisiones ajenas [23]. Por tanto, solo la imagen que reproduce los rasgos físicos auténticos de una persona puede albergar dicho contenido moral. Siendo así las cosas, en los casos de elaboración del *deepfake sexual* no puede hablarse de vulneración de *la imagen íntima* como derecho fundamental. Hay que tener en cuenta que en el *depfake* se adhiere normalmente el contexto sexual al rostro auténtico de una persona, con lo cual la figura corporal que desarrolla la escena pornográfica no se corresponde con el titular del rostro. Siendo dicha figura simulada, o perteneciente a terceros, no existe una identidad que permita concluir que se trata de la imagen íntima de dicha persona. Sin embargo, el hecho de manipular la representación del rostro sin el consentimiento del titular sí puede dar lugar a la protección civil que ofrece la Ley 1/1982, ya que, como mínimo, supone una lesión de la facultad de disponer de la reproducción de la propia imagen.

Además, y como ya he señalado más arriba, tampoco creo que en estos casos pueda hablarse de un delito contra la integridad moral del artículo 173.1 CP, puesto que dicho precepto exige una actuación directa, física o síquica, sobre otra persona, con un efecto inmediato sobre su esfera corporal, otorgando a ésta un trato contrario a su dignidad y sometiéndola a determinados comportamientos que la dejan a merced del sujeto activo, el cual la instrumentaliza y somete a una situación de dependencia y envilecimiento [24]. En definitiva, hay

[23] STC 81/2001, de 26 de marzo, FJ 2.º, añadiendo: «Con independencia de la cuestión debatida en casación acerca de si esta imagen era suficiente o no para identificar al recurrente y podía por ello generar una vulneración del valor comercial de esa imagen, la referida representación gráfica no se refiere ni afecta al recurrente como sujeto en su dimensión personal, individual o privada...con lo que, como queda dicho, en ese anuncio no quedaba concernido el bien jurídico protegido por el derecho fundamental a la propia imagen».

[24] Tamarit Sumalla, J. M., «De las torturas y otros delitos contra la integridad moral», en Quintero Olivares, G. (dir.), *Comentarios al nuevo Código penal,* Navarra (Aranzadi), 2005, p. 930; De la Mata Barranco, N. / Pérez Machío, A. I., 2005, p. 32; Barquín Sanz, J., *Delitos contra la integridad moral,* Barcelona, 2001, pp. 68 y ss.; Cuerda Arnau, M. L., 2023, p. 204. STS 547/2022, de 2 de junio: «Aun reconociendo las dificultades que encierra la fijación del concepto de integridad moral, la jurisprudencia se ha pronunciado en diversas ocasiones, en relación con el art. 173.1 del Código Penal (cfr. STS 20/2011, de 27 de enero) (…), señalando que la integridad moral se identifica con las nociones de dignidad e inviolabilidad de la persona y que, exigiendo el tipo que el autor inflija a otro un trato degradante, por éste habrá de entenderse, según la STS 1122/1998, de 29 de septiembre, «aquel que pueda crear en las

que recordar que en los casos del *deepfake sexual* el autor *manipula la imagen digital* de otra persona, pero no la manipula a ella misma, ni hay una intervención sobre su esfera corporal para lograr su sumisión. Por tanto, es difícil alcanzar con una conducta de esta naturaleza los resultados exigidos por el artículo 173.1 CP que, además, exigen implícitamente determinados medios comisivos.

C) Por último, en el caso de que sean menores las personas afectadas con la elaboración y difusión del *deepfake sexual,* se ha planteado también la posible aplicación del delito de pornografía infantil del artículo 189.1 CP, apartado segundo, letras c) y d), en las que se introdujeron nuevas modalidades de pornografía con la Ley de reforma penal 1/2015, de 30 de marzo, incluyendo aquí la *pornografía simulada* [25]. Como ya ha puesto reiteradamente de manifiesto la doctrina, debe criticarse la inclusión en el concepto de pornografía infantil de conductas en las que no se ven involucrados personalmente los menores de edad, equiparándolas al resto de comportamientos que recoge el artículo 189.1 CP. La Circular 2/2015, de la Fiscalía General del Estado, sobre los delitos de pornografía infantil tras la reforma operada por la Ley Orgánica 1/2015, ajena a los problemas típicos que se plantean, sostiene que dichas representaciones falsas pueden incardinarse en el mencionado precepto. Sin embargo, desde mi punto de vista, y con carácter general, resulta desproporcionado incardinar dentro del concepto de pornografía infantil del artículo 189 CP las conductas simuladas en las que no se utiliza directamente a un menor de edad. En este sentido era más acertado el texto del anterior art. 189.7 CP (derogado por la Ley de reforma 1/2015), que castigaba en un tipo específico, con la pena de prisión de tres meses a un año o multa de seis meses a dos años, «al que produjere, vendiere, distribuyere, exhibiere o facilitare por cualquier medio material pornográfico en el que no habiendo sido utilizados directamente menores o incapaces, se emplee su voz o imagen alterada o modificada». En todo caso, sigue existiendo la posibilidad de calificar también estos casos de *deepfake sexual* de menores como delitos de injurias.

---

víctimas sentimientos de terror, de angustia y de inferioridad susceptibles de humillarles, de envilecerles y de quebrantar, en su caso su resistencia física o moral»».

[25] Artículo 189 CP: «1. Será castigado con la pena de prisión de uno a cinco años: (…) A los efectos de este Título se considera pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección: (…) c) Todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita, real o simulada, o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, salvo que la persona que parezca ser un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes. d) Imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales».

A modo de conclusión puede decirse que, sin perjuicio de la necesidad de abrir un debate de política criminal sobre los delitos que pueden cometerse con el uso de la inteligencia artificial, de forma urgente podría plantearse la posibilidad de llevar a cabo una modificación legislativa en dicho delito de injurias, para incluir expresamente los casos de elaboración y difusión de un *deepfake sexual,* proporcionado así seguridad jurídica sobre la calificación de esta clase de comportamientos [26].

[26] A estos efectos existe una proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de inteligencia artificial, presentada el 13 de octubre de 2023 por el grupo parlamentario SUMAR, proponiendo la tipificación en un nuevo artículo 208 bis CP.

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.

LA PROTECCIÓN PENAL DE LA HISTORIA CLÍNICA DIGITAL

Carlos Trincado Castán *

I. INTRODUCCIÓN

En el ámbito sanitario, el conjunto de datos más relevante para un ciudadano se recoge en su historia clínica que, con el impulso de las políticas de papel cero y digitalización de administraciones públicas (y, en su caso, hospitales y clínicas privadas), han pasado a estar de forma generalizada en formato electrónico y contenidas en bases de datos informatizadas, habitualmente gestionadas por hospitales o centros sanitarios de titularidad pública.

En este contexto, como en cualquier otro relacionado con el almacenamiento, tratamiento y gestión de datos informatizados, existen riesgos de que se produzcan accesos no autorizados a los ficheros que los contienen que exceden de los que se podrían producir si tales archivos estuviesen en papel. Si bien el fenómeno de la cibercriminalidad vinculado a los accesos a datos íntimos contenidos en sistemas informáticos suele vincularse a *hackers* o sujetos desconocidos que pueden realizar tales accesos desde y hacia cualquier lugar del país o, incluso, del mundo, en el caso de los datos contenidos en historias clínicas cuando se producen accesos indebidos estos son generalmente llevados a cabo por sujetos pertenecientes a la misma organización que almacena y gestiona los datos.

* Profesor ayudante. Universidad de La Laguna (Santa Cruz de Tenerife).

II. EL DELITO DE DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS DEL ARTÍCULO 197.2 DEL CÓDIGO PENAL EN EL ÁMBITO SANITARIO

El artículo 197.2 del Código Penal tipifica como delito la conducta de quien *«sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero».*

Si bien se considera de forma general que el bien jurídico protegido en este precepto es la libertad informática, considerada, de acuerdo con la postura doctrinal mayoritaria [1], como una dimensión del derecho a la intimidad, otros autores plantean que éste es en realidad un derecho autónomo, dotado de un contenido propio respecto de la intimidad [2]. En todo caso, la libertad informática es entendida como el derecho a tener poder de disposición y control sobre los datos personales que sean recogidos y tratados informáticamente en bases de datos (STS 250/2021, de 17 de marzo).

La estructura y redacción del artículo 197.2 CP han sido criticadas por la doctrina [3], en la medida que describe en dos incisos distintos conductas difícilmente diferenciables *(apoderarse y acceder o modificar y alterar)* o que directamente se repiten *(utilizar),* sin que se dé un criterio claro para diferenciar en qué supuestos se debe aplicar uno u otro inciso. Se han planteado diversos criterios desde la doctrina a estos efectos, habiendo autores que consideran que la diferencia reside en el objeto de la conducta, esto es, que las acciones típicas del segundo inciso se proyectarían sobre *«los ficheros o soportes informáticos, electrónicos...»,* mientras que las del primer inciso lo harían sobre los propios *«datos reservados»* [4], porque de lo contrario se estaría tipificando dos veces la

---

[1] Rueda Martín, M. Á., *La nueva protección de la vida privada y de los sistemas de información en el Código penal,* Barcelona (Atelier), 2018, p.37.

[2] Romeo Casabona, C. M., «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en Romeo Casabona, C. M. / Sola Reche, E. / Boldova Pasamar, M. Á. (coords.), *Derecho Penal, Parte Especial,* Granada (Comares), 2023, p. 301.

[3] Gómez Navajas, J., «La protección de los datos personales en el código penal español», *Revista Jurídica de Castilla y León,* núm. 16, 2008, p. 334

[4] González Cussac, J. L., «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en González Cussac, J. L. (coord.) *et al., Derecho Penal, Parte Especial,* Valencia (Tirant lo Blanch), 2019, p. 293; Sierra López, M. V., «Los delitos de descubrimiento y revelación de secretos en el Código Penal de 2015», en Del Carpio Delgado, J. (coord.), *Algunas cuestiones de parte especial tras la reforma de 2015 del Código Penal,* Valencia (Tirant lo Blanch), 2018, p. 143.

alteración y utilización de los datos [5]; otros, defienden que la diferencia entre ambos incisos debe establecerse en función de la «posición subjetiva del autor», aplicándose el primero en aquellos casos en los que, estando el sujeto autorizado para acceder a los datos, estaría extralimitándose en el ejercicio de tal autorización, interpretación que tiene en cuenta que en el primer inciso no se incluye como conducta típica el mero acceso (en la medida que el sujeto está autorizado a realizarlo, no puede ser considerado como un delito) [6], quedando reservado el segundo inciso para aquellos casos en los que quien accede a los datos lo hace sin autorización *ab initio* [7]. Esta última aproximación ha sido seguida por el Tribunal Supremo en alguna sentencia, en la que ha tenido teniendo en cuenta si el sujeto estaba autorizado o no para acceder a los datos, pudiendo rebasarse el nivel de acceso para el que estaba autorizado (STS 412/2020, de 20 de julio). No obstante, en sentencias posteriores, el Alto Tribunal ha aplicado la conducta de «acceder» del inciso segundo a sujetos inicialmente autorizados, por lo que no se puede considerar que la diferenciación entre los incisos según la posición subjetiva del autor sea una línea jurisprudencial consolidada (SSTS 178/2021, de 1 de marzo; 250/2021, de 17 de marzo).

Si bien no es una cuestión pacífica, siguiendo la aproximación a la interpretación del artículo 197.2 CP por la que se diferencia la aplicación del inciso primero respecto del segundo en función de la posición subjetiva del autor respecto de los datos, los supuestos de hecho protagonizados por funcionarios y empleados de los sistemas públicos de salud serían subsumibles en las conductas descritas en el primer inciso, al ser sujetos autorizados para acceder a los datos reservados almacenados en ficheros informáticos de los sistemas de salud públicos, pero que se extralimitan o hacen un uso inadecuado de dicha autorización.

III. BASE LEGAL PARA LA AUTORIZACIÓN DE ACCESO A HISTORIAS CLÍNICAS

La norma en la que se prevén los supuestos en los que el personal sanitario está autorizado para acceder las historias clínicas de los pacientes es la Ley 41/2002 de Autonomía del Paciente. La *historia clínica,* de acuerdo con el artículo 3 de esta norma, es *«el conjunto de documentos que contienen los*

[5] Barrio Andrés, M., *Delitos 2.0: Aspectos penales, procesales y de seguridad de los delitos,* Madrid (Wolters Kluwer), 2018, p. 84.

[6] Romeo Casabona, C. M., 2023, p. 307.

[7] Rueda Martín, M. Á., 2018, p. 120.

datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial».

En el artículo 16 de la Ley 41/2002 se prevén los diversos usos para los que el personal sanitario está autorizado a acceder a las historias clínicas, siendo el más relevante el acceso para llevar a cabo el diagnóstico y tratamiento del paciente (artículo 16.1 Ley 41/2002). Si bien este artículo 16 prevé otros usos y escenarios en los que se autoriza el acceso a historias clínicas (principalmente usos de administración y gestión, pero también motivos epidemiológicos, estadísticos, judiciales, organizativos, etc.), por lo general un acceso realizado por personal sanitario por razones distintas a las asistenciales, ya sea porque el titular de los datos no es su paciente o porque se acceda por razones distintas a su tratamiento y diagnóstico, será un acceso no autorizado, como por ejemplo los accesos por razones personales (STS 312/2019, de 17 de junio, en la que un doctor accede a un parte médico de su exmujer para usarlo en el proceso judicial de divorcio) o por mera curiosidad (STS 178/2021, de 1 de marzo).

IV. ACCESOS NO AUTORIZADOS A HISTORIAS CLÍNICAS

Si analizamos la jurisprudencia sobre accesos no autorizados a historias clínicas, siguiendo la diferenciación entre los incisos primero y segundo planteada en el epígrafe II, la mayoría de supuestos que se producen en la práctica consisten en la conducta de apoderamiento descrita en el inciso primero del art. 197.2 CP, sin que se deba entender este concepto como la necesidad de que se produzca una aprehensión material de la información, como por ejemplo un traslado del sistema informático a otro distinto de aquél en el que están contenidos los datos, o del mismo a un soporte físico (como un papel o una fotografía), sino que basta con una captación intelectual de los datos y la información que contienen (STS 40/2016, de 3 de febrero), aunque sobre esta cuestión existen posiciones doctrinales que defienden criterios distintos [8].

Esto es especialmente relevante en los supuestos de accesos a historias clínicas informatizadas, en los que normalmente el sujeto que accede no copia ni traslada la información a ningún dispositivo o soporte físico, sino que lo

[8] González Cussac, J. L., 2019, p.293 y Barrio Andrés, M., 2018, p.84, consideran que el inciso segundo del artículo 197.2 CP no va dirigido a proteger los datos reservados, sino los ficheros o registros que los contienen, por lo que la conducta de «acceso» se referiría a la entrada y visualización de la información en ellos contenida y la de «apoderamiento» implicaría una toma de posesión de los mismos, ya sea de forma material (imprimiéndolos) o virtual (copiándola en una memoria USB o enviándola por correo electrónico).

hace para conocer los datos que está buscando, sin dejar otro rastro que la huella digital del acceso en el registro electrónico de accesos.

V. LA HISTORIA CLÍNICA COMO FICHERO DE DATOS RESERVADOS DE CARÁCTER PERSONAL Y FAMILIAR

No todos los datos contenidos en ficheros o soportes informáticos son susceptibles de protección penal, sino que debe tratarse de *«datos reservados de carácter personal o familiar»*. Son «reservados» aquellos datos *«que no son susceptibles de ser conocidos por cualquiera»* (STS 1328/2009, de 30 de diciembre). Desde un punto de vista sistemático, este concepto de datos «reservados» debería ser interpretado como equivalente al concepto de «secreto» utilizado en el artículo 197.1 CP, entendiendo como tales aquellos datos o conocimientos desconocidos u ocultos que el sujeto pasivo no quiere que se conozcan y que el sujeto activo no conoce o no está seguro de conocer (STS 532/2015, de 23 de septiembre). Por otra parte, los datos deberán tener *carácter personal y familiar,* perteneciendo al ámbito privado y personal del paciente. Esto no implica que deban ser parte de lo que se conoce como núcleo duro de la privacidad (STS 358/2007, de 30 de abril), pero sí que es necesario que se afecte a la intimidad personal del sujeto (STS 1328/2009, de 30 de diciembre).

Los datos que pertenecen al ámbito más estricto de la intimidad, como es el caso de los datos de salud, son considerados como datos «sensibles» que gozan de una especial protección (STS 178/2021 de 1 de marzo). El concepto de dato sensible se define desde la perspectiva de una persona media de nuestra cultura, siendo aquellos que pertenecen a un reducto que normalmente no se pretende que trascienda fuera de la esfera de privacidad de una persona o de su núcleo familiar (STS 392/2020, de 15 de julio).

En particular, las historias clínicas, entendidas como conjuntos de documentos que contienen datos de salud e información sobre la situación clínica de un paciente, son consideradas como ficheros que contienen datos sensibles que forman parte del núcleo duro de la privacidad (STS 532/2015, de 23 de septiembre y STS 178/2021, de 1 de marzo). Sin embargo, no se debe caer en el automatismo de considerar que todos los datos contenidos en una historia clínica son datos sensibles. En una historia clínica, junto a los datos de salud, hay datos administrativos como, por ejemplo, el nombre del médico de cabecera del paciente (STS 1328/2009, de 30 de diciembre) o la mera constancia administrativa de la existencia de bajas por incapacidad laboral (STS 392/2020, de 15 de julio). Por ello, solo deberán ser considerados como accesos a datos

sensibles los accesos a datos de salud contenidos en la historia clínica y no otros tipos de datos.

VI. EL REQUISITO DEL PERJUICIO DEL TERCERO

Debe señalarse que el artículo 197.2 CP, en su inciso primero, establece que la conducta debe realizarse *«en perjuicio de tercero».* Parte de la doctrina considera este requisito como un elemento subjetivo del tipo, siendo necesaria la concurrencia de un específico ánimo de perjudicar a un tercero al realizar la conducta de apoderamiento, utilización o modificación de los datos por parte del autor del delito, sin ser necesario que éste se produzca de forma efectiva para que el delito se consume [9]. Otro sector de la doctrina [10] considera este requisito como un elemento objetivo del tipo, requiriéndose que se produzca este «perjuicio» como resultado de la conducta ejecutada. Esta última postura ha sido la seguida por el Tribunal Supremo (STS 1328/2009, de 30 de diciembre). Cualquiera que sea la interpretación que se realice, se debe producir una afectación a la intimidad y la libertad informática de la víctima, afectación que se valora como ínsita a la conducta de acceso a datos sensibles, como son los datos de salud.

No obstante, la indeterminación de este requisito da lugar a casos como el de la STS 312/2019, en la que un médico accedió a información reservada (un parte de lesiones y una radiografía) de su expareja para utilizarla en un proceso de divorcio. El Tribunal Supremo absolvió al médico argumentando que no accedió a datos que fuesen nuevos o desconocidos para él, por lo que no se produjo el resultado de vulneración de la intimidad de la víctima en el caso concreto, quedando impune (al menos desde lo penal, nada se dice en la sentencia sobre el ámbito disciplinario) el acceso por un miembro del personal sanitario a información contenida en una base de datos con información reservada en contravención de sus deberes de respetar la confidencialidad de esa información y de los protocolos y políticas internas de acceso a datos reservados, siendo además un interés personal el que motivó el acceso ilegítimo, lo cual es especialmente problemático si se parte de una concepción del derecho a la autodeterminación informativa, que en un caso de estas características se vería vulnerado como un derecho o bien jurídico autónomo del derecho a la intimidad.

---

[9] Muñoz Conde, F., *Derecho Penal, Parte Especial,* 22.ª ed., Valencia (Tirant lo Blanch), 2019, p. 259; Romeo Casabona, C. M., 2023, p. 263.

[10] Queralt Jiménez, J. J., *Derecho penal español, Parte especial,* Valencia (Tirant lo Blanch), 2015, p. 302.

VII. CIRCUNSTANCIAS AGRAVANTES EN EL CONTEXTO SANITARIO: DATOS ESPECIALMENTE SENSIBLES Y FUNCIONARIOS

Los delitos del capítulo I del Título X presentan una inacabable estructura de tipos agravados en función de diversas circunstancias, como son que los secretos indebidamente obtenidos de acuerdo con los apartados 1 y 2 del artículo 197 sean difundidos (art. 197.3 CP), que se trate de determinadas categorías de datos especialmente sensibles (art. 197.5 CP), que el autor del delito sea el encargado del tratamiento de los datos (art. 197.4 CP) o un funcionario (art. 198 CP), o que los hechos se realicen con ánimo de lucro (art. 197.6 CP). En el contexto de los accesos no autorizados a historias clínicas son dos las circunstancias que potencialmente pueden agravar la pena: el carácter de los datos de salud como datos sensibles y la condición de funcionario público del sujeto activo del delito.

El artículo 197 CP recoge en su apartado 5 un tipo agravado (que prevé la aplicación de la pena en su mitad superior) para los casos en los que los datos a los que se acceda, entre otros supuestos, sean datos que revelen información especialmente relevante, como la ideología, religión, creencias y, entre los que este apartado recoge expresamente, la salud. Sin embargo, si se considerase la condición de datos sensibles de los datos de salud tanto, como hemos visto en el anterior epígrafe, para valorar la producción del perjuicio y, conjuntamente, para aplicar el tipo agravado, se estaría vulnerando el principio *non bis in ídem*. Por ello, se viene entendiendo que el tipo agravado del artículo 197.5 CP deberá aplicarse únicamente en casos de especial gravedad, es decir, cuando los datos a los que se acceda conlleven un especial daño por la naturaleza del daño descubierto o porque se afecte de forma conjunta a otros bienes jurídicos (STS 178/2021, de 1 de marzo).

En los casos en los que el acceso no autorizado a la historia clínica es realizado en un centro sanitario público, los miembros del personal médico, de enfermería y administrativo que trabajan en ellos tienen la condición de funcionarios. Ello implica que en estos supuestos se deberá aplicar el tipo agravado del art. 198 CP, que prevé la aplicación de las penas de prisión del art. 197 CP en su mitad superior junto con una de inhabilitación absoluta de 6 a 12 años. Esta agravación se traduce en que el marco penal del artículo 197.2 CP de 1 a 4 años de prisión pasa a uno con una pena mínima de 2 años y 6 meses, lo cual tiene importantes implicaciones desde el punto de vista de la suspensión de la pena, en la medida que, en ausencia de circunstancias atenuantes, la pena mínima será siempre superior a los 2 años que establece el artículo 80 CP para la aplicación

del régimen ordinario de suspensión de la pena de prisión, lo que a su vez implica que prácticamente en todos los supuestos el autor del delito deberá ingresar de forma efectiva en un centro penitenciario para el cumplimiento efectivo de la pena privativa de libertad.

Si bien la vulneración de la intimidad y la libertad informática de los pacientes, así como el recto cumplimiento por los servidores públicos de sus deberes en relación con la custodia y uso de esta información representan valores cuya infracción tiene la entidad suficiente como para ser objeto de respuesta penal, tal como están configurados los artículos 197 y 198 CP, prácticamente no hay diferencias significativas a nivel de pena entre la realización de uno o múltiples accesos, o entre los accesos realizados con el objetivo de utilizar posteriormente los datos frente a otros en los que se realizan uno o pocos accesos por «mera curiosidad», una conducta que, si bien es reprochable por parte de un empleado público, parece debatible que deba valorarse como una conducta tan grave como para requerir por defecto un ingreso en prisión del autor del delito así como la pérdida, en su caso, de la plaza de funcionario como consecuencia de la inhabilitación absoluta, todo ello sin tener en cuenta otras consideraciones de política criminal o penitenciaria como podría ser los efectos de la entrada en prisión del condenado, así como los de la inhabilitación absoluta en relación con la posterior reinserción social del condenado, al que se le dificulta su reincorporación profesional (si bien debe tenerse en cuenta que existe la posibilidad de su posterior rehabilitación). En este contexto puede debatirse, también, si el reproche de estas conductas debería limitarse al ámbito administrativo sancionador, sin necesidad de intervención penal.

VIII. CONCLUSIÓN

El delito tipificado en el artículo 197.2 CP presenta diversos problemas de aplicación e interpretación como consecuencia de una mejorable redacción y estructura, cuyos efectos se dejan notar especialmente en relación con los accesos no autorizados a datos reservados especialmente sensibles como son los relacionados con la salud de una persona. Sería conveniente una reforma del artículo con la que solventar estas cuestiones, evitándose la reiteración de conductas en la descripción del tipo, aclarando cuándo se debe aplicar uno u otro inciso, así como las cuestiones de proporcionalidad derivadas de la aplicación de los tipos agravados vinculados a la condición de los datos de salud como datos sensibles y la condición de funcionario público del sujeto activo del delito.

Colección
Derecho Penal y Procesal Penal

Director:
Luis Rodríguez Ramos

Títulos publicados:

16. Códigos penales españoles, dos volúmenes
    Jacobo Barja de Quiroga
    Luis Rodríguez Ramos
    Lourdes Ruiz de Gordejuela López
17. Minería de ADN en la investigación criminal
    Fernando Ruiz Domínguez
18. Responsabilidad penal y negocios estándar: los casos del asesor fiscal y del abogado, dos volúmenes
    Mónica de la Cuerda Martín
19. Tratamiento jurídico-penal del acoso en España
    Cristian Sánchez Benítez
20. El principio de responsabilidad penal por el hecho
    Directores: Mirentxu Corcoy Bidasolo, Víctor Gómez Martín
    Coordinadores: Juan Carlos Hortal Ibarra, Vicente Valiente Ivañez
21. El derecho penal estudiado en principios y en la legislación vigente en España por Luis Silvela
    Presentación por: Gonzalo Quintero Olivares
22. La pena y su renuncia en la justicia transicional. ¿Puede trasladarse el fundamento premial a la violencia terrorista?
    David Gallego Arribas
23. Una propuesta de reforma para la regulación racional de la concurrencia delictiva en el Código penal español
    Directores: Enrique Peñaranda Ramos, Laura Pozuelo Pérez
    Coordinador: Nicolás Cantard
24. Límites de la protección del Derecho penal al inicio y fin de la vida humana en la sociedad moderna
    Coordinadores: Juan Pablo Montiel, Laura Neumann, Helmut Satzger, Víctor Gómez Martín

En un mundo cada vez más globalizado y conectado, las tecnologías digitales han transformado todos los aspectos de nuestra vida cotidiana, abriendo nuevas posibilidades en ámbitos tan diversos como la comunicación, la economía, la educación o la cultura. Sin embargo, junto a estas oportunidades, también han surgido riesgos y amenazas que desafían los marcos legales tradicionales. Así, el fenómeno del cibercrimen, en su creciente e imparable expansión, nos ha mostrado la necesidad de enfrentarnos no sólo a nuevas formas delictivas que afectan a diversos bienes jurídicos, sino a hacerlo en un nuevo escenario: un espacio digital, interconectado y globalizado al que se puede acceder desde cualquier lugar del planeta, y en el que el anonimato se configura como un elemento clave que dificulta la trazabilidad y la perseguibilidad de los ataques (que, a mayor abundamiento, pueden llevarse a cabo de manera instantánea y escalar rápidamente, afectando a multitud de personas en cuestión de segundos).

Esta obra examina el tratamiento penal que la persecución de estos delitos exige para evitar su impunidad, las dificultades de tipificación de los ilícitos, la necesaria colaboración internacional y las particularidades y retos que plantean ciertos ilícitos, como el delito de acoso y la revelación de datos de historiales clínicos.