Algunas dificultades en la detección e investigación de los ciberdelitos económicos

Some Difficulties in the Detection and Investigation of Economic Cybercrimes

Daniel González Uriel[1]
Letrado del Tribunal Constitucional, España.
daniel.gonzalez@poderjudicial.es | https://orcid.org/0000-0001-8966-0571

DOI: https://doi.org/10.14201/cp.32207
Recibido: 20-12-2024 | Aceptado: 23-12-2024

Resumen
En este trabajo se lleva a cabo un análisis sobre algunos de los principales problemas que se aprecian en la investigación de los ciberdelitos de contenido económico. Para ello se efectúa una descripción sobre el fenómeno de la ciberdelincuencia, se apuntan algunos de los principales delitos que se pueden cometer en este campo y, finalmente, se expone una serie de cuestiones de índole judicial y policial. Se trata de un enfoque multidisciplinar, en que se integran aspectos criminológicos, penales y procesales. Tiene una finalidad práctica, destinada a la prevención, a la detección precoz y a la mejora en la lucha contra estas tipologías delictivas.

Palabras clave
Ciberdelincuencia; Ciberestafas; Delitos económicos; Investigación; Proceso penal.

Abstract
In this paper, we carry out an analysis on some of the main problems that are seen in the investigation of cybercrimes with economic content. We make a description of the phenomenon of

1. Magistrado (en servicios especiales). Doctor en Derecho. Profesor (acr.) contratado doctor ANECA.

cybercrime, we note some of the main crimes that can be committed in this field and, finally, we expose a series of judicial and police issues. It is a multidisciplinary approach, which integrates criminological, criminal and procedural aspects. It has a practical purpose, aimed at prevention, early detection and improvement in the fight against these criminal types.

Keywords
Cybercrime; Cyber scams; Economic crimes; Investigation; Criminal proceedings.

1 Introducción

La revolución tecnológica en que nos hallamos inmersos ha propiciado que las tecnologías de la información y de la comunicación (TIC) se erijan en elementos clave en el desarrollo social, económico, laboral, educativo, comercial o comunicativo de los ciudadanos. El ciberespacio se ha convertido en un nuevo ámbito relacional al que se han trasladado prácticamente todos los aspectos de la vida cotidiana de las personas, desde los más sencillos –como mandar un email– hasta otros más complejos, como realizar diferentes negocios jurídicos de corte patrimonial. Ello comporta notables ventajas en orden a la inmediatez, a la reducción de tiempos, a la conectividad, a la eliminación de las fronteras y de las barreras y, por ende, a una mayor agilidad y celeridad. Si bien, y como contrapartida, el delito también se ha visto favorecido por esta facilidad comunicativa, ya sea mediante la adaptación de algunas modalidades clásicas al ámbito de las TIC, ya sea a través del surgimiento de nuevas tipologías delictivas. La cibervictimización constituye un riesgo creciente, global y generalizado. Además, dicho peligro se ve incrementado por las nuevas tecnologías, aplicaciones y herramientas y, de modo especial, por el desarrollo de la inteligencia artificial (IA).

No descubrimos nada nuevo si decimos que, hoy día, la ciberdelincuencia constituye uno de los principales –por no decir el principal– ámbitos de expansión en el fenómeno delictivo. Este hecho es constatable si acudimos a los datos oficiales en nues-

tro país, en concreto, si tomamos en consideración los balances e informes sobre criminalidad emitidos, periódicamente, por el Ministerio del Interior[2] del Gobierno de España. Podemos atender al informe sobre la cibercriminalidad en España del año 2023 (Ministerio del Interior, 2023), que nos servirá para extraer una serie de interesantes elementos de juicio. En dicho documento se aprecia un importante incremento de los ciberdelitos en los últimos años. En él se detalla la evolución acaecida desde el año 2019 hasta el año 2023. Si atendemos a los ciberdelitos conocidos podemos observar que, en 2019, se cifraron en 218.302, en 2020 se elevaron a 305.477, en 2022 se incrementaron hasta los 374.737 hechos conocidos, mientras que, en el año 2023, alcanzaron los 472.125. Y, añadiendo un dato más, en el año 2023, el 90,5 % de tales casos se correspondían con supuestos de "fraude informático", según la terminología empleada en el informe, y que se corresponde con las ciberestafas –en este punto debemos puntualizar que nuestro Código Penal (CP) no acoge la denominación de "fraude informático", que sí se contiene en el Convenio de Budapest–[3].

Si abundamos un poco más en los datos estadísticos del citado informe, podemos inferir que, en los supuestos de ciberdelitos, existe una elevada tasa de casos sin resolver. En este sentido, para que nos sirva también como término de comparación, volveremos a manejar el mismo lustro de referencia que hemos tomado en consideración en el párrafo anterior (2019-2023), para que apreciemos, en toda su magnitud, la dimensión, los efectos y las consecuencias de la problemática tratada. Pues bien, en el año 2019, se esclarecieron 30.841 casos; en 2020, 38.046; en 2021, 46.141; en 2022, 51.642, y, en 2023, 60.197. Como se desprende de estos datos, nos encontramos ante una fenomenología delictiva con una baja tasa de esclarecimiento, en comparación con el volumen de casos. Y no solo eso, sino que,

2. *Vid*. al respecto https://www.interior.gob.es/opencms/es/prensa/balances-e-informes/. Los delitos que se recogen en dicho informe son: acceso e interceptación ilícita, amenazas y coacciones, delitos contra el honor, delitos contra la propiedad intelectual e industrial, delitos sexuales, falsificación informática, fraude informático, interferencia en datos y en sistemas.

3. Hacemos alusión al Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001.

como después anotaremos, esto debe ser puesto en relación con la existencia de una relevante –aunque desconocida– cifra negra de denuncias, lo que podría incrementar, exponencialmente, la magnitud de esta forma de criminalidad.

Con todo, no existe una definición unívoca de ciberdelincuencia, ni contamos con una regulación uniforme, sistemática y específica que trate dicho fenómeno de un modo autónomo e independiente. De modo general, y como primera aproximación, podríamos tomar en consideración la descripción que nos brinda el *Diccionario de la Real Academia Española (DRAE)*, que la define como "actividad delictiva que se lleva a cabo a través de Internet". En este sentido, llama la atención que el propio *Diccionario Panhispánico del Español Jurídico de la RAE (DEJ)* no contiene ninguna entrada para el vocablo que empleamos, sino que acude a la fórmula "delito informático", que caracteriza como "infracción penal cometida utilizando un medio o un instrumento informático". Por lo tanto, en esta contribución partimos de que la ciberdelincuencia abarcaría todo delito cometido por medio o a través de las TIC. Patrocinamos así una comprensión amplia del fenómeno, que se centre en el instrumento o cauce a través del que se vehicula o instrumenta el ilícito penal.

Pues bien, los ciberdelitos, aunque presenten una gran heterogeneidad y no sean reconducibles a una única categoría o clasificación, se encuentran presididos por una serie de rasgos propios, que podríamos reconducir, en su esencia más básica, a que se cometen en el ciberespacio. En este sentido, el ciberespacio, entendido por el *DRAE* como el "ámbito virtual creado por medios informáticos", tiene una serie de características que nos permiten comprender mejor algunas dinámicas delictivas *online*. Tal y como explica Miró Llinares (2012), el ciberespacio se caracteriza por: (i) el carácter transnacional, dado que no existen fronteras ni distancias; (ii) porque la Red es neutral, ya que no existen restricciones ni censuras de acceso; (iii) porque es un espacio no centralizado, que se encuentra distribuido y donde no existen nodos que actúen como centros locales; (iv) porque se encuentra anonimizado, puesto que no existe identificación de usuarios; (v) que está sometido a una revolución permanente y abierto al cambio, debido a la evolución tecnológica; (vi) en el que no hay guardianes formales; (vii) donde las

variables espacio y tiempo presentan un nuevo diseño; y (viii) que está popularizado, por lo que es tendencialmente universal.

Por su parte, López Gorostidi (2021) también anota una serie de caracteres del ciberespacio, de corte criminológico, con influencia en la comisión de ilícitos penales, entre las que señala: (i) en cuanto a sus aspectos técnicos, que las TIC atesoran una gran capacidad para albergar, procesar y distribuir cantidades ingentes de datos, y realizan tales acciones a gran velocidad; (ii) el elevado porcentaje de población mundial que accede a diario a las TIC y el creciente número de valores personales que se introducen en el ciberespacio; (iii) la posibilidad de simulación de identidad que Internet ofrece a sus usuarios; y (iv) los fenómenos de permanencia y automatismo del hecho.

Los usuarios de las TIC, mediante nuestro acceso y navegación por la Red, incorporamos nuestros bienes jurídicos al ciberespacio. Somos nosotros quienes delimitamos, mediante nuestra actuación en el ciberespacio, el ámbito en el que podemos ser victimizados *online*, por lo que este dato deviene en un punto de referencia esencial: el ciberespacio se convierte en un nuevo espacio de oportunidad delictiva en el que los sujetos podemos ser victimizados en tanto en cuanto interactuemos con terceros en él. Con nuestro comportamiento *online* concretamos qué bienes jurídicos de nuestra esfera de intereses pueden ser susceptibles de ser lesionados o puestos en peligro. Los bienes jurídicos que pueden ser lesionados o puestos en peligro son variados y, a título meramente ejemplificativo, podemos aludir al patrimonio, al honor, a la intimidad personal y familiar, a la propia imagen, a la libertad e indemnidad sexuales o a la libertad, entre otros. Si bien, y como reiteramos, debemos destacar que somos los usuarios de las TIC los que incorporamos a ese nuevo ámbito una parte de nuestra esfera de derechos e intereses, por lo que hemos de adoptar las cautelas y medidas de salvaguarda precisas para evitar o, cuando menos, limitar, las posibilidades de su lesión o menoscabo. En el bien entendido de que, con esta alusión, no estamos haciendo referencia a desorbitados deberes de autoprotección que, por otro lado, no se exigen por los tipos penales, ni estamos culpabilizando a las víctimas de su proceso de victimización. No obstante, este particular será retomado en las sucesivas líneas.

Como se aprecia con el análisis de los datos estadísticos manejados en las fuentes oficiales, la mayor parte de los ciberdelitos –más de un 90 % de ellos en 2023– tenían por finalidad la obtención de un lucro económico, por lo que podemos derivar una clara conclusión: la finalidad principal de la comisión de ciberdelitos es el enriquecimiento patrimonial. Por este motivo, ante dicha constatación, en este estudio nos centraremos en la ciberdelincuencia que podemos calificar como económica y que, a grandes rasgos, se catalogaría como aquel conjunto de delitos, cometidos mediante las TIC, y que afectan a los bienes jurídicos tutelados en el Título XIII, "De los delitos contra el patrimonio y el orden socioeconómico", del Libro II del CP, así como a aquellos otros ilícitos que, aunque sistemáticamente no se incardinen en dicho título, tengan relevancia, repercusión e incidencia en el sustrato patrimonial, económico o socioeconómico.

Con las páginas que prosiguen se pretende realizar, de modo modesto, un esbozo general sobre la problemática delictiva tratada, aunando tres vertientes: el análisis criminológico, penal y procesal de los ciberdelitos de naturaleza económica. Se opta por un enfoque tripartito, aunque integrado, a los fines de dar una visión de conjunto, completa y didáctica, huyendo de tratamientos fragmentarios que compartimenten o encapsulen el fenómeno y que diluyan una visión conjunta, transversal e integral. Por este motivo, en las líneas que siguen, se aglutinarán, de un modo pretendidamente armónico, postulados criminológicos, apuntes de dogmática penal y problemas procesales, con la intención de efectuar una prognosis certera, de apuntar posibles riesgos, retos y desafíos y, en resumidas cuentas, de brindar al lector un arsenal de instrumentos para profundizar en el análisis de una fenomenología delictiva que ha venido para quedarse, para expandirse y a la que hemos de hacer frente mediante esfuerzos teóricos y aplicaciones prácticas.

2 El ciberespacio como entorno criminógeno

Como anotamos, este nuevo entorno virtual también propicia que los sujetos puedan ser objeto de cibervictimizaciones. Al

efectuarse un traslado al ámbito *online* de todas las facetas de la vida, incorporamos nuestros derechos e intereses e interactuamos con terceros. Este comportamiento en la Red determinará que podamos ser objeto de ciberdelitos. Tal y como se advirtió, las cibervictimizaciones pueden ser variadas y plurales. En este sentido, todos los usuarios de las TIC somos potenciales víctimas, por lo que todos los agentes sociales somos susceptibles de ser victimizados, tanto personas físicas como jurídicas. Por lo tanto, no existe un único perfil de víctima, sino que presenta carácter múltiple, contingente y variable.

Ya hemos indicado que una de las principales peculiaridades de esta tipología de delitos es que es la propia víctima quien determina los bienes jurídicos de su esfera de intereses que pueden ser agredidos, mediante su incorporación a las TIC, su comportamiento en ellas y la interactuación con terceras personas. Así las cosas, es la propia víctima quien define el perímetro de actuación sobre el que pueden incidir los ciberdelincuentes. Si bien, hemos de advertir que con estas afirmaciones no se reprocha a la víctima nada, ni se le culpabiliza de ser victimizada, sino que se corrobora el presupuesto fáctico de los ciberdelitos. Pues bien, tomando como referente dicha situación, debemos constatar que, en ocasiones, el contexto *online* propicia que los sujetos lleven a cabo determinados actos de riesgo o que modifiquen su conducta y se comporten de un modo diferente a como lo hacen en el espacio físico. Es lo que se ha dado en llamar "online desinhibition effect", que Agustina Sanllehí (2014) sintetiza en que se da una disparidad de conductas porque las personas se encuentran "menos constreñidas, más sueltas y se expresan de una forma mucho más abierta". Dicho autor resume en seis los rasgos del efecto desinhibidor *online*, que aquí solo enumeraremos: i) la anonimidad disociativa, ii) la invisibilidad, iii) la asincronicidad, iv) la introyección solipsística, v) la imaginación disociativa y vi) la minimización del *status* y de la autoridad. A continuación, subraya que estos elementos "elevan, lógicamente, las probabilidades de que los usuarios incurran en conductas de riesgo y acaben siendo cibervictimizados".

Además de esta cierta modificación de las pautas de conducta en el entorno *online*, que nos hacen ser más atrevidos y pueden llevarnos a efectuar comportamientos de riesgo –pensemos en

interacciones con terceros desconocidos, lo que no haríamos en el espacio físico; el hecho de visitar determinados sitios web no seguros; descargar archivos de dudosa procedencia y origen, o efectuar compraventas de bienes y servicios sin conocer a la contraparte ni la realidad de la oferta, entre otros–, podemos traer a colación, en este punto, una de las teorías criminológicas clásicas para explicar las causas del delito y su factible adaptación al ciberespacio. Nos referimos a la Teoría de las Actividad Rutinarias (TAR), formulada por Felson y Cohen (1979), y que ha sido adaptada a las TIC por Miró Llinares (2012). En la formulación original de Felson y Cohen se parte de un enfoque situacional, basado en que el delito surge cuando se da la oportunidad delictiva. En apretado esquema, podemos resumir en tres los elementos que conforman dicha teoría explicativa del delito: (i) la existencia de objetivos adecuados, que puedan ser susceptibles de victimización; (ii) la aparición de un agresor motivado, dispuesto a cometer hechos delictivos; y (iii) la ausencia de guardianes capaces, tanto formales como informales, ya sean agentes policiales o conciudadanos que aparezcan en el lugar de los hechos y frustren la expectativa del agresor. En su atinada exposición, Miró Llinares (2012) aplica tales postulados al ciberespacio y sostiene que nos hallamos ante un nuevo espacio de oportunidad criminal en el que concurre una multitud de sujetos victimizables y donde no existen distancias, lo que facilita la inmediatez y el contacto entre sujetos. Añade que la ausencia de guardianes capaces alude tanto a los guardianes formales como a los informales, o a los programas informáticos.

En su disertación, dicho autor explica que estos tres elementos se combinan en las TIC sobre la base de la conducta de la víctima, en atención a las horas empleadas, las páginas web consultadas, la realización de actividades *online* –compraventa de servicios o interacciones con desconocidos– y las medidas de protección que adopte el usuario en su navegación, poniendo el foco en su adopción y en la actualización de los sistemas de protección de los dispositivos informáticos. Afirma que el usuario de las TIC es prácticamente un "autoguardián" y que la clave se encuentra en la conducta de la víctima, que es quien propicia la oportunidad delictiva. Pone de manifiesto que la modificación de las relaciones entre las variables espacio y tiempo en el ciberespacio permite que los ciberdelincuentes, con un solo acto –por

ejemplo, el envío de un mail malicioso–, accedan a una multitud indeterminada de víctimas potenciales. Menciona que un contenido malicioso puede permanecer latente mucho tiempo después de que se suba a las TIC por su autor, y que puede causar daños cuando los usuarios interactúen con él, lo que evidencia que se pueden causar resultados lesivos y nocivos mucho tiempo después de la acción, por lo que, además de la inmediatez, la asincronía juega un destacado papel.

Sin embargo, debemos subrayar que existen notables dificultades a la hora de cuantificar, con precisión, la magnitud del fenómeno tratado. Más allá de los datos oficiales sobre hechos conocidos, porque han sido denunciados, es de prever que un importante porcentaje de hechos engrosen la conocida como "cifra negra" de ciberdelitos. Las causas de ello son variadas: (i) el desconocimiento, por parte de la víctima, de que se ha cometido un delito. Podríamos pensar en aquellos supuestos en los que se dé una ciberestafa de una cuantía ínfima de dinero –unos pocos céntimos– y la víctima no reciba una notificación de su banca electrónica con cada movimiento que se produzca en su cuenta. Sería dable que una transferencia de pocos céntimos pudiera pasar inadvertida; (ii) que la propia víctima, aun conociendo el hecho, no considere que se trate de un delito, *v. gr.*, tentativas de estafa a los que no se les otorga la mayor credibilidad o actos preparatorios de estafas muy alejados de integrar actos ejecutivos –envío de mail con *spam*–; (iii) los propios sentimientos encontrados de la víctima, pudiendo mencionar la culpa o la vergüenza por el delito padecido. Como ejemplo que ilustre esta situación, podríamos mencionar la denominada "estafa romántica", en que el ciberdelincuente hace creer a su víctima que mantienen una relación sentimental telemática, la embauca, se gana su confianza y, finalmente, le solicita dinero con promesa de devolución, lo que nunca sucede. En este caso, la víctima, al sentirse burlada, puede rehusar la denuncia de los hechos por la vergüenza de relatar lo sucedido ante las instancias formales de persecución del delito.

Por otra parte, en cuanto a supuestos en los que se dé el sentimiento de culpa de la víctima, podríamos aludir a la ciberestafa en la que a un sujeto se le promete la obtención de un lucro –*v. gr.*, una cuantiosa herencia– a cambio de un desembolso dinerario

de poca cuantía –el pago de unos impuestos especiales–, si bien, efectuado el abono, nunca recibe la suculenta contraprestación prometida; (iv) la desconfianza en el sistema policial y/o judicial, ante la convicción de que no se va a descubrir al autor del delito ni se va a recuperar lo perdido; (v) el cálculo de intereses y la ponderación entre el coste temporal de un proceso judicial y los perjuicios sufridos con el ciberdelito; (vi) podemos agregar que, en el ámbito empresarial, el riesgo reputacional puede llevar a silenciar hechos delictivos para, precisamente, evitar que se dé una publicidad negativa. Piénsese en el caso de una entidad bancaria que sufre un ataque de *ransomware* –secuestro de datos– y prefiere abonar el rescate y omitir su denuncia, so riesgo de mostrarse en la opinión pública como vulnerable y carente de medidas de ciberseguridad, lo que puede disuadir a futuros clientes de confiar en ella.

Estos son algunos de los argumentos –sin pretensión de exhaustividad– que nos mueven a afirmar, con un importante sector doctrinal, que en el ámbito de la ciberdelincuencia existe una relevante cifra negra. Así las cosas, Montiel Juan (2016) llama la atención sobre los problemas metodológicos en la medición de los ciberdelitos, y señala que la dificultad que presentan las estadísticas oficiales es que dependen de la forma en que se definen los delitos en cada legislación, lo que no necesariamente coincide con la definición criminológica del fenómeno tratado. Además, dicha autora indica que algunos fenómenos cibercriminales pueden implicar la comisión de diferentes delitos tipificados en los textos penales. Considera que la disociación entre los tipos penales y las formas de criminalidad produce un conocimiento muy fragmentario de estos fenómenos. Advierte que las encuestas de cibervictimización y/o ciberdelincuencia autorrevelada arrojan datos diferentes y muy superiores a las cifras oficiales. Mientras que algún autor ha puesto el acento de la cifra negra en elementos técnicos, como la facilidad de alteración de la huella informática, el anonimato en los ciberdelitos, o bien, "el simple hecho de que es necesaria una capacidad técnica mínima para navegar con pleno conocimiento de la Red" (López Gorostidi, 2021), o bien, en la rigidez en la presentación física de denuncias, frente a otros modelos policiales en los que se permite su presentación telefónica o telemática (Kemp, 2021).

3 La ciberdelincuencia económica

3.1 Aspectos generales

Antes de efectuar un repaso por algunos de los principales ciberdelitos económicos que vamos a exponer, forzoso es que hagamos una breve mención a la clasificación que seguimos en esta contribución. Ya indicamos que la ciberdelincuencia carece de un tratamiento unitario y sistemático en el ordenamiento punitivo patrio. Con todo, y pese a asumir que existen diferentes aproximaciones doctrinales, en este trabajo seguiremos la clasificación criminológica patrocinada por Miró Llinares (2012), que diferencia entre ciberdelitos económicos, sociales y políticos, en atención al objeto sobre el que recae, de modo principal, la conducta delictiva. Consideramos que dicha propuesta resulta descriptiva, analítica y que permite aglutinar distintos tipos delictivos, en atención a su bien jurídico tutelado, por lo que facilita su comprensión. Si bien, y como hemos resaltado, somos conscientes de que existen delitos en los que puede haber más de un objeto protegido, y que podrían, en consecuencia, ser subsumidos en una categoría u otra. Por ello, hemos destacado que tal clasificación parte del objeto principalmente protegido.

De esta manera, los ciberdelitos económicos serían aquellos en los que prevalezca un componente patrimonial. Los ciberdelitos sociales aglutinarían una amalgama de variados supuestos delictivos, que tendrían como eje que recaerían sobre bienes jurídicos personales –o personalísimos– de los individuos, y conectados con los atributos propios de su esfera relacional –*v. gr.*, libertad, libertad e indemnidad sexuales, honor, intimidad o propia imagen, entre otros–. Por último, los ciberdelitos políticos serían todos aquellos que se cometerían con una motivación ideológica, y entre ellos podríamos incluir el ciberterrorismo o el *hacktivismo*.

Si descendemos a los ciberdelitos económicos, podemos concebirlos como aquellos cibercrímenes que recaen sobre

intereses patrimoniales. Si retomamos el citado informe sobre cibercriminalidad en España del año 2023, observamos que más del 90 % de los ciberdelitos son de corte patrimonial y, entre ellos, de manera absoluta, predominan las estafas informáticas –ya indicamos que el informe alude a "fraude"–. De hecho, de los 472.125 ciberdelitos conocidos en el año, 427.448 fueron ciberestafas, 15.137 fueron casos de "falsificación informática", 1.659 de interferencia en datos y en sistemas informáticos y 64 casos denunciaron ciberdelitos contra la propiedad intelectual e industrial. Como se puede colegir de lo que antecede, la finalidad lucrativa se encuentra detrás de una buena parte de los ciberataques. Estas acciones se ejecutan para obtener, de modo ilícito, dinero procedente de individuos, empresas u otras organizaciones.

Podemos anotar varias causas que facilitan o dan pie a que las TIC se conviertan en cauce para ejecutar delitos contra el patrimonio. En primer lugar, los usuarios de las TIC han trasladado al ciberespacio buena parte de su operativa económica, lo que, indefectiblemente, también abre un portillo a que puedan sufrir ciberataques. A título de ejemplo, podemos señalar que un porcentaje significativo de los usuarios de las TIC emplea la banca *online*, realiza compraventas de bienes y servicios a través de la Red, concierta negocios jurídicos y efectúa transferencias diversas en el ciberespacio. Para llevar a cabo tales actos, se insertan las contraseñas y las claves personales en los dispositivos informáticos y en los *smartphones*. Algo tan –aparentemente– inocuo como el pago de unas entradas de un concierto que se han visto en un anuncio en redes sociales puede comportar una pérdida patrimonial, al no advertir la víctima que se trataba de una estafa. Pues bien, no solo se corre el riesgo de que el anuncio visualizado sea engañoso, lo que hace generar desconfianza en los cibernautas y en el tráfico económico, sino que existe el peligro cierto de que los dispositivos informáticos sean infectados con *malware* y los ciberdelincuentes puedan acceder a nuestras claves y contraseñas.

Como podemos observar con este breve esbozo, los intereses económicos presentes en las TIC son ingentes. Además, los ciberdelincuentes pueden dirigirse a una pluralidad indeterminada de potenciales víctimas con el mismo ataque, por lo que se reducen

los esfuerzos e inversiones espacio-temporales. Por lo tanto, la obtención de un lucro económico se ve estimulada por la inmediatez, por la ausencia de fronteras, por la interconexión y por la mundialización de la Red. Además, se acude a argucias más o menos sofisticadas, como las técnicas de ingeniería social, facilitadas por el anonimato, la suplantación de identidad y la generación de confianza en el receptor de la comunicación o mensaje. También se emplean instrumentos técnicos, como VPN, deslocalizadores de direcciones IP, *proxy*, empleo de redes WiFi públicas en abierto y distintos artificios para enmascarar la procedencia del ataque, para diluir el rastro de los ciberdelincuentes y para romper la trazabilidad de las comunicaciones y de los fondos detraídos.

A ello se suma que, en ocasiones, los usuarios de las TIC no empleamos todas las medidas de seguridad precisas, más allá del antivirus, puesto que, entre otros aspectos, no contamos con las actualizaciones de los programas y aplicaciones, no usamos cortafuegos, no tenemos contraseñas seguras –ni gestores de contraseñas–, reunimos toda nuestra información y claves en un mismo dispositivo, no contamos con copias de seguridad de nuestros datos, interactuamos con desconocidos, llevamos a cabo navegaciones web por entornos no seguros, descargamos inopinadamente links y documentos sin cerciorarnos de su procedencia, efectuamos compraventas *online* y facilitamos nuestros datos personales –tales como fotografías personales o del DNI– con demasiada facilidad. Por si ello fuera poco, no podemos soslayar el auge de determinados elementos, como la IA, las criptomonedas y el empleo, por los cibercriminales, de la *dark web*, como aquella parte cifrada de Internet a la que se accede mediante navegadores especializados, oculta a los motores de búsqueda tradicionales, con direcciones IP enmascaradas, y donde se pueden obtener bienes, servicios y actividades ilícitas.

Este conjunto de elementos tecnológicos y personales, unido a las características del ciberespacio, explica, en buena medida, que asistamos a este auge de los ciberdelitos y, entre ellos, de la ciberdelincuencia económica. El lucro económico se alza, así, como la motivación principal de los ciberdelincuentes, ante la facilidad para victimizar a una pluralidad de sujetos, la dificultad en su detección y, por ende, la rentabilidad, en términos de

costes-beneficios, de esta serie de modalidades delictivas. A ello debemos agregar la internacionalización de la Red, la disparidad normativa entre las diferentes legislaciones nacionales, las disfunciones en la cooperación judicial internacional en algunas jurisdicciones y las dudas que genera la propia delimitación de los órganos judiciales con competencia para conocer de tales ilícitos. Es decir, y en suma, nos hallamos ante un cóctel de circunstancias que promueven que, a través de las TIC, se cometan ciberdelitos y que estos sean, en la mayor parte de supuestos, de índole económica.

3.2 Principales ciberdelitos económicos

En este apartado pretendemos realizar un acercamiento a algunos de los principales ciberdelitos económicos que se cometen a través de las TIC. Vaya por delante que no se efectuará un listado exhaustivo de los tipos del texto punitivo ni se llevará a cabo un análisis profundo y pormenorizado de cada uno de ellos. No es ese el objeto de esta contribución. Antes bien, lo que se realizará será destacar algunos rasgos criminológicos de tales ilícitos que nos sirvan para comprender mejor el porqué de las cibervictimizaciones y la causa de que las TIC se erijan en un vehículo adecuado para su comisión. En concreto, por su incidencia práctica, por su repercusión y por su relevancia político-criminal, hemos seleccionado cuatro delitos del Título XIII del Libro II del CP: estafas, delitos de daños, delitos contra la propiedad intelectual e industrial y blanqueo de dinero. Consideramos que constituyen una muestra lo suficientemente representativa, obedecen a *modus operandi* diferentes y resultan ilustrativos de distintas tipologías delictivas con incidencia en el patrimonio, en el orden socioeconómico y, en definitiva, en la esfera patrimonial.

3.2.1 Estafas y ciberestafas (arts. 248-251 CP)

Constituyen, sin duda, los principales ciberdelitos, tanto cuantitativa como cualitativamente, por lo que también son los ciberdelitos económicos más importantes. Debemos poner de relieve que la estafa tradicional o clásica y la estafa informática se recogen en los arts. 248 y 249[4] CP. La diferencia basilar entre

ambas estriba en que, como sabemos, la estafa tradicional obedece a la conjunción de cinco elementos que han de darse de modo sucesivo: el empleo de engaño bastante, que induce a error a la víctima, y le hace realizar un acto de disposición patrimonial, en perjuicio propio o de tercero, existiendo entre todos los elementos de la cadena descrita una relación de causalidad. Por su parte, hasta el año 2022, la estafa informática figuraba como un apéndice de la estafa clásica, en el art. 248 CP, y se caracterizaba porque no concurría el engaño como medio comisivo, sino que se aludía a la obtención de una transferencia patrimonial inconsentida mediante "alguna manipulación informática o artificio semejante". Un relevante sector doctrinal había llamado la atención sobre la imposibilidad de engañar a las máquinas y rehusaba la pretendida equivalencia con el molde de la estafa canónica.

Pues bien, la LO 14/2022, de 22 de diciembre, ha venido a dotar de independencia a la estafa informática, ubicándola sistemáticamente en el art. 249[5] CP, ampliando sus modalidades de conducta y solapándose, en buena medida, con los verbos nucleares del delito de daños informáticos del art. 264 CP. Si bien, debemos anotar que, a los efectos de nuestro trabajo, lo más relevante es que surgen discrepancias interpretativas a propósito de si la estafa tradicional puede ser aplicada en las ciberestafas –con lo que cabría la posibilidad del delito leve de estafa–, o bien, si el legislador ha pretendido que todas las estafas cometidas en las TIC se incardinen en el cauce del art. 249 CP, que no contiene ninguna modalidad de delito leve, con todo lo que ello comportaría en materia procesal: no sería posible acudir al juicio por delito leve, siempre habrían de tramitarse por el procedimiento abreviado y existiría una fase de instrucción, con la posibilidad de adoptar diligencias de investigación y actos de cooperación judicial internacional, de gran relevancia en materia de ciberestafas ante la ausencia de fronteras en

4. Sobre la nueva redacción del art. 249 CP, *vid*. Bustos Rubio (2023); y, en concreto, sobre el uso fraudulento de medios de pago distintos del efectivo, *vid*. Abadías Selma (2023).

5. Para una acabada comprensión, se recomienda una lectura de los arts. 248 y 249 CP, comparando el texto anterior a la LO 14/2022 y el actualmente vigente.

las TIC y el carácter transnacional de muchos de estos ilícitos. En nuestra opinión, y de modo telegráfico, consideramos que ambas figuras son compatibles en este ámbito, puesto que obedecen a presupuestos fácticos diferentes. En aquellos supuestos en los que se dé una relación bilateral entre dos sujetos y medie engaño que induzca a error al sujeto pasivo, no habría óbice para estimar que nos hallamos ante una estafa subsumible en el art. 248 CP –siempre y cuando concurran los restantes elementos típicos–. No obstante, no siempre será fácil deslindar con tanta nitidez, por lo que habrá de estarse al caso concreto y a sus circunstancias específicas.

Con todo, no se trata de una cuestión que se pueda zanjar en una afirmación simplista o reduccionista, inopinada y que no se sustente en argumentos dogmáticos o de técnica penal, sino que habrá de estarse al caso concreto para valorar qué concretos elementos típicos se dan. En este sentido, no podemos obviar que en aquellos casos en los que las TIC constituyan únicamente el medio comisivo –instrumental–, pero no haya ningún artificio informático o técnico, se puede sostener que existe una estafa tradicional. El caso prototípico sería el de un anuncio de venta falso en una página web, a través del cual se ponen en relación dos personas para la venta de un bien o servicio, la víctima abona el precio y la contraprestación no se produce. En este esquemático supuesto ha existido un engaño que ha inducido a error al perjudicado, y en cuya virtud ha realizado el acto de disposición patrimonial generador del perjuicio.

Somos conscientes de que la voluntad del legislador en la LO 14/2022 es dotar de autonomía a las ciberestafas y, al hilo de la normativa comunitaria, potenciar y reforzar su ámbito de aplicación. Ello se observa en la Consulta 1/2024, de la Fiscalía General del Estado, de 21 de marzo, sobre algunas cuestiones relacionadas con la utilización fraudulenta de instrumentos de pago distintos del efectivo. En este texto se aporta una serie de criterios de interpretación del art. 249 CP. En él se afirma que: “En opinión de la doctrina mayoritaria, tanto la estafa informática como la utilización fraudulenta de medios de pago de los arts. 249.1.a) y 249.1.b) CP se consideran modalidades típicas que tienen auténtica autonomía y sustantividad frente al tipo básico de estafa del art. 248 CP”. Además, la citada consulta

rechaza que quepa el delito leve de estafa informática *ex* art. 249 CP, cuando zanja que "al margen del tenor literal del art. 249 CP y del art. 9 de la Directiva (UE) 2019/713 y con independencia de la *voluntas legislatoris* expresada en la MAIN del anteproyecto de ley, existen razones de carácter teleológico y lógico-sistemático para rechazar que los supuestos en los que la cuantía defraudada no supere los 400 euros puedan ser calificados como delito leve de estafa".

Pues bien, ello no es óbice para mantener las afirmaciones expresadas con anterioridad, antes, al contrario. Hemos de discriminar cuándo existe una estafa clásica (del art. 248 CP) –aunque se cometa a través de las TIC, como mero cauce, canal o herramienta a través del que se vehicule el engaño– y cuándo nos hallamos ante una estafa informática, cuya regulación se contiene en el art. 249 CP. Como podemos apreciar, se trata de cauces diferentes y con tratamientos distintos. Si bien, reiteramos, en algunas ocasiones será complejo discernir cuál de los dos preceptos resulta aplicable, sobre todo, cuando aparezcan, entremezclados, elementos de engaño –como medio comisivo típico– y manipulaciones informáticas o artificios semejantes, con accesos, inmisiones e intromisiones. En tal caso, podríamos acudir al principio de especialidad, contenido en la regla 1.ª[6] del art. 8 CP, y considerar aplicable el art. 249 CP, si se aprecia dicho concurso de normas. Por el momento no contamos con doctrina jurisprudencial actual, tras la reforma de la LO 14/2022, que brinde criterios de delimitación nítidos, precisos y extrapolables a casos similares, por lo que habrá que aguardar los avances en la práctica judicial.

En todo caso, si nos adentramos en las diferentes clases de ciberestafas, podemos apreciar que existe una gran variedad de tipologías y modalidades comisivas. Algunas de ellas más burdas y obvias –como envíos de correos *spam*–, otras, más elaboradas y sofisticadas. Lo primero que llama la atención es que su comisión se ve favorecida por el empleo de técnicas de ingeniería social,

6. Art. 8.1.ª CP: "Los hechos susceptibles de ser calificados con arreglo a dos o más preceptos de este Código, y no comprendidos en los artículos 73 a 77, se castigarán observando las siguientes reglas: 1.ª El precepto especial se aplicará con preferencia al general".

que el Instituto Nacional de Ciberseguridad (INCIBE) define como[7] "técnicas de manipulación psicológica con el objetivo de conseguir que los usuarios revelen información confidencial o realicen cualquier tipo de acción que pueda beneficiar al ciberdelincuente", y que consisten en el uso de canales de propagación masivos, como el correo electrónico, llamadas telefónicas, aplicaciones de mensajería o redes sociales. El INCIBE alude a dos modalidades de técnicas de ingeniería social, dependiendo del número de interacciones que requieran por parte del ciberdelincuente: (i) *hunting*, que busca afectar al mayor número de usuarios realizando, únicamente, una comunicación, y que es común en campañas de *phishing* realizado contra entidades bancarias o energéticas, o bien, en acciones que pretenden realizar acciones de infección de *malware* para efectuar ulteriores ataques de *ransomware*; (ii) *farming*, donde los ciberdelincuentes realizan varias comunicaciones con las víctimas hasta conseguir su objetivo u obtener la mayor cantidad de información posible, donde se podrían incluir las campañas que pretenden infundir temor al receptor con la existencia de vídeos privados suyos o futuros ataques contra su organización. Desde el INCIBE se explica que estos ataques de manipulación de las víctimas suelen seguir una serie de principios básicos: el respeto a la autoridad, la voluntad de ayudar –fundamentalmente, en entornos laborales–, el temor a perder un servicio, el respeto social y la gratuidad.

Por poner algunos ejemplos clásicos de ciberestafas, podemos mencionar: (i) la ciberestafa extorsiva, en la que se comunica mediante mail o sms que hemos sido objeto de una sanción administrativa, de una multa de tráfico, de una inspección tributaria o de la Seguridad Social, etc., y se nos solicita un pago para poner fin a dicho procedimiento. Suelen remitirse desde direcciones de correo electrónico que pretenden emular los correos corporativos de tales entidades, con membretes y links a páginas web que, en realidad, no son las legítimas, por lo que también efectúan suplantaciones de identidad de tales entes –*spoofing*–, aunque suelen ser montajes burdos y toscos. En otras ocasiones, se amenaza con la difusión de un vídeo de contenido íntimo si

7. INCIBE (2019). Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse. Publicado el 5 de septiembre de 2019. https://www.incibe.es/empresas/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse

el sujeto no obedece a la petición formulada; (ii) la ciberestafa de lotería, en la que se anuncia al receptor que ha obtenido un premio –de un concurso o sorteo en que no ha participado– y se le indica que, para su cobro, ha de abonar una suerte de tasa o adelanto; (iii) las ciberestafas laborales, en las que se oferta al destinatario un puesto de trabajo, a desempeñar desde su domicilio, con una alta rentabilidad, a cambio de facilitar sus datos personales y de facilitar una cuenta bancaria. Se indica que la empresa está radicada en el extranjero y que la pasarela de pagos no admite sus cuentas bancarias, por lo que se interesa al candidato al puesto que aperture una cuenta –o facilite la suya– y, a través de este medio, vehicular diferentes pagos. En realidad, las cibervíctimas suelen ser utilizadas, en muchas ocasiones, como mulas de los fondos ilícitamente obtenidos; (iv) las ciberestafas románticas, en las que los ciberdelincuentes se ganan la confianza del receptor, le hacen ver que están iniciando una relación sentimental y, en un momento dado, tras ganarse su confianza, le solicitan abonos dinerarios con diferentes excusas; (v) el fraude del CEO, en que el ciberdelincuente, tras haber obtenido determinada información de una organización, remite a uno de sus integrantes un mail, haciéndose pasar por otro sujeto –el CEO o una persona con capacidad de mando, o directivo de algún departamento–, y requiere una modificación en las transferencias por determinados servicios, o varía una orden de pago; (vi) fraudes en herencias, similar a la estafa de la lotería, se comunica que existe una herencia muy cuantiosa y que el receptor puede obtener dicho monto si abona una tasa o pago por cuestiones burocráticas de tramitación interna; (vii) comunicaciones –vía SMS o mail– sobre problemas existentes en un envío de correos, para lo que es preciso verificar algunas cuestiones en un link que se remite en el cuerpo del mensaje. Esta ciberestafa tiene la particularidad de que, dado el alto volumen de compras *online* que se realizan, es muy factible que el destinatario del mensaje esté esperando la llegada de un paquete, por lo que no le sorprendería recibir una comunicación al respecto –de Correos, SEUR, MRW, Amazon, FedEx...–, podría otorgar credibilidad al remitente y, en consecuencia, hacer *click* en el enlace malicioso. Constituye una buena muestra de cómo la variación de nuestros hábitos de consumo puede abrir el portillo a ulteriores victimizaciones; (ix) anuncios fraudulentos de compraventa de bienes y servicios en los que la característica es que

la víctima toma la iniciativa, contacta con el número de teléfono o mail que ha insertado el anuncio, abona el precio convenido y, finalmente, nunca recibe la contraprestación pactada –teléfonos móviles, videoconsolas, entradas de conciertos, perros...–. Sin lugar a dudas, esta modalidad es la más relevante, numéricamente, en la práctica de los juzgados y tribunales. Por tal motivo, señalaremos algunos de sus rasgos característicos con mayor profundidad que las restantes. Los precios requeridos no superan los 400 euros, lo que provoca que nos hallemos ante ciberdelitos leves –si asumimos que sigue operando el art. 248 CP y que en ellas predomina el engaño–, en los que no cabría realizar una fase de instrucción.

Los anuncios se insertan en portales legítimos de compraventa de artículos, camuflados entre otros anuncios reales. Los ciberdelincuentes entablan conversaciones con los supuestos compradores y les facilitan datos personales y hasta fotografías de DNI, lo que dota de verosimilitud al engaño y crea un cierto clima de confianza recíproca. Hemos de apuntar que, en muchas ocasiones, tales DNI son de anteriores víctimas, por lo que resulta usual que, en la práctica, nos encontremos con personas que han sido victimizadas, denuncien la estafa padecida y, con posterioridad, tales personas se vean denunciadas por hechos similares posteriores, dado que los ciberdelincuentes han empleado sus datos personales para cometer otras estafas. Asimismo, se observan anuncios reduplicados en distintos portales web, y que los mismos sujetos oferten diferentes bienes y servicios, sin relación entre ellos.

En este punto, debemos subrayar la posibilidad de que distintos tipos de ciberestafas sean cometidas mediante IA, lo que introduce mayores elementos de complejidad. En este sentido, Alonso Cebrián y Velasco Núñez (2024) advierten que la suplantación de datos personales digitalizables, como la voz o la imagen, se está utilizando, en el campo económico, para llevar a cabo distintas estafas, y mencionan la estafa del CEO, así como la del supuesto hijo que comunica a sus padres que tiene problemas en el aeropuerto. También citan la ciberestafa consistente en suplantar la identidad, en la que se lleva a cabo la apertura de cuenta bancaria, y en la que "agregan reclamos con aparentes elementos identitarios (voz, imagen) falseados/creados con IA

para suplantar personas que mueven a hacer los desplazamientos patrimoniales perseguidos", y apuntan otras modalidades tan sofisticadas como el SIM *swapping*, "emitido por algoritmos de IA controlada una vez se conocen datos 'pescados' de quien se quiere suplantar para recibir del banco las claves necesarias para autenticar la cuenta a defraudar". Asimismo, podemos resaltar, siguiendo a Morillas Fernández (2023), que se pueden cometer, a través de IA, actos de *spear phishing*, en los que se envían correos electrónicos –o bien, se replican páginas web legítimas o mensajes de texto–, y se solicita información a la víctima, o bien, que inicie sesión en alguna plataforma, y donde lo relevante es la obtención del acceso. Pues bien, como sintetiza dicho autor, a través de esta información, los sistemas de IA pueden analizar los hábitos de los usuarios de las TIC y confeccionar emails fraudulentos "mucho más sofisticados que los que han sido elaborados a través de tradicionales técnicas de *social engineering*", y concluye que, de esta forma, se incrementan "las posibilidades de inducir a error a los internautas obteniendo de forma ilícita datos personales contenidos en tarjetas de crédito, credenciales para acceder *a home banking*, datos sanitarios, etc.". En esta misma línea, Jiménez (2024) centra la atención en el elevado grado de sofisticación de las estafas telefónicas cometidas mediante IA. Destaca que esta no solo es capaz de imitar las voces, sino también de replicar las pausas, las muletillas y las características que hacen única cada forma de hablar. Indica que en Reino Unido se cometió una estafa de 240.000 euros, cuando un empleado recibió una llamada telefónica de su presunto jefe, en la que le ordenaba que realizase, con urgencia, una transferencia. En realidad, el supuesto jefe resultó ser una voz clonada generada mediante IA.

Tras llamar la atención sobre algunos de los casos prototípicos de ciberestafas y advertir de los riesgos que comporta la IA en este ámbito, de un alcance insospechado e insospechable en estos momentos, debemos aludir, en este punto, a otro aspecto basilar de las ciberestafas, que nos permitirá catalogar los hechos como delito o no. Hacemos referencia a los denominados "deberes de autoprotección" que tendría la víctima. En apretada síntesis podemos indicar que tales deberes consisten en ciertas cautelas o medidas de salvaguarda que ha de adoptar un sujeto para evitar ser víctima de delitos. No aparecen regulados, como

tales, en el Código Penal; no obstante, nos sitúan en el ámbito de la influencia que puede tener el comportamiento de la víctima en su proceso de victimización y, a efectos penales, en la calificación jurídica de los hechos cuando se omiten tales cautelas. Su análisis ha de llevarse a cabo al valorar la imputación objetiva del resultado dañoso al autor de la conducta que, causalmente, ha generado un concreto resultado lesivo. Por lo que respecta a nuestro ámbito, en el delito de estafa, no cabe extralimitar su alcance. Debemos tomar en consideración que el tipo no alude a ellos, por lo que no es dable un recurso exacerbado a dicha figura, so riesgo de perpetuar situaciones de impunidad. Es evidente que ha de descartarse la idoneidad del engaño en los supuestos de ardides burdos, evidentes, toscos o grotescos, si bien, ello ha de analizarse, de modo fundamental, desde la perspectiva de la conducta defraudatoria, tomando como base las características personales de la víctima. La jurisprudencia de la Sala 2.ª del Tribunal Supremo (TS) ha llevado a cabo una evolución, desde supuestos en los que se destacaba la atipicidad de la conducta por la ausencia de los deberes de autoprotección, a otra intelección restrictiva, en la que estima que no cabe imponer a la víctima desproporcionados y excesivos deberes de autotutela[8].

Por lo tanto, en el ámbito de la ciberdelincuencia, los usuarios de las TIC han de adoptar las cautelas y medidas de seguridad necesarias, tanto en sus dispositivos telemáticos, como en sus prácticas y en la utilización de las TIC. Existe una pluralidad de medidas de diligencia y cautelas recomendables, si bien, no cabe realizar una interpretación maximalista de las consecuencias de la omisión de tales cautelas. En este sentido, ha de promoverse una intelección restrictiva de la virtualidad exculpatoria de la omisión de los deberes de protección en el ciberespacio, a la vista de la normativa comunitaria, en que se promueve la detección, persecución y sanción de tales fraudes. Puesto que abundan las posibilidades de victimización, ante la nueva configuración de las relaciones espacio-temporales, deben tomarse en consideración todos los elementos concurrentes. Ha de ponerse en relación con el concepto de riesgo permitido, con el concreto

8. *Vid*. al respecto STS 230/2021, de 11 de marzo, ponente Excmo. Sr. D. Javier Hernández García, ECLI:ES:TS:2021:996.

giro, tráfico o sector en que se lleva a cabo la acción, con los principios de confianza y de buena fe, y, de modo esencial, con las características personales del sujeto que opera su autopuesta en peligro.

Asimismo, a modo de cierre del apartado, y a simple título de esbozo, no podemos pasar por alto que pueden darse algunas áreas de confluencia de la ciberestafa con otros tipos delictivos, por lo que pueden surgir dudas a propósito de si nos hallamos ante un concurso de normas, o bien, de delitos y, en este último caso, a la hora de precisar qué concreta relación concursal se da. Sin pretensión de agotar la materia y a los meros efectos ejemplificativos, más allá de los clásicos ejemplos concursales de la estafa tradicional con los delitos de apropiación indebida o de falsedades, podríamos aludir a otras tres situaciones concursales, que presentarían mayor conexión con las TIC, y que surgen en relación con los delitos contra la intimidad (art. 197 CP), de daños informáticos (art. 264 CP) o de usurpación del estado civil (art. 401 CP). Por lo que hace a los delitos contra la intimidad, podemos pensar en el supuesto de una persona que se apodera de los datos personales de otro, que están registrados en un fichero o soporte –un *smartphone* o un ordenador donde están almacenadas las claves bancarias– y, a continuación, lleva a cabo la transferencia inconsentida. Existirían argumentos para defender que se trata de un concurso real de delitos, aunque tampoco sería descabellado apreciar que nos encontramos ante un concurso medial, en que el ataque a la intimidad es el medio para llegar al fin perseguido, de naturaleza patrimonial.

En segundo término, si prestamos atención a la relación concursal entre la ciberestafa y el delito de daños, debemos efectuar varias matizaciones: se aprecia un solapamiento de algunas modalidades de conducta entre el art. 249 CP y el art. 264 CP, puesto que en ambos delitos se mencionan, como verbos nucleares, "borrar", "alterar" y "suprimir" datos informáticos. Observamos que la pena es idéntica en ambos delitos. Así las cosas, podríamos abogar por la existencia de un concurso de normas, a resolver mediante el principio de especialidad, en virtud del ánimo de lucro que guía al sujeto activo en la estafa, por lo que podría prevalecer dicho tipo. Incluso, podría argumentarse que los daños constituyen un medio para cometer la estafa: se

emplean tales comportamientos, lesivos para los datos y que los dañan, para conseguir la transferencia inconsentida. Por lo tanto, se deja abierto el supuesto, dado que únicamente se apuntan las alternativas en presencia, pero sin pretensión de exhaustividad.

En último lugar, por lo que hace al delito de usurpación del estado civil, pese a que en algún momento se haya podido indicar que es dable apreciar un concurso de delitos con la estafa, cuando se empleen los datos personales y señas de un tercero para cometer la estafa, debemos excluir dicha posibilidad si no existe una permanencia en el tiempo, puesto que la jurisprudencia de la Sala 2.ª exige una continuidad temporal, como se indicó en la STS 1045/2011[9], de 14 de octubre, en la que se expresa que "la conducta del agente exige una cierta permanencia y es ínsito al propósito de usurpación plena de la personalidad global del afectado". Si bien, debemos recordar que la LO 10/2022, de 6 de septiembre, introdujo el art. 172 ter 5 CP, en el que se castiga 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 víctima una situación de acoso, hostigamiento o humillación. No obstante, *prima facie*, no concurrirían los requisitos del art. 401 CP en el supuesto de hecho que hemos indicado.

Con todo, tanto en los tres supuestos que hemos anotado, como en otras posibles situaciones concursales que se puedan originar, habrá que estar a las circunstancias del caso concreto para determinar, con precisión, qué nexo, engarce o ligazón se produce entre los distintos tipos en presencia, si es que se da dicha conexión. Por lo tanto, reiteramos que las soluciones apuntadas aquí son provisionales, genéricas y parciales, por lo que nos mostramos expectantes y aguardamos las propuestas doctrinales y los pronunciamientos judiciales que arrojen luz sobre dicha materia.

9. STS 1045/2011, de 14 de octubre, ponente Excmo. Sr. D. Juan Ramón Berdugo Gómez de la Torre, ECLI:ES:TS:2011:6858.

3.2.2 Delitos de daños informáticos (arts. 264-264 quater CP)

La afectación al patrimonio de los delitos de daños resulta incuestionable, aunque nos hallamos ante delitos patrimoniales sin enriquecimiento, por lo que constituyen una suerte de rareza en el Título XIII[10]. Pues bien, si atendemos a los delitos de daños informáticos, podemos convenir en que, en ocasiones, la finalidad que guía al ciberdelincuente puede ser variada. No podemos obviar que, en algunos casos de intrusiones o de ataques de denegación de servicio –ataques *DoS*–, o distribuidos de denegación de servicio –ataques *DDoS*–, se pretende llevar a cabo actos de *hacktivismo*, con motivaciones políticas o ideológicas, lo que se puede observar en el colapso temporal de servidores web de grandes empresas multinacionales o de servicios públicos, en los que se persigue exteriorizar una reivindicación política. En otras ocasiones, según la magnitud del ataque, sus destinatarios y sus consecuencias, podríamos hallarnos ante casos de ciberterrorismo, por lo que, como podemos apreciar, en estos supuestos nos hallaríamos, más bien, ante ciberdelitos de corte político y no meramente económicos. Con ello constatamos que, algunas veces, las líneas divisorias entre las clasificaciones de ciberdelitos son permeables, porosas y permiten diversas gradaciones. Podemos discriminar los delitos de "sabotaje informático" o interferencia ilegal en datos informáticos –art. 264.1 CP–, cuya conducta típica se configura de modo mixto alternativo, el delito de daños informáticos a sistemas –art. 264 bis.1 CP–, donde se reprime obstaculizar o interrumpir el funcionamiento del sistema informático ajeno y un adelantamiento de las barreras de punición, contenido en el art. 264 ter CP, en el que nos hallaríamos ante actos preparatorios o protopreparatorios de los anteriores. Cabe significar que, al igual que en los restantes delitos de daños, el bien jurídico tutelado es la propiedad, si bien, en algunas de las conductas tipificadas se pone de relieve que se trasciende del patrimonio individual y se atiende a intereses supraindividuales, toda vez que en los tipos cualificados se valora que la afectación se pro-

10. Para una exposición completa de los delitos de daños, *vid*. González Uriel (2022). Nuevamente, se aconseja una lectura de los preceptos citados, a los efectos de una comprensión acabada.

pague a una pluralidad de sistemas informáticos, o bien, que afecte al funcionamiento de servicios públicos que puedan ser reputados como esenciales, o a la provisión de bienes de primera necesidad, que se afecte a una "infraestructura crítica", o que se ponga en peligro la seguridad estatal, de la UE o de un Estado miembro de la UE. Como se puede observar, en tales supuestos no solo se está tutelando la propiedad privada, sino que se pone de manifiesto la capacidad dañina de los ataques informáticos y la posibilidad de que se afecten los intereses generales y la propia seguridad nacional.

Por lo que a nosotros interesa, debemos señalar los peligros que se derivan de determinados delitos de daños, como los ataques de *ransomware* o secuestros de datos, en los que se produce un acceso inconsentido en un sistema informático ajeno, mediante un *malware* que lo infecta y accede a la totalidad o parte de sus datos, que se cifran, y se impide a su titular el acceso a ellos, en todo o en parte, y se solicita el pago de un rescate para poder recuperar el acceso o los datos en cuestión. Asimismo, en muchas ocasiones, la petición del rescate se hace en criptomonedas, para robustecer el anonimato, evitar la trazabilidad de los fondos y la persecución de los autores del ataque. Conviene destacar que tales ciberataques se realizan tanto a personas físicas como jurídicas, públicas y privadas, y gozan de especial repercusión mediática cuando se efectúan a servicios públicos, como hospitales, por los notables perjuicios personales que irrogan, no solo por los actos médicos que se cancelan y dilatan, sino también por la obtención de datos sensibles de multitud de pacientes, que pueden acabar vendiéndose en la *dark web* –no está de más recordar el manido lema de que los datos personales constituyen el petróleo del siglo XXI–. Además, cabe agregar que se han dado casos de ataques de *ransomware* recurrentes frente a las mismas víctimas, con posterioridad a que hubieran abonado el rescate. Podemos vaticinar que existe una notable cifra negra en este campo, sobre todo, en el ámbito empresarial, toda vez que las corporaciones desean evitar cualquier publicidad negativa o desconfianza en sus sistemas de ciberseguridad, toda vez que la denuncia de estos hechos expondría, públicamente, la existencia de vulnerabilidades en sus sistemas de protección, lo que generaría un notable daño reputacional.

En segundo lugar, como ciberdelito de daños con repercusión patrimonial, debemos destacar que los ataques *DoS* y *DDoS*, que en muchas ocasiones son ejecutados a través de redes de *bots*, consisten en dirigir una multitud de peticiones a sitios web y redes, hasta saturarlas, sobrecargando sus servidores y evitando que sean accesibles a usuarios legítimos, lo que provoca su parálisis. Estos ciberataques se han dirigido frente a grandes empresas y también frente a organismos públicos, saturando sus servidores y portales web. Podemos hacernos una idea de los notables perjuicios económicos que se pueden derivar de la paralización de los servidores web de una empresa, si pensamos en la contratación *online*, en la formalización de pedidos o, incluso, en su propio sistema de comunicaciones con terceros –acreedores, proveedores, deudores...–. Estos ciberataques pueden prolongarse en el tiempo, por lo que los efectos producidos se pueden dilatar, incrementando el perjuicio económico.

3.2.3 Delitos contra la propiedad intelectual e industrial (arts. 270-277 CP)

Dentro de estas figuras delictivas, podemos destacar la relevancia de la piratería informática o digital, esto es, la descarga de contenidos amparados por derechos de autor sin el abono de los pagos correspondientes. Desde una perspectiva criminológica se han propuesto diferentes explicaciones sobre un fenómeno tan extendido y normalizado. En este sentido, desde la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, 2019) se ha explicado que "las normas socioculturales y el comportamiento y la dinámica de grupo influyen en las tasas de piratería digital". También destaca que los autores de delitos contra la propiedad intelectual cometidos a través de las TIC utilizan cierta técnicas de "neutralización" –entre otras, negación de responsabilidad, negación de la víctima, negación del daño, condena de los condenadores y apelación a una mayor lealtad–, si bien, se ha matizado que dichas técnicas varían y, en otras investigaciones sintetizadas por UNODC, se expresa que las "asimetrías digitales" –como puede ser la falta de supervisión inmediata de las acciones realizadas *online*– "pueden contribuir a que las personas 'opten' hacia la desviación digital y accedan a información o recursos que apoyen o normalicen actos delictivos como la piratería". Además, desde UNODC se atiende a otros aspectos

etiológicos de los ciberdelitos contra la propiedad intelectual, como el sentimiento antiempresarial o los altos costos –reales o percibidos– de las obras amparadas por derechos de propiedad intelectual y, en este sentido, se refleja que "si los consumidores creen que existe una discrepancia injusta entre el valor, la calidad y el precio, buscan medios alternativos para obtener el bien (a un precio más bajo o mediante la piratería, la obtención, el acceso o el uso no autorizado de la propiedad intelectual de otro)". Asimismo, en la exposición realizada por UNODC se finaliza indicando que también se ha sugerido por diferentes autores que el drástico incremento de la piratería digital desde finales de la década de 1990 se produjo como "respuesta pública al exceso de legislación en materia de protección de la propiedad intelectual".

No podemos obviar que el volumen de piratería digital (art. 270 CP) irroga elevadísimos perjuicios económicos a los titulares de los derechos de propiedad intelectual, puesto que se trata de un comportamiento globalizado, continuo y permanente. Nos hallamos ante una práctica extendida, generalizada, en la que se relativiza su carácter delictivo, se normalizan tales acciones y se asume su realización. A su vez, la descarga ilícita de contenidos se encuentra amparada por su facilidad de realización, toda vez que es sencillo, para cualquier usuario, acceder a portales web en que se ofertan tales ilícitos servicios. Además, el objeto sobre el que recae tal conducta es variado, plural y heterogéneo. No solo hacemos referencia a producciones audiovisuales –discos, películas, series o videojuegos–, sino que también se propagan servidores, páginas, aplicaciones y servicios de mensajería con bibliotecas pirata, en las que se puede descargar cualquier libro.

Mención especial merece, en sede de delitos contra la propiedad industrial (art. 274 CP), la existencia de portales web que venden falsificaciones de ropa de marca, de complementos, de joyas, de dispositivos electrónicos o de medicamentos, entre otros, a un precio inferior al del producto legítimo. Las TIC constituyen un gran cauce de difusión y propagación para estos mercados irregulares, que producen importantes mermas de facturación a las marcas legítimas. Además, se produce la paradoja de que, cuando se cierra o suprime un portal de este tipo, al poco tiempo se produce un traslado a otra página web o servidor en

que se ofrece la misma mercancía. Este traslado casi inmediato se explica por la propia estructura de las TIC y la facilidad en la creación de los portales web.

Si bien, debemos matizar una cuestión relevante. En un mercado ilícito como el de la difusión de competiciones deportivas –significadamente, partidos de fútbol–, con un gran volumen de oferta y demanda, con multitud de portales web en que se anuncia el acceso, ilícitamente, a tales contenidos, la Sala 2.ª del TS llevó a cabo una importante puntualización en la STS 546/2022[11], de 2 de junio, al abordar la retransmisión no autorizada de partidos de fútbol, y consideró que no se trata de un delito contra la propiedad intelectual (art. 270.1.4 CP), sino de un delito relativo al mercado y a los consumidores (art. 286). El Alto Tribunal estimó que contravendría el principio de legalidad su calificación como delito contra la propiedad intelectual, ya que no tiene encaje en la noción de obra o prestación literaria, artística o científica.

Hemos de realizar una mención especial a lo expresado por Interpol (2024) a propósito de esta tipología de delitos. Resume en siete los principales métodos de piratería digital: (i) aplicaciones ilegales, (ii) robo de contenidos antes de su estreno, (iii) proveedores de servicios de alojamiento extraterritorial, (iv) extracción de secuencias o *stream ripping*, (v) servicios de almacenamiento en línea o *cyberlockers*, (vi) criptomonedas y (vii) tecnologías emergentes. En su análisis, destaca que esta modalidad de ciberdelincuencia afecta a los ingresos estatales y

11. STS 546/2022, de 2 de junio, ponente Excmo. Sr. D. Manuel Marchena Gómez, ECLI:ES:TS:2022:2315, en la que se expresa: "No es fácil fijar los límites del tipo cuando éste acoge elementos normativos que evocan la literatura, el arte o la ciencia. Precisamente por ello, las pautas exegéticas para delimitar ese alcance han de ser extremadamente prudentes para no desbordar los contornos de lo que cada vocablo permite abarcar. El fútbol, desde luego, no es literatura. Tampoco es ciencia. Es cierto que en un partido de fútbol –en general, en cualquier espectáculo deportivo– pueden sucederse lances de innegable valor estético, pero interpretar esos momentos o secuencias de perfección técnica como notas definitorias de un espectáculo artístico puede conducir a transgredir los límites del principio de tipicidad. Un partido de fútbol es un espectáculo deportivo, no artístico".

expone a los consumidores al riesgo de sufrir pérdidas financieras. Apunta que, además, la piratería digital comporta riesgos para la seguridad, tales como el robo de identidad, o bien, la exposición de menores a contenidos inapropiados. Sintetiza que nos hallamos ante un delito lucrativo, ya que los servicios de piratería obtienen sus ingresos por varios medios: (i) publicidad, (ii) donaciones de sus usuarios, (iii) servicios de suscripción, (iv) venta de datos de sus usuarios a terceros y (v) publicidad de afiliados. Además, Interpol advierte de que el dinero de los usuarios de estos servicios, al utilizarlos, "se desvía a cuentas bancarias piratas mediante complejas técnicas de blanqueo de capitales". En punto a la propia ciberseguridad de los usuarios de estas plataformas, Interpol señala que tales sitios web presentan riesgos, por contener *malware* y virus, que pueden ser usados para dañar los dispositivos informáticos o para sustraer información confidencial. Anota que tales *malwares* se pueden propagar por las redes corporativas o domésticas, comprometiendo la seguridad de la organización. Subraya que también pueden servir como trampolín para el robo de identidad, y que los consumidores se enfrentan a un riesgo jurídico, "al suscribirse a servidores *proxy* que podrían haberse usado para participar en ataques de denegación de servicio distribuida o de otro tipo en el pasado". Enumera otro conjunto de riesgos: (i) que los contenidos pirateados se empleen como trampa para el robo de datos personales, información bancaria u otro tipo de información confidencial; (ii) que los métodos de pago no seguros pueden dar lugar a fraudes con tarjetas de crédito o débito, u otras estafas financieras; (iii) que las actualizaciones de *software* –o su ausencia– para productos obtenidos de modo ilegal pueden provocar fallos de seguridad.

3.2.4 Blanqueo de dinero (arts. 301-304 CP)

En último lugar, debemos aludir a la viabilidad del blanqueo de dinero mediante las TIC. La propia configuración normativa de este tipo[12], su imparable expansionismo –legislativo e interpretativo– y las características del ciberespacio

12. Para un análisis en profundidad del delito de blanqueo de dinero, *vid.* González Uriel (2021).

propician que este nuevo ámbito de oportunidad criminal sea especialmente apto para la comisión de actos de ciberlavado de activos. En resumen, podemos describir el blanqueo de dinero como el proceso por el cual se pretende la reintroducción en el tráfico económico-financiero de curso legal de unos bienes que proceden de un delito. Por lo tanto, en su configuración más elemental, el blanqueo no pasa de ser –ni más, ni menos– el alejamiento de los bienes de su ilícita procedencia y su afloramiento con la finalidad de dotarles de una pátina de legitimidad, obtenida a través de diferentes negocios jurídicos. Nos hallamos ante un delito de referencia, que precisa de un delito fuente al que ir referido, pero que es autónomo, y que además se configura como un tipo pluriofensivo, que tutela la licitud de los bienes en el tráfico económico-financiero de curso legal y la Administración de Justicia. Además, coexiste con la normativa administrativa de prevención, la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, lo que puede provocar áreas de confluencia, solapamiento y confusión.

El anonimato que permiten las TIC es una cualidad que favorece que sean empleadas para llevar a cabo actos de lavado. Asimismo, también influye la ausencia de fronteras, la posibilidad de deslocalización y el empleo de artilugios técnicos para ocultar y modificar la IP. Debemos convenir en que, a través de las TIC, se mueve una gran cantidad de bienes con contenido económico. Es un ámbito abonado para la facilidad en las transferencias de bienes y para el desarrollo de una pluralidad de negocios jurídicos de contenido patrimonial. Pensemos que algunos ámbitos como los juegos de azar, las apuestas o los casinos *online* son entornos idóneos para camuflar ganancias procedentes de un delito. Además, nuevos elementos, como los juegos *online*, se han convertido en terrenos empleados para llevar a cabo la legitimación de fondos. En este sentido, debemos subrayar que las TIC se pueden emplear tanto para lavar el dinero obtenido en el entorno *offline* como para legitimar los propios fondos dimanantes de ciberdelitos –*v. gr.*, las cantidades obtenidas mediante ciberestafas o los pagos de rescates para que cesen ataques de *ransomware*–.

Precisamente, hemos de conectar el fenómeno del lavado de bienes con las organizaciones criminales, dado que constituye uno de sus principales ámbitos operativos. Se ha observado que las organizaciones criminales tradicionales están llevando a cabo una traslación parcial al ciberespacio para asegurar sus montos de procedencia delictiva, como se ha apreciado en alguna operación policial[13], por lo que están diversificando los cauces a través de los cuales reciclan los activos delictivos, y la legitimación de fondos se lleva a cabo tanto por los canales tradicionales como a través de las TIC. En este sentido, Interpol señala que la delincuencia organizada utiliza las ganancias obtenidas para otras actividades ilegales, como el juego ilegal en línea, la explotación sexual en línea, el tráfico de drogas, la trata de personas, el tráfico de armas o el blanqueo de dinero. Además, se ha constatado que otras organizaciones criminales han surgido en el propio ciberespacio y su actividad delictiva se desarrolla en él: podemos aquí hacer alusión a las organizaciones internacionales dedicadas a la realización de ataques de *ransomware* por todo el mundo.

Pues bien, a la hora de favorecer el anonimato, romper la trazabilidad de los fondos, diluir su rastro, ocultar su procedencia delictiva y llevar a cabo su afloramiento ulterior, en la actualidad, juegan un papel destacado las criptomonedas (Casals Fernández, 2022). En el art. 3.1.5) del Reglamento (UE) 2023/1114, del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937, se definen los criptoactivos como "una representación digital de un valor o de un derecho que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro distribuido o una tecnología similar". Podemos apostillar que los criptoactivos no constituyen dinero de curso legal, no están sometidos a una autoridad central, ni presentan una regulación, un tipo de cambio ni una normativa oficial. De hecho, el punto de conexión entre el blanqueo

13. *Vid.* la noticia "La mafia italiana se pasa al cibercrimen desde Tenerife". *Diario El País* el 25 de septiembre de 2021. https://elpais.com/tecnologia/transformacion-digital/2021-09-25/la-mafia-italiana-se-pasa-al-cibercrimen-desde-tenerife.html

de dinero y los criptoactivos viene dado por su capitalización, su monetarización y conversión en dinero FIAT. En este aspecto juegan un destacado papel los *exchangers*, los servicios de conversión de criptoactivos, por lo que resulta esencial que cumplan con las obligaciones de información y registro impuestas por la normativa europea, en orden a prevenir operativas de lavado de activos, por lo que se erigen en sujetos especialmente obligados al cumplimiento de una serie de obligaciones y deberes. La adquisición de criptoactivos por las organizaciones criminales y sujetos que pretendan blanquear se basa en el anonimato tendencial que presentan, toda vez que, en la tecnología *blockchain* que emplean, lo que consta es la existencia de las transacciones, ligadas a monederos –*wallets*–, pero no a personas físicas individualmente identificadas. Además, existen distintas aplicaciones y servidores que funcionan como "mezcladores" –*mixers*–, que permiten romper la trazabilidad de las operaciones y mezclar criptomonedas procedentes de diversos monederos, provocando que se dificulte –o impida– el rastreo de la procedencia de tales activos. Así las cosas, las criptomonedas se emplean como refugio de dinero sucio obtenido en el entorno *offline*, y como lugar para asegurar las ilícitas ganancias derivadas de los ciberdelitos cometidos en Red. De este modo, mediante la sucesión de transferencias, de negocios jurídicos y de actos llevados a cabo en línea es dable desligar los bienes delictivos de su fuente, alejarlos y darles una pátina de legalidad.

Con todo, y pese a las advertencias que realizamos de la posibilidad del empleo de las TIC para llevar a cabo operativas de blanqueo de capitales, al igual que hemos reiterado en otros lugares (González Uriel, 2023), debemos patrocinar una interpretación sumamente restrictiva de la aplicación del delito de blanqueo, para contrarrestar algunos excesos intelectivos que se aprecian en materia concursal y en la comprensión de determinadas figuras, fundamentalmente, en el blanqueo imprudente. Por ende, sobre todo en los casos de ciberestafas, ha de abogarse por mantener el título de imputación a los coacusados, y por efectuar una valoración global del hecho que atienda a la aplicación de las reglas del concurso aparente de normas del art. 8 CP. De ahí que no todo delito del que derive una ganancia patrimonial vaya a implicar, *per se*, la existencia de un concurso real con el delito de blanqueo –porque exista una adquisición, pose-

sión o utilización de tales bienes–, sino que habrá de estarse al caso concreto, y habrán de tomarse en consideración diferentes criterios de restricción, como los actos neutros, el riesgo permitido, la lesión o puesta en peligro del bien jurídico tutelado, el principio de insignificancia –desechando conductas de bagatela– o, jurisprudencialmente, la exigencia de finalidad en todas las modalidades de conducta blanqueadoras –criterio este que no comparte un relevante sector doctrinal–. De especial relevancia es la figura de las mulas en las ciberestafas, cuya intervención ha sido calificada, en no pocas ocasiones, como constitutiva de un delito de blanqueo imprudente, en lugar de como una cooperación necesaria en la estafa. Hemos de eludir consideraciones apriorísticas y hemos de rechazar la traslación de deberes policiales –o parapoliciales– a los particulares, toda vez que el tipo de blanqueo no los exige, y se pueden producir situaciones de paralización de la economía, con la instauración de una suerte de desconfianza generalizada. Si bien, somos conscientes de que las TIC constituyen un terreno abonado para que las organizaciones criminales laven sus fondos delictivos, por lo que abogamos por la especialización en la materia de todos los operadores jurídicos y de las Fuerzas y Cuerpos de Seguridad del Estado (FFCSE) concernidos, ante la gran magnitud económica que pueden conllevar tales operativas de lavado y dada la complejidad técnica de estas cuestiones.

4 Algunas dificultades procesales en la detección e investigación de los ciberdelitos económicos

En este último apartado seremos deliberadamente escuetos y esquemáticos, toda vez que pretendemos dar una visión global de la problemática. En primer lugar, conviene destacar que nos hallamos ante ciberdelitos de difícil detección, puesto que, en ocasiones, la propia víctima no es consciente de su comisión –recordemos las ciberestafas de montos escasos–. Además, la propia arquitectura del ciberespacio propicia que surjan dificultades a la hora de determinar qué jurisdicción nacional está en condiciones de perseguir el delito: como ya advertimos, se trata de una delincuencia globalizada, transnacional, y que, en múltiples

ocasiones, los ciberdelincuentes emplean artificios técnicos para camuflar y deslocalizar su dirección IP, como *proxy* o VPN. Por lo tanto, en ocasiones será necesario acudir a la Ley 26/2015, de 7 de julio, por la que se regula el estatuto del miembro nacional de España en Eurojust, los conflictos de jurisdicción, las redes judiciales de cooperación internacional y el personal dependiente del Ministerio de Justicia en el Exterior. A su vez, puede generar problemas de determinación del lugar de comisión del delito cuando la acción se lleva a cabo en un país y los resultados se producen en otro u otros. En este mismo sentido, y una vez que se ha determinado la jurisdicción de los tribunales españoles, puede resultar complejo concretar qué órgano judicial es objetivamente competente, en supuestos en los que se diluyen entre diferentes partidos judiciales elementos de un tipo delictivo e, incluso, ante la posibilidad de que conozca de los hechos la Sala de lo Penal de la Audiencia Nacional, *ex* art. 65 LOPJ.

Salvados los escollos de la jurisdicción y de la competencia –ya de por sí problemáticos–, el siguiente obstáculo viene representado por la determinación de la concreta autoría. Podemos hallarnos ante supuestos de empleo de redes WiFi públicas, utilizadas por una pluralidad indeterminada de personas. En otros casos, los ciberdelincuentes pueden usurpar la clave y contraseñas de otras personas para cometer ciberdelitos. Además, y en los supuestos en que la dirección IP arroje un concreto domicilio, podrían surgir dificultades a la hora de concretar la persona que haya cometido el delito, cuando sean varios los moradores del inmueble. Otro aspecto que complica las investigaciones viene representado por aquellos casos en los que quepa el ciberdelito leve –significadamente, estafas de menos de 400 euros–, lo que veda la posibilidad de que se efectúe una instrucción judicial, con lo que se limita la potencialidad investigadora. A ello hemos de agregar que, en muchas ocasiones, y bajo la fachada de delitos leves aislados, nos encontramos ante auténticas organizaciones criminales que cometen una multitud de tales delitos. Si bien, y como lamentamos, esa desconexión en las investigaciones policiales y en la tramitación judicial de cada delito leve lleva a que no seamos conscientes de la presencia de auténticas industrias del cibercrimen, y demos tratamientos aislados y singulares a supuestos que, en puridad, forman parte de un *contínuum*.

Asimismo, en ocasiones, una misma víctima de un ciberdelito aparece como victimario en una pluralidad de cibercrímenes, en diferentes partidos judiciales porque, en su proceso de victimización, facilitó sus datos personales –fotografía y DNI– a los ciberdelincuentes, y dichos datos se emplean en una multitud de ilícitos posteriores. Con ello se perpetúan situaciones de victimización y se irrogan perjuicios adicionales, siquiera, a los efectos de contestar a cada citación judicial a un juicio por delito leve como investigado.

En punto a la ciberdelincuencia económica, debemos consignar que nos hallamos ante modalidades delictivas de difícil investigación, debido a la sofisticación técnica de alguna de las operativas empleadas, a los artificios tecnológicos utilizados, a la propia volatilidad de los elementos de prueba en el entorno *online*, a la complicación para seguir el rastro del cibercrimen y para determinar con precisión el alcance del hecho, sus autores y partícipes. Todo ello se agrava si los hechos se vehiculan a través de la *dark web*. Somos conscientes de que resulta complejo obtener la totalidad de las fuentes de prueba. En ocasiones surgen dudas a la hora de delimitar las diligencias de investigación a practicar. Pensemos en el fraude del CEO, en que se desconoce qué ha sucedido con los montos ilícitamente transferidos y no se tiene ningún indicio de quién ha cometido el hecho. Aquí juegan un papel destacado las periciales informáticas y la realización de complejas y exhaustivas investigaciones patrimoniales. A su vez, y cuando existen criptomonedas, aparecen dificultades a la hora de efectuar su trazabilidad –dado su anonimato tendencial– o, incluso, cuando se efectúa una entrada y registro en un domicilio y se obtiene un *pen drive* que contiene un *wallet* con criptomonedas, ante la ausencia de una regulación procesal específica, aparecen varias posibilidades de actuación procesal: (i) convertir la criptomoneda en dinero FIAT e ingresar la cantidad aprehendida en la cuenta de depósitos y consignaciones del juzgado; (ii) crear un *wallet* en el propio juzgado y transferir la criptomoneda; (iii) mantener el propio *wallet* del sujeto investigado, bajo la custodia del LAJ, y cambiar su clave de acceso. No se trata de una cuestión baladí, puesto que puede afectar a la responsabilidad civil en casos en que, al enjuiciarse los hechos, se produzca una variación sustancial del valor de la criptomoneda, entre la fecha de la aprehensión y la del fallo. A su vez, si se opta por mante-

ner el *wallet* del investigado, podrían acceder a él otros sujetos implicados en la trama a través de la "frase semilla", o frase de recuperación, que funciona como una llave maestra para acceder a las criptomonedas y ofrece una red de seguridad en caso de pérdida, robo o fallo de funcionamiento del dispositivo.

Puesto que hemos mencionado en repetidas ocasiones que nos hallamos ante una fenomenología delictiva transnacional, va a tener una gran relevancia el empleo de instrumentos de cooperación judicial internacional. De este modo, no solo van a existir retrasos y dilaciones en la obtención de fuentes de prueba en el extranjero, sino también en cuanto a su conservación y a su transmisión al procedimiento judicial español, por lo que hemos de tomar en consideración tales aspectos. En este sentido, y frente a la excesiva burocratización y ralentización procesales que acarrean las comisiones rogatorias internacionales, puesto que constituyen un cauce de cooperación entre autoridades gubernativas, basadas en la existencia de tratado, de ley, o en el principio de reciprocidad, en el ámbito de la UE se agiliza la cooperación a través de las órdenes europeas de investigación (OEI). Dicho instrumento reduce los trámites, puesto que la comunicación se realiza, directamente, entre autoridades judiciales. Pues bien, en el ámbito de la lucha contra la ciberdelincuencia económica podemos hacer alusión a una serie de relevantes diligencias que se contienen en los arts. 198 y ss. de la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea: (i) peticiones de información sobre cuentas bancarias y financieras; (ii) peticiones de información sobre operaciones bancarias y financieras; (iii) intervenciones de telecomunicaciones; (iv) identificación de titulares de IP; y (v) adopción de diferentes medidas cautelares reales, como aseguramientos de bienes o embargos.

Estos son solo algunos de los aspectos procesales que surgen en la fase de instrucción –si es que la hay, lo que no se da en los delitos leves–, y que ponen de manifiesto la complejidad en la detección, la investigación y el enjuiciamiento de la ciberdelincuencia económica. Nos hallamos ante un fenómeno delictivo novedoso, en auge y en continua evolución en cuanto a sus operativas y dinámicas comisivas, pero no contamos con la totalidad de herramientas procesales para hacerle frente,

por lo que, y aunque suene a tópico, vamos un paso por detrás de los ciberdelincuentes. Se trata de un ámbito dinámico, técnico, que permite el empleo de artilugios tecnológicos para eludir las labores de prevención y detección del delito. Por tal motivo, debemos ser conscientes de la ardua tarea que conlleva la investigación de algunos supuestos complejos de ciberdelitos económicos, cometidos por organizaciones criminales con ramificaciones internacionales y en los que se refugien los fondos en criptomonedas y se causen multitud de perjudicados en diferentes Estados.

No obstante, no podemos obviar que contamos con importantes instrumentos para la investigación de estas tipologías delictivas. Debemos destacar la reforma de la Ley de Enjuiciamiento Criminal (LCERIM) operada por la LO 13/2015, en la que se reconoció la insuficiencia de la regulación vigente hasta ese momento[14], y, sobre todo, la incorporación de una serie de disposiciones relativas a la interceptación de las comunicaciones telefónicas y telemáticas, a la captación

14. En el apartado IV del Preámbulo de la LO 13/2015 se expresa: "La Ley de Enjuiciamiento Criminal no ha podido sustraerse al paso del tiempo. Renovadas formas de delincuencia ligadas al uso de las nuevas tecnologías han puesto de manifiesto la insuficiencia de un cuadro normativo concebido para tiempos bien distintos. Los flujos de información generados por los sistemas de comunicación telemática advierten de las posibilidades que se hallan al alcance del delincuente, pero también proporcionan poderosas herramientas de investigación a los poderes públicos. Surge así la necesidad de encontrar un delicado equilibrio entre la capacidad del Estado para hacer frente a una fenomenología criminal de nuevo cuño y el espacio de exclusión que nuestro sistema constitucional garantiza a cada ciudadano frente a terceros. Por muy meritorio que haya sido el esfuerzo de jueces y tribunales para definir los límites del Estado en la investigación del delito, el abandono a la creación jurisprudencial de lo que ha de ser objeto de regulación legislativa ha propiciado un déficit en la calidad democrática de nuestro sistema procesal, carencia que tanto la dogmática como instancias supranacionales han recordado. Recientemente, el Tribunal Constitucional ha apuntado el carácter inaplazable de una regulación que aborde las intromisiones en la privacidad del investigado en un proceso penal. Hoy por hoy, carecen de cobertura y su subsanación no puede obtenerse acudiendo a un voluntarista expediente de integración analógica que desborda los límites de lo constitucionalmente aceptable. Solo así se podrá evitar la incidencia negativa que el actual estado de cosas está proyectando en relación con algunos de los derechos constitucionales que pueden ser objeto de limitación en el proceso penal".

y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, a la utilización de dispositivos técnicos de seguimiento, a la localización y captación de la imagen, al registro de dispositivos de almacenamiento masivo de información y a los registros remotos sobre equipos informáticos. Estas medidas de investigación se regulan en los arts. 588 bis y ss. LECRIM, constituyen un poderoso arsenal de diligencias que han de ser acordadas con prudencia, en atención a la injerencia en derechos fundamentales que conllevan. Debemos recordar los principios que han de ser tomados en consideración a la hora de interesar y de adoptar tales medidas: especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad. Del mismo modo, la citada LO 13/2015 amplió las potencialidades del agente encubierto, incorporando en el art. 282 bis LECRIM la figura del agente encubierto informático[15].

Así las cosas, aunque hemos asumido las insuficiencias, las áreas susceptibles de mejora y algunas debilidades con las que contamos a la hora de perseguir los ciberdelitos económicos, forzoso es reconocer que la normativa procesal penal española contiene poderosas herramientas de lucha contra estas tipologías delictivas. Frente a ellas no queda sino la especialización de jueces, magistrados, fiscales y miembros de FFCCSE, la llamada a la colaboración entre las autoridades judiciales nacionales, la conformación de equipos conjuntos de investigación, la lealtad interinstitucional en el desarrollo de las investigaciones y, sobre todo, la formación continua, la actualización de contenidos y el reciclaje en una fenomenología delictiva que ha llegado para quedarse y frente a la que debemos estar preparados.

15. Art. 282 bis.6 LECRIM: "6. El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a.

El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos".

5 Conclusiones

1.ª El ciberespacio constituye un nuevo entorno de oportunidad criminal, en el que el ámbito de victimización viene determinado por la propia víctima que es quien, con su conducta, delimita qué concretos bienes jurídicos suyos pueden ser lesionados o puestos en peligro. Por lo tanto, y sin que ello implique responsabilizar a la víctima de su proceso de victimización, hemos de partir del hecho de que la incorporación de los bienes jurídicos al ciberespacio se lleva a cabo por la propia víctima. El ciberespacio puede provocar variaciones en el comportamiento de sus usuarios, y que lleven a cabo actos de riesgo que no verificarían en el entorno *offline*, dado que, en ocasiones, se produce la influencia del "efecto desinhibitorio *online*".

2.ª Los ciberdelitos constituyen la tipología delictiva que más aumenta, según los últimos datos oficiales sobre criminalidad en España. Ello se debe a que buena parte de los actos y actividades cotidianas de las personas se han trasladado, parcial o completamente, al ciberespacio. De este modo, se ha trasladado a las TIC la mayor parte de los ámbitos de desarrollo de las personas: social, económico, comercial, relacional, laboral, cultural, educativo... Y ello propicia que dicha incorporación vaya acompañada de un auge de los ciberdelitos, lo que se ve favorecido por las propias condiciones y circunstancias del ciberespacio como medio de comisión de actividades ilícitas, dado que no existen barreras, ni fronteras, ni instituciones centralizadas de control, y ante el rediseño de las relaciones entre las variables espacio y tiempo, lo que propicia que con un solo acto se llegue a una multitud de potenciales víctimas.

3.ª Dentro de los ciberdelitos, los de contenido económico resultan preponderantes, tanto cualitativa como cuantitativamente. Los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas informáticos, el desconocimiento de los sujetos y las potencialidades que brinda el ciberespacio

para cometer delitos con una finalidad lucrativa. El principal ciberdelito que se comete es el fraude –estafa–. Existe una pluralidad de modalidades comisivas de dicho delito, algunas más sofisticadas y elaboradas, y otras más burdas y zafias. En todo caso, todas ellas persiguen la obtención de un lucro por fines espurios, empleando para ello engaños y ardides, o bien, manipulaciones informáticas, técnicas o artificios semejantes. No obstante, ante la rentabilidad de estos comportamientos, se ha observado una proliferación en los ciberdelitos de corte económico, y también se han incrementado los delitos de daños informáticos, los delitos contra los derechos de propiedad intelectual e industrial, así como los actos de blanqueo de los fondos delictivamente obtenidos en el ámbito de las TIC, por lo que podríamos atender a nuevas modalidades de ciberblanqueo.

4.ª Nos hallamos ante delitos de difícil persecución, ante la complejidad para determinar las conductas punibles, su alcance y sus resultados, resultando complicado establecer la autoría y la participación en estos comportamientos. En estas tipologías delictivas va a ser muy importante obtener las fuentes de prueba con celeridad, ante su volatilidad. Es preciso efectuar rigurosas investigaciones patrimoniales en las que se pueda verificar la trazabilidad de los fondos. Otra dificultad viene dada por el carácter tendencialmente internacional de estos delitos, por la implicación de organizaciones criminales y por las dudas en cuanto a las diligencias de investigación a practicar. Es preciso que se optimicen los cauces de cooperación judicial internacional, que se constituyan equipos conjuntos de investigación y que se aclaren los criterios de atribución competencial en cada uno de los delitos investigados.

5.ª Se trata de una serie de delitos en continua evolución, dinámicos, cambiantes, y donde surgen elementos distorsionadores, como las criptomonedas o la inteligencia artificial, que exigirán pronto nuevas respuestas específicas, ante la insuficiencia de los medios actuales con algunas de sus aplicaciones prácticas. Ante los avances técnicos, es preciso que la normativa se acompase y adapte, que se brinden a los juzgados y tribunales las herramientas necesarias para la persecu-

ción de estas modalidades delictivas y que esa actualización se produzca en unos plazos temporales razonables. No obstante, hemos de convenir en que la reforma de la LECRIM del año 2015 cristalizó una serie de criterios jurisprudenciales y dotó a los investigadores de una serie de potentes medidas de lucha contra los ciberdelitos, incardinadas en los arts. 588 bis y ss. LECRIM. Dichas medidas posibilitan notables mejoras en la investigación de los delitos, si bien, y dado su elevado nivel de injerencia en los derechos fundamentales, han de ser solicitadas y adoptadas con mesura, prudencia y cautela y, en todo caso, respetando los principios de especialidad, necesidad, idoneidad, excepcionalidad y proporcionalidad. Por ello, debemos subrayar que, en la actualidad, la normativa procesal penal española permite realizar investigaciones judiciales rigurosas, completas, profundas y con salvaguarda de los derechos fundamentales, aunque, inevitablemente, los medios con los que contamos hoy puede que sean insuficientes para las necesidades del mañana, por lo que es necesario que el legislador adopte una postura proactiva, sensible a las necesidades prácticas, de carácter técnico y en cuya elaboración participen equipos multidisciplinares, que aborden la problemática de la ciberdelincuencia desde una perspectiva integral.

Referencias bibliográficas

Abadías Selma, A. (2023). La nueva regulación del delito de uso fraudulento de medios de pago distintos del efectivo al albur de la reforma de 22 de diciembre de 2022: Un análisis del art. 249.1 b) y 249.2 b) del CP. *Estudios de Deusto: Revista de Derecho Público*, *71*(1), 15-82.

Agustina Sanllehí, J. R. (2014). Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización. *Cuadernos de Política Criminal*, *114*, 143-178.

Alonso Cebrián, J. M. y Velasco Núñez, E. (2024). Delitos por/con inteligencia artificial: presente y futuro. *Ciberderecho*, *84*.

Bustos Rubio, M. (2023). La reforma de la ciberestafa y la incorporación de los medios de pago digitales en el Código Penal. *IDP: Revista de Internet, Derecho y Política*, *38*.

Casals Fernández, A. (2022). Las criptomonedas frente al delito de blanqueo de capitales y la complejidad de la prueba pericial en el ámbito ciberdelincuente. *Anuario de Derecho Penal y Ciencias Penales*, *75(1)*, 421-446.

Cohen, L. y Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44(4)*, 588-608.

González Uriel, D. (2021). *Aspectos básicos del delito de blanqueo de dinero*. Comares.

González Uriel, D. (2022). Delito de daños (arts. 263-267 CP). En A. Abadías Selma y M. Bustos Rubio (coords.), *Temas prácticos para el estudio del derecho penal económico*. Colex.

González Uriel, D. (2023). Cibermulas y criptomulas: a medio camino entre la estafa y el blanqueo. *Revista Aranzadi Doctrinal*, *6*.

INCIBE (5 de septiembre de 2019). Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse. https://www.incibe.es/empresas/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse

INTERPOL (2024). *Piratería digital*. https://www.interpol.int/es/Delitos/Productos-ilegales/Compre-de-forma-segura/Pirateria-digital.

Jiménez, I. (12 de febrero de 2024). La era de las estafas inteligentes: Cómo la IA está cambiando el juego del engaño. *Blog de Innovación Legal y Nuevas Tecnologías*. https://www.abogacia.es/publicaciones/blogs/blog-de-innovacion-legal/la-era-de-las-estafas-inteligentes-como-la-ia-esta-cambiando-el-juego-del-engano/

Kemp, S. (2021). *Cibercriminalidad y ciberfraude durante una pandemia: cifra negra y tendencias para el futuro*. *Minipapers PostC*. https://postc.umh.es/minipapers/cibercriminalidad-y-

ciberfraude-durante-una-pandemia-cifra-negra-y-tendencias-para-el-futuro/

López Gorostidi, J. (2021). Los valores tradicionales como bienes jurídicos protegidos también en el ciberespacio: a propósito del confinamiento provocado por la crisis sanitaria del COVID-19. *Revista Penal*, *47*, 126-152.

Ministerio del Interior. Gobierno de España. (2023). *Informe sobre la cibercriminalidad en España 2023*. https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Informe-Cibercriminalidad_2023.pdf.

Miró Llinares, F. (2012). *El Cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons.

Montiel Juan, I. (2016). Cibercriminalidad social juvenil: la cifra negra. *IDP: Revista de Internet, Derecho y Política*, *22*.

Morillas Fernández, D. L. (2023). Implicaciones de la inteligencia artificial en el ámbito del Derecho Penal. En J. Miguel Peris Riera y A. Massaro (coords.), *Derecho Penal, Inteligencia Artificial y Neurociencias*. Roma: Tre-Press.

UNODC (2019). *Causas, razones, y justificaciones percibidas para los delitos de derecho de autor y de marca propiciados por medios cibernéticos*. https://www.unodc.org/e4j/es/cybercrime/module-11/key-issues/causes-for-cyber-enabled-copyright-and-trademark-offences.html