La lucha contra el cibercrimen y las últimas reformas penales en España e Italia: luces y sombras

The fight against cybercrime and the most recent criminal law reforms in Spain and Italy: lights and shadows

CHIARA CRESCIOLI

Abogada

Abogada y Doctora en Derecho Penal por las Universidades de Verona (Italia) y Bayreuth (Alemania)

cresciolichiara@gmail.com

https://orcid.org/0009-0002-5452-4005

Resumen: La necesidad de la regulación de la ciberdelincuencia ha llamado la atención de las instituciones supranacionales como la Unión Europea y el Consejo de Europa. Por lo tanto, los legisladores nacionales de los diferentes países de la UE, como España e Italia, han tenido que modificar varias veces sus propios códigos penales para cumplir con las obligaciones de los convenios internacionales, las Decisiones Marco y las Directivas relativas a los ataques informáticos y al cibercrimen. Sin embargo, las medidas adoptadas por el legislador europeo y, por consiguiente, por los legisladores nacionales que regulan los ciberdelitos en sus Códigos penales (como el español y el italiano), todavía no se ajustan completamente a las características de la criminalidad cibernética actual, así como al fenómeno delictivo denominado Cybercrime-as-a-Service. En el presente trabajo se analiza, en perspectiva comparada entre España e Italia, la evolución de la legislación penal contra el cibercrimen y su aplicación jurisprudencial, con especial referencia a las estafas informáticas y al empleo ilícito de los medios de pagos distintos del efectivo, intentando ofrecer

Recepción: 10/04/2024 Aceptación: 01/11/2024

Cómo citar este trabajo: CRESCIOLI, Chiara, "La lucha contra el cibercrimen y las últimas reformas penales en España e Italia: luces y sombras", *Revista de Estudios Jurídicos y Criminológicos*, n.º 10, Universidad de Cádiz, 2024, pp. 403-427, DOI: https://doi.org/10.25267/REJUCRIM.2024.i10.12

hipotéticas soluciones para mejorar las normas penales en el mencionado ámbito de criminalidad, que afecta cada día a más usuarios y entidades públicas.

Abstract: *The need to regulate cybercrime has attracted the attention of supranational institutions such as the European Union and the Council of Europe. As a result, the national legislators of several EU countries, such as Spain and Italy, have amended their criminal codes on several occasions to comply with the obligations of international conventions, framework decisions, and directives on cyber-attacks and cybercrime. However, the measures taken by the European legislator and, consequently, the national legislators that regulate cybercrime in their criminal codes (such as those of Spain and Italy), are not yet entirely in line with the characteristics of current cybercrime and the criminal phenomenon known as Cybercrime-as-a-Service. This paper analyses the evolution of criminal legislation against cybercrime and its jurisprudential application from a comparative perspective between Spain and Italy, with particular reference to computer fraud and the illicit use of means of payment, trying to offer hypothetical solutions to improve the legal framework against cybercrime, which affects more and more users and public entities every day.*

Palabras clave: ciberdelincuencia, reformas penales, fraude informático, medios de pago.

Keywords*: cybercrime, criminal law reforms, computer fraud, means of payment.*

1. INTRODUCCIÓN: LA CIBERDELINCUENCIA Y SU REGULACIÓN SUPRANACIONAL

Hoy en día el uso masivo de dispositivos tecnológicos e Internet ofrecen numerosas ventajas a los ciudadanos y, por consiguiente, a la sociedad. Los nuevos medios de pago distintos del efectivo nos permiten realizar transacciones comerciales en cualquier parte del mundo y en un corto período de tiempo, pudiendo además rastrear en su caso el origen del dinero y país de procedencia.

No obstante, al mismo tiempo, las nuevas tecnologías son sumamente vulnerables a los ciberataques, que se están perfeccionando cada vez más. En el presente trabajo sólo se analizarán los dirigidos contra el patrimonio ajeno, que provocan pérdidas económicas significativas y constituyen una gran amenaza para la economía digital. Según las estadísticas más recientes, el 90,5% de las denuncias que se presentan en el

ámbito de la cibercriminalidad en España son por fraude informático[1]. Este dato por sí solo es suficiente para comprender la necesidad de adoptar medidas de Derecho penal eficaces y eficientes para proteger los medios de pago distintos del efectivo.

Existen muchos tipos de ciberataques. Uno de los más conocidos es el *phishing*: el ciberdelincuente utiliza el lenguaje, el formato y las imágenes de las entidades bancarias o financieras para enviar correos electrónicos o SMS engañosos en los que se solicitan los datos personales de las víctimas alegando diferentes motivos. Así, el ciberdelincuente utiliza sin autorización del usuario su la contraseña, realizando una transferencia no autorizada de dinero, en perjuicio del mismo[2]. Aunque conocido, aún tiene éxito, porque todavía no hay un sistema informático realmente eficaz que sea capaz de identificar con antelación y sin errores todos los mensajes engañosos[3].

Para enviar mensajes engañosos, los ciberdelincuentes utilizan también la técnica llamada *spoofing*, que permite suplantar la identidad de los remitentes ocultando el correo o el número de teléfono real y sustituyéndolo por el de un remitente de confianza[4]. Además, la inteligencia artificial permite la creación masiva de mensajes fraudulentos personalizados para la víctima, por ejemplo, cambiando el nombre del remitente mediante *spoofing*, de manera que la víctima crea que se trate de un remitente conocido, y enviando un mensaje falso con el texto muy parecido a los que la víctima realmente recibe del contacto en cuestión[5].

Existen muchas variantes del *phishing*, por ejemplo el *pharming*. En este caso el ciberdelincuente se apodera de la contraseña de su víctima a través de una página web engañosa que replica casi exactamente la página original de las entidades bancarias o financieras[6]. En el *phishing man-in-the-middle*, se produce una combinación de ataque directo e indirecto: el *phisher* intercepta los mensajes dirigidos a la página

---

1 Ministerio del Interior, *Informe sobre la cibercriminalidad en España 2023*, p. 18, (https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Informe-Cibercriminalidad_2023.pdf&ved=2ahUKEwic2uTzu_WJAxXA_rsIHRTLNxYQFnoECB8QAQ&usg=AOvVaw0_RJ5qH9zZAJY6Unw-EpU0, consulta: 29/11/2024).

2 GHAZI-TEHRANI, A./ PONTELL, H., "Phishing Evolves: Analyzing the Enduring Cybercrime", *Victims & Offenders*, vol. 16, n. 3, 2021, p. 319; RUTHERFORD, R., "The changing face of phishing", *Computer Fraud & Security*, n. 11, 2018, p. 6.

3 ALMOMANI, A./GUPTA, B.B./ATAWNEH, A./MEULENBERG, A./ALMOMANI, E., "A Survey of Phishing Email Filtering Techniques", *IEEE Communications Surveys & Tutorials*, Vol. 15, n. 4, 2013, p. 2070.

4 RAMESH BABU, P./LALITHA BHASKARI, D./SATYANARAYANA, CH., "A Comprehensive Analysis of Spoofing", *International Journal of Advanced Computer Science and Applications*, vol. 1, n. 6, 2010, p. 158.

5 CADWELL, M./ANDREWS, J.T.A./TANAY, T./GRIFFIN, L.D., "AI-enabled future crime", *Crime Science*, vol. 9, n. 14, 2020, p. 8.

6 AZEEZ, N.A./OLADELE, S.S./OLOGE, O., "Identification of Pharming in Communication Networks using Ensemble Learning", *Nigerian Journal of Technological Development*, vol. 19, n. 2, 2022, p. 172.

web elegida por cualquier usuario, guarda las informaciones que le interesan, luego retransmite los mensajes a la página web elegida por la víctima y, por último, reenvía las respuestas a la víctima[7]. En cambio, el *smishing* y el *vishing* son variantes del *phishing* cometidas a través de SMS o teléfono[8]. Los ciberdelincuentes también pueden utilizar el *spamming*, es decir, el envío no consentido de mensajes publicitarios por correo electrónico a una multitud de desconocidos: el falso mensaje publicitario puede contener un enlace que en realidad contiene un *malware* y que permite al cibercriminal de apoderarse de manera ilícita de los datos personales del usuario[9]. También se utilizan virus informáticos que capturan las pulsaciones del teclado en las páginas web como el *keylogger* o el *screenlogger*.

Tras la estafa, los ataques pueden ser también destructivos, provocando p. ej. denegación de servicios o bloqueo de datos. El más peligroso es el *ransomware*: en este caso, el cibercriminal bloquea el acceso al sistema informático o a los datos y amenaza en convertir el bloqueo en borrado, si en un plazo corto de tiempo no se paga un rescate[10].

Por lo tanto, el *phishing* y sus variantes consisten esencialmente en el "robo de datos" reservados por el usuario para un uso posterior no autorizado y perjudicial. La sustracción y la utilización de usuarios y contraseñas de acceso al sistema bancario o a otras instituciones suele ir seguida de la realización de un fraude informático y, por consiguiente, del perjuicio patrimonial de la víctima. Sin embargo, en los últimos años se ha consolidado el fenómeno delictivo denominado «*Cybercrime-as-a-Service*». Este consiste básicamente en el comercio, tanto en la web como en la "web profunda", de diferentes tipos de servicio y "paquetes de herramientas" para llevar a cabo ciberataques, que incluyen la creación de programas informáticos diseñados para cometer delitos y la venta de datos personales como usuarios y contraseñas o informaciones necesarias para realizar los ciberataques[11].

Hackers expertos, en lugar de llevar a cabo ellos mismos los ciberataques, ponen sus capacidades a disposición de terceros a título oneroso, a través de la creación y distribución de *malware* o *phishing kits* que otros pueden utilizar para lanzar ciberataques[12]. La oferta de servicios es muy amplia: el usuario puede limitarse a comprar números de tarjetas de crédito o identidades digitales ajenas para la

---

7 CAJANI, F./COSTABILE, G./MAZZARACO, G., *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*, Giuffré, Milano, 1° ed., 2008, p. 28 s.

8 *Ibid.*

9 ANARTE BORRALLO, E., "Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho Penal en la sociedad de la información", *Derecho y conocimiento. Anuario jurídico sobre la sociedad de la información*, 2001, vol. 1, p. 199.

10 DELGADO-MOHATAR, O./SIERRA-CÁMARA, J.M./ANGUIANO, E., "Blockchain-based semi-autonomous ransomware", *Future Generation Computer System*, vol. 112, 2020, p. 590; RYAN, M., *Ransomware Revolution: The Rise of a Prodigious Cyber Threat*, Spinger, Cham, 1° ed., 2021, p. 2.

11 MANKY, D., "Cybercrime as a service: a very modern business", *Computer Fraud & Security*, n. 6, 2013, p. 9.

12 GANGULI, P., "The Rise of Cybercrime-as-a-Service: Implications and Countermeasures", *International Journal for Multidisciplinary Research*, vol. 6, n. 5, 2024, p. 3.

utilización fraudulenta de medios de pago distintos del efectivo o puede adquirir una red *bootnet* completa, es decir, una red informática formada por dispositivos infectados con un *malware* especializado llamado *bot*, que puede tener diversas funciones, como el envío masivo de correos spam o la sobrecarga del servidor[13].

También forma parte de este fenómeno el *Obfuscation-as-a-Service*: en este caso, los ciberdelincuentes ofrecen a los usuarios, previo pago, la posibilidad de ocultar la función perjudicial del programa, para que el sistema antivirus no detecte el *malware*[14].El *Cybercrime-as-a-Service* permite obtener grandes ganancias con menos riesgos que los autores del fraude. En Italia recientemente ha causado un gran revuelo el caso de un joven experto informático de 24 años, arrestado en octubre tras años de investigación y acusado de haber ganado ilícitamente más de 7 millones de euro en bitcoin a través de la venta de credenciales y contraseñas obtenidas ilegalmente. En particular, el hacker accedió al sistema de información de la compañía de telecomunicaciones *Telecom Italia Mobile*, adquiriendo los datos de millones de usuarios y poniéndolos a la venta en la *dark web*[15].

El *Cybercrime-as-a-Service* ha cambiado significativamente la delincuencia informática. Hoy en día para cometer una ciberestafa u otro delito informático aún no es necesario poseer determinados conocimientos técnicos. Cualquier persona puede convertirse en cibercriminal, es suficiente que compre un virus informático diseñado por otros, los números de tarjetas de crédito que otros han sustraído o incluso toda la red de arranque infectada. El que desarrolla un virus, el que se apodera de los números de las tarjetas de crédito mediante *keylogger* y el que se limita a comprar un *phishing kit* para apoderarse del dinero de otras personas son todos cibercriminales, aunque las acciones que realizan no son las mismas. Por lo tanto, la persona que efectúa la transferencia de dinero no autorizada por el titular de la cuenta corriente o de la tarjeta de crédito, no es siempre la misma que ha sustraído los datos y las claves de la víctima de manera fraudulenta. A menudo, tanto los que diseñan o venden el programa maligno o los usuarios y contraseñas como los que los compran y utilizan en daño de otras personas, pertenecen a una organización o a un grupo criminal[16]. Tal vez se unen a un fin común, es decir, llevar a cabo un ciberataque contra un sistema informático determinado, tal vez ni siquiera se conocen entre sí y sólo uno de ellos es miembro de un grupo criminal.

---

13 WEBER, A., *Die Strafbarkeit von Plattformbetreibern im Darknet*, Nomos, Baden-Baden, 1° ed., 2022, p. 54.

14 ŠEMBERA, V./PAQUET-CLOUSTON, M./GARCIA, S./ERQUIAGA, M., "Cybercrime Specialization: An Expose of a Malicious Android Obfuscation-As-A-Service", *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2021, p. 213.

15 (https://www.ilpost.it/2024/10/05/carmelo-miano-hacker-ministero-della-giustizia/, consulta: 29/11/2024).

16 RUTGER LEUKFELDT, E./LAVORGNA, A./KLEEMANS, E.R., "Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime", *European Journal on Criminal Policy and Research*, vol. 23, n. 3, 2016, p. 291.

Los grupos criminales que se dedican específicamente a la comisión de delitos cibernéticos no tienen una jerarquía estricta, sino divisiones por tareas. En este sentido, se distingue entre miembros principales (*core members*), facilitadores (*enablers*) y muleros (*money mule*): los primeros son los que organizan y coordinan los ciberataques contra instituciones; los facilitadores son los que facilitan a los miembros principales proporcionándoles malware, contraseñas u otras herramientas útiles para llevar a cabo el ciberataque, mientras que los muleros son los que se encargan de ocultar el origen ilícito del dinero o los bienes sustraídos ilegalmente por los miembros principales[17]. A veces algunos miembros de estos grupos pertenecen también a organizaciones criminales tradicionales, que quieren participar en nuevos y lucrativos tráficos ilícitos[18].

La necesidad de la regulación de la ciberdelincuencia ha llamado la atención de diferentes instituciones supranacionales, concretamente, de la Unión Europea y del Consejo de Europa.

El ciberespacio no ocupa un determinado lugar físico o geográfico y tiene naturaleza transfronteriza, así que, para una lucha eficaz contra el cibercrimen, es necesario que los diferentes países lleguen a un enfoque común respecto a los elementos constitutivos de las infracciones penales.

Por consiguiente, es fundamental el Convenio sobre el Cibercrimen, suscrito en Budapest el 23 de noviembre de 2001, que recomienda explícitamente el castigo de algunos delitos cometidos en el ciberespacio, como el acceso ilícito, la interceptación ilícita, los ataques a la integridad de los datos y a la integridad del sistema y el fraude informático. Esta lista de delitos coincide en gran parte con las directrices establecidas en la Recomendación R (89)9, adoptada por el Consejo de Europa el 13 de septiembre de 1989, la primera relativa en concreto a la criminalidad informática. Los principales objetivos del Convenio son armonizar los elementos de los delitos informáticos de cada país, establecer los poderes necesarios para la investigación y el procesamiento de dichos delitos y establecer un régimen rápido y eficaz de cooperación internacional en dicha materia[19]. El Convenio ha sido suscrito por la Unión Europea y ratificado por todos sus Estados miembros.

La Unión Europea ha elaborado una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia. En particular, ha promulgado la Directiva (UE) 2013/40 relativa a los ataques contra los sistemas de información y la Directiva (UE) 2019/713 sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo. La primera garantiza que los ataques contra los sistemas de información sean castigados penalmente en todos los Estados miembros, mientras que la segunda

17 *Ibid*.

18 EUCPN, *Cyber-OC-Scope and manifestation in selected EU member states*, BKA, Wiesbaden, 2016, p. 223.

19 MIQUELON-WEISSMAN, M., "The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?", *UIC John Marshall Journal of Information Technology & Privacy Law*, vol. 23, 2005, n. 2, p. 330.

establece medidas de derecho penal para proteger los medios de pago distintos del efectivo contra el fraude y la falsificación. Se trata de materias estrechamente relacionadas, porque el fraude informático presupone un ataque previo contra el sistema informático. Ambas sustituyen previas decisiones marco, con el objetivo de efectuar los cambios necesarios para adaptar las normas a los avances tecnológicos. Sin embargo, como se examinará más adelante, a pesar de ser bastante recientes, no han tenido debidamente en cuenta los complejos aspectos criminológicos de la ciberdelincuencia y no siempre están al día de las últimas tendencias delictivas, que han tenido un desarrollo muy rápido, especialmente con el fenómeno del *Cybercrime-as-a-Service*.

2. EL DELITO DE ESTAFA INFORMÁTICA EN ESPAÑA E ITALIA Y SUS MODIFICACIONES A LO LARGO DEL TIEMPO

Como se observa, las iniciativas supranacionales en este ámbito han sido varias y los legisladores nacionales de diversos Países de la UE han tenido varias veces que modificar sus propios códigos penales para cumplir con las obligaciones de los diferentes convenios internacionales, las decisiones marco y las Directivas relativas a los ataques informáticos y al cibercrimen.

Dado que las iniciativas supranacionales se refieren a varios países, resulta útil hacer un análisis comparativo, para ver cómo diferentes países han adaptado su legislación y también para comprobar si las medidas nacionales adoptadas para transponer la directiva consiguieron el objetivo de las Directivas, o sea aproximar las diferentes legislaciones penales en relación con los ciberdelitos. Para este tipo de análisis se eligieron cuales ejemplos paradigmáticos España e Italia, dos países con un rendimiento digital muy diferente[20] y que, a pesar de muchas similitudes, presentan diferencias significativas en algunos institutos de la parte general del derecho penal (p. ej., la disciplina de los actos preparatorios o de autoría y participación en el delito), aspecto que también se refleja en la estructura de los distintos delitos. Sin embargo, a diferencia de otros países europeos, tanto el Código Penal italiano como el español regulan expresamente el concurso de leyes, aunque de forma diferente, aspecto que es muy significativo para este análisis, porque, como se analizará a continuación, los hechos que forman parte de un ciberataque contra el patrimonio son incluibles en varios preceptos penales.

20 En la edición de 2022 del Índice de Digitalización de la Economía y la Sociedad (DESI) calculado por la Comisión Europea, Italia ocupa el puesto 18 de 27 países, con avances significativos en los últimos cinco años, pero aún por debajo de la media europea. De lo contrario, España ocupa el puesto número 7 de los 27 Estados miembros de la UE y es uno de los países de la UE que mejores resultados obtiene. Véase el *Índice de la Economía y la Sociedad Digitales (DESI) 2022* (https://digital-strategy.ec.europa.eu/es/policies/desi, consulta: 29/11/2024).

El análisis se centrará en los delitos contemplados en la Directiva (UE) 2019/713 sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, es decir, el fraude informático y la falsificación y utilización ilícito de dichos medios, que, como se ha señalado anteriormente[21], estadísticamente son los más numerosos entre los ciberdelitos denunciados.

El primero es el delito de estafa informática, que el legislador español introdujo en Código Penal de 1995 en el mismo artículo de la estafa tradicional y modificó en distintas ocasiones, en el 2004, 2010 y en 2022, por medio de la Ley Orgánica 14/2022, de 22 de diciembre, de transposición de Directivas europeas y otras disposiciones para la adaptación de la legislación penal al ordenamiento de la Unión Europea, y reforma de los delitos contra la integridad moral, desórdenes públicos y contrabando de armas de doble uso. Esta última ley ha transpuesto la citada la Directiva (UE) 2019/713 sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión Marco 2001/413/JAI del Consejo.

A partir de la reforma de 2022, el artículo 248 CP queda circunscrito al delito genérico de estafa, mientras que el reformado artículo 249 CP sanciona las manipulaciones informáticas, los actos preparatorios a la ciberestafa, la utilización fraudulenta de cualquier medio de pago distinto del efectivo y la sustracción, apropiación o adquisición de forma ilícita con finalidad de utilización fraudulenta de cualquier medio de pago distinto del efectivo.

Así que hoy, igual que en Italia, donde se regula *la frode informatica* en el art. 640-*ter* del *Codice penale*, la estafa por medios informáticos está situada en un precepto independiente, aunque conectado con la estafa[22]. Sin embargo, a diferencia de lo que ocurre en Italia, el nuevo artículo 249 CP español no castiga únicamente la estafa cometida por medios informáticos. En este se describen hasta cinco conductas distintas relacionadas con los fraudes informáticos y el uso de los nuevos medios de pago.

Los elementos estructurales del delito de estafa informática son bastante similares en los dos países[23]: ambos son delitos contra el patrimonio y delitos de resultado[24].

---

21 Véase la nota 1.

22 Sigue siendo la fórmula «*también se consideran reos de estafa*».

23 Para profundizar, véase GARCÍA GARCÍA-CERVIGÓN, J., "El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico", *Icade. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, n. 74, 2008, p. 290 y ss.

24 GALÁN MUÑOZ, A., *El fraude y la estafa mediante sistemas informáticos. Análisis del artículo 248.2 C.P.*, Tirant lo blanch, Valencia, 1ª ed., 2005, p. 269 e 282; CHOCLÁN MONTALVO, J.A., *El delito de estafa*, Bosch, Barcelona, 1ª ed., 2002, p. 35; DOPICO GÓMEZ-ALLER, J., *Estafas y otros fraudes en el ámbito empresarial*, en DE LA MATA BARRANCO, N.J.,/DOPICO GÓMEZ-ALLER, J./LASCURAÍN SÁNCHEZ, J.A./NIETO MARTÍN, A., *Derecho penal económico y de la empresa*, Dykinson, Madrid, 1ª ed., 2018, p. 231; ANARTE BORRALLO, E., "Incidencia de las nuevas tecnologías en el sistema penal", cit., p. 236; MANNA, A., "Artifici e raggiri on-line: la truffa contrattuale, il falso informatico e l'abuso dei mezzi di pagamento elettronici", *Diritto dell'informazione e dell'informatica*, n. 6, 2002, p. 965; MINICUCCI, G., *Le frodi informatiche*, en *Cybercrime* (dir. Cadoppi, A./ Canestrari, S./Manna,

Pero el art. 249 CP español hace referencia a la transferencia no consentida de cualquier activo patrimonial, diferente del "acto de disposición" previsto por la estafa tradicional, mientras que en el art. 640-*ter* CP italiano se castiga la realización del provecho con daño para otro, igual que en la estafa. No tienen ni el elemento del engaño, ni del error, ambos elementos que no pueden predicarse respecto a un medio digital.

El objeto de delito es muy parecido: en España es el "sistema de información", mientras que en Italia se trata de "*un sistema informático o telemático*". Según la jurisprudencia de la *Cassazione*, equivalente al Tribunal Supremo, un sistema informático puede ser cualquier aparato, como el simple ordenador personal o el móvil[25].

En ambos casos, el elemento subjetivo se concreta en el dolo, pero el artículo 249 CP español requiere también el ánimo de lucro, que supone la intención de enriquecimiento a costa del empobrecimiento de la víctima[26].

Por otro lado, las conductas castigadas son diferentes y, paradójicamente, esta diferencia se puso de manifiesto al aplicar la mencionada Directiva sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo. Con la última reforma de 2022 el legislador español amplió las conductas típicas del delito de ciberestafa. A la manipulación informática y al uso de otro "artificio semejante" se han añadido la obstaculización, la interferencia indebida en el funcionamiento de un sistema de introducción, y la introducción, alteración, borrado, transmisión o supresión indebida de datos informáticos. Estas conductas son las mismas mencionadas en el artículo 6 de la citada Directiva (UE) 2019/713 sobre la lucha contra el fraude y la falsificación de medios de pago. No obstante, se señala que el artículo 249 CP es muy similar al artículo 3 de la previa Decisión Marco, donde ya figuraba una lista de conductas típicas del fraude informático. Pero, al aplicar la Decisión Marco, el legislador español no consideró necesario modificar el delito de fraude informático añadiendo las conductas previstas en la lista. Por lo tanto, no está clara la razón por la que esta vez decidió actuar así, incluso teniendo en cuenta que la conducta de manipulación informática ya es muy amplia. Efectivamente, según la jurisprudencia y la doctrina española, la manipulación informática es cualquier alteración o modificación de los datos[27] y también se configura cuando el autor

A./Papa, M.), Utet, Milano, 2ª ed., 2023, p. 903; PICA, G., *Diritto penale delle tecnologie informatiche*, Utet, Torino, 1ª ed., 1999, p. 141.

25 Cass. pen., Sección 4.ª, 4 de octubre de 1999, n. 3065.

26 STS, Sección 1.ª, 2 de abril de 1998.

27 ROMEO CASABONA, C.M., *Poder informático y seguridad jurídica*, Fundesco, Madrid, 1ª ed., 1987, p. 47; MATA Y MARTÍN, R.M., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 1ª ed., 2001, p. 48.; GALÁN MUÑOZ, A., *Los ciberdelitos en el ordenamiento español*, UOC, Barcelona, 1ª ed., 2019, p. 144; MIRÓ LLINARES, F., "La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing", *Revista Electrónica de Ciencia Penal y Criminología*, n. 15-12, 2013, p. 12:14. Según FARALDO CABANA, P., *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*, Tirant lo blanch, Valencia, 1ª ed., 2009, p. 89, la manipulación

modifica materialmente el programa informático indebidamente o lo utilice sin la debida autorización o en forma contraria al deber[28]. Y la referencia al "artificio semejante" es una cláusula general para permitir una rápida adaptación de la norma a las nuevas realidades[29]. Así que las conductas de obstaculización, interferencia indebida en el funcionamiento, introducción, alteración, borrado, transmisión o supresión indebida de datos informáticos ya entraban en el ámbito de la estafa informática. Por este motivo, se está de acuerdo con aquellos autores que valoran negativamente este cambio[30], porque no sólo no aporta nada nuevo al tipo, sino que es superabundante y potencialmente engañoso.

Al contrario, el legislador italiano nunca ha modificado los elementos estructurales del fraude informático, que ha permanecido idéntico desde su introducción por la Ley 23 de diciembre 1993, n. 57. Las conductas típicas siguen siendo únicamente la alteración en cualquier modo del funcionamiento de un sistema informático o telemático y la intervención sobre los datos sin derecho. Se trata de una terminología amplia, según la cláusula general "en cualquier modo", que incluye la obstaculización, la interferencia indebida en el funcionamiento, la introducción, la alteración, el borrado, la transmisión o supresión indebida de datos informáticos[31]. Ambas pueden darse sobre el *hardware* o sobre el *software*. Por este motivo, el legislador italiano no consideró necesario modificarlas, tampoco con motivo de la transposición de la citada Directiva (UE) 2019/713.

Con el tiempo, se han añadido diferentes circunstancias agravantes del fraude informático, también con la transposición de la citada Directiva. Estas circunstancias tienen una influencia muy significativa, porque las agravaciones previstas se aplican en un número muy elevado de casos. Aparte de las que ya existían en 1993, pero que no tuvieron mucho éxito y se aplicaron en un número muy reducido de casos, la primera fue añadida con la Ley del 15 de octubre de 2013, n. 119. Esta circunstancia agravante castiga el fraude informático cometido mediante el «*robo o uso indebido de la identidad digital en perjuicio de una o más personas*». La intención del legislador era sancionar de manera más grave el fraude informático cometido a través del *phishing*. Pero la solución adoptada ha sido muy insatisfactoria, porque el legislador decidió intencionadamente no dar ninguna definición ni de "robo o uso indebido

informática coincide con la conducta descrita en el artículo 3 de la Decisión Marco 2001/413/JAI, así que «*debe entenderse que constituye manipulación informática la introducción, alteración, borrado o supresión indebidos de datos informáticos, especialmente datos de identidad, y la interferencia indebida en el funcionamiento de un programa o sistema informático*». En jurisprudencia véase las SSTS Sección 1.ª, 20 de noviembre de 2001; 20 de junio de 2006.

28 STS Sección 1.ª, 21 de diciembre de 2004.

29 MATA Y MARTÍN, R.M., *Delincuencia informática*, cit., p. 48.

30 BUSTOS RUBIO, M., "La reforma de la ciberestafa y la incorporación de los medios de pago digitales en el Código Penal", *Revista de Internet, Derecho y Política*, 2023, n. 38, p. 6 (https://raco.cat/index.php/IDP/article/view/n38-bustos, consulta: 29/11/2024).

31 PECORELLA, C., *Il diritto penale dell'informatica*, Cedam, Padova, 2ª ed., 2006, p. 82.

de la identidad digital", ni de "identidad digital". Así que la conducta típica descrita en este apartado ha sido criticada por su vaguedad[32]. Doctrinalmente la identidad digital se define como el usuario y la contraseña que se utilizan en una cualquier página web[33]. Pero así las conductas de robo y de uso indebido de usuarios y contraseñas sancionadas por el art. 640-*ter* co. 3 CP, coinciden con las ya castigadas por los delitos contra la intimidad informática, en particular el artículo 615-*ter* CP, que sanciona el acceso ilegal a un sistema informático o telemático, o el artículo 615-*quater* CP, que sanciona la posesión, difusión e instalación no autorizada de equipos, códigos y otros medios de acceso al sistema informáticos o telemático[34]. Por lo tanto, en vez de facilitar el trabajo, hay que resolver la problemática que suscita la concurrencia de varias disposiciones penales aparentemente aplicables a un mismo hecho, operación que en el ordenamiento italiano no es nada fácil y que, en la mayoría de los ciberdelitos, implica la aplicación de dos o más delitos, con consiguiente vulneración del principio *ne bis in idem*[35]. Cabe señalar también que, en casi todas las estafas informáticas, el cibercriminal, para realizar la transferencia del dinero, necesita la contraseña o el número de tarjeta de crédito y, por lo tanto, la agravación acaba siendo siempre aplicable, que se traduce en un aumento significativo de la pena del fraude informático.

Otra circunstancia agravante fue añadida con el *Decreto legislativo* 8 de noviembre de 2021, n. 184, de transposición de la citada Directiva (UE) 713/2019. Así que hoy

---

32 MALGIERI, G., "La nuova fattispecie di "indebito utilizzo d'identità digitale": un problema interpretativo", *Diritto penale contemporaneo. Rivista trimestrale,* 2015, n. 2, p. 144 (https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/it/archivio, consulta: 29/11/2024).

33 MARGIOCCO, M., *Frode informatica*, en *Diritto dell'informatica* (dir. Finocchiaro, G./ Delfini, F.), Utet, Torino, 2014, p. 1110; FLOR, R., *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, en *Cybercrime* (dir. Cadoppi, A./Canestrari, S./Manna, A./ Papa, M.), Utet, Milano, 2ª ed., 2023, p. 183. Véase también Cass. pen., Sección 2.ª, 13 de marzo de 2024, n. 13559 y 8 de septiembre de 2023, n. 38027.

34 Con más profundidad, sobre los delitos contra la intimidad informática en el Código penal italiano, reformados por la Ley 23 de diciembre de 2021, n. 238, véase, en la doctrina, SALVADORI, I., *I reati contro la riservatezza informatica*, en *Cybercrime* (dir. Cadoppi, A./Canestrari, S./Manna, A./ Papa, M.), Utet, Milano, 2ª ed., 2023, p. 693 y ss.

35 Entre los principios de solución del concurso de leyes, el Código penal italiano ha acogido expresamente el solo principio de especialidad. Por lo tanto, es muy controvertido si, cuando hecho normalmente que acompaña a otro, como en el caso del fraude informático y del acceso al sistema informático, pueda aplicarse el principio de consunción. La jurisprudencia mayoritaria lo excluye y afirma que en esos casos hay concurso real de delitos. También hay que considerar que en el ordenamiento penal italiano no existe el concurso medial y cuando una infracción es medio necesario para cometer otra se trata simplemente de concurso real. Para profundizar el tema, véase FROSALI, R.A., *Concorso di norme e concorso di reati*, Giuffré, Milano, 1ª ed., 1971, p. 501; MANTOVANI, F., *Concorso e conflitto di norme nel diritto penale*, Zanichelli, Bologna, 2ª ed., 1966, p. 178; ANTOLISEI, F., "Concorso formale di reati e conflitto apparente di norme", *Giustizia penale*, vol. II, 1942, p. 209; DELITALA, G., "Concorso di norme e concorso di reati", *Scritti di diritto penale*, Giuffré, Milano, 1976, p. 487 y ss.; PAGLIARO, A., "Concorso di norme", en *Enciclopedia del Diritto*, vol. VIII, Giuffré, Milano, 1961, p. 545 y ss.; CONTI, L., "Concorso apparente di norme", en *Novissimo Digesto Italiano*, vol. III, Utet, Torino, 1958, p. 1007 ss.; Véase también Cass. pen., Sezioni Unite, 23 de febrero de 2017, n. 20664; Cass. pen., Sezioni Unite, 22 de junio de 2017, n. 41588.

en el art. 640-*ter* párrafo dos se hace una específica mención a la agravación en el caso de que «*el hecho produzca una transferencia de dinero, de valor monetario o de moneda virtual*». Como se observa, esta circunstancia, cuya formulación encaja con lo dispuesto en el art. 6 de la Directiva (UE) 713/2019, coincide casi perfectamente con el daño de la estafa informática española, que requiere que el perjuicio patrimonial sea causado por la transferencia no consentida de un valor patrimonial activo, excepto por la referencia a la moneda virtual. Dado que, como se ha señalado, el fraude informático italiano tiene una estructura similar a la de la estafa informática española, es evidente que esta circunstancia agravante coincide con el elemento estructural del resultado del delito de fraude informático. De hecho, es difícil siquiera imaginar que a través de una manipulación informática cometida con el fin de realizar una estafa informática se pueda producir un daño patrimonial que no implique también una transferencia de dinero o de un valor patrimonial. Tampoco la referencia a la moneda virtual aporta nada nuevo al tipo, porque, a pesar de no ser clasificable como dinero[36], el hecho de que pueda intercambiarse por este último la hace comparable a un valor patrimonial[37]. Sin embargo, esta circunstancia se aplica en todos los casos de fraude informático, con la consecuencia de que la pena es considerablemente mayor. Tampoco este cambio se puede valorar positivamente y resulta evidente que la transposición de la Directiva no ha sido satisfactoria en ninguno de los dos países. Además, curiosamente, en lugar de ser una oportunidad para alinear la legislación en este ámbito, ha sido una ocasión en la que los Estados miembros han adoptado diferentes "soluciones creativas", lo cual va en contra del objetivo perseguido por la Directiva misma.

Como se ha señalado, el artículo 249 CP español, en su apartado n. 2, sanciona también los actos preparatorios. Este párrafo fue introducido por primera vez por la Ley Orgánica 15/2003, de 25 de noviembre, en el art. 248.2 b) CP y se castigaba la fabricación, introducción, posesión o facilitación de programas informáticos específicamente destinados a la comisión de estafas previstas en el presente artículo. Con la reforma llevada a cabo por la Ley Orgánica 14/2022, de 22 de diciembre, este precepto fue ampliado y hoy castiga «*los que fabricaren, importaren, obtuvieren, poseyeren, transportaren, comerciaren o de otro modo facilitaren a terceros dispositivos, instrumentos o datos o programas informáticos, o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas previstas en este artículo*». A las conductas típicas han sido añadidas la importación, la obtención, el transporte, el comercio y la facilitación a terceros en cualquier modo. Tras la reforma, los dispositivos, instrumentos, datos o programas deben ser designados o específicamente adaptados a la comisión de la estafa informática. De esta manera, queda claro que este requisito

36 European Central Bank, *Virtual currency schemes – A further analysis*, 2015, p. 23, (https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf&ved=2ahUKEwj_r8XXsrKFAxVPoAIHHRUoDqMQFnoECBEQAQ&usg=AOvVaw0p6cPAbokB8OTj1tbAWitz, consulta: 29/11/2024).

37 La Directiva misma en el Considerando n. 10 precisa que «*debe aplicarse a las monedas virtuales solo en la medida en que puedan usarse de manera habitual para efectuar pagos*».

debe entenderse no sólo como una idoneidad objetiva para cometerlas, sino también como una orientación subjetiva: el sujeto debe fabricarlos, poseerlos, etc. a sabiendas de que serán empleados para la comisión de estafas[38].

Estos actos preparatorios se castigan con la misma pena que la estafa consumada, lo cual ha sido muy criticado porque implica la vulneración del principio de proporcionalidad[39].

Al contrario, en Italia no se castigan expresamente los actos preparatorios del delito de fraude informático. Esto porque no hay el principio de impunidad y tal vez estos actos pueden ser castigados como tentativa, cuya formulación es mucho más amplia[40]. Además, en esos casos casi siempre se configuran también los delitos contra la intimidad informática, como el mencionado artículo 615-*quater* CP, recién modificado por la Ley 28 de junio de 2024, n. 90, que sanciona la posesión, la difusión e la instalación no autorizada de equipos, códigos y otros medios de acceso al sistema informáticos o telemático o el artículo 617-*quater* CP, también recién modificado por la misma Ley n. 28/2024, que castiga la interceptación de comunicaciones entre sistemas informáticos. En este caso se configura el concurso real de delitos entre estos delitos contra la intimidad informática y el fraude informático, porque los bienes jurídicos protegidos son diferentes y se consuman en momentos diferentes[41]. Por tanto, parece correcta la decisión de no sancionar de manera autónoma los actos preparatorios de los fraudes informáticos, ya que se trata de conductas que ya están sancionadas de manera autónoma en otros preceptos.

Este solapamiento entre los delitos contra los sistemas de información y las fraudes y falsificaciones de medios de pago distintos del efectivo, se verifica en el ordenamiento español también. Efectivamente, para conseguir la transferencia de dinero electrónico e, incluso antes, obtener o poseer datos o programas informáticos necesarios para realizarla, antes hay que interceptar la transmisión de los datos,

---

38 DOPICO GÓMEZ-ALLER, J., *Estafas y otros fraudes en el ámbito empresarial*, cit., p. 231. Con más profundidad sobre este requisito y en general el tema de los *dual-use software* véase SALVADORI, I., "Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software"", *Rivista italiana di diritto e procedura penale*, n. 2, 2017, p. 747 y ss.

39 FARALDO CABANA, P., *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*, cit., p. 111; DOPICO GÓMEZ-ALLER, J., *Estafas y otros fraudes en el ámbito empresarial*, cit., p. 231; CRUZ DE PABLO, J.A., *Derecho penal y nuevas tecnologías. Aspectos sustantivos. Adaptado a la reforma operada en el Código Penal por Ley Orgánica 15/2003 de 25 noviembre, especial referencia al nuevo artículo 286 CP*, Grupo difusión, Madrid, 2006, p. 46. Según MUÑOZ CONDE, F., *Derecho Penal. Parte Especial*, Tirant lo blanch, Valencia, 25ª ed., 2023, p. 457 «*La razón de esta equiparación punitiva se debe a la importancia que tienen actualmente los dispositivos, instrumentos, datos y programas informáticos en el tráfico económico en general y a que de este modo se le otorga una protección especial reforzada al sistema informático como bien jurídico colectivo*».

40 SEMINARA, S., *Il delitto tentato*, Giuffré, Milano, 1ª ed., 2012; GIACONA, I., *Il concetto d'idoneità della struttura del delitto tentato*, Giappichelli, Torino, 1ª ed., 2000, p. 6 y ss.

41 Véase Cass. pen., Sección 5.ª, 19 de febrero de 2020, n. 17360. De la misma opinión Cass. pen., Sección 2.ª, 29 de mayo de 2019, n. 26604; Cass. pen., Sección 5.ª, 30 de septiembre de 2009, n. 1727; Cass. pen., Sección 5.ª, 19 de diciembre de 2003, n. 2672.

conducta sancionada por el artículo 197 *bis*.2 CP, u obtener las contraseñas, los códigos de acceso o datos similares que permitan el acceso a la aplicación móvil del banco, conducta castigada por el artículo 197-*ter* CP. Esto se debe a la falta de coordinación entre las diferentes Directivas y, por consiguiente, las normas nacionales, que regulan ámbitos estrechamente relacionados, en particular la mencionada Directiva sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y la Directiva (UE) 2013/40 relativa a los ataques contra los sistemas de información. Este problema no se ha considerado mucho, pero es relevante. La obtención de números y claves de las tarjetas de crédito o del usuario y contraseña mediante las mencionadas técnicas del *keylogger*, *phishing*, *skimming*, *smishing* o *pharming* no sólo constituye un acto preparatorio del fraude informático, sino también un delito informático vinculados a la tutela de la confidencialidad de datos y sistemas, es decir el artículo 197 ter CP. Por lo tanto, hay que resolver la problemática que suscita la concurrencia de varias disposiciones penales, operación que ni en Italia ni en España resulta fácil, ya que hay muy pocas cláusulas de subsidiariedad expresa y en muchos casos las penas son idénticas. Por lo tanto, existe el riesgo que se generen situaciones de vulneración del principio *ne bis in idem*, dado que el mismo hecho es castigado por varias normas.

3. LA FALSIFICACIÓN Y UTILIZACIÓN FRAUDULENTA DE MEDIOS DE PAGO DISTINTOS DEL EFECTIVO

La falsificación y la utilización fraudulenta de medios de pago distintos del efectivo son otras disposiciones que han sido modificadas para su adaptación a los avances tecnológicos y el cumplimiento de las obligaciones de la mencionada Directiva (UE) 713/2019.

Tanto en España como en Italia se sancionan estas conductas ilícitas, pero de manera diferente.

Como se ha señalado en el párrafo anterior, el legislador español sanciona el uso indebido de tarjetas, cheques y otros medios de pago distintos del efectivo en el mismo precepto de la estafa informática, en el recién modificado art. 249.1 b) CP. En particular, se castiga la utilización de forma fraudulenta de los medios de pago material o inmaterial distinto del efectivo «*o los datos obrantes en cualquiera de ellos*». Al contrario, la falsificación de instrumentos de pago es castigada por un precepto independiente, es decir, el artículo 399 *bis* CP. En este delito las conductas castigadas son la alteración, la copia, la reproducción y la falsificación "de otro modo" de los instrumentos de pago distintos al efectivo. Ambas fueron introducidas por la reforma del Código penal operada por la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, y han sido modificadas por la mencionada Ley Orgánica 14/2022, de 22 de diciembre.

Al contrario, en Italia la falsificación y el uso indebido de instrumentos de pago son dos delitos distintos que concurren entre ellos, pero castigados por el mismo artículo 493-*ter* CP, titulado «*Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti*» y que se encuentra en el título del Código penal dedicados a las falsificaciones. Esto tiene consecuencias. Dado que el art. 493-*ter* CP se sitúa entre los delitos de falsificación, el bien jurídico protegido no es el patrimonio, sino la fe pública[42]. Esto significa que el consentimiento del titular del medio de pago no excluye la responsabilidad penal, porque la disposición protege algo diferente del patrimonio individual, es decir, un interés supraindividual en el desarrollo adecuado y seguro de la actividad financiera mediante sustitutos del efectivo[43]. Así que el artículo 493-*ter* CP italiano castiga también los que utilicen el instrumento de pago de otra persona con su consentimiento.

La solución adoptada por el legislador español parece más adecuada, porque evita una criminalización excesiva. Efectivamente, si se toma como ejemplo el caso de una persona mayor que entrega la tarjeta a un familiar para que retire una determinada cantidad de dinero o efectúe una determinada operación de pago, no se ve cómo esta conducta pueda dañar "el desarrollo adecuado y seguro de la actividad financiera", dado que la tarjeta se utiliza con el consentimiento del titular y dentro de los límites de disponibilidad, sin ser alterada de ninguna manera.

Todos los artículos mencionados, tanto en España como en Italia, han sido modificados para transponer la citada Directiva sobre la lucha contra el fraude y la falsificación de medios de pago. Los cambios fueron similares, porque ambos legisladores tipificaron los medios de pago distintos del efectivo en el seno de estos delitos. Hoy en día, en ambos países, objeto de los delitos de falsificación y utilización fraudulenta de medios de pago distintos del efectivo son todos los instrumentos de pago, materiales o inmateriales, distintos del efectivo.

Por supuesto la elección del legislador español e italiano de transponer los artículos 4 y 5 de la mencionada Directiva, que se refieren a las infracciones relacionadas con la utilización fraudulenta de instrumentos de pago materiales (art. 4) e inmateriales (art. 5) distintos del efectivo, se ajusta a las disposiciones de la misma y tiene debidamente en cuenta el crecimiento exponencial de la economía y de los servicios digitales, que en los últimos tiempos ha determinado una proliferación de nuevos instrumentos de pago muy diferentes a las tradicionales tarjetas de crédito y cheques[44]. No obstante, plantea un problema importante, es decir, la dificultad de

42 PICOTTI, L., "Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati", en *Il diritto penale dell'informatica nell'epoca di Internet*, (dir. Picotti, L.), Cedam, Padova, 1ª ed., 2004, p. 56 y 57.

43 Cass. pen., Sección 2.ª, 16 de febrero de 2021, n. 18609 de 2021; Sección 2.ª, 17 de septiembre de 2020; Sección 1.ª, 19 de febrero de 2004, n. 11023.

44 PRIETO DEL PINO, A.M., "Criminal offences against property and against the social-economic order in Spain: a global overview and a detailed approach to some particularly relevant issues", *Philia journal of Judicial Studies*, vol. 1, 2022, p. 95, lamentaba la obsolescencia de la referencia a los cheques

distinguir claramente cuándo se comete el delito de fraude informático y cuándo, en cambio, se trata de falsificación o uso indebido de instrumentos de pago distintos del efectivo. La cuestión es muy relevante, porque las penas de los diferentes artículos no son iguales. Un caso paradigmático es el del *pharming*: aquí el ciberdelincuente, para apropiarse del dinero del titular de la cuenta, antes tiene que falsificar la página web o la aplicación móvil del banco. Como la aplicación móvil y la página *web* del banco pueden ser incluidos entre los medios de pago inmateriales distintos del efectivo[45], en ambos los países examinados se plantea el problema de establecer si se trata de estafa informática o de falsificación de medios de pago, porque la conducta corresponde a la falsificación, pero también constituye una manipulación informática o una alteración del sistema informático.

Es evidente que existe un solapamiento entre el fraude informático y la falsificación de medios de pago distintos del efectivo, que se hizo aún más problemático con la transposición de la citada Directiva. Esto ocurrió porque la Directiva misma no se preocupó de distinguir de forma eficaz entre los dos delitos.

Con respeto a la legislación italiana, cuando se produce una transferencia no consentida de dinero, como no hay especialidad entre los preceptos de fraude informático y falsificación de medios de pago distintos del efectivo (mientras que sí hay especialidad entre el fraude informático y el delito de utilización fraudulenta de dichos medios[46]), hay que afirmar que existe concurso de delitos, con aplicación del tratamiento del delito continuado[47]. Pero esta solución no es nada satisfactoria, porque las penas para los dos delitos son muy elevadas y hay una vulneración del principio *ne bis in idem*. Otra solución podría ser aplicar sólo el artículo 493-*ter* CP cuando no hay el perjuicio patrimonial y, en caso contrario, considerar el fraude informático agravado por el robo de identidad digital y por la transferencia del valor patrimonial como *reato complesso*, aplicando únicamente el artículo 640-*ter* párrafo 2 y 3 CP[48]. Sin embargo, esta solución acaba en la abrogación tácita de una parte de

de viaje en el CP español, debida a una tardía transposición de la Decisión Marco 2001/413/JAI.

45 Cuya definición, en virtud del artículo 2, a) de la Directiva (UE) 2019/713, es la siguiente: «*un dispositivo, objeto o registro protegido, material o inmaterial, o una combinación de estos, exceptuada la moneda de curso legal, que, por sí solo o en combinación con un procedimiento o conjunto de procedimientos, permite al titular o usuario transferir dinero o valor monetario incluso a través de medios digitales de intercambio*». De la misma opinión ABADÍAS SELMA, A., "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*, Vol. 71, n. 1, 2023, p. 30.

46 Cass. pen., Sección 2.ª, 15 de abril de 2011, n. 17748; Sección 2.ª, 13 octubre de 2015, n. 50140.

47 A diferencia de su homólogo español, el *reato continuato* italiano no supone la unidad del hecho, sino el concurso real de delitos y sirve únicamente para dispensar un trato más favorable que el correspondiente al concurso real. La pena correspondiente será la señalada para la infracción más grave, aumentada hasta tres veces. Para profundizar véase AMBROSETTI, E.M., *Problemi attuali in tema di reato continuato. Dalla novella del 1974 al nuovo codice di procedura penale*, Cedam, Padova, 1ª ed., 1991; ZAGREBELSKY, V., *Reato continuato*, Giuffré, Milano, 2ª ed., 1976.

48 El art. 84 Código penal italiano establece que no hay concurso de delitos, sino un solo delito cuando «*la ley considera como elementos constitutivos, o como circunstancias agravantes de un mismo delito,*

la reforma del mencionado *Decreto legislativo* n. 184/2021, porque el articulo 493-*ter* CP acaba aplicándose sólo a los instrumentos de pago materiales, exactamente igual que antes de la reforma. Pero en la actualidad parece ser la solución más correcta para evitar el *ne bis in idem*.

El mismo problema se plantea en la legislación española. El Tribunal Supremo, a excepción del caso del art. 399 *ter*.3 CP[49], excluye que la sanción por el delito de falsificación de tarjetas de crédito pueda absorber el desvalor jurídico penal que se deriva de su uso posterior. Por lo tanto, no hay concurso de leyes entre el delito de falsedad de tarjetas de crédito y el delito de estafa, sino concurso medial, dado que la falsificación es un medio para cometer la estafa[50]. Si este principio se aplicaba a las tarjetas de crédito, más aún se aplica ahora a los nuevos instrumentos de pago inmateriales. En este caso, el tratamiento es más benévolo que lo del concurso real, pero tampoco es una solución muy satisfactoria. Otra solución podría ser la aplicación del principio de alternatividad, que conduciría a la aplicación del precepto penal más grave, es decir, el delito de falsificación de los medios de pago distintos del efectivo[51].

Sin embargo, cabe señalar que, como se ha examinado anteriormente, en el *phishing* clásico no hay alteración o falsificación del medio de pago, sino su utilización ilícita. Por lo tanto, conforme a las soluciones mencionadas, en el caso del *phishing* el ciberdelincuente será castigado por la menos grave estafa informática, mientras que en el caso del *pharming* por la más grave falsificación de medios de pago o, en el caso del concurso medial, con una pena más grave. Por lo tanto, estas soluciones no parecen correctas, dado que no hay razón criminológica para castigar el *pharming* más severamente que el *phishing*, tratándose del mismo fenómeno delictivo. Efectivamente, el objetivo de estas tipologías de ciberataques es la realización de una transferencia no consentida de un valor patrimonial. Sólo la estafa informática exige, además de la conducta de alteración o manipulación, la realización del resultado. Así que se puede considerar como presupuesto adicional y el art. 249 CP el precepto especial aplicable. Esta solución resolvería el problema señalado anteriormente, pero aún no goza del favor de la jurisprudencia del Tribunal Supremo.

hechos que, por sí solos, constituirían un delito».

49 «*El que sin haber intervenido en la falsificación usare, en perjuicio de otro y a sabiendas de la falsedad, tarjetas de crédito o débito, cheques de viaje o cualesquiera otros instrumentos de pago distintos del efectivo falsificados, será castigado con la pena de prisión de dos a cinco años*».

50 SSTS Sección 1.ª, 23 de abril de 2014; 17 de junio de 2013.

51 Con más profundidad, sobre los principios de solución del concurso de leyes, en particular el principio de alternatividad, véase, en la doctrina, CASTELLÓ NICÁS, N., *El concurso de normas penales*, Editorial Comares, Granada, 1ª ed., 2000, p. 115 y ss.; GARCÍA ALBERO, R.M., *"Non bis in Idem" material y concurso de leyes penales*, Cedecs, Barcelona, 1ª ed., 1995, p. 321 y ss.; MUÑOZ CONDE, F./GARCÍA ARÁN, M., *Derecho Penal. Parte General*, Tirant lo blanch, Valencia, 11ª ed., 2022, p. 440; MIR PUIG, S., *Derecho Penal. Parte General*, Editorial Reppertor, Barcelona, 10ª ed., 2015, p. 687.

4. LOS ACTOS PREPARATORIOS

Los cambios también afectaron a los actos preparatorios. En el ordenamiento español los actos preparatorios de la falsificación de los medios de pagos distintos al efectivo se castigan en el artículo 400 CP. En este caso, las conductas sancionadas (fabricación, recepción, obtención, tenencia, distribución, puesta a disposición o comercialización de útiles, materiales, instrumentos, sustancias, datos y programas informáticos, aparatos, elementos de seguridad o cualquier otro medio diseñado o adaptado específicamente para la comisión de la falsificación de los medios de pago) son casi idénticas a las mencionadas en el artículo 7 de la Directiva (UE) 2019/713. Incluso aquí los actos preparatorios se castigan con la misma pena señalada para el delito consumado[52]. Por otra parte, en lo que respecta a los actos preparatorios de la utilización fraudulenta de medios de pagos, tratándose de fraude informático, están castigados por el art. 249.2.a) CP. No obstante, a través de la LO 14/2022 han sido añadidos dos apartados nuevos, cuyas disposiciones encuentran su paralelismo en el art. 4 de la mencionada Directiva (UE) 2019/713. El primero es el art. 249.2.b) CP, donde se castigan las conductas de adquisición ilícita de tarjetas, cheques o instrumentos de pago distintos del efectivo para su uso fraudulento. No queda clara la razón por la cual el legislador español decidió añadir este apartado, porque la adquisición ilícita de tarjetas de crédito materiales ya está castigada por el hurto, mientras que la adquisición de los datos obrantes en los medios de pago por el art. 249.1.b) CP. Por último, como tipo atenuado, se sancionan en el art. 249.3 CP, con pena en su mitad inferior las conductas de posesión, distribución o, en general, de puesta a disposición de terceros de dichos medios de pago. En todos estos delitos hay la expresa tipificación de los medios de pago distintos del efectivo.

El legislador italiano también, con el *Decreto legislativo* 8 de noviembre de 2021, n. 184, de transposición de la citada Directiva (UE) 713/2019, ha añadido un nuevo delito en el nuevo art. 493-*quater* CP, que castiga los actos preparatorios de los delitos «*relacionados con el utilizo de medios de pago distintos del efectivo*». Las conductas sancionadas son las mismas mencionadas en el artículo 7 de la citada Directiva, o sea la producción, importación, exportación, venta, transporte, distribución, la puesta a disposición de terceros y la obtención. Objetos de la acción son los aparados, dispositivos y programas informáticos «*diseñado principalmente o adaptado específicamente*» para cometer cualquiera de las infracciones a que se refieren estos medios de pagos. Así que puede tratarse de un fraude informático también. La elección del legislador italiano de añadir este nuevo delito no se puede valorar positivamente. No sólo porque dichas conductas en el ordenamiento italiano ya podrían ser sancionadas como tentativa, sino también porque las acciones y los objetos del delito son los mismos que ya castigan los delitos contra la intimidad informática y es difícil establecer si hay concurso de leyes o concurso de delito. En este caso hay una cláusula de subsidiariedad expresa, pero en algunos casos persiste

52 FARALDO CABANA, P., *Las nuevas tecnologías en los delitos contra el patrimonio*, cit., p. 289.

el solapamiento entre los delitos, porque se castigan con la misma pena y no es nada fácil encontrar una solución satisfactoria.

5. CONSIDERACIONES FINALES Y PERSPECTIVAS *DE LEGE FERENDA*

Como se ha examinado, los delitos de estafa informática y de falsificación y utilización fraudulenta de medios de pago distintos del efectivo son bastante similares en Italia y España. Sin embargo, la comparación demuestra que paradójicamente las diferencias han aumentado en el tiempo, a través de las leyes de transposición de aquellas Directivas cuyo objetivo era lo contrario, es decir, aproximar las legislaciones de los Estados miembros.

La comparación también ha permitido constatar que existe un problema objetivo de solapamiento entre las normas, en particular entre el fraude informático y la falsificación/utilización de instrumentos de pago distintos del efectivo. Los convenios supranacionales revisten una importancia fundamental, pero, especialmente cuando se toman decisiones para un determinado grupo de países, hay que considerar las disposiciones de otros convenios que ya existen y adoptar medidas para evitar el solapamiento. El Convenio sobre el Cibercrimen ya recomendaba castigar el fraude informático, cuyas conductas ya estaban sancionadas como delito en todos los países europeos. Así que la repetición de esta obligación por la Directiva (UE) 2019/713 no sólo no añadió nada nuevo al tipo, sino que ha "confundido" al legislador italiano y español, que consideraron erróneamente que había obsolescencia del tipo penal y aportaron modificaciones que causan confusión, por ejemplo, añadir a los objetos de los delitos de falsificación y utilización fraudulenta de medios de pago distintos del efectivo los instrumentos de pago inmateriales, o superfluas. También hay que tener en cuenta que muchas conductas descritas en la Directiva (UE) 2019/713 coinciden con las ya castigadas por los delitos contra la intimidad informática. Por tanto, no sólo hay solapamiento entre los ciberdelitos contra el patrimonio, sino también entre estos últimos y los delitos contra la intimidad informática. Se trata de un problema que el legislador europeo ha ignorado por completo, pero que en la práctica tiene importantes repercusiones. La comparación permitió comprobar que ni siquiera la regulación expresa del concurso de leyes en cada Estado miembro es concluyente.

Sin embargo, no obstante el solapamiento, no todas las conductas de los ciberdelincuentes hoy se sancionan adecuadamente. El legislador europeo tiene razón cuando afirma que hay obsolescencia de los ciberdelitos, pero esta no se debe a la falta de conductas en la lista de las que ya son sancionadas o a la no mención de las monedas virtuales como objeto de las acciones, sino en la desatención de las formas de delinquir que se han producido en este ámbito. El legislador europeo mismo, en el Considerando n. 5 de la Directiva (UE) 2013/40 relativa a los ataques contra los sistemas de información, ha reconocido que la mayoría de los ciberataques se debe

a la creación y utilización de redes enteras infectadas, las mencionadas *botnets*, pero no ha tenido debidamente en cuenta el fenómeno del *Cybercrime-as-a-Service* y ha promulgado las sanciones sin diferenciar mínimamente entre los diferentes perfiles de los ciberdelincuentes, es decir, entre los que se dedican profesionalmente a la realización y a la venta de *malware*, *phishing kits*, etc., y los que se limitan a adquirir dichos servicios, quizás realizando daños patrimoniales lleves.

Paradigmático es el artículo 7 de esta Directiva, titulado «*Instrumentos utilizados para cometer las infracciones*»: aquí hay una larga lista de conductas heterogéneas, como la venta, la adquisición para el uso, la importación o la distribución de programas informáticos y contraseñas, que se consideran como "actos preparatorios" de otros preceptos, por ejemplo, de la interferencia ilegal en los datos. Pero hay que considerar que vender un gran número usuarios o de programas informáticos malignos para permitir a otros de realizar fraudes, no es la misma cosa que comprar un número de tarjeta de crédito de otra persona para posteriormente hacer compras por Internet. La primera conducta parece más participación en el delito de estafa informática que un acto preparatorio, porque tiene la eficacia etiológica causal con respecto a la comisión de dicho delito. En este caso, existe una relación causal entre la acción de cada persona y la comisión del delito: la prestación del servicio de *hacking* facilita o permite al autor del ciberdelito posterior la obtención de beneficios ilícitos. Al contrario, la adquisición de contraseñas de otras personas para su posterior utilización fraudulenta es un acto preparatorio, porque no es nada más que una fase, es decir, un medio para cometer la estafa informática. En este último caso sí que es correcto castigar dicha conducta con pena más lleve que el fraude informático consumado e incluso considerarla absorbida por este último delito.

Lo mismo ha pasado con la mencionada Directiva (UE) 2019/713: en este caso legislador europeo tampoco ha tenido en cuenta del fenómeno delictivo del *Cybercrime-as-a-Service* y, en el artículo 7, titulado «*Herramientas utilizadas para cometer infracciones*» considera como "actos preparatorios" una larga lista de conductas heterogéneas.

En el mencionado caso del *hacker* italiano, que ha ganado más de siete millones de euros con la venta de usuarios y contraseñas, no parece correcto considerar su conducta como "acto preparatorio" para la comisión de más graves delitos cibernéticos y castigarla de la misma manera de la persona que adquiere el código de una tarjeta de crédito para comprar algo por Internet. La peligrosidad que conlleva su acción es mayor del usuario que recurre a él por sus servicios ilícitos, porque permitió a un número potencialmente infinito de personas de cometer ciberdelitos.

No se puede valorar positivamente la elección del legislador europeo de poner en el mismo precepto una larga lista de conductas que no tienen nada que ver unas con otras. Es cierto que los Estados miembros son libres de distinguir entre las distintas conductas previstas en la Directiva y sancionar unas más gravemente que otras, pero la inclusión de una lista amplia hace que todos parezcan iguales, lo que confunde a

los legisladores nacionales. La comparación demostró que en España y en Italia no se hace distinción alguna.

Como se ha señalado, la gran mayoría de ciberdelincuentes y grupos criminales que se dedican a la colección de datos informáticos, creación de *malware* y a la venta posterior, no son los mismos que los compran y utilizan en daño de otras personas. Pero la conducta que se caracteriza por una mayor gravedad es la primera, porque se trata de una verdadera actividad económica delictiva, que permite obtener ilícitamente grandes cantidades de dinero con muy pocos riesgos y constituye la *conditio sine qua non* que permite a otros de realzar ciberataques en perjuicio de otras personas y del sistema financiero. Además, quienes prestan servicios de piratería informática suelen ganar mucho más que quienes los utilizan.

No obstante, hoy en día lo que se castiga de manera más grave es lo que realiza la conducta más arriesgada, es decir, la transferencia de dinero. Sin embargo, el solapamiento entre las normas agrava esta situación. Eso es porque sus acciones son incluibles en varios preceptos penales, así que su pena será mayor de la prevista para los que se dedican a la venta o difusión de los programas malignos, que se sancionan únicamente como "actos preparatorios" de otros delitos cibernéticos o como delitos contra la intimidad informática, castigados con una pena más leve. Esto es muy evidente sobre todo en la legislación italiana, donde la venta de contraseñas y datos se castiga en manera mucho menor del fraude informático consumado, menos en la legislación española, donde los actos preparatorios del fraude y de la falsificación de medios de pago se castigan con la misma pena prevista para los delitos consumados. La comparación muestra que ninguna de las dos soluciones es correcta: las normas de ambos países agrupan conductas muy diferentes, sin diferenciarlas, con el resultado de que en algunos casos se castiga demasiado (adquisición) y en otros demasiado poco (comercio/venta).

El legislador debe mantenerse al corriente de los desarrollos tecnológicos y por supuesto no puede ignorar un fenómeno delictivo tan importante como el *Cybercrime-as-a-Service* y la peligrosidad de los ciberdelincuentes que ofrecen sus servicios ilícitos para permitir a un número indeterminado de personas de delinquir. Así que para una correcta tipificación de delitos cibernéticos hay que distinguir entre las diferentes conductas y castigar la fabricación, la venta y el comercio de instrumentos, datos o programas informáticos que sirven para la comisión de otros delitos cibernéticos en un precepto independiente, con la misma pena que el fraude informático. Eso porque dichas conductas tienen eficacia etiológica causal con respecto a la comisión de dicho delito, porque constituyen un acto sin el cual no se habría efectuado. Además, la peligrosidad de dichas conductas, que ponen en peligro cientos de miles de usuarios, justifica la previsión de la misma pena. Al contrario, las acciones que verdaderamente constituyen actos preparatorios, como la obtención y tenencia de estos instrumentos, tiene que ser castigadas con menor pena y, de esta manera, no sólo no hay vulneración del principio de proporcionalidad, sino que se pueden considerar absorbidas por la estafa informática consumada y no ser

sancionadas separadamente.

De lege ferenda, el esfuerzo del legislador, en lugar de añadir nuevos delitos o circunstancias agravantes, tiene que ir encaminado a la racionalización de los ciberdelitos vigentes, distinguiendo entre las diferentes conductas en relación con sus gravedad y peligrosidad y suprimir las irrelevantes, p. ej. la importación o la exportación. De esta forma se podrá establecer una correcta tipificación de delitos cibernéticos, sin que haya solapamiento entre ellos y problemas de vulneración del principio *ne bis in idem*. Por consiguiente, las penas previstas serán proporcionadas al hecho, sin que la aplicación de una multitud de delitos implique sanciones excesivamente elevadas y, al contrario, el fenómeno del *Cybercrime-as-a-Service* sea castigado con penas más graves, adecuadas a su gravedad.

6. BIBLIOGRAFÍA

ABADÍAS SELMA, A., "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*, Vol. 71, n. 1, 2023, pp. 15-82.

ALMOMANI, A./GUPTA, B.B./ATAWNEH, A./MEULENBERG, A./ALMOMANI, E., "A Survey of Phishing Email Filtering Techniques", *IEEE Communications Surveys & Tutorials*, Vol. 15, n. 4, 2013, pp. 2070-2090.

AMBROSETTI, E.M., *Problemi attuali in tema di reato continuato. Dalla novella del 1974 al nuovo codice di procedura penale*, Cedam, Padova, 1ª ed., 1991.

ANARTE BORRALLO, E., "Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho Penal en la sociedad de la información", *Derecho y conocimiento. Anuario jurídico sobre la sociedad de la información*, 2001, vol. 1, pp. 191-257.

ANTOLISEI, F., "Concorso formale di reati e conflitto apparente di norme", *Giustizia penale*, parte II, 1942, p. 609-614.

AZEEZ, N.A./OLADELE, S.S./OLOGE, O., "Identification of Pharming in Communication Networks using Ensemble Learning", *Nigerian Journal of Technological Development*, vol. 19, n. 2, 2022, pp. 172-180.

BUSTOS RUBIO, M., "La reforma de la ciberestafa y la incorporación de los medios de pago digitales en el Código Penal", *Revista de Internet, Derecho y Política*, 2023, n. 38, pp. 1-11 (https://raco.cat/index.php/IDP/article/view/n38-bustos, consulta: 29/11/2024).

CADWELL, M./ANDREWS, J.T.A./TANAY, T./GRIFFIN, L.D., "AI-enabled future crime", *Crime Science*, vol. 9, n. 14, 2020, pp. 1-13.

CAJANI, F./COSTABILE, G./MAZZARACO, G., *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*, Giuffré, Milano, 1° ed., 2008.

CASTELLÓ NICÁS, N., *El concurso de normas penales*, Editorial Comares, Granada, 1ª ed., 2000.

CHOCLÁN MONTALVO, J.A., *El delito de estafa*, Bosch, Barcelona, 1ª ed., 2002.

CONTI, L., "Concorso apparente di norme", en *Novissimo Digesto Italiano*, vol. III, Utet, Torino, 1958, p. 1007-1017.

CRUZ DE PABLO, J.A., *Derecho penal y nuevas tecnologías. Aspectos sustantivos. Adaptado a la reforma operada en el Código Penal por Ley Orgánica 15/2003 de 25 noviembre, especial referencia al nuevo artículo 286 CP*, Grupo difusión, Madrid, 2006.

DELGADO-MOHATAR, O./SIERRA-CÁMARA, J.M./ANGUIANO, E., "Blockchain-based semi-autonomous ransomware", *Future Generation Computer System*, vol. 112, 2020, pp. 589-603.

DELITALA, G., "Concorso di norme e concorso di reati", *Scritti di diritto penale*, Giuffré, Milano, 1976.

DOPICO GÓMEZ-ALLER, J., *Estafas y otros fraudes en el ámbito empresarial*, en DE LA MATA BARRANCO, N.J./DOPICO GÓMEZ-ALLER, J./LASCURAÍN SÁNCHEZ, J.A./NIETO MARTÍN, A., *Derecho penal económico y de la empresa*, Dykinson, Madrid, 1ª ed., 2018, pp. 169-234.

FARALDO CABANA, P., *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*, Tirant lo blanch, Valencia, 1ª ed., 2009.

FLOR, R., *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, en *Cybercrime* (dir. Cadoppi, A./Canestrari, S./Manna, A./ Papa, M.), Utet, Milano, 2ª ed., 2023, pp. 153-208.

FROSALI, R.A., *Concorso di norme e concorso di reati*, Giuffré, Milano, 1ª ed., 1971.

GALÁN MUÑOZ, A., *El fraude y la estafa mediante sistemas informáticos. Análisis del artículo 248.2 C.P.*, Tirant lo blanch, Valencia, 1ª ed., 2005.

GANGULI, P., "The Rise of Cybercrime-as-a-Service: Implications and Countermeasures", *International Journal for Multidisciplinary Research*, vol. 6, n. 5, 2024, pp. 1-46.

GARCÍA ALBERO, R.M., *"Non bis in Idem" material y concurso de leyes penales*, Cedecs, Barcelona, 1ª ed., 1995.

GARCÍA GARCÍA-CERVIGÓN, J., "El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico", *Icade. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, n. 74, 2008, pp. 289-308.

GHAZI-TEHRANI, A./ PONTELL, H., "Phishing Evolves: Analyzing the Enduring Cybercrime", *Victims & Offenders*, vol. 16, n. 3, 2021, pp. 316-342.

GIACONA, I., *Il concetto d'idoneità della struttura del delitto tentato*, Giappichelli, Torino, 1ª ed., 2000.

MANKY, D., "Cybercrime as a service: a very modern business", *Computer Fraud & Security*, n. 6, 2013, pp. 9-13.

MANNA, A., "Artifici e raggiri on-line: la truffa contrattuale, il falso informatico e l'abuso dei mezzi di pagamento elettronici", *Diritto dell'informazione e dell'informatica*, n. 6, 2002, pp. 955-970.

MANTOVANI, F., *Concorso e conflitto di norme nel diritto penale*, Zanichelli, Bologna, 2ª ed., 1966.

MALGIERI, G., "La nuova fattispecie di "indebito utilizzo d'identità digitale": un problema interpretativo", *Diritto penale contemporaneo. Rivista trimestrale,* 2015, n. 2, pp. 143-151, p. 144 (https://dpc-rivista-trimestrale.criminaljustice-network.eu/it/archivio, consulta: 29/11/2024).

MARGIOCCO, M., *Frode informatica*, en *Diritto dell'informatica* (dir. Finocchiaro, G./ Delfini, F.), Utet, Torino, 2014, pp. 1107-1114.

MATA Y MARTÍN, R.M., *Delincuencia informática y derecho penal*, Edisofer, Madrid, 1ª ed., 2001.

MINICUCCI, G., *Le frodi informatiche*, en *Cybercrime* (dir. Cadoppi, A./ Canestrari, S./Manna, A./Papa, M.), Utet, Milano, 2ª ed., 2023, pp. 893-923.

MIQUELON-WEISSMAN, M., "The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?", *UIC John Marshall Journal of Information Technology & Privacy Law*, vol. 23, 2005, n. 2, pp. 329-361.

MIR PUIG, S., *Derecho Penal. Parte General*, Editorial Reppertor, Barcelona, 10ª ed., 2015.

MIRÓ LLINARES, F., "La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing", *Revista Electrónica de Ciencia Penal y Criminología*, n. 15-12, 2013, pp. 12:1-56.

MUÑOZ CONDE, F., *Derecho Penal. Parte Especial*, Tirant lo blanch, Valencia, 25ª ed., 2023.

MUÑOZ CONDE, F./GARCÍA ARÁN, M., *Derecho Penal. Parte General*, Tirant lo blanch, Valencia, 11ª ed., 2022.

PAGLIARO, A., "Concorso di norme", en *Enciclopedia del Diritto*, vol. VIII, Giuffré, Milano, 1961, p. 545-561.

PECORELLA, C., *Il diritto penale dell'informatica*, Cedam, Padova, 2ª ed., 2006.

PICA, G., *Diritto penale delle tecnologie informatiche*, Utet, Torino, 1ª ed., 1999.

PICOTTI, L., "Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati", en *Il diritto penale dell'informatica nell'epoca di Internet*, (dir. Picotti, L.), Cedam, Padova, 1ª ed., 2004, pp. 21-94.

PRIETO DEL PINO, A.M., "Criminal offences against property and against the social-economic order in Spain: a global overview and a detailed approach to some particularly relevant issues", *Philia journal of Judicial Studies*, vol. 1, 2022, pp. 82-105.

RAMESH BABU, P./LALITHA BHASKARI, D./SATYANARAYANA, CH., "A Comprehensive Analysis of Spoofing", *International Journal of Advanced Computer Science and Applications*, vol. 1, n. 6, 2010, p. 157-162.

ROMEO CASABONA, C.M., *Poder informático y seguridad jurídica*, Fundesco, Madrid, 1ª ed., 1987.

RUTGER LEUKFELDT, E./LAVORGNA, A./KLEEMANS, E.R., "Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime", *European Journal on Criminal Policy and Research*, vol. 23, n. 3, 2016, pp. 287-300.

RUTHERFORD, R., "The changing face of phishing", *Computer Fraud & Security*, n. 11, 2018, pp. 6-9.

RYAN, M., *Ransomware Revolution: The Rise of a Prodigious Cyber Threat*, Spinger, Cham, 1° ed., 2021.

SALVADORI, I., *I reati contro la riservatezza informatica*, en *Cybercrime* (dir. Cadoppi, A./Canestrari, S./Manna, A./ Papa, M.), Utet, Milano, 2ª ed., 2023, pp. 693-761.

SALVADORI, I., "Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software"", *Rivista italiana di diritto e procedura penale*, n. 2, 2017, p. 747-788.

ŠEMBERA, V./PAQUET-CLOUSTON, M./GARCIA, S./ERQUIAGA, M., "Cybercrime Specialization: An Expose of a Malicious Android Obfuscation-As-A-Service", *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2021, p. 213.

SEMINARA, S., *Il delitto tentato*, Giuffré, Milano, 1ª ed., 2012.

WEBER, A., *Die Strafbarkeit von Plattformbetreibern im Darknet*, Nomos, Baden-Baden, 1° ed., 2022.

ZAGREBELSKY, V., *Reato continuato*, Giuffré, Milano, 2ª ed., 1976.