Estudios de Deusto

Revista de Derecho Público

Vol. 71/1 enero-junio 2023

DOI: https://doi.org/10.18543/ed7112023

ESTUDIOS

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

The new regulation of fraudulent use of non-cash means of payment under the december 22nd, 2022, reform: an analysis of article 249.1 b) and 2 b) of the Spanish Criminal Code

Alfredo Abadías Selma
Profesor Contratado Doctor en Derecho penal
Universidad Internacional de La Rioja (UNIR)
Grupo investigación Penalcrim

https://doi.org/10.18543/ed.2788

Recibido: 01.02.2023
Aceptado: 13.06.2023
Publicado en línea: junio 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

The new regulation of fraudulent use of non-cash means of payment under the december 22nd, 2022, reform: an analysis of article 249.1 b) and 2 b) of the Spanish Criminal Code

Alfredo Abadías Selma[1]
Profesor Contratado Doctor en Derecho penal[2]
Universidad Internacional de La Rioja (UNIR)
Grupo investigación Penalcrim

https://doi.org/10.18543/ed.2788

Recibido: 01.02.2023
Aceptado: 13.06.2023
Publicado en línea: junio 2023

«El maquinismo, que crea abundancia, nos deja en la necesidad.
Nuestro conocimiento nos ha hecho cínicos.
Nuestra inteligencia, duros y secos.
Pensamos demasiado, sentimos muy poco»

Fragmento del discurso final de «El gran dictador» (1940)

Charles Chaplin, (1889-1977)

[1] Contacto con el autor: alfredo.abadias@unir.net / aabadiasselma@gmail.com

[2] El presente trabajo se incardina en el Proyecto: «Medidas inclusivas para menores en situación de exclusión social», con referencia ProyExcel_00514. Investigadores principales: Dr. Octavio García Pérez y Dra. Carmen Sánchez Hernández. Financiado por la Junta de Andalucía, año 2022.

Resumen

Indudablemente, nos ha tocado vivir en unos tiempos complejos y cambiantes que afectan a muchas facetas de nuestras vidas, y por supuesto a la realidad delictiva. Desde una contextualización y ejemplificación detallada de los cambios históricos que nos han llevado al momento actual, en el presente artículo pretendemos abordar la reforma del CP de 22 de diciembre de 2022, centrándonos en el art. 249.1 b) y 249.2 b), que penaliza el uso fraudulento de los medios de pago distintos del efectivo metálico, y que toma sustento en la Directiva 2019/713, de 17 de abril, del Parlamento Europeo y del Consejo, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, por la que se sustituyó la Decisión Marco 2001/413 JAI, del Consejo. La citada y necesaria reforma del delito de estafa del art. 249 CP, que entendemos que proviene de una obsolescencia causada por los avances tecnológicos raudos e imparables de los últimos tiempos, incorpora una serie de medios de pago indeterminados o abiertos «…cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos», que aperturan cierta incertidumbre en relación con la seguridad jurídica y su eficacia real en la lucha contra el delito, y por ende para el servicio a la ciudadanía, y sobre todo, para aquellos colectivos más vulnerables. Ello requiere una reflexión que toma como base la jurisprudencia y la doctrina científica más autorizada para realizar una exégesis crítica del tipo y ofrecer propuestas concretas que aquí proponemos.

Palabras clave

Uso fraudulento de tarjetas de crédito, tarjetas de débito, cheques de viaje, uso fraudulento de medios de pago.

Abstract

Undoubtedly, we have to live in complex and changing times that affect many facets of our lives, and of course the criminal reality. From a detailed contextualization and exemplification of the historical changes that have led us to the present moment. In this article we try to the reform of the CP of December 22, 2022, focusing on art. 249.1 b) and 249.2 b), which penalizes the fraudulent use of means of payment other than metallic cash, and which is based on Directive 2019/713, of April 17, of the European Parliament and of the Council, on the fight against fraud and falsification of means of payment other than cash, which replaced Framework Decision 2001/413 JHA, of the Council. The aforementioned and necessary reform of the crime of fraud of art. 249 CP, which we understand to be the result of obsolescence caused by the fast and unstoppable technological advances of recent times, incorporates a series of indeterminate or open means of payment "...any other tangible or immaterial payment instrument other than cash or the data on hand in any of them", which open up some uncertainty in relation to legal certainty and its real effectiveness in the fight against crime, and therefore for the service to the citizenry, and above all, for those most vulnerable groups. This requires a reflection that is based on jurisprudence and the most authoritative scientific

doctrine to carry out a critical exegesis of the type and offer concrete proposals that we propose here.

Keywords

Fraudulent use of credit cards, debit cards, travelers' checks, fraudulent use of means of payment.

Sumario: I. Introducción. II. El tránsito de la moneda física a la virtual. III. Estructura del artículo 249.1. B) y 249. 2 B) CP. 1. Bien jurídico protegido. 2. Acción típica. 3. Sujeto activo. 4. Sujeto pasivo. 5. Elemento subjetivo. 6. *Iter criminis*. 7. Concursos. 8. Penalidad. 9. Responsabilidad civil. IV. Conclusiones y propuestas. V. Referencias bibliográficas.

I. INTRODUCCIÓN

Nos encontramos en unos tiempos convulsos y de desarrollo exponencial que requieren de una sociedad en constante adaptación. Una situación así bien nos evoca a las teorías de Charles R. Darwin[3].

Podemos afirmar que situaciones extremas como la pandemia de la COVID-19, a pesar de encontrarnos inmersos en una era en la que hemos llegado a creer que los límites de nuestro avance se encuentran limitados exclusivamente por nuestra imaginación y voluntad, nos han recordado de la forma más amarga posible que el hombre y la mujer son en esencia frágiles, especialmente ante situaciones y escenarios que exceden nuestra capacidad de previsión y de respuesta[4]. La enfermedad, la mortalidad y la morbilidad han golpeado por doquier de forma inmisericorde al ser humano, pero con distinta afectación final, pues como es lamentablemente habitual en situaciones de gravedad, quien de más recursos dispone, mejor puede zafarse frente a los embates del infortunio en una clara muestra de lo que son las grandes diferencias que existen a nivel socioeconómico en un

[3] Ya en 1837 se hablaba de la adaptación perfecta como un argumento de explicación de la evolución con un correlato de utilidad como aquello que es beneficioso para la vida y que permite la supervivencia, a diferencia de las teorías de Lamarck, que se centraban en el ejercicio de una función que daba sentido a un órgano. Darwin daba explicación a las adaptaciones imperfectas como una herencia de antiguos actos de adaptación directa que desplazan a la adaptación imperfecta para explicar la evolución. El argumento de Darwin de la adaptación perfecta tiene una gran similitud a la de Paley, si bien en 1838 lo contextualiza en el tiempo y la adaptación se convierte en un concepto dinámico. Como bien explica Kuhn, Darwin sustituye el concepto de adaptación diferencial hasta las explicaciones de Malthus constituyendo un punto de inflexión histórico y decisivo.

[4] Según datos oficiales del Ministerio de Sanidad español, la situación con relación a la pandemia por COVID-19 en España en fecha 25 de noviembre de 2022 era la siguiente: 13.595.504 de casos confirmados notificados; 3.007.020 de casos confirmados notificados en la franja de ≥ 60 años; 115.901 casos de fallecidos notificados y 40.677.172 de españoles con pauta completa de vacunación. Datos extraídos de: Ministerio de Sanidad., Disponible en: https://www.sanidad.gob.es/profesionales/saludPublica/ccayes/alertasActual/nCov/situacionActual.htm. (Fecha de última consulta: 26 de enero de 2023).

Estudios de Deusto
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 71/1, enero-junio 2023, págs. 15-82
https://doi.org/10.18543/ed.2788 • http://www.revista-estudios.deusto.es/

orden globalizado[5]. Los colectivos más vulnerables, si cabe, todavía lo son más, precisando políticas que tiendan a paliar diferencias que no deberían existir jamás en ámbitos tan necesarios y sensibles como la salud, y es que como decía la canción «Quien nació para martillo del cielo le llueven los clavos»[6].

La crisis de la sociedad del bienestar, el *Welfare State*[7], en el marco del imperio de la *lex mercatoria*[8] y un entorno geopolítico altamente inestable, está revelando que solamente tenemos la «seguridad de lo inseguro» en un mundo que muta vertiginosamente. Los hitos acumulados durante la segunda mitad del siglo XX, que empezaban a dar forma a una humanidad que se preveía, por fin, modélica, esperanzadora, y justa, se han ido derrumbando ante la realidad inevitable de los defectos asociados a nuestra naturaleza social, que además es poco proclive a tolerar el riesgo, tal y como teorizó brillantemente

[5] Bauman advierte que es necesario romper con esa lógica de la desigualdad: en casi todas partes del mundo esta desigualdad está creciendo de forma muy rápida, y esto significa que los ricos cada vez son mucho más ricos, mientras que los pobres, y especialmente los muy pobres, son cada vez más pobres (en su mayor parte en términos relativos, pero, en cada vez un mayor número de casos, en términos absolutos). *Vid*. BAUMAN, Z., *¿La riqueza de unos pocos nos beneficia a todos?* (Traducción de Alicia Capel Tatjer). Paidós Estado y Sociedad, Barcelona, 2014, p. 22.

[6] Este refrán fue cantado por Rubén Blades en el tema «Pedro Navaja» y más tarde se popularizó con la Orquesta Platería. Los «clavos» nos llevan a pensar en los problemas que aparecen de manera constante máxime cuando se trata de personas desasistidas u olvidadas por la fortuna.

[7] El sociólogo británico Thomas H. Marshall describió el estado de bienestar moderno como una combinación que es propia de un estado democrático en el que predomina el bienestar social dentro de un marco socioeconómico capitalista, eso es de economía de mercado. Sin embargo, de todos es sabido que el capitalismo, como todo modelo socioeconómico, tiene sus fallos y defectos sistémicos, que en este caso afectan sobremanera a los colectivos más vulnerables. Además, en los últimos tiempos el estado de bienestar, que intentaba cubrir la mayoría de las necesidades de la población, está muy desprestigiado por la elevada presión fiscal, la mala gestión pública de los recursos y la corrupción. *Vid*. MARSHALL, T. H., *Citizenship and social class, and other essays*, Cambridge University Press, Londres, 1950.

[8] Se trata de la *Lex Mercatoria* a la que se refiere Terradillos Basoco, cuando plantea que en el contexto actual existe un sustrato natural de búsqueda de la rentabilidad más alta, inmediata, deslocalizada y ajena a todo control público, pues los instrumentos de regulación quedan en manos de sujetos privados que mueven el mercado siempre para obtener lo máximo en detrimento de la protección de los derechos fundamentales del ciudadano. En este punto el autor hace referencia a que cada vez más situaciones quedan fuera de la capacidad normativa de los Estados tanto por cuestiones de forma, como la transferencia de competencias a organizaciones supranacionales e internacionales, como fácticas. Así las cosas, el apoyo constitucional a los derechos fundamentales queda debilitado por los recortes de impuestos y las políticas de austeridad en un nuevo orden económico mundial. *Vid*. Terradillos Basoco, J.M.ª, *Aporofobia y plutofilia: la deriva jánica de la política criminal contemporánea*, Bosch, Barcelona, 2020, pp. 28 y 29.

Ulrich Beck a quien tantos penalistas de nuestra tradición jurídica actual deben parte de sus planteamientos de corte sociológico.

Las relaciones interpersonales se han instalado en la llamada «Modernidad líquida» a la que hace referencia BAUMAN[9], una sociedad en la que lo perecedero y lo transitorio se impone, donde impera el individualismo, la falta de solidaridad y empatía en el contexto de un liberalismo exacerbado y malinterpretado con incesantes privatizaciones que dejan al hombre y a la mujer sin un horizonte claro hacia dónde dirigir sus vidas. Yendo más al extremo y en alusión al concepto antedicho, ALBERTO ROYO[10] y URRA PORTILLO[11] hablan de «sociedad gaseosa». Se trata de una «Modernidad tardía» a la que se alude BENITO SÁNCHEZ[12], donde las relaciones laborales tienden a la externalización[13], la deslocalización, la gentrificación[14], la exclusión y la nueva pobreza urbana.

Estamos ante la cultura de la inmediatez, de la falta del suficiente sosiego para reflexionar y meditar si nos conviene una decisión u otra. Se trata de lo que venimos a denominar «*Culture touch*»[15], una cultura que persigue mediante

[9] BAUMAN, Z., *Modernidad líquida*, Fondo de cultura económica, México, 2009, *passim*.

[10] ALBERTO ROYO, A., *La sociedad gaseosa*, Tusquets, Barcelona, 2009, *passim*.

[11] URRA PORTILLO, J., *El pequeño dictador crece: padres e hijos en conflicto*, La Esfera de los libros, Madrid, 2015, *passim*.

[12] BENITO SÁNCHEZ, D., «Exclusión social y gobierno de la pena. Un análisis sobre la legitimidad de la producción penal de la exclusión», BENITO SÁNCHEZ, D. y GÓMEZ LANZ, J. (Dirs.), VV.AA., *Sistema penal y exclusión social,* Aranzadi, Pamplona, 2020, p. 21.

[13] Sobre este fenómeno puede verse LESSENICH, S., *La sociedad de la externalización*, Herder, Barcelona, 2019, p. 51.

[14] Término que procede del inglés, *gentry* = burgués, como un proceso de transformación urbana en el que la población original de un barrio popular se ve desplazada por nuevos vecinos de mayor poder adquisitivo. Esta aparentemente sencilla definición esconde un complejo proceso de reestructuración del espacio urbano con múltiples consecuencias con efectos muy distintos en ciudades y barrios que siempre afecta de forma negativa a los colectivos más vulnerables. Son varios los estudiosos que se han acercado al análisis de este fenómeno desde diversos campos del saber, como la historia, la sociología, la arquitectura, el urbanismo, etc.

La elevación desmesurada del precio de los bienes inmuebles que se ha producido de forma incesante ya desde la década de los 70 y ahora con la compra masiva de grandes fondos inmobiliarios, también denominados «fondos buitre», ha generado que se expulse a la gente del barrio de toda la vida y se vayan construyendo o reformando edificios que uniformizan el paisaje urbanístico con grandes cadenas comerciales, como si realmente se tratase de una perfecta clonación que diluye el encanto original y distintivo de muchas ciudades. Malasaña o Chueca en Madrid y el Raval (eufemismo del antiguo barrio chino) son un claro ejemplo de lo que aquí se explica. Sobre el fenómeno de la gentrificación puede verse entre otros KERN, L., *La gentrificación es inevitable y otras mentiras*, Bellaterra, Barcelona, 2022 y SEQUERA FERNÁNDEZ, J., *Gentrificación: Capitalismo cool, turismo y control del espacio urbano*, Los libros de la catarata, Madrid, 2020.

[15] Término acuñado por ABADÍAS SELMA en ABADÍAS SELMA, A., *Justicia juvenil e inteligencia artificial en la era de la cultura «touch»*, Tirant lo Blanch, Valencia, 2022, *passim*.

el leve deslizar de las yemas de nuestros dedos por una pantalla táctil que se pueda acceder y conseguir todo lo que se desea sin aparente esfuerzo y con la máxima celeridad. Se puede comprar y vender todo o casi todo a través de estos terminales táctiles a los que les podemos pedir desde una comida *take away* hasta un crédito de una entidad financiera preconcedido por sofisticados algoritmos que nos perfilan con cada vez mayor precisión llevándonos quizás hacia una «Nada»[16] que describía de forma magistral Carmen Laforet.

Uno de los elementos o conceptos técnicos que vehiculan esta nueva realidad son las denominadas «aplicaciones informáticas», también conocidas como *Apps*. Las *Apps* son algo totalmente cotidiano: si deseamos comida rápida, ropa o cualquier «gadget» que llegue a la puerta de nuestros hogares, no importa que sea festivo, llueva, caiga nieve o luzca un sol asfixiante, pues un *rider* –posiblemente en el futuro próximo será un 'simple' dron– de grandes compañías como Amazon (que acaba de anunciar que despedirá aproximadamente a 18.000 empleados)[17] hará que nuestros anhelos se conviertan en realidad en tiempo cada vez más récord[18].

[16] *Nada,* de la autora barcelonesa Carmen Laforet, está considerada una de las cien mejores novelas en español del siglo XX, y la traemos a colación porque la autora describía desde un punto de vista impresionista un antes y un después de la España de la Guerra civil española. Hoy en día, también estamos viviendo una serie de «antes y después», como pueden ser hitos históricos como la caída del Muro de Berlín, el hundimiento de las Torres gemelas en pleno corazón del imperio norteamericano, la pandemia mundial de la COVID-19, la guerra de Ucrania, la hiperinflación galopante y el reto de la sostenibilidad de los recursos del planeta, etc. No vivimos un antes y un después, sino varios, que nos sumergen en una constante situación de inseguridad a todos los niveles. *Vid*. Laforet Díaz, C., *Nada*, Ediciones Destino, Barcelona, 1969.

[17] Agreda, M., «Amazon se suma a los despidos masivos, 18 mil trabajadores se quedarán sin empleo», en MSV. Disponible en: https://mvsnoticias.com/mundo/2023/1/5/amazon-se-suma-los-despidos-masivos-18-mil-trabajadores-se-quedaran-sin-empleo-578594.html. (Fecha de última consulta: 5 de enero de 2023). Entre las grandes multinacionales lamentablemente los despidos en estos tiempos se suceden, como en el caso de Twitter, que despide al 83% de su plantilla en España (*Vid*. Díaz Guijarro, R. «Twitter despide al 83% de su plantilla en España», en *Cinco días*, disponible en: https://cincodias.elpais.com/cincodias/2023/01/24/companias/1674591010_214512.html. (Fecha de última consulta: 28 de enero de 2023). Por su parte, la pionera y gigante de la informática IBM anuncia 3.900 despidos, en un panorama realmente desolador. *Vid*. al respecto Expansión.com., «IBM anuncia 3.900 despidos tras ganar un 71% menos en 2022», disponible en: https://www.expansion.com/economia-digital/companias/2023/01/26/63d29e27e5fdeace7a8b45ef.html., (Fecha de última consulta: 26 de enero de 2023). En esta noticia se afirma que «International Business Machines (IBM) registró un beneficio neto de 1.639 millones de dólares (1.504 millones de euros) en 2022, lo que supone una caída del 71,5% respecto del resultado del año anterior ante el impacto del acuerdo sobre pensiones alcanzado en el tercer trimestre por la compañía, que recortará 3.900 puestos de trabajo, alrededor del 1,5% de su plantilla».

[18] Sobre la explotación laboral puede verse el interesantísimo artículo de Gil Nobajas, en Gil Nobajas, M.ª S., «Respuesta penal a la criminalidad empresarial en supuestos

Con esa leve caricia de nuestros dedos por una pantalla táctil también podremos conocer y saber de todo, o al menos así nos lo hacen creer, sumergidos en un mar de información desorganizada, manipulada y sin filtro, en una «infoxicación»[19] que nos ilustra para aparentar que somos falsamente doctos en las más variadas y dispares disciplinas.

Vivimos «Deprisa deprisa»[20], y acéptese la premeditada repetición para recordar aquel ya mítico filme de los atrevidos y descarados ochenta de la Transición que narraba el desenfreno, lo desaforado que es el paso por esta vida si no tenemos unos cimientos sólidos con los que sustentar nuestra existencia dirigida hacia bienes impregnados de nobleza y bondad.

«*Big data*», «*blockchain*», «criptomonedas», inteligencia artificial, etc. son términos que expresan la constante evolución de las tecnologías que han entrado en nuestras vidas en las últimas décadas, primero a través de los videojuegos, y ya con un empuje final forzado durante la pandemia de la COVID-19 y el obligado confinamiento, manifestándose una «brecha digital»[21] que ha

de explotación laboral», en Benito Sánchez, D. y Gómez Lanz, J. (Dirs.), VV.AA., *Sistema penal y exclusión social,* Aranzadi, Pamplona, 2020, p. 176, donde la autora destaca que «la protección primaria de las condiciones laborales en el marco de una prestación de trabajo frente a un eventual abuso por parte del empleador, no la ofrece el derecho penal, sino el orden social. La regulación penal otorga una protección reforzada, con los problemas que conlleva en ocasiones delimitar la frontera entre lo que constituye una infracción social y un ilícito penal».

[19] Se trata de un término acuñado por Alfons Comella en 1996 con origen en Internet, que se equipara con el término inglés *Overload Information*. La infoxicación describe una situación en la que disponemos de grandes cantidades de información que, en la mayoría de las ocasiones, nos llega desorganizada y que puede generar una angustia por la sobreabundancia de datos que están a nuestro alcance a golpe de un solo clic. Esto puede generar angustia, nerviosismo y malestar, por miedo a perderse algo de los *inputs* que nos llegan, y que en algún momento pudieran llegar a ser importantes. Asimismo, esta ingente cantidad de datos que tenemos a nuestro alcance puede generar un bloqueo mental. Puede verse sobre este concepto a Comella Solans, A., «Ignorancia profunda, ignorancia conocedora e internet», *El profesional de la información*, Vol. 8, n.º. 4, 1999, p. 37; asimismo es de interés Martínez Cañadas, E., *El mito de la infoxicación,* UOC, Barcelona, 2021, *passim*.

[20] *Deprisa, deprisa,* es un filme español dirigido por Carlos Saura en 1981. Cuenta la historia de una banda de delincuentes juveniles, cuatro amigos del extrarradio madrileño de la Transición, cuya falta de expectativas es suplida por el dinero fácil y las drogas. La película ganó el Oso de oro a la mejor película en 1981 en el Festival Internacional de Cine de Berlín.

[21] El concepto de brecha digital no tiene una definición única y aceptada universalmente. Este término hace referencia a la desigualdad en el acceso, uso o impacto de las Tecnologías de la Información y la Comunicación (TIC) entre grupos sociales. Estos grupos se suelen determinar tomando como base criterios económicos, geográficos, de género, de edad o culturales. Entre los diferentes tipos de brecha digital que existen, la brecha digital de acceso es una de las más habituales. Se refiere a las posibilidades que las personas tienen de acceder a este recurso. Aquí entran en juego las diferencias socioeco-

acrecentado las diferencias sociales y el «analfabetismo informático» en el que se encuentran desprotegidos colectivos vulnerables, y es aquí cuando recordamos a PRENSKY[22] que alude a los nativos e inmigrantes digitales.

«Globalización» o «Mundialización»[23], «Aldea global»[24], «Cuarta revolución industrial», «Era digital», o el término procedente del mundo de las

nómicas entre las personas y los países. El otro tipo más común es el de la brecha de uso, que hace referencia a la falta de competencias digitales que impide el manejo de la tecnología. Según la Unión Internacional de Telecomunicaciones (UIT), el organismo especializado de la Organización de las Naciones Unidas (ONU), a finales de 2019 había 40 países en los que más de la mitad de su población no sabía adjuntar un archivo a un correo electrónico. La «brecha digital» también la sufre el colectivo de personas que padecen una discapacidad, como bien indica PRADOS GARCÍA, que asevera que durante la pandemia se incrementó la problemática de la accesibilidad a las nuevas tecnologías para este colectivo, puesto que ya partían de una desigualdad preexistente, siendo preciso garantizar una sociedad inclusiva. En relación con esta problemática el Observatorio Estatal de la Discapacidad puso de relieve que se han incrementado de forma considerable las barreras entre este colectivo y el acceso a la información. *Vid.* PRADOS GARCÍA, C., *et al.* pp. *45-64* y OBSERVATORIO DE LA DISCAPACIDAD., disponible en: https://www.observatoriodeladiscapacidad.info/ (Fecha de última consulta: 12 de enero de 2023).

[22] Marc Prensky fundó y es director de Games2train, empresa que se dedica a fomentar el aprendizaje basado en el juego. También fundó The Digital Multiplier, corporación dedicada a paliar y/o eliminar la brecha digital existente hoy en día entre generaciones. Puede verse entre otros, PRENSKY, M., *Enseñar a nativos digitales,* Ediciones SM, Madrid, 2011, *passim*.

[23] La Globalización, también denominada «Mundialización» es todo un proceso de carácter económico, tecnológico, político, social y cultural del que se ha hablado mucho y que viene a explicar una cada vez más intensa interrelación e interdependencia multinivel que se ha visto acelerada por las TIC en favor de un sistema económico más liberal favorecedor de grandes multinacionales y fondos de inversión. Además, si a este panorama añadimos el creciente fenómeno de las criptomonedas, que ya se utilizan masivamente sin controles gubernamentales firmes y seguros (nótese que, a la fecha de redacción del presente artículo, el así denominado Reglamento Mica, pretende dar una regulación integral en lo relativo a los emisores de criptoactivos, plataformas de intercambio y las criptomonedas con intención de armonización de la legislación en todos los Estados Miembros de la Unión Europea, se encuentra aún pendiente de aprobación) nos encontramos en una nueva era marcada por unas nuevas relaciones económicas que han de ser supervisadas, o al menos así lo entendemos, por los diferentes estados en aras de conseguir que exista una distribución equitativa de la riqueza y no se acrecienten las diferencias socioeconómicas que acechan a colectivos vulnerables, como pueden ser los menores y/o jóvenes, que intentan labrarse un porvenir cuando por ejemplo los alquileres de las viviendas están batiendo récords históricos y las políticas públicas de promoción del derecho no fundamental a la vivienda, se están revelando insuficientes. Así las cosas, se requiere con premura que el Derecho se articule a nivel global y de forma efectiva mediante grandes pactos en favor del humanismo, que parece haberse olvidado. Sobre el asunto puede verse *ad exemplum* a STIGLITZ en STIGLITZ, J.E., (Trad. PRADERA SÁNCHEZ, A.) *El precio de la desigualdad,* De bolsillo, Madrid, 2015, *passim*.

[24] El término fue acuñado por el sociólogo canadiense Marshall McLuhan (1911-1980) y aparece en diversas ocasiones en títulos como *La aldea global* y *La guerra y la paz en la aldea*

gigantescas corporaciones como «Meta», de donde proviene «Metaverso»[25] entre otros, intentan dar explicación a la realidad y/o virtualidad que nos circunda, con faz poliédrica, multifactorial y dinámica que nos interrelaciona en la distancia, y a la que como vemos, se le busca una etiqueta con más o menos fortuna desde distintas ramas del saber.

II. EL TRÁNSITO DE LA MONEDA FÍSICA A LA VIRTUAL

En este contexto cada vez más inmaterial e inmediato, la moneda física y su utilización como medio de pago va perdiendo protagonismo en favor de las tarjetas de crédito y débito, con distintos tipos de formato cada vez más

global. Este término se refiere a las consecuencias socioculturales de un tipo de comunicación que se propaga a nivel mundial de forma prácticamente inmediata, viéndose acelerado este fenómeno mediante las potentes redes que transportan ingentes cantidades de datos a unas velocidades nunca imaginadas. Se hace referencia a que vivimos hechos que nos afectan como si fueran cotidianos y muy cercanos cuando en realidad están sucediendo a grandes distancias espacio-temporales, hechos que nos informan de datos que ni tan solo hemos elegido entre infinitos contenidos. Al albur de los tiempos podemos afirmar que McLuhan fue un verdadero visionario, pues cuando falleció en 1980 la informática solo estaba al alcance de gobiernos y grandes corporaciones, e Internet tan solo existía para usos estrictamente militares.

[25] Metaverso, proviene del nombre Meta (procede del mismo término griego μετά, que significa «más allá de» o «después de»), que es la nueva denominación que ha adoptado Marc Zuckerberg para Facebook. De este nuevo nombre surge Metaverso como un concepto que comprende el mundo virtual en el que Google, Microsoft, Nvidia, entre otras corporaciones han apostado muy fuerte con sus activos para comercializar a diversos niveles un mundo virtual con grandes posibilidades de expansión. Las gafas que permiten viajar en la virtualidad son solo un ejemplo entiendo muy iniciático sobre lo que apunta este fenómeno. Sin embargo, no todo son buenos augurios para esta realidad virtual, pues el 29 de noviembre de 2022, a las 21:00 h, la Unión Europea organizó una fiesta para la Comisión Europea en el Metaverso a la cual solo asistieron seis personas. Este evento fue financiado con el dinero de los contribuyentes, obtuvo una visualización del evento de 44 personas y asistieron solamente 6. Se trataba de un metaverso desarrollado por Meta, que al conectarse solicitaba pocos datos, un nombre y apellido y el usuario de la red social Instagram. El anuncio se hizo público en la página del Metaverso Global Gateway. Para poder celebrar esta fiesta digital se gastaron alrededor de 387.000 euros en concepto del pago a Meta por haber desarrollado el espacio virtual, que, si bien es muy conocido por los jóvenes para las redes sociales, es muy desconocido en referencia con la labor de las instituciones. El proyecto fue presentado por la UE mediante Úrsula Von der Leyen para conseguir nuevas infraestructuras en países que están en vías de desarrollo. Todo y el fracaso de este evento, la UE tiene previsto invertir 300,000 millones de euros para engrandecer las infraestructuras en otros países con una fecha límite de 2027 para el desarrollo de estas plataformas. *Vid*. Jiménez Bravo, R., «La Unión Europea gastó casi 400,000 euros en una fiesta programada en el metaverso y tuvo solamente 6 asistentes», Cointelegraph, disponible en: https://es.cointelegraph.com/news/the-european-union-spent-nearly-400-000-euros-on-a-party-scheduled-in-the-metaverse-and-had-only-6-attendees, (Fecha de última consulta: 7 de diciembre de 2022).

cómodos para el usuario, de uso inmediato y proclive a la utilización irreflexiva, como el *Contactless*[26], que no solamente puede utilizarse con las tarjetas tradicionales, sino que cada vez con mayor frecuencia se gestiona con un terminal de teléfono o un reloj tipo *smartwatch*.

La forma de pago mediante las tarjetas de crédito y/o débito es algo tan usual que ya en la mayoría de los comercios no se requiere ni un mínimo importe para el pago, y se utiliza para abonar incluso un sencillo café o una barra de pan. Esta comodidad puede comportar que alguien se haga con una tarjeta que no es la suya y realice pagos inferiores a los veinte euros (este importe se elevó en la mayoría de las entidades a los cincuenta euros durante el periodo de confinamiento de la COVID-19 para evitar al máximo el contacto físico, y por ende el contagio), establecidos como límite para comprar sin marcar el PIN de seguridad.

Esta sencillez de uso, sin embargo, también tiene peligros que pueden favorecer la criminalidad mediante la clonación o la suplantación de identidad, entre otras formas delictivas.

BECK describió a la nueva «Sociedad del riesgo» situada en una era postindustrial donde la humanidad dispone de una serie de avances tecnológicos de gran relieve que van a permitir disfrutar de un nivel de bienestar que nunca se había vivido. Por contra, el mismo autor apunta que esta sociedad inmersa en un riesgo permanente tiene peligros ilimitados desde el punto de vista espacial, temporal y social quebrando las tradicionales reglas de la imputabilidad en relación con la causalidad y la responsabilidad, en un marco donde los riesgos no pueden ser asegurados ni compensados[27].

[26] El sistema *contactless* incorpora una tecnología de comunicación inalámbrica que funciona en un radio de acción muy corto. Así, el pago se realiza al situar la tarjeta sobre un datáfono, sin necesidad de introducirla en el TPV o pasarla por el lector de banda. Si bien se trata de un sistema cómodo, también ofrece el peligro consistente en que sea más sencillo el captar la información de la banda magnética por parte de los delincuentes cibernéticos, pues se ha demostrado que puede realizarse, por ejemplo, traspasándose las paredes de un bolso o un billetero, aunque sea algo nada sencillo. Esto es posible ya que las tarjetas con el sistema *contactless* utilizan NFC (*Near Field Communication*), que es la misma tecnología que disponen los móviles para llevar a cabo algunas comunicaciones entre sí. Se trata de una especie de «*Bluetooth*», pero con una distancia bastante menor. Este tipo de sistema de transmisión inalámbrica sirve para poder identificarnos y efectuar pagos siempre que exista un terminal compatible con esta tecnología. Cada una de las tarjetas que sean compatibles con el *contactless* tiene en su parte interior una antena NFC que no puede verse a simple vista porque es muy fina. Esta permitirá que se inicie la comunicación con el TPV y así poder efectuar pagos. No hemos de confundir este sistema con el chip visible que disponen algunas tarjetas (EMV cuyo nombre proviene de sus fundadores: Europay, MasterCard y Visa) y que tiende a la desaparición.

[27] Beck, U., *La sociedad del riesgo: hacia una nueva modernidad*, Editorial Planeta, Barcelona, 1998, págs., 19 y ss.

Los avances tecnológicos y el bienestar social de la sociedad en la que vivimos podemos afirmar que tienen una doble cara cual dios Jano[28], con bondades y peligros que podrán afectar a gran cantidad de ciudadanos, algunos de estos constituyendo colectivos altamente vulnerables, como pueden ser las personas de edad avanzada y los menores.

El imparable crecimiento de la utilización de Internet, su utilización masiva y doméstica como algo totalmente cotidiano que está al alcance de cualquier persona y cada vez en edades más tempranas, hace que el legislador deba proteger sobre todo a los intereses de quienes son más débiles ante, por ejemplo, ciertos usos del *blockchain*, las criptomonedas, o distintas formas de pago como por ejemplo el exitoso Bizum, que empezó como un medio de pago para pequeñas cantidades destinadas a regalos de fiestas de cumpleaños y que se ha extendido de forma exponencial llegando a ser la aplicación móvil más utilizada para realizar pequeñas transacciones, superando ya los 20 millones de usuarios en todo el mundo. El principal problema que tiene este tipo de transferencias bancarias es la inmediatez y que no tiene retorno. Con introducir un número de teléfono móvil o de cuenta bancaria del destinatario a quien queremos transferir un importe de dinero es suficiente, y son muchos los errores que pueden cometerse en esta simple operación si se realiza de forma precipitada. Se recomienda realizar estas transacciones con suficiente sosiego comprobando muy bien la numeración, porque si existe una equivocación de destinatario solamente cabe contactar con este y solicitarle la devolución explicando que se ha tratado de un error, y si no accede a la devolución se debería recurrir a un procedimiento judicial para la recuperación del importe, que a veces no resultará práctico ni rentable por la escasa cuantía que normalmente se maneja.

En la década de los ochenta la informática comenzaba a entrar con fuerza en los hogares de todos los españoles mediante consolas tipo Spectrum, evidentemente sin conexión a ninguna red, pero ya fue un paso muy importante para el uso doméstico y la democratización de las tecnologías. En esta misma década Ramos Portero[29] ya empezaba a hablar de «delito informático», y asimismo también lo hacía Davara Rodríguez[30] cuando indicaba que la acción delictiva cometida mediante la informática recoge las características

[28] Jano es representado con dos caras, mirando hacia ambos lados de su perfil, y no tiene parangón en la mitología griega. Al igual que Prometeo, Jano es un tipo de héroe cultural, ya que se le atribuye entre otras cosas la invención del dinero, la navegación y la agricultura. *Vid*. Martín, R., *Diccionario de la mitología clásica*, Espasa Calpe, México, 1998, *passim*.

[29] Ramos Portero, R., «Los delitos informáticos», en *Revista Latinoamericana de Derecho Penal y Criminología*, n.º 6, 1989, págs.176 y ss.

[30] Davara Rodríguez, M.Á., *Derecho Informático*, Editorial Aranzadi, Pamplona, 1993, p. 302.

que delimitan el concepto de delito cuando se haya llevado a cabo utilizando un elemento informático vulnerando los derechos del titular, ya sea mediante *hardware* o *software*.

Por su parte Romeo Casabona[31] señalaba que, si acudimos al significado prístino del concepto, no se puede hablar de delito informático y sí de una serie de delitos que tienen como denominador común el hecho de haber sido cometidos mediante ordenadores.

En este orden de cosas, cabe destacar que en el Código Penal no existe una categoría específica de «delito informático»[32] *per se*, si bien es notorio que hay un ámbito criminal caracterizado por utilizar medios informáticos con una cibercriminalidad muy cambiante, especializada y transnacional. De hecho, una de las grandes cuestiones de la dogmática penal en el ámbito de la ciberdelincuencia es, precisamente, la conceptualización de cada *nomen iuris* utilizado en este campo del conocimiento jurídico y sus consecuencias sistemáticas e interpretativas.

III. ESTRUCTURA DEL ARTÍCULO 249.1. B) Y 249.2 B) CP

1. *Bien jurídico protegido*

Este tipo penal protege el patrimonio[33], y el objeto de la acción, puesto que es una estafa, viene constituido por cualquier activo patrimonial que el sujeto activo consiga transferir dentro de la esfera de su poder, pudiendo ser bienes muebles o inmuebles, derechos o servicios.

El activo patrimonial está constituido por el conjunto de bienes, inversiones y derechos de propiedad. Se trata de aquellos bienes e inversiones adquiridos que se mantienen en movimiento y fácilmente se pueden convertir en dinero. Asimismo, dentro de este concepto podemos incluir todo aquello que

[31] Romeo Casabona, C., «De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal», en AA.VV. (Coord. Romeo Casabona, C.)., *El cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Editorial Comares, Granada, 2006, p. 8.

[32] Con el despunte de las computadoras personales, en la década de los 80, comienza a utilizarse el término «delincuencia informática», para referirse «[al] abuso de medios informáticos con fines delictivos». Concepto que no debe confundirse con el de «ciberdelincuencia», de más reciente aparición. Pérez López, X., «Introducción», en: Fernández Bermejo, D. (Dir.), *Blanqueo de Capitales y TIC: Marco Jurídico Nacional y Europeo, Modus Operandi y Criptomonedas. Ciberlaundry. Informe de situación*., Aranzadi, Pamplona, 2019, p. 11.

[33] La doctrina mayoritaria entiende este término en su ámbito económico-jurídico y no meramente personal, comprendiendo, a la postre, aquellos bienes susceptibles de contenido económico a los que les sea otorgado reconocimiento por el Ordenamiento Jurídico. Gallego Soler, J.I., *Op. cit.*, p. 856.

tiene un valor en el mercado y que pueda convertirse en dinero, que podrá ser contable o documental, el crédito y la obtención de servicios, siempre que no se trate de objetos que puedan tener su propio tratamiento penal, como podría ser el caso de los secretos industriales.

Como hemos indicado anteriormente, el engaño es un elemento fundamental del presente delito y es por lo que, entendemos que no solamente se protege el patrimonio, sino también la buena fe o las relaciones de confianza que han de regir con normalidad el tráfico jurídico.

2. *Acción típica*

Ya en la época de más esplendor del derecho romano la estafa tuvo la denominación de *Crimen stellionatus,* un crimen en el que se recogían conductas punibles muy variadas y donde existía una imprecisión jurídica considerable. Tal y como señaló Quintano Ripollés[34]: «indica bien a las claras la imprecisión de su naturaleza, variable e indecisa cual la del saurio[35], del cual tomó por eso el nombre». El Estelionato en aquel momento histórico era verdaderamente un cajón de sastre para delitos que no tenían ni tan solo denominación.

El tipo penal que aquí comentamos recoge el concepto de estafa[36], que entró a formar parte de nuestra legislación en la reforma del CP de 1983, acogiendo las tesis del maestro Antón Oneca[37] de 1958 que disponía de unánime acuerdo doctrinal en el sentido de considerar que los elementos de la acción típica son: el engaño idóneo o bastante para generar el error de otro, el desplazamiento patrimonial y un perjuicio económico en el patrimonio de quien es estafado o de un tercero.

Las estafas pueden adoptar múltiples formas, desde el popular «Tocomocho»[38], pasando por el «El nazareno»[39] o el «Timo de la

[34] Quintano Ripollés, A., *Tratado de la Parte Especial del Derecho penal*, en *Revista de Derecho privado,* Madrid, 1977, Tomo II, pp. 562 y ss.

[35] Esa referencia a un «saurio» –que algunos autores han vinculado metafóricamente con el camaleón para justificar el «carácter camaleónico» del Estelionato– podría tener su origen en una segunda acepción del término latino *Stellio*, que significa lagarto.

[36] Sobre el término «Estafa», véase Antón Oneca, J., «Voz "Estafa"», *Nueva Enciclopedia Jurídica*, Seix, Barcelona, 1958, págs., 56 y ss.

[37] Antón Oneca, J. y Rodríguez Muñoz, J.A., *Derecho penal Parte especial*, tomo – II, Reus, Madrid, 1949, *passim*.

[38] Según el Diccionario de la RAE: Timo cometido con un billete de lotería falso con el que se estafa a alguien vendiéndoselo o intentando vendérselo como premiado, a un precio inferior al de su premio. Disponible en: https://dle.rae.es/tocomocho?m=form. (Fecha de última consulta:1 de febrero de 2023).

[39] El Nazareno, es una de las estafas más conocidas en España que, como otros delitos, se ha transformado y adaptado al entorno tecnológico. Principalmente, los estafadores

estampita»[40] que popularizó el mítico Tony Leblanc[41], llegando a nuestros días con una serie de engaños que se cometen a través de las redes y medios informáticos como: las promesas de beneficios estratosféricos en poco tiempo con una mínima inversión inicial en productos de «dietas milagrosas», «sea su jefe trabajando desde casa», «introduzca los datos de su tarjeta de crédito y/o débito para comprobar su seguridad –desde una *interface* clonada de una entidad financiera»–, invierta en apuestas deportivas, invierta en criptomonedas, etc. Todo ello sin olvidar las muy bien

centran su actividad delictiva en empresas suministradoras de productos de fácil salida el mercado negro, como electrodomésticos, material informático, bebidas alcohólicas... «en general productos de primera necesidad». Los estafadores, conocidos en el argot como nazarenos, se ganan la confianza de la empresa proveedora basándose en técnicas de ingeniería social. Así, los ciberdelincuentes, logran comprometer el «eslabón más débil» de la seguridad en los entornos digitales, «que siguen siendo las personas». Para generar confianza, el estafador ofrece como fachada estar representando a una empresa de apariencia solvente y de reconocido prestigio, de la que aporta todos los documentos necesarios y que previamente han sido falsificados. Después de una primera compra, que pacta pagar con letras de cambio o medios similares siempre con la intención de ganar tiempo para que la estafa se descubra lo más tarde posible, suele intentar una segunda compra en similares condiciones que la anterior. Existen varias recomendaciones para evitar a los nazarenos, dado que la mayoría de los fraudes son cometidos exclusivamente en entornos digitales, sin participación física de persona alguna, donde se crea un entorno ficticio de apariencia creíble. *Vid*. STS 1015/2013, de 23 de diciembre.

[40] El timo de la estampita es una estafa muy antigua y conocida por el público general. El timo discurre de la siguiente forma: La víctima (o 'primo' en la jerga de los truhanes), es abordada en la calle cuando está sola, por un estafador que hace el papel de 'tonto'. Normalmente le pregunta dónde está un colegio o una iglesia (así ha ocurrido en el último caso en la capital del Jerte) y le enseña un paquete o un sobre con un fajo de billetes. En ese momento le dice que son estampitas como las antiguas de los santos, que son todas iguales, llegando en ocasiones a romper un billete delante de él para hacer ver la poca importancia que da a los supuestos billetes. Es entonces cuando aparece el otro estafador, 'el listo', que al ver el dinero le propone a la víctima ir a medias, quedándose con el paquete lleno de billetes a cambio de darle al 'tonto' algo para no dejarle desvalido. El estafador 'listo' pone su parte y al preguntarle a la víctima qué aporta, da el dinero que tenga encima y las joyas. Si no tiene nada encima, le llevan a su casa a por dinero o joyas y al banco. Para realizar este desplazamiento el 'listo' siempre suele tener su coche cerca. Una vez que los estafadores tienen el botín, el 'listo' se ofrece a llevar al 'tonto' en su coche al colegio o a la iglesia a la que iba, mientras le pide al 'primo' que le espere en la calle o en un bar con el paquete. Los estafadores se van y no vuelven, y cuando el 'primo' se dispone a ver su tesoro se da cuenta del engaño, al ver el abultado fajo de dinero son solo papeles. *Vid*. STS 124/2014.

[41] Un cartel de lujo que contó con: Tony Leblanc, Concha Velasco, Antonio Ozores, Laura Valenzuela, Juan Calvo, Antonio Riquelme, José Luis López Vázquez, Manolo Gómez Bur, Jesús Puente, José María Tasso, entre otros, protagonizaron en 1959 el filme «Los tramposos», donde Paco y Virgilio encarnaban a dos golfos madrileños que vivían del timo en todas sus variantes: desde el «Timo de la estampita» al «Tocomocho». Este filme de gran éxito fue dirigido por Pedro Lazaga con guión de José Luis Dibildos.

elaboradas estafas piramidales[42] estilo Ponzi[43] como la que protagonizó Bernard Madoff[44] en EE. UU. y las estafas sufridas por miles de ciudadanos/as en España, en los casos Afinsa[45] y Fórum Filatélico[46].

Es evidente que los tiempos han cambiado, y el ordenamiento jurídico penal español, ya sea en su vertiente sustantiva y/o adjetiva se construyó con

[42] Sobre las estafas piramidales, *Vid.* Fernández-Salinero San Martín, M.A., *Las estafas piramidales y su trascendencia jurídico penal*, Dykinson, Madrid, 2019, p. 19. Fernández-Salinero San Martín afirma que al no existir en el CP español una definición de lo que es jurídicamente una estafa «piramidal», deviene necesario acudir a la interpretación jurisprudencial y cita la Sentencia de la Audiencia Nacional de 9 de marzo de 2017, que ofrece en su Fundamento de Derecho cuarto una definición clara y concisa.

[43] El nombre proviene de Charles Ponzi que, en Estados Unidos, en la década de 1920, acumuló una gran fortuna utilizando el arbitraje legítimo de cupones de respuesta internacionales para sellos postales que después desviaba desde los inversionistas para abonar a otros inversionistas anteriores. Este esquema de estafa piramidal está basado en la confianza de quien recomienda el producto que supuestamente generará pingües beneficios, y todo funciona sin ningún problema hasta que un número importante de inversionistas decide recuperar el dinero, produciéndose entonces el colapso.

[44] El fraude que perpetró Bernard Madoff llegó a alcanzar los 64.800 millones de dólares, hecho que le convirtió en la persona que había perpetrado el mayor fraude de la historia. En junio de 2009 fue sentenciado a cadena perpetua *de facto*, pues la sentencia era de 150 años de prisión, el máximo que admitía el caso. Madoff falleció en prisión de muerte natural en abril de 2021.

[45] AFINSA fue un grupo empresarial español que invertía mayormente en numismática y otros bienes tangibles. Este grupo operaba en diversos mercados de Europa, Asia y Estados Unidos de Norteamérica. Tenía sucursales en: Barcelona, Vigo, Valladolid, Lisboa, Londres y París. En 2004 llegó a tener un centenar de sucursales, unos 2600 empleados, y contaba con 143.000 clientes. El volumen de negocio de ese año fue de 542 millones de euros y sus ganancias llegaron a ascender hasta 51 millones, si bien después de su intervención se llegó a demostrar que tenía un pasivo exigible con sus clientes de más de 1700 millones de euros. AFINSA en 2006 fue intervenida por orden judicial acusada de delitos contra la Hacienda pública, blanqueo de capitales e insolvencias punibles, y varios de sus directivos fueron condenados a penas privativas de libertad y a abonar 2574 millones de euros a los casi 200.000 inversores que tenía.

[46] Fórum Filatélico fue una sociedad española que invertía primordialmente en numismática. El 9 de mayo de 2006 fue acusada de estafa, blanqueo de capitales, insolvencia punible y administración desleal. Los directivos de esta empresa fueron condenados en 2018 a penas de hasta 12 años de cárcel que fueron confirmadas por el Tribunal Supremo en 2020.

El atractivo de esta empresa consistía en que prometía una rentabilidad fija que no dependía de la evolución del mercado y que estaba muy por encima de cualquier inversión tradicional. Miles de inversores confiaron sus ahorros de toda la vida, y cuando se produjo la intervención judicial se pudo demostrar que se trataba de una estafa piramidal, pues el activo real era ínfimo.

Fórum Filatélico llegó a patrocinar a un equipo de baloncesto de primera división a los efectos de conseguir tener una buena imagen ante la opinión pública.

base en un sustento de delincuencia física, y normalmente individual, que nada tiene que ver con la realidad actual, la informática, Internet y la creciente relación virtual entre los operadores de los medios de transacciones económicas. Como consecuencia, los paradigmas de la investigación criminal tradicional han tenido que ser modificados a marchas forzadas para la persecución de una delincuencia con una alta y cambiante tecnificación[47].

Centrándonos en el delito que aquí se analiza, como exigencias que derivan de la tipicidad encontramos la necesidad de la relevancia del comportamiento criminal, la relación de causalidad[48] y la imputación objetiva del resultado. Todos ellos, elementos que la jurisprudencia ha venido recogiendo de forma reiterada[49].

Si bien se trata de un delito que se perpetra con una acción se plantea la doctrina la posibilidad de comisión por omisión.

En Alemania suele afirmarse que la estafa puede cometerse por omisión siempre que el sujeto tenga el deber de obrar, y de esta forma Schönke[50] lo fundamenta en la lealtad obligada cuando hay determinadas relaciones de confianza entre el sujeto activo y el pasivo.

Asimismo, la doctrina que parte de la promulgación del Código Penal de 1995 ha hecho especial inciso en la necesidad de la comprobación de una relación de riesgo coherente entre la acción y el resultado final de conformidad con los criterios de la imputación objetiva. Llegados aquí, existe el requisito fundamental para que pueda cometerse el engaño típico, que requiere un

[47] Una interesante reflexión sobre este nuevo panorama puede verse *ad exemplum* en Corcoy Bidasolo, M., «Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos», en *Eguzkilore*: *Cuaderno del Instituto Vasco de Criminología*, n.º 21, 2007, *passim*. Se plantean problemas realmente complejos en relación con la detección y prueba de las conductas delictivas que se producen con la utilización fraudulenta de medios de pago electrónicos, ya que los cibercriminales cada vez utilizan sistemas de comisión delictiva mucho más difíciles de perseguir. Sobre la cuestión probatoria puede verse por todos a Velasco Núñez, E., *Delitos cometidos a través de Internet. Cuestiones procesales,* La Ley, Madrid, 2010, y Velasco Núñez, E., *Delitos tecnológicos, definición, investigación y prueba en el proceso penal,* Sepín, Madrid, 2016.

[48] Según establece la STS 633/2016, 14 de julio –ECLI: ES:TS:2016:3503–, es necesario que exista una relación de causalidad entre el engaño que provoca el error y el acto de disposición que da lugar al perjuicio, de forma que entre engaño y perjuicio debe mediar la existencia de un nexo causal que implique que el detrimento en el patrimonio es consecuencia directa de la conducta engañosa, todo ello amparado por el ánimo de lucro como elemento subjetivo del injusto.

[49] *Ad exemplum:* SSTS de 29 julio 2002, 25 marzo 2004, de 2 noviembre 2004, 15 julio 2004, 11 julio 2005, 19 mayo 2005, 27 abril 2006, entre otras.

[50] Citado por Luzón Cuesta en Luzón Cuesta, J.M.ª, *Compendio de Derecho penal. Parte Especial*, Dykinson, Madrid, 2022, p. 226.

acto que pueda derivar *ex ante* en un riesgo penal de lesión del bien jurídico protegido, que es el patrimonio de la víctima.

Entendemos que este riesgo de lesión *ex ante* en los casos de utilización fraudulenta de tarjetas de crédito, débito, cheques de viaje u otros medios de pago queda cada vez más difuminado a los ojos del legítimo titular, pues no es nada infrecuente el encontrar casos en los que la víctima no se da cuenta hasta pasado un largo tiempo porque las cantidades que se van extrayendo son mínimas.

Para que pueda concretarse la estafa ha de existir una situación de verosimilitud, pues no es nada creíble, por ejemplo y con *animus iocandi*, que compremos un vehículo que utilice pasta de dientes como combustible. El llamado «engaño burdo»[51] no entraría en el ámbito de la estafa, si bien se ha de tener en cuenta las características de la víctima, pues no es lo mismo estafar a una persona de edad media con estudios superiores que a una persona de edad avanzada que prácticamente no conoce otro medio de pago que no sea el efectivo metálico.

Es bien cierto que la codicia humana no tiene límite y ello hace que se cometan estafas con productos financieros que prometen intereses muy elevados, incluso diríamos «ilusorios» en momentos de bajada generalizada de tipos de interés. Traemos a colación el caso de los pagarés[52] de Nueva

[51] En este sentido la STS 228/2014, de 26 de marzo, considera que únicamente el burdo engaño, esto es, aquel que puede apreciar cualquiera, impide la concurrencia del delito de estafa, porque, en ese caso, el engaño no es 'bastante'. Dicho de otra manera: el engaño no tiene que quedar neutralizado por una diligente actividad de la víctima (STS 1036/2003, de 2 de septiembre), porque el engaño se mide en función de la actividad engañosa activada por el sujeto activo, no por la perspicacia de la víctima.

[52] El 23 de febrero de 2009 se realizó la primera emisión de pagarés de Nueva Rumasa a través de la empresa Carcesa, dedicada al sector de la alimentación y propietaria de las marcas comerciales Apis y Fruco. Se llegaron a realizar cinco emisiones de pagarés siempre a través de empresas que escapaban al control de la Comisión Nacional del Mercado de Valores. A causa de las características de estos pagarés, en cuya emisión no intervenía ninguna entidad financiera, y que no tenía ningún tipo de control de la CNMV, este organismo regulador emitió hasta 7 comunicados a través de su web en los que advertía de los riesgos de estas operaciones y pedía a los potenciales inversores que se informaran convenientemente a través de asistencia financiera especializada. El 14 de abril de 2010, a instancia de la CNMV, el Gobierno reformó el artículo 30 bis de la Ley 24/1988 del mercado de valores de forma que en la venta de títulos dirigida al público en general, empleando cualquier forma de comunicación publicitaria, tuviera que existir como intermediario un gestor financiero autorizado que debía responder ante la CNMV.

En junio de 2010, Nueva Rumasa realizó una quinta emisión de pagarés con una rentabilidad del 10% si la inversión se realizaba a un año y del 12% si se realizaba a dos años, con una compra mínima de cincuenta mil euros. La emisión no fue publicitada en los medios de comunicación como sí lo fueron las anteriores, de forma que a esta no le afectaba la modificación de la ley del mercado de valores y por lo tanto no requirió la existencia de un intermediario ni quedó bajo la supervisión de la CNMV.

Rumasa, que en momentos en los que las entidades financieras remuneraban los ahorros de sus clientes con una TAE de alrededor del 3 %, los empresarios jerezanos prometían una rentabilidad asegurada de un 10 % anual, y ello se anunciaba en medios televisivos a pesar de las advertencias de la CNMV. Todo ello se producía todo y conociéndose los antecedentes histórico-delictivos que tiene el nombre del que fue el mayor holding de la historia de España, Rumasa, con más de 700 empresas y que llegó a alcanzar la cifra de 60.000 empleados.

Antes de la reforma del Código Penal mediante Ley Orgánica 14/2022[53], de 22 de diciembre el artículo 248 rezaba de la siguiente forma:

> «1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.
>
> 2. También se consideran reos de estafa:
>
> a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.
>
> b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.
>
> c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero».

Este precepto recogía un *numerus clausus* de medios mediante los que se podía cometer la estafa y ello, desde nuestro punto de vista, generaba una verdadera «obsolescencia legislativa programada» porque de todos es sabido que los medios de pago han avanzado de forma imparable adoptando diversas formas que escaparían del castigo del artículo 248.2 c) CP. Esta cuestión, también fue planteada de forma muy atinada por Solari Merlo, que destacaba que el precepto contenía una enumeración taxativa de medios a través de los que se podía cometer la estafa –tarjetas de crédito, débito o cheques de viaje– que suponía la atipicidad de conductas en las que el sujeto activo se valiera de otros instrumentos de eficacia similar[54].

[53] 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. Sobre la cuestión, puede verse a mayor abundamiento el trabajo de Bustos Rubio, en Bustos Rubio, M., «La reforma de la ciberestafa y la incorporación de los medios de pago digitales en el Código Penal», en *Revista de Internet, Derecho y Política*, n.º 38, 2023.

[54] Solari Merlo, M., «Del dinero de plástico al dinero intangible. Interpretación penal de las tarjetas de pago con especial consideración de la Directiva (UE) 2019/713»,

Asimismo, la conducta típica descrita en este artículo ha sido criticada por su vaguedad, si bien entendemos que una descripción demasiado concreta de los actos tipificados podría llegar a constituir un elemento que haría que a muy corto plazo el precepto se convirtiese en obsoleto por los continuos cambios que acontecen en el ámbito tecnológico.

A partir de la reforma de referencia, el artículo 248 CP queda circunscrito para el delito genérico de estafa y la utilización fraudulenta de tarjetas de crédito, débito y cheques de viaje del antiguo art. 248. 2 c) ha pasado a regularse en el art. 249. 1 b) y 249.2 b) CP, que en la actualidad tiene el siguiente tenor literal:

> «Artículo 249.
>
> 1. También se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años:
>
> a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.
>
> b) Los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.
>
> 2. Con la misma pena prevista en el apartado anterior serán castigados:
>
> a) 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.
>
> b) Los que, para su utilización fraudulenta, sustraigan, se apropiaren o adquieran de forma ilícita tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo.
>
> 3. Se impondrá la pena en su mitad inferior a los que, para su utilización fraudulenta y sabiendo que fueron obtenidos ilícitamente, posean, adquieran, transfieran, distribuyan o pongan a disposición de terceros tarjetas de crédito o débito, cheques de viaje o cualesquiera otros instrumentos de pago materiales o inmateriales distintos del efectivo».

Esta nueva regulación de la utilización fraudulenta de medios de pago distintos del efectivo se ha llevado a cabo por la necesidad acorde con los

en *Revista Electrónica de Ciencia Penal y Criminología,* RECPC 23-21 2021. Disponible en: http://criminet.ugr.es/recpc/23/recpc23-21.pdf, p. 21. (Fecha de consulta: 30 de diciembre de 2022).

tiempos, de la transposición de normativa de la Unión Europea, como la Directiva 2019/713, de 17 de abril[55] en relación con el art. 5 del Tratado de la Unión europea, que persigue los siguientes objetivos señalados en el Considerando 40:

> «[…] garantizar que el fraude y la falsificación de medios de pago distintos del efectivo sean castigados con penas efectivas, proporcionadas y disuasorias, y mejorar y fomentar la cooperación transfronteriza entre las autoridades competentes, así como entre las personas físicas y jurídicas y las autoridades competentes, no pueden ser alcanzados de manera suficiente por los Estados miembros, sino que, debido a sus dimensiones o efectos, pueden lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del TUE. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, la presente Directiva no excede de lo necesario para alcanzar dichos objetivos».

Si acudimos al Preámbulo de la Ley Orgánica 14/2022, de 22 de diciembre[56] en su parte primera, encontramos de forma muy clarificadora que se hace una expresa referencia a la obsolescencia de algunos tipos penales y a la necesidad de la regulación de medios de pago distintos del efectivo, que atiende de forma prioritaria a los diferentes bienes jurídicos tutelados o puestos en peligro, como el patrimonio, la seguridad del tráfico o la fe pública, y no solamente al concreto modo de comisión. También se hace especial inciso en la creciente

[55] Directiva (UE) 2019/713 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión Marco 2001/413/JAI del Consejo. *Vid*. *Diario Oficial de la Unión Europea*, de 10 de mayo de 2019. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019L0713&from=es. (Fecha de última consulta: 26 de enero de 2021).

[56] *Vid*. Boletín Oficial del Estado del viernes 23 de diciembre de 2022, págs., 1-3. Disponible en: https://www.boe.es/boe/dias/2022/12/23/pdfs/BOE-A-2022-21800.pdf. (Fecha de última consulta: 31 de diciembre de 22). «Ello implica la necesidad de una ajustada y diligente transposición al ordenamiento jurídico español, en concreto, de diversas directivas que afectan al ámbito penal sustantivo. Tal es el caso, en primer lugar, de la Directiva (UE) 2019/713 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, […] Esta Directiva (UE) 2019/713 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, se inserta dentro de la línea de la política criminal europea de lucha contra la criminalidad organizada, ámbito en el que los instrumentos de pago no dinerarios se han articulado como un medio para facilitar la obtención y blanqueo de las ganancias obtenidas con dichas acciones delictivas […] La Directiva, sin embargo, se centra en una regulación conjunta del fraude y de la falsificación de los medios de pago distintos del efectivo, alejándose de la sistemática clásica de nuestro Código Penal, que atiende prioritariamente a los diferentes bienes jurídicos tutelados o puestos en peligro…».

importancia de los medios de pago inmateriales[57] entre los cuales se encuentran los soportes digitales de intercambio en un contexto en el que la criminalidad cibernética ha incrementado como consecuencia del aumento de la «ciberpoblación» en el ámbito de Internet, con la comisión de los denominados «eurodelitos», que tienen una transcendencia transfronteriza[58] y que entendemos que han de regularse mediante una legislación que permita la persecución internacional de forma ágil, pues los ciberdelincuentes no entienden de fronteras.

El art. 248.2 c) CP (reformado en diciembre de 2022) fue ampliado tras la reforma 5/2010 del CP, un cambio *ad hoc* muy necesario a causa de los avances tecnológicos y, por la variedad de formas de delinquir que pueden producirse en este ámbito.

El tipo que aquí analizamos quizás sea más extenso de lo que se precisaba, pues incluye supuestos que ya encontraban su ubicación en la estafa

[57] Es preciso acudir a los artículos del 3 al 6 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión Marco 005/222/JAI del Consejo, donde se indica expresamente que son punibles una serie de infracciones relacionadas con la utilización fraudulenta de instrumentos de pago inmateriales que no sean efectivo. A tenor de la directiva citada y entre los arts. 3 al 6 lo son las siguientes: acceso ilegal a los sistemas de información, interferencia ilegal en los sistemas de información, borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información, intencionalmente y sin autorización, sea sancionable como infracción penal, interceptación ilegal (por medios técnicos, de transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos informáticos, intencionalmente y sin autorización). Es de gran interés el art. 10, que recoge la responsabilidad penal de las personas jurídicas cuando estas infracciones sean cometidas en su beneficio por cualquier persona que, actuando a título particular o como parte de un órgano de la persona jurídica, ostente un cargo directivo en el seno de esta. Esta responsabilidad se basa en el poder de representación de dicha persona jurídica, o la capacidad para tomar decisiones en nombre de esta, o la capacidad para ejercer un control efectivo en su seno. La falta de supervisión o control por parte de alguna de las personas que tienen las facultades antedichas, son el gozne sobre el que se gravita la responsabilidad penal. En el apartado tercero del art. 10 de la directiva se indica expresamente que la responsabilidad de las personas jurídicas en virtud de los apartados 1 y 2 no excluirá la incoación de acciones penales contra las personas físicas que sean autoras, inductoras o cómplices.

[58] En este sentido en el Considerando 29 de la Directiva (UE) 2019/713 del Parlamento Europeo y del Consejo, de 17 de abril de 2019 se indica expresamente que: «Las infracciones a que se refiere la presente Directiva suelen ser de naturaleza transfronteriza. Para combatirlas es necesaria, por tanto, una cooperación estrecha entre los Estados miembros. Se anima a los Estados miembros a velar, en la medida adecuada, por la aplicación efectiva de los instrumentos de reconocimiento mutuo y asistencia judicial en relación con las infracciones contempladas en la presente Directiva». Se refuerza lo dicho sobre la necesaria cooperación entre países en el Considerando 40.

común con el uso fraudulento de las tarjetas o la suplantación del titular de estas. Dopico Gómez-Aller[59] remarca que ello no tiene relevancia, pues el tipo del art. 248.1 y el del art. 248.2 CP tenían a la postre la misma penalidad.

El artículo 248.2 a) del Código Penal castigaba en primer lugar las manipulaciones informáticas, que no tenían una clara respuesta penal y donde no se podía aplicar la analogía *in malam partem*, proscrita en Derecho Penal.

En el apartado b) del art. 248 CP se castigaba la fabricación, introducción, posesión o facilitación de programas informáticos específicamente destinados a la comisión de estafas previstas en el presente artículo, y aquí podemos observar que se castigaban una serie de actos técnicos preparativos para una ulterior comisión del delito. Concretamente este apartado se incorporó al CP mediante la LO 15/2003 de 25 de noviembre de reforma del Código Penal.

Cuando se mencionan los programas de ordenador se hace referencia a aquellos que permiten causar un perjuicio a la víctima, no a la aptitud del sujeto activo, que podría ser más o menos experto en la materia. De ello se infiere que existen programas que pueden servir *ab initio* para producir un daño, sin embargo, si el sujeto activo no tiene los conocimientos informáticos suficientes existirá una imposibilidad *de facto* para la comisión delictiva.

La tercera conducta que se castigaba en el artículo 248. 2 c), actual art. 249.1 b) y 249.2 b) del Código Penal, que es el núcleo central del presente artículo, contemplaba la utilización de tarjetas de crédito, débito, cheques de viaje o datos obrantes en cualquiera de ellos para realizar operaciones sin perjuicio de su titular o de un tercero. Este apartado provenía de la reforma del CP operada por LO 5/2010, de 22 de junio como una novedad de gran importancia dada la utilización masiva de las tarjetas ya desde la década de los años 80, cuando entonces no existían los terminales TPV.

Con la reforma llevada a cabo por la Ley Orgánica 14/2022 de 22, de diciembre de 2022, se castiga en el artículo 249.1 b) CP como estafa la utilización de forma fraudulenta de tarjetas de crédito o débito, cheques de viaje, y en este punto se ha ampliado la punición a cualquier otro instrumento de pago material o inmaterial distinto del efectivo[60] o datos obrantes en

[59] Dopico Gómez-Aller, J., «Estafas y otros fraudes en el ámbito empresarial», De La Mata Barranco, N. J., Lascuraín Sánchez, J. A., Nieto Martín, A., *Derecho penal económico y de la empresa*, Dykinson, Madrid, 2018, pp. 232 y ss.

[60] Es preciso tener en cuenta que cuando en el CP se habla explícitamente de «instrumento de pago distinto del efectivo», hemos de acudir a la Directiva 2019/713, de 17 de abril y concretamente al art. 2 de los apartados a y b, que reza: «A los efectos de la presente Directiva, se entenderá por: a) «instrumento de pago distinto del efectivo», 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; b) «dispositivo, objeto o documento protegido»,

cualquiera de ellos. Entendemos que aquí el legislador ha dejado una fórmula abierta a las diferentes formas de pago que van apareciendo de consuno a la constante evolución tecnológica, como pueden ser: Bizum[61], criptomonedas, tarjetas virtuales, etc. Sin embargo, se mantienen en el articulado los cheques de viaje, que prácticamente ya están en desuso. Entendemos que con la nueva regulación también se recoge la utilización fraudulenta de las tarjetas de compra (que con tanto éxito comercializan marcas como El Corte Inglés, Zara, Pull & Bear, Mango, y un largo etcétera), que en referencia a estas y de forma muy acertada Faraldo Cabana[62] destaca que las otorgan los establecimientos comerciales y pueden quedar equiparadas a la moneda legal, pues su funcionamiento es muy parecido al de las tarjetas de crédito o débito, ya que permiten efectuar una compra y postergar el abono hasta la facturación, es decir, pueden conceder un crédito, y por lo tanto deben ser consideradas como un instrumento de pago a los efectos del artículo 387 del Código Penal.

Núñez Castaño[63] es del parecer que la conducta típica de este tipo de estafa recoge el hecho de ejecutar operaciones de cualquier tipo, y que esto puede comportar todo tipo de negocios jurídicos que se lleven a cabo con una transferencia patrimonial que genera un perjuicio para el sujeto pasivo. La misma autora entiende que de igual forma que en el tipo de la estafa genérica se exige que se materialice un perjuicio patrimonial respecto del titular de los medios de pago o de un tercero, que normalmente será una entidad financiera que los habrá emitido.

Por su parte, Gallego Soler[64] especifica que este tipo penal castiga los supuestos de utilización de la tarjeta de crédito o débito y/o cheque de viaje sin el consentimiento del titular, pudiendo incluso existir una apropiación de

un dispositivo, objeto o registro dotado de una medida de seguridad contra la imitación o la utilización fraudulenta, por ejemplo mediante el diseño, un código o una firma».

[61] El sistema de transacción Bizum, si bien está teniendo un gran éxito en los últimos tiempos comporta también una serie de riesgos, como pueden ser las estafas que se cometen a través de compras de segunda mano, petición de pagos por adelantado, supuestos abonos de la Seguridad Social o el aviso de pago por error mediante WhatsApp, entre otros.

[62] Faraldo Cabana, P., *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico,* Tirant lo Blanch, Valencia, 2009, *passim*.

[63] Núñez Castaño, E., «Estafas realizadas mediante tarjetas de crédito o débito y cheques de viaje (art. 248.2 c CP)», en Núñez Castaño, E., Galán Muñoz, A., *Manual de derecho penal económico y de la empresa*, Tirant lo Blanch, Valencia, 2018, p. 63.

[64] Gallego Soler, J. I., «Delitos contra bienes jurídicos patrimoniales defraudatorios», Corcoy Bidasolo, M. (Dir.); Santana Vega, D. M.ª (Coord.); Gómez Martín, V.; Bolea Bardon, C., Cardenal Montraveta, S., Joshi Jubert, U., Hortal Ibarra, J.C., Fernández Bautista, S., Carpio Briz, D., Díaz Morgado, C., Vera Sánchez, J.S., Valiente Ivañez, V., Castellví Monserrat, C., Ramírez Martín, G., Bages Santacana, J., Miranda, G., Rogé Such, G., *Manual de Derecho penal parte especial*, Tirant lo Blanch, Valencia, 2019, p. 50.

la información que contienen estos soportes. No podemos soslayar que, con la tecnología actual, los cibercriminales tienen cada vez más instrumentos para poder captar información de forma ilegal extraída de las diferentes modalidades de tarjetas.

El mismo autor indica que el *modus operandi* puede ser muy variado y que puede consistir en la obtención de números y claves de las tarjetas utilizando diversas técnicas, como pueden ser: *keyloggers*[65]*, nigerian phising*[66]*, skimming*[67]*, smishing (sinónimo de vishing)*[68], *spyware*[69], *pharming*[70],

[65] Un *keylogger* es un *Software* espía que se utiliza para rastrear y registrar lo que se escribe en el teclado. Los ciberdelincuentes se aprovechan de estos programas infectando intencionalmente dispositivos vulnerables y registrando información privada sin el conocimiento del usuario, robando así contraseñas y otra información. También se suelen utilizar dispositivos extraíbles, como unidades *flash*.

[66] Dicha estafa consiste en ilusionar a la potencial víctima con una fortuna inexistente y persuadirla para que pague o transfiera una suma de dinero por adelantado, como condición para acceder a la fortuna prometida.

[67] El *E-skimming* o *Web skimming* es una técnica utilizada por ciberdelincuentes para obtener información bancaria y personal de tiendas online legítimas que posteriormente será vendida en el mercado negro, o utilizada directamente por los ciberdelincuentes en su propio beneficio. El primer paso que deben llevar a cabo los ciberdelincuentes consiste en obtener acceso a la tienda *online*, para ello se suelen valer de vulnerabilidades no parcheadas en el gestor de contenidos o mediante campañas de *Phishing*. Una vez han conseguido acceso a la tienda, modifican parte de su código fuente para que, cuando el cliente introduce información personal o bancaria, sea enviada al banco y también robada. De esta forma, tanto el cliente como el comercio no son conscientes del robo, ya que el pago es correcto, sin embargo, toda esa información ya está en manos de los ciberdelincuentes. Al respecto, pueden verse, por ejemplo, las SSTS, n.º 450/2014, de 27 de mayo, ECLI:ES:TS:2014:2377 y n.º 560/2013, de 17 de junio, ECLI:ES:TS:2013:3612. Sobre todos estos términos véase Instituto Nacional de Seguridad (INCIBE). Disponible en: https://www.incibe.es/protege-tu-empresa/blog/e-skimming-y-proteger-tu-tienda-esta-tecnica-maliciosa. (Fecha de última consulta: 2 de enero de 2023).

[68] Es un tipo de estafa de ingeniería social por teléfono en la que, a través de una llamada, se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la víctima.

[69] El *Spyware*, también conocido como *Spybot*, es un tipo de programa malicioso. Es un tipo de *software* utilizado para recopilar información de una computadora o dispositivo informático y transmitirla a entidades externas sin el permiso del propietario de la computadora. El término *Spyware* también se utiliza para productos que no se corresponden estrictamente con este tipo de *Malware*.

Las funciones de este tipo particular de *Malware* son: recopilar datos e información privada, hábitos de navegación, nombres de usuario, mostrar anuncios no solicitados (ventanas emergentes), redirigir solicitudes de página e instalar marcadores telefónicos, entre otras.

[70] La palabra *Pharming* deriva del término *farm* (DOTA) (granja en inglés). Este método aprovecha una vulnerabilidad del *Software* de los servidores DNS y que consiste

phishing[71], *whaling*[72], etc. También existen formas más rudimentarias para utilizar las tarjetas de forma fraudulenta, como la que consiste en apoderarse de forma momentánea del medio de pago para introducir una serie de datos y comprar algún producto o servicio a través de Internet para posteriormente devolver la tarjeta de forma inmediata, tal y como recoge el actual artículo 249.2 b) CP.

Muñoz Conde[73] nos recuerda una situación que se produce de forma muy común y que consiste en que el titular de la tarjeta o cheque de viaje excede el límite del importe que tiene concedido y efectúa compras perjudicando a la entidad emisora que, en este caso, sería el sujeto pasivo. El propietario del medio de pago cuando se excede puede ser que no lo haga a sabiendas, así pues, solamente se trataría de una estafa en el caso en que lo hiciera de forma dolosa, con los elementos cognitivo y volitivo característicos del tipo. En esta situación la realidad consiste en que el establecimiento que detecta que el usuario se ha extralimitado del importe que tiene concedido por la entidad financiera emisora, avisa a esta para que conceda una ampliación, y si lo hace, entendemos que es porque previamente ha habido un muy detallado estudio de riesgo financiero que prácticamente excluiría la posibilidad de que el usuario de la tarjeta consiga engañar y perjudicar con un desplazamiento patrimonial.

También en relación con esta situación Vázquez Iruzubieta[74] señala que el comerciante no sería estafado ni engañado, pues cobrará por sus servicios o ventas, y quien podría ser damnificado sería el banco o entidad emisora.

---

en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad (comúnmente una entidad bancaria) de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a una dirección IP donde se aloja una web falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad.

[71] El término *Phishing* (robo de identidad en español), acrónimo de *Password Harvesting Fishing* (pesca y captura de contraseñas) se refiere al acto de intentar obtener información personal de alguien de manera fraudulenta. La mayoría de estos ataques de *Phishing* comienzan con un correo electrónico o mensaje de texto en el que el remitente se hace pasar por un banco, una empresa o cualquier organización real para generar una situación de engaño.

[72] Sinónimo de «Fraude del CEO». La forma en que se comete el ataque bajo esta figura es muy similar a la de los ataques de *Phishing*. Se procede mediante el envío de correos electrónicos falsos que contienen enlaces a sitios web fraudulentos, con la diferencia de que en el *Phishing* el afectado no es necesariamente un directivo o alto cargo de la organización.

[73] Muñoz Conde, F., *Derecho penal parte especial*, Tirant lo Blanch, Valencia, (24ª. Ed.), 2022, p. 351.

[74] Vázquez Iruzubieta, C., *Código Penal Comentado,* Atelier, Barcelona, 2015, pp. 431 y 432.

El mismo autor argumenta que el titular de la tarjeta aparenta una solvencia que no existe y en todo caso lo que sí habría es un uso excesivo de confianza, que el banco o entidad financiera habría depositado en su cliente asumiendo el riesgo de la operación.

La tendencia jurisprudencial que entendía que seguir utilizando una tarjeta a sabiendas de que los fondos se habían agotado constituía un uso de apariencia engañosa con fingimiento de un crédito para inducir a error a los comerciantes, que vendían fiándose de una aparente solvencia que no se disponía ha quedado superada, pues en la actualidad cuando una entidad emisora detecta que se sobrepasa el crédito, de inmediato bloquea el medio de pago.

Habitualmente las entidades financieras dejan un margen para el endeudamiento en las tarjetas de crédito e incluso en las de débito, dependiendo de la solvencia del cliente, siempre previo estudio –hoy ya con algoritmos muy precisos– pudiendo resultar perjudicadas si no se satisface lo debido, si bien para estos casos existe el procedimiento civil correspondiente para reclamar.

Como indica Gallego Soler[75], el criterio interpretativo que se impone en el tipo penal que analizamos es la utilización no autorizada de los medios de pago que hemos citado, o de los datos que se contengan en los mismos, ya sea el número de la tarjeta, fecha de caducidad, código de seguridad (últimos tres dígitos que aparecen en el reverso).

Por otra parte, la utilización fraudulenta de tarjetas de crédito, débito y cheques de viaje que son falsificados para conseguir datos de otro titular y así operar con cargo a este, constituye una conducta que tiene como finalidad la defraudación, si bien tiene puntos de contacto con la falsedad documental.

En la actualidad la conducta que persigue defraudar no siempre se comete mediante el uso físico de la tarjeta, pues basta la obtención de su numeración y código secreto para utilizarla de forma fraudulenta. La forma de obtención de la numeración de las tarjetas con ánimo de defraudar es variopinta, y se utilizan muchas y diferentes argucias para perpetrar el delito, por ejemplo, mediante ofertas de productos a través de las redes sociales, que precisan que el usuario complete una serie de campos para obtener datos de sus tarjetas que serán utilizados para estafar.

Vázquez González[76] es del parecer que este tipo penal tiene un difícil encaje en la estafa común y que estas actuaciones deberían de ser reconducidas al delito de robo con fuerza en las cosas, pues el autor entiende que es una tarjeta mal utilizada en perjuicio de la víctima que se asemeja a una llave

[75] Gallego Soler, J. I. *Op. cit*. p. 50.

[76] Vázquez González, C., «Estafa», en Serrano Gómez, A., Serrano Maíllo, A. y Serrano Tárraga, M.ª D., *Curso de Derecho penal parte especial*, Dykinson, Madrid, 2019, p. 295.

física falsa. El mismo autor[77], de forma muy acertada hace referencia a otros medios de pago que son de mucho uso en nuestros tiempos, como pueden ser las tarjetas de compra de centros comerciales, de transporte o incluso de teléfono, que juntamente con los cheques, talones y letras de cambio no se recogían en este tipo, a nuestro modo de ver de forma errónea en relación con los tiempos en los que estamos viviendo.

Esta cuestión fue muy debatida entre la doctrina[78] hace años y a los efectos de clarificar la cuestión sobre si estamos ante un tipo de llave que permite

[77] *Ibidem.*

[78] Serrano Gómez y Serrano Maíllo también entienden que estamos en la esfera de la utilización de tarjetas fraudulentas y que la conducta es equiparable al robo con fuerza. *Vid.* Serrano Gómez, A. y Serrano Maíllo, A., *Derecho penal parte especial*, Dykinson, Madrid, 2011, p. 436. Choclán Montalvo también se inclinó por el robo con fuerza en las cosas, pero matizó que sería en el caso de que se acceda al sitio donde el cajero se encuentra y de esta forma la tarjeta sí que se emplearía como llave. Choclán Montalvo, J.A., «Infracciones patrimoniales en los procesos de transferencia de datos», en Morales García, Ó., (Dir.), *Delincuencia informática. Problemas de responsabilidad, Cuadernos de Derecho Judicial IX-2002*, CGPJ, Madrid, pp. 241-280. Por otra parte, Suárez Mira Rodríguez entiende que la extracción de dinero en cajeros automáticos mediante el uso de tarjetas de crédito no constituye un delito de robo con fuerza mediante uso de llave falsa y sí un delito de estafa. Suárez-Mira Rodríguez, C., (Dir. y coord.)., Judel Prieto, Á., Piñol Rodríguez, J. R., *Manual de Derecho penal parte especial,* tomo II, Aranzadi, Pamplona, 2020, p. 376. En esta línea es muy interesante la postura que adopta Gómez Rivero cuando señala que esta conducta típica abarca todos los casos en los que las tarjetas de crédito o débito se lleguen a emplear para efectuar compras en un establecimiento comercial o de cualquier otro tipo, pero también pueden incluirse las extracciones de dinero en efectivo de un cajero automático con la introducción de un PIN (código de identificación) planteándose de esta forma un concurso de leyes con el delito de robo con fuerza en las cosas, que se resolvería a favor del delito de estafa en virtud del principio de especialidad. *Vid*. Gómez Rivero, M.ª C. (Dir.)., «Delitos patrimoniales de enriquecimiento mediante defraudación (I): estafa», Nieto Martín, A., Cortés Bechiarelli, E., Núñez Castaño, E., Pérez Cepeda, A. M.ª, *Nociones fundamentales de derecho penal parte especial,* Tecnos, Madrid, 2020, p. 122. Pastor Muñoz distingue que es posible argumentar que el uso de las tarjetas para la extracción de dinero de un cajero automático ha de ser considerado como un caso de robo con fuerza, ya que este medio se utiliza para una sustracción, mientras que el artículo 248.2 c) CP (antes de la reforma de diciembre de 2022) recogería los casos de realización, utilización de una tarjeta, operaciones de compraventa o pago de prestaciones, como podría ser el abono de un peaje en una autopista o la compra de entradas para un espectáculo, incluyéndose también las operaciones realizadas en un cajero automático. Así pues, entendemos que la delimitación entre el robo con fuerza y la aplicación del artículo 248.2 c) CP radicaría en si se extrae o no dinero de un cajero automático de forma indebida para perjudicar al sujeto pasivo. *Vid*. Pastor Muñoz, N., «El delito de estafa», en Silva Sánchez, J.Mª. (Dir.)., *et al. Lecciones de Derecho penal económico y de la empresa.* Parte general y especial, Atelier, Barcelona, 2020, pp. 272 y 273. Es accesorio que se acceda con la tarjeta (lo que no siempre es así) al recinto donde se halla el cajero y

la utilización fraudulenta de estos medios de pago llevándonos hacia el delito de fuerza en las cosas, colige traer a colación la Sentencia del Tribunal Supremo n.º 369/2007, de 9 de mayo en relación con la apropiación indebida de una tarjeta bancaria y su uso para extraer dinero de un cajero que dejó resuelta la cuestión.

De la citada sentencia extractamos el siguiente apartado por su meridiana claridad:

> «En efecto no basta con que la tarjeta sea llave, es necesario que ésta haya sido empleada para acceder al lugar en el que las cosas se guardan. La fuerza en las cosas típica del robo es aquella precisa para «acceder al lugar donde éstas se encuentren», tal y como lo define legalmente el art. 237 CP. Y el dinero en los cajeros se halla en un cajetín en el interior de este al que en ningún momento se accede».

Al operar con la tarjeta en un cajero, lo esencial es que se introducen datos en el ordenador y que el sistema efectúa una disposición patrimonial no consentida con el titular y se llega a registrar en una contabilidad.

Si nos centramos en el tenor literal del artículo 248.2 c) CP, que con la última reforma se ubica en el art. 249.1 b) y que reza:

Se considerarán reos de estafa… «los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos, realizan operaciones de cualquier clase en perjuicio de su titular o de un tercero».

Por otra parte, puede darse el caso de que las tarjetas de crédito, débito o cheques de viaje se empleen por su legítimo titular de forma abusiva incluso falsificando alguno de sus datos, como la fecha de caducidad o el importe de los cheques para llevar a cabo pagos u obtener reintegros por encima de las posibilidades que tiene el medio de pago en cuestión. Aquí Mestre Delgado[79] señala que no existiría una manipulación informática, tampoco un

---

no cabe afirmar que se acceda al lugar donde el dinero se guarda. El empleo de la tarjeta como llave permite calificar de robo cuando con la misma se accede al lugar donde están las cosas (v.gr. la tarjeta es la llave de la habitación del hotel a la que se consigue entrar para robar algún objeto). Entendemos que la utilización de forma fraudulenta también comprende la extracción de dinero en metálico de un cajero y por lo tanto la conducta quedaría subsumida en este artículo, procediendo descartar el robo con fuerza, pues de lo contrario, podríamos llegar al absurdo de vaciar de contenido este artículo. Hemos de tener en cuenta que una extracción de dinero puede consistir en un traspaso de una cuenta a otra mediante una tarjeta con exactamente el mismo efecto perjudicial que si la misma se produce de forma física en un cajero, y es así como una visión finalista y global del acto nos conduce a esta conclusión.

[79] Mestre Delgado, E., «El phishing y la responsabilidad penal de los muleros o cibermulas a la luz del artículo 248.2 A) del Código penal». Abadías Selma, A., Breto-

engaño interpersonal ni una operativa correcta del sistema operativo del cajero automático. Si el estafador ha falsificado el instrumento de pago no tendrá nada que ver, ya que es incluso un acto previo a la ejecución del fraude por una alteración del sistema operativo de las máquinas que se han empleado para defraudar. En este punto la utilización de estos instrumentos no se insertaría directamente en el proceso de ejecución de la acción defraudatoria, sino en un momento anterior, por lo que no se produciría la manipulación informática típica de la perpetración de la ciberestafa.

El mismo autor señala que la situación sería pareja si esos instrumentos los utilizara un tercero que los haya robado o descubierto para utilizar sus claves de acceso mediante medios informáticos.

A esta realidad delictiva se suma el uso de las tarjetas virtuales que cada vez son más utilizadas y que pueden ser objeto de utilización fraudulenta, si bien requieren de una alta especialización en informática por parte del ciberestafador. Con la última reforma, entendemos que este tipo de conductas quedarían recogidas en el artículo 249.1 b) *in fine* CP: «… o cualquier otro instrumento de pago material o inmaterial distinto del efectivo con los datos obrantes en cualquiera de ellos…».

Otra forma de pago que se asemeja sobremanera a las tarjetas virtuales es el PayPal[80]. En este punto estamos de acuerdo con Dopico Gómez-Aller[81] en que se trata de un negocio crediticio concreto y no de una tarjeta de crédito o débito y que, si se ha llevado a cabo la defraudación al utilizar algún tipo de manipulación o artificio informático, sería procedente la aplicación del artículo 248.2 a) CP, que con la actual reforma se trataría del artículo 249.1 a) CP.

Si el sujeto activo consigue averiguar las claves de PayPal de la víctima y llega a realizar operaciones no consentidas, estaríamos ante la misma

---

nes Alcaraz, F.J., Cámara Arroyo, S., Carou García, S., Fernández Bermejo, D., García Valdés, C., Gil Gil, A., Marcos Ayjón, M., Martínez Atienza, G., Martínez Galindo, G., Pérez López, X., Roca De Agapito, L., Romero Jaime, D.J., Sanz Delgado, E., Téllez Aguilera, A., Tejada De La Fuente, E., De Urbano Castrillo, E., *Tratado de delincuencia cibernética*, Aranzadi, Pamplona, 2021, p. 355.

[80] PayPal Holdings, Inc. es una empresa multinacional estadounidense de tecnología financiera que opera sistemas de pago en línea en la mayoría de los países que permiten transferencias de dinero telemáticas y sirve como una alternativa electrónica a los métodos tradicionales basados en papel, como cheques y giros postales. La empresa opera como un procesador de pagos para vendedores en línea, sitios de subastas y muchos otros usuarios comerciales, y cobra una tarifa por ello. Fundada en 1998 con el nombre de Confinity, PayPal se hizo pública a través de una oferta pública inicial en 2002. Ese mismo año, se convirtió en una subsidiaria de propiedad total de eBay, valorada en 1500 millones de dólares. En 2015, eBay escindió de PayPal a sus accionistas y se convirtió nuevamente en una empresa independiente. La compañía ocupó el puesto 143 en la lista Fortune 500 de 2022 de las corporaciones más grandes de los Estados Unidos por ingresos.

[81] Dopico Gómez-Aller, J., *Op. cit*. pp. 232 y ss.

problemática *ut supra* comentada en relación con las operaciones con cuentas ajenas.

Por último, en el numeral 2 b) del artículo 249 CP también se castiga la sustracción, apropiación o adquisición de forma ilícita con finalidad de utilización fraudulenta de los medios de pago que acabamos de mencionar.

En la práctica diaria puede producirse una pérdida de la tarjeta o incluso una sustracción de esta y que se utilice de forma fraudulenta sin consentimiento del titular para llevar a cabo transacciones en perjuicio de este. En estos casos normalmente el titular de la tarjeta se verá resarcido por parte de la entidad financiera que deberá responder del mal uso.

Al respecto existe normativa[82] de la Unión Europea y del Banco de España, y además, no en vano las entidades financieras que emiten estas

[82] Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, donde se regulan todos los sistemas de pago que la propia ley define en su artículo 1.2, y entre ellos, están comprendidos las tarjetas de crédito. Este RDLey, deroga la Ley 16/2009, de 13 de noviembre, de servicios de pago. *Vid.* el art. 43. «Notificación y rectificación de operaciones de pago no autorizadas o ejecutadas incorrectamente. 1. El usuario de servicios de pago obtendrá la rectificación por parte del proveedor de servicios de pago de una operación de pago no autorizada o ejecutada incorrectamente únicamente si el usuario de servicios de pago se lo comunica sin demora injustificada, en cuanto tenga conocimiento de cualquiera de dichas operaciones que sea objeto de reclamación, incluso las cubiertas por el artículo 60, y, en todo caso, dentro de un plazo máximo de trece meses contados desde la fecha del adeudo. Los plazos para la notificación establecidos en el párrafo primero no se aplicarán cuando el proveedor de servicios de pago no le haya proporcionado ni puesto a su disposición la información sobre la operación de pago con arreglo a lo establecido en el título II. 2. Cuando intervenga un proveedor de servicios de iniciación de pagos, el usuario de servicios de pago deberá obtener la rectificación del proveedor de servicios de pago gestor de cuenta en virtud del apartado 1, sin perjuicio de lo dispuesto en el artículo 45.2, y el artículo 60.1.». A partir de la necesaria comunicación sin demora del usuario existe la responsabilidad objetiva impuesta con carácter general en el artículo 147 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (TRLGDCU), y con carácter especial el artículo 148 del mismo texto, que se pronuncia en los siguientes términos «Se responderá de los daños originados en el correcto uso de los servicios, cuando por su propia naturaleza, o por estar así reglamentariamente establecido, incluyan necesariamente la garantía de niveles determinados de eficacia o seguridad, en condiciones objetivas de determinación, y supongan controles técnicos, profesionales o sistemáticos de calidad, hasta llegar en debidas condiciones al consumidor y usuario». Además, hay que añadir la inversión de la carga de la prueba que se establece en el artículo 44.1 Real Decreto-Ley 19/2018, en virtud del cual «1. Cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, corresponderá al proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado por el proveedor

tarjetas suelen cobrar un seguro a los clientes para los casos de utilización fraudulenta.

Tal y como indica Fernández Teruelo[83], el Banco de España de forma meridianamente clara insiste en que este tipo de actuaciones fraudulentas han de estar cubiertas por parte de las entidades que han emitido estas tarjetas siempre y cuando el usuario haya hecho un uso correcto de estas y haya procedido a denunciar la pérdida.

La Directiva de la Unión Europea 2015/2366 del Parlamento Europeo (Segunda Directiva de servicios de pago o DSP2)[84] señala que la entidad financiera deberá hacerse cargo del dinero robado –entendemos que también

de servicios de pago». A mayor abundamiento el artículo 44.3 del mismo Real Decreto-Ley señala que «Corresponderá al proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, probar que el usuario del servicio de pago cometió fraude o negligencia grave». En cuanto a la prueba este extremo ya venía siendo recogido por la jurisprudencia en diversas decisiones recogiendo el término de la diligencia exigible del artículo 1104 del Código civil. Por otra parte, es preciso que los damnificados puedan acogerse a los artículos 69 y 70 RDLey 19/2018, que regulan el Servicio de atención al cliente y la mediación y arbitraje como procedimientos de resolución alternativa a la vía judicial, de los posibles litigios.

[83] Fernández Teruelo, J.G., «Respuesta penal frente a fraudes cometidos en internet: estafa, estafa informática y los nudos de la red», en *Revista de Derecho Penal y Criminología,* 2.ª época*,* n.º 19, 2007, p. 226.

[84] En concordancia con: Reglamento Delegado (UE) 2020/1423 de la Comisión, de 14 de marzo de 2019, por el que se completa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo que respecta a las normas técnicas de regulación relativas a los criterios de nombramiento de puntos de contacto centrales en el ámbito de los servicios de pago y a las funciones de estos puntos de contacto centrales (DO L 328 de 9.10.2020, pp. 1-3).

Reglamento de Ejecución (UE) 2019/410 de la Comisión, de 29 de noviembre de 2018, por el que se establecen normas técnicas de ejecución relativas a los pormenores y la estructura de la información que deban notificar, en el ámbito de los servicios de pago, las autoridades competentes a la Autoridad Bancaria Europea de conformidad con la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo (DO L 73 de 15.3.2019, pp. 20-83).

Reglamento Delegado (UE) 2019/411 de la Comisión, de 29 de noviembre de 2018, por el que se completa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo que respecta a las normas técnicas de regulación por las que se establecen requisitos técnicos sobre el desarrollo, la gestión y el mantenimiento del registro electrónico central en el ámbito de los servicios de pago y sobre el acceso a la información que dicho registro contenga (DO L 73 de 15.3.2019, pp. 84-92).

Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017, por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros (DO L 69 de 13.3.2018, pp. 23-43).

cubriría el hurto– desde que se cancela la tarjeta, aunque los primeros 50 euros hasta que sea notificado a la entidad el robo o se cancele la tarjeta serán responsabilidad del cliente. Así pues, si previamente a la cancelación de la tarjeta la utilización fraudulenta alcanza los 100 euros, el banco abonará 50 euros, pero si se notifica antes de la acción fraudulenta, la entidad tendrá que devolver el montante completo, es decir los 100 euros.

Como hemos indicado *ut supra*, la casuística es muy variada, y podemos encontrar situaciones en las que se realiza un duplicado de tarjeta y el cliente sigue teniendo la suya en formato físico. Ante esta situación la víctima no es consciente de lo que está sucediendo y tampoco podrá conocer que se está utilizando su medio de pago de forma fraudulenta hasta el momento en el que la operación se lleve a cabo y la operativa pueda verse reflejada en extractos de la entidad financiera. En este supuesto la entidad emisora de las tarjetas tendrá que abonar la totalidad de la cantidad sustraída de forma ilegal.

Hemos de remarcar que existe un gran desconocimiento por parte de la ciudadanía sobre sus derechos en el caso de la utilización fraudulenta de medios de pago, y las entidades financieras suelen intentar exonerarse de su responsabilidad, que además puede ser reclamada ante el servicio de reclamaciones del Banco de España.

Es preciso que exista una protección penal del uso creciente y masivo del llamado «dinero de plástico» que en la actualidad cada vez es menos de plástico y más virtual. Dopico Gómez-Aller[85] es muy crítico con la regulación penal de la utilización fraudulenta que aquí analizamos por la imprecisión terminológica del articulado, pues «realizar operaciones de cualquier clase en perjuicio de su titular o de un tercero» *ex* art. 249.1 b) CP no contiene términos que quizás hubieran sido deseables incluir como «artificio» o «manipulación», y critica también que a duras penas se encuentra un elemento que nos hable no solamente de un fraude, sino de una simple antijuricidad. Coincidimos con este autor, pues se impone una interpretación restrictiva en aras de la seguridad jurídica, y puesto que se trata de un tipo que está contenido en la rúbrica «De las defraudaciones» hemos de entender que nos encontramos ante una serie de operaciones realizadas sin consentimiento ni autorización.

Y por último, en el numeral tres del citado art. 249 CP se castiga con la pena en su mitad inferior a quienes todo y saber que ha existido una obtención ilícita, posean, adquieran, transfieran, distribuyan o pongan a disposición de terceros tarjetas de crédito o débito, cheques de viaje o cualesquiera otros instrumentos de pago materiales.

A tenor de la Directiva 2019/713, de 17 de abril y acudiendo al art. 4 se consideran como acciones típicas las siguientes:

[85] Dopico Gómez-Aller, *Op. cit,* pp. 232 y ss.

> «a) la sustracción o cualquier otra forma de apropiación ilícita de un instrumento de pago material distinto del efectivo;
>
> b) la falsificación o alteración fraudulenta de un instrumento de pago material distinto del efectivo;
>
> c) la posesión, para su utilización fraudulenta, de un instrumento de pago material distinto del efectivo que haya sido objeto de robo u otra forma de apropiación ilícita, o de falsificación o alteración;
>
> d) la obtención, para uno mismo o para otra persona, incluida la recepción, apropiación, compra, transferencia, importación, exportación, venta, transporte o distribución, de un instrumento de pago material distinto del efectivo que haya sido robado, falsificado o alterado para su utilización fraudulenta».

La realidad existente pone de manifiesto que Internet brinda muchas oportunidades, pero también implica una complejidad intrínseca a causa de su carácter descentralizado, puesto que contiene una ingente cantidad de sujetos que operan con sistemas informáticos que trabajan en redes con una transmisión de datos que cada vez se transmiten a una mayor velocidad.

3. *Sujeto activo*

Dicho esto, el sujeto activo del delito objeto de análisis, responsable penal y civil de los hechos puede serlo cualquiera y, por lo tanto, es un delito de carácter común. Asimismo, será responsable penalmente aquel que provoque conspire o proponga la comisión del delito de estafa *ex* arts. 249 y 269 CP.

El autor del delito ha de disponer de una capacidad necesaria para que pueda producirse el engaño en la víctima del delito, que podrá ser medida de forma abstracta, o bien con una vinculación con las capacidades de la víctima, hecho que entendemos es más acertado y que matizaremos *ad infra*.

En este tipo de delito lo único que tiene que hacer el autor es engañar, los demás elementos los tiene que realizar la propia víctima; en realidad, el autor es un inductor de la autolesión que la propia víctima sufre –el engañado o un tercero– según Agudo Fernández, Jaén Vallejo y Perrino Pérez[86].

Los delitos que sean perpetrados mediante las TIC en la mayoría de las ocasiones precisan de un sujeto activo experto en la materia y es muy común que la comisión delictiva se lleve a cabo por parte de organizaciones criminales que están muy bien estructuradas, hecho que se constata muy especialmente en el caso de los medios de pago diferentes del dinero en metálico, como pueden ser todo tipo de tarjetas físicas o virtuales. Aquí la pericia del

[86] Agudo Fernández, E., Jaén Vallejo, M. y Perrino Pérez, Á. L., *Derecho penal aplicado. Especial. Delitos contra el patrimonio y contra el orden socioeconómico,* Dykinson, Madrid, 2019, p. 97.

cibercriminal se impone como un elemento que entendemos es necesario para conseguir el éxito en la consumación del delito.

En este punto queremos hacer referencia al término «Hacker», que, si bien de inicio tiene una serie de connotaciones negativas, su origen es bien distinto, pues como nos recuerda Himanem[87] los «Hacker» eran auténticos expertos que se dedicaban a la programación informática de forma muy entusiasta con el convencimiento de que transferir información a la sociedad era algo muy positivo. Los «Hacker» ponían especial énfasis en el sentido de comunidad y de compartir algo que ellos tenían y que era positivo para todos y todas para de alguna forma democratizar el uso de grandes cantidades de información que podrían estar al alcance de cualquiera si no tuvieran control alguno.

Casos recientes como los de Assange, Snowden o el fenómeno Anonymous muestran una cara bien distinta de los «Hackers», que en estos casos buscaban compartir información con la sociedad en aras de conseguir luchar contra la opresión del poder y de la corrupción[88] y llegar hasta la anhelada transparencia, al menos en «teoría».

La otra cara de la cuestión viene de la mano de los llamados «*Influencers*»[89] que con el argumento de la democratización de las finanzas y al amparo del anonimato y la dificultad de seguimiento de las redes informáticas comercializan a diario ingentes cantidades de dinero en forma de criptomonedas, toda vez que organizan eventos muy pomposos para captar clientes que buscan ganar dinero de forma rápida y sencilla[90] –luego víctimas de estafas–, que por

[87] Himanem, P., *La ética del hacker y el espíritu de la era de la información*, Editorial Destino, Madrid, 2002, p. 5.

[88] Sobre la cuestión pueden verse al respecto Coleman, G., *Las mil caras de Anonymous*. Editorial Arpa Editores, Barcelona, 2016 y Molist Ferrer, M., *Hackstory.es: La historia nunca contada del underground hacker en la Península Ibérica.* Editorial Amazon, Madrid, 2015, *passim*.

[89] Durante la última década, hemos visto crecer rápidamente la importancia de las redes sociales. Más de 4590 millones de personas utilizan activamente las redes sociales. Los «*influencers*» en las redes sociales son personas que han construido una reputación por su conocimiento y experiencia en un tema específico, que no siempre tiene que ser nocivo. Realizan publicaciones periódicas sobre ese tema en sus canales de redes sociales preferidos y generan muchos seguidores de personas entusiastas y comprometidas que prestan mucha atención a sus puntos de vista. Existen marcas que pagan grandes cantidades de dinero por una publicidad que llevan a cabo este tipo de promotores.

[90] Entendemos como algo muy necesario que frente a la criminalidad que se perpetra mediante mediante distintos tipos de estafas se lleve a cabo una prevención muy decidida por parte de las administraciones, y que necesariamente habrá de pasar porque los ciudadanos aprendan a defenderse antes de ser víctimas mediante la autoprotección, y ello no es nada fácil, ya que las promesas de ganancias cuantiosas sin apenas invertir dinero ni trabajo es algo siempre muy tentador que proviene de la insaciable tendencia humana en pos del lucro rápido y fácil. Pensamos que desde las escuelas sería muy necesario que se explicase lo que es real-

las técnicas de persuasión se asemejan sobremanera a los de algunas sectas altamente peligrosas.

En relación con el *phishing*[91], que hemos mencionado con anterioridad hay que señalar que en este tipo de estafas informáticas pueden aparecer personas que no tienen por qué tener un conocimiento inicial de la comisión del delito, pero sí que son conscientes a la hora de encubrir los beneficios obtenidos de forma ilegal. Son los llamados «Muleros». Estas personas suelen ser captadas mediante falsas ofertas de empleo, teletrabajo, grandes beneficios en poco tiempo, etc. y normalmente a cambio de una previa detracción de una comisión que les generará beneficios, contribuyen directamente a la perpetración del *Phishing,* ya sea aperturando una cuenta corriente en la que reciben diferentes remesas de cantidades económicas o incluso usando una cuenta propia para recibir cantidades procedentes de estafas. El resto del dinero lo enviarán al defraudador, normalmente al extranjero, mediante servicios de pago electrónico como PayPal y Money Gram entre otros, dificultando así el seguimiento policial[92], la confiscación y la identificación del verdadero responsable último de la suplantación generadora de la estafa.

---

mente una estafa y las distintas formas que puede presentar, no sin antes fomentar un espíritu de sacrificio y laboriosidad para ganarse aquello que uno se merece, ni más ni menos, como contraste a la inmediatez de obtención de beneficios de procedencia más que dudosa.

[91] *Vid*. Rey Huidobro, L.F., «La estafa informática: relevancia penal del *phishing* y el *pharming», en Diario La Ley*, n.º 7926, sección Doctrina, 19 de septiembre de 2012, Ref. D-322, LALEY 16076/2012, en relación con el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera donde ya en el preámbulo se indica que: «Consolidada la zona única de pagos, se hace preciso avanzar en la adaptación de la regulación a los nuevos cambios tecnológicos que permiten a los usuarios disponer de forma más fiable de nuevos servicios de pago y nuevos agentes que van implantándose de forma cada vez más intensa, especialmente en el contexto de un mercado más amplio que el nacional. El aprovechamiento de las innovaciones producidas en los últimos años y la necesidad de generar un entorno más seguro y fiable para su desarrollo se encuentran en la base de la aprobación de la nueva Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 y se deroga la Directiva 2007/64/CE, en sustitución de la del 2007, que junto al Reglamento (UE) 2015/751 del Parlamento Europeo y del Consejo, de 29 de abril de 2015, sobre las tasas de intercambio aplicadas a las operaciones de pago con tarjeta, forman las piezas de ensamblaje del nuevo marco regulador de los servicios de pago. Este nuevo marco europeo, que este real decreto-ley incorpora parcialmente a nuestro ordenamiento jurídico, tiene como principales objetivos facilitar y mejorar la seguridad en el uso de sistemas de pago a través de internet, reforzar el nivel de protección al usuario contra fraudes y abusos potenciales, respecto del previsto en la Ley 16/2009, de 13 de noviembre, así como promover la innovación en los servicios de pago a través del móvil y de Internet».

[92] Es notorio que el entorno virtual facilita la comisión de delitos y obvio que hay una gran probabilidad de alteración de pruebas, destrucción y utilización de estas de forma

Es relevante dirimir el tipo de responsabilidad penal que tienen los «Muleros», cuestión que no es baladí, pues existen resoluciones que consideran que al no constar uno de los elementos necesarios del tipo penal de la estafa, como es el dolo, la posición que tendrían sería de meros instrumentos, y por lo tanto en algunas resoluciones se ha procedido a su libre absolución, como es el caso de la Sentencia de la Audiencia Provincial de Toledo de 5 de octubre de 2016, sin embargo existen otras decisiones, como la de la Sentencia de la Audiencia Provincial de Oviedo de 30 de mayo de 2017 que condenó a los acusados como cooperadores necesarios del delito de estafa. Por nuestra parte, entendemos que, si esta figura es absolutamente necesaria e imprescindible para la comisión delictiva, estamos en la esfera de la participación necesaria, pues además la entrada de dinero en las cuentas de estas personas hace pensar que los elementos cognitivo y volitivo del dolo están presentes –también en forma de dolo eventual–. Asimismo, hay que tener en cuenta que es preciso disponer de cuentas a beneficio de las cuales se puedan ordenar las transferencias, de manera que exista una posibilidad real del cobro del importe de lo defraudado, previa comisión.

Dicho esto, el abordaje penal presenta no pocos problemas de autoría en este caso de los «Muleros» pues intervienen numerosas personas en el entramado delictivo, cuya identidad en la gran mayoría de ocasiones resulta muy compleja de conocer, amén de los problemas de competencia territorial, y por supuesto también existen problemas para la ejecución de una hipotética futura condena con responsabilidad civil.

Es posible plantear la responsabilidad de los «Muleros» como intermediarios que esperan una recompensa en dinero, y como podemos ver, la jurisprudencia no es unánime en criterio, y es por lo que será necesario realizar la distinción de aquellos que realmente desconocen que están colaborando en un delito, de los que sean conscientes o al menos puedan intuir la situación ilegal, entrando aquí incluso la posibilidad del dolo eventual. Roso Cañadillas[93] analiza la cuestión en relación con esta figura que participa en

dolosa, además de la más que posible suplantación de identidades para eludir la acción de la justicia, entre otras maniobras torticeras que hacen que los procedimientos transnacionales suelan ser demasiado dilatados en el tiempo a la vez que costosos y favorecedores de impunidad. En relación con esta problemática, las Fuerzas y Cuerpos de Seguridad del Estado hoy en día han de disponer de equipos interdisciplinares cada vez más preparados para la prevención y lucha contra la ciberdelincuencia, y ello comporta un coste muy alto para las distintas administraciones públicas, y por ende, para la ciudadanía, si bien se trata de algo que se revela como muy necesario.

[93] *Vid*. al respecto Roso Cañadillas, R., «Algunas reflexiones sobre los nuevos fenómenos delictivos, la teoría del delito y la ignorancia deliberada», en: *Dogmática del Derecho penal material y procesal y política criminal contemporáneas. Homenaje a*

la comisión delictiva de una forma u otra y apunta a la posibilidad también del dolo eventual a partir de la teoría restringida del consentimiento.

Fernández Bermejo[94] entiende que, para exigir el dolo directo en la actuación del mulero, este debe ser consciente de que está colaborando en un delito de estafa y que tiene un ánimo de enriquecimiento con un conocimiento del origen ilícito del dinero, cuestión que entendemos que no será nada fácil a efectos probatorios a no ser que el movimiento de dinero sea constante, fluido y en cantidades que revelen la intencionalidad.

No podemos olvidar que a tenor del artículo 268 del Código Penal no concurre responsabilidad criminal y solamente concurrirá la responsabilidad civil para:

> «…los cónyuges que no estuvieren separados legalmente o de hecho o en proceso judicial de separación, divorcio o nulidad de su matrimonio y los ascendientes, descendientes y hermanos por naturaleza o por adopción, así como los afines en primer grado si viviesen juntos, por los delitos patrimoniales que se causaren entre sí, siempre que no concurra violencia o intimidación, o abuso de la vulnerabilidad de la víctima, ya sea por razón de edad, o por tratarse de una persona con discapacidad.
>
> 2. Esta disposición no es aplicable a los extraños que participaren en el delito».

Por lo que se refiere a los autores que tengan la condición de autoridad o funcionario público *ex* art. 24 CP, la responsabilidad penal se regula con las especialidades recogidas en el artículo 438 CP:

> «La autoridad o funcionario público que, abusando de su cargo, cometiere algún delito de estafa o de fraude de prestaciones del Sistema de Seguridad Social del artículo 307 ter, incurrirá en las penas respectivamente señaladas a éstos, en su mitad superior, pudiéndose llegar hasta la superior en grado, e inhabilitación especial para empleo o cargo público y para el ejercicio del derecho de sufragio pasivo por tiempo de tres a nueve años, salvo que los hechos estén castigados con una pena más grave en algún otro precepto de este Código».

Por último, no podemos obviar que en muchas ocasiones estos delitos de uso fraudulento de medios de pago son perpetrados por los mismos trabajadores de empresas que abusan de su puesto de trabajo, son los llamados *insiders*[95],

Bernd Schünemann por su 70 aniversario, Tomo I, Lima (*Gaceta Penal & Procesal Penal, Gaceta Jurídica*), 2014, pp. 423 y ss.

[94] Fernández Bermejo, D., «El phishing y la responsabilidad penal de los muleros o cibermulas a la luz del artículo 248.2 A) del Código penal». VV.AA. *Tratado de delincuencia cibernética*, Aranzadi, Pamplona, 2021, pp. 371 y ss.

[95] Se conoce como *insiders* de la bolsa a aquellos consejeros o accionistas significativos de una compañía que realizan operaciones de compra/venta de títulos de la empre-

y estos casos no se suelen denunciar para evitar la difusión de una pésima imagen empresarial, finalizando el asunto habitualmente con un despido y una indemnización que genera una perversa impunidad y un incremento de la cifra negra que escapa a la investigación.

4. *Sujeto pasivo*

Sujeto pasivo o víctima del delito de estafa es quien ha sufrido un daño patrimonial, pero también lo es aquel que ha actuado a causa de un error y ha sido engañado, ejerciendo una disposición patrimonial en perjuicio del primero. Si se da esta situación, ambos son víctimas del delito de estafa, pues uno se verá afectado a causa del engaño que le condujo a realizar una conducta ilícita, y el otro también será una víctima por haber sufrido las consecuencias del comportamiento ilícito[96].

En relación con el error, se trata de una representación mental que no se corresponde con la realidad. Si el engaño puede llegarse a objetivar, el error es un elemento del delito de estafa completamente subjetivo. Si no existe la falsa representación de la realidad en la mente del sujeto engañado no sería posible hablar de estafa.

Es por lo que no todas las disposiciones patrimoniales en perjuicio de un sujeto pueden ser constitutivas de delito de estafa, si bien hayan podido ser precedidas de una serie de manipulaciones espurias de la realidad. Solamente sería constitutivo de estafa la falsa representación de la realidad (el error) que procedería del engaño bastante dirigido al sujeto pasivo de la acción típica, como bien señala Benítez Ortúzar[97].

Es importante diferenciar este delito de la estafa común, ya que aquí no existe siempre un sujeto pasivo que sea engañado y un acto de disposición en su perjuicio o en el de un tercero. Ello se pone de manifiesto cuando se consigue extraer dinero de un cajero automático con una tarjeta manipulada, pues aquí la entidad financiera resultaría damnificada, pero faltaría el elemento fundamental del engaño.

Es reiterada la doctrina que tiene en cuenta las circunstancias concretas del sujeto pasivo y sus capacidades. El autor del delito normalmente conoce

sa en que realizan su actividad. Debido a su cargo cuentan con información privilegiada de la compañía en la que llevan a cabo su actividad.

[96] En relación con lo dicho puede verse por ejemplo la STS, n.º 1476/2004, de 21 de diciembre, ECLI:ES:TS:2004:8324.

[97] Benítez Ortúzar, I., «Delitos contra el patrimonio y el orden socioeconómico (V)», en Morillas Cueva, L., (Dir.), Del Rosal Blasco, B., Olmedo Cardenete, M., Peris Riera, J., Sáinz-Cantero Caparrós, J.E., *Sistema de derecho penal. Parte especial*, Dykinson, Madrid, 2021, pp. 370-371.

bien las características de la víctima y se aprovecha de su ignorancia, edad e incluso capacidades intelectuales mermadas. En este ámbito es preciso tener en cuenta parámetros objetivos y subjetivos para aquilatar correctamente la situación[98].

Al sujeto pasivo se le exige que desarrolle un mínimo de autoprotección, que entendemos que no es más que coherencia y sentido común cuando, por poner un ejemplo, en una compra y venta inmobiliaria puede asegurarse de forma fehaciente de quien es el auténtico propietario y si existen cargas o no dirigiéndose al registro de la propiedad correspondiente.

La jurisprudencia también señala que, por ejemplo, la profesión del sujeto pasivo es decisiva, pues el engaño podía haber sido evitado, y así se puede apreciar en la Sentencia del Tribunal Supremo n.º 748/2014, de 7 de noviembre[99]: «El engaño, según la jurisprudencia, no puede considerarse bastante cuando la persona que ha sido engañada podía haber evitado fácilmente el error cumpliendo con las obligaciones que su profesión le imponía».

Es más, el sujeto activo puede darse el caso de que se aproveche de todo un colectivo muy vulnerable, como puede ser el de las personas de edad avanzada que desconoce los últimos avances de las tecnologías y la informática o de las últimas formas de pago y transacciones. Así pues, el conocimiento de la víctima, según Quintero Olivares[100], queda difuminado en casos de estafas masivas muy bien pergeñadas por quienes han diseñado el plan criminal con una relación muy lejana en relación con quienes han sufrido el daño, como en el caso de Fórum filatélico y AFINSA, que hemos comentado anteriormente. En estos casos la estafa estaba muy bien diseñada por los actores del delito, pues iba dirigida primordialmente a un sujeto pasivo de perfil muy conservador en el ahorro, de edad avanzada[101] y que

[98] *Vid.* STS de 22 mayo 2003.

[99] ECLI:ES:TS:2014:4646.

[100] Quintero Olivares, G., «De las defraudaciones», en Morales Prats, F., Morón Lerma, E., Tamarit Sumalla, J Mª., Ramón Ribas, E., Villacampa Estiarte, C., Hernández García, J., Ortega Lorente, J. M., Aguilar Romo, M., Camarena Grau. S., Torres Rosell, N., García Albero, R., Llarena Conde, P., Demetrio Crespo, E., Bañeres Santos, F., Ramírez Ortiz, J. L., Calvo López, M.ª., Navarro Blasco, E., Rueda Soriano, Y., Cugat Mauri, M., Ramos Rubio, C., De La Peña Oliete, M., Portilla Contreras, G., García Rivas, N., Salat Paisal, M., Ortega Gutiérrez-Maturana, M., en Quintero Olivares, G., (Dir.), *Comentarios a la parte especial del Derecho penal*, Aranzadi, Navarra, 2016, pp. 248 y ss.

[101] Es de destacar que el Tribunal Supremo ha interpretado que el sujeto pasivo ha de gozar de cierta capacidad de discernimiento, que muchas veces en personas de edad avanzada está muy limitada. STS n.º 675/2007, de 17 de julio, ECLI:ES:TS:2007:5439. «(...) la exigencia de «engaño bastante para producir error» exige que el concernido goce de cierta capacidad de discernimiento, que es la que deberá ser vencida mediante la puesta en juego de la insidia».

invertía en filatelia y numismática como valores seguros «de toda la vida», tangibles y con una solera muy asentada. Las víctimas además solían ser personas que recomendaban estos productos financieros a otros familiares y amigos íntimos, convirtiéndose en verdadera «cadena transmisora» de una estafa piramidal que afectó a miles de ciudadanos españoles.

En esta tipología de casos podemos decir que estamos ante la figura de una «estafa-masa», que se generará cuando aquel que es engañado engañe a otros generando una situación en cadena, pues los actos de disposición se realizan en favor de alguien que se aprovecha de su estado inicial como si fuera un «primer eslabón».

Cuando nos encontramos ante una afectación de múltiples víctimas con esta tipología de conductas se plantea la consideración del llamado «sujeto pasivo masa» *ex* art. 74.2[102] CP: «Si se tratare de infracciones contra el patrimonio, se impondrá la pena teniendo en cuenta el perjuicio total causado. En estas infracciones el Juez o Tribunal impondrá, motivadamente, la pena superior en uno o dos grados, en la extensión que estime conveniente, si el hecho revistiere notoria gravedad y hubiere perjudicado a una generalidad de personas…».

Dicho esto, hemos de destacar que la jurisprudencia respecto a esta tipología de casos tiende a recurrir al tipo agravado de estafa en relación con el daño ocasionado *ex* art. 250 CP.

Por otra parte, como bien apuntan Barja de Quiroga y Granados Pérez[103], en este tipo de estafas en relación con los medios de pago existe una defraudación en la que intervienen sistemas informáticos o máquinas, y las mismas no pueden ser objeto de engaño ni tampoco ser inducidas a error, añadiéndose además que el «otro» al que hace referencia el artículo ha de ser

[102] La aplicación del límite superior de la pena resulta procedente cuando las concretas acciones que se suman en el delito continuado o el resultado en el que desembocan, desborda el marco de reproche previsto por el legislador para los distintos comportamientos individuales; esto es, cuando, observando la intensidad con que resienten el orden penal el conjunto de acciones enjuiciadas y evaluando en qué medida sobrepasan el daño inherente a cada uno de los comportamientos que se integran, se concluye que el límite máximo de la pena prevista para el delito más grave, no guarda correspondencia con el comportamiento que se enjuicia, bien porque hay procederes individuales que serían merecedores por sí mismos de la máxima punición, bien porque la homogeneidad, el número o la gravedad de los comportamientos ilícitos que se acumulan o reiteran, muestran la insignificancia del reproche a la reiteración delictiva si todos los comportamientos se sancionaran globalmente con la pena prevista para el delito más grave, por más que la pena se exacerbara hasta su máxima extensión (STS Sala 2.ª n.º 1004/2016, de 23 de enero).

[103] Barja De Quiroga, J. y Granados Pérez, C., *Manual de Derecho penal parte especial,* tomo II, Aranzadi, Pamplona, 2018, p. 284.

una persona[104]. En este sentido también Mestre Delgado[105], cuando afirma que las máquinas no pueden ser engañadas y que más bien se trataría de un apoderamiento telemático de los bienes del otro, teniendo que existir una relación de causalidad, y desde el prisma que estas actividades tienen una desemejanza con el delito de estafa tradicional.

5. *Elemento subjetivo*

El elemento subjetivo integra el dolo[106] de la defraudación con el ánimo de lucro[107], y así las cosas, se precisa que concurran los elementos cognitivo y volitivo característicos de esta forma de delinquir. El elemento cognoscitivo ofrece al autor una información fundamental de la víctima para asegurarse la consumación del delito y así provocar una disposición que comporte un perjuicio patrimonial[108], y el elemento volitivo determina que este va a uti-

[104] En este sentido puede verse *ad exemplum* la Sentencia del Tribunal Supremo n.º 185/2006, de 24 de febrero: «Es claro que el delito de estafa, único por el que el recurrente ha sido acusado, no concurre en estos casos, dado que solo puede ser engañada una persona que, a su vez, pueda incurrir en error. Por lo tanto, ni las máquinas pueden ser engañadas –es obvio que no es «otro», como reclama el texto legal–, ni el cajero automático ha incurrido en error, puesto que ha funcionado tal como estaba programado que lo hiciera, es decir, entregando el dinero al que introdujera la tarjeta y marcara el número clave».

[105] Mestre Delgado, E., «Delitos contra el patrimonio y el orden socioeconómico». Lamarca Pérez, C., Alonso de Escamilla, A., Rodríguez Núñez, A., *Delitos. La parte especial del Derecho penal*, Dykinson, Madrid, 2021, pp. 398 y 399.

[106] Según el tenor literal de la STS, n.º 72/2017, de 8 de febrero, (ECLI:ES:TS:2017:442) «(...) el dolo se aprecia cuando el autor conoce que con los actos que ejecuta está poniendo de manifiesto al sujeto pasivo del engaño una situación que aparenta ser real pero que no lo es en alguno de sus aspectos relevantes, induciéndole con ello a realizar un acto de disposición del que resultará un perjuicio propio o de tercero. Y que, con ese conocimiento, decide ejecutar aquellos actos».

[107] *Vid.* la STS, n.º 1581/2003, de 28 de noviembre, ECLI:ES:TS:2003:7580. «(...) En efecto: el ánimo de lucro en el delito de estafa no requiere que el autor persiga su propio y definitivo enriquecimiento. Por el contrario: en el delito de estafa el ánimo de lucro también es de apreciar cuando la ventaja patrimonial antijurídica se persigue para luego beneficiar a otro. Dicho de otra manera: la finalidad de un enriquecimiento antijurídico no depende de lo que el autor piense hacer luego con las ventajas patrimoniales obtenidas contradiciendo la norma del art. 248 CP».

[108] Muñoz Conde entiende que: «La dinámica lucro-perjuicio es, en definitiva, el *leitmotiv* de toda estafa. Pero ello no quiere decir que el perjuicio tenga que ser directamente querido por el sujeto activo de la estafa. El autor de la estafa lo único que pretende es enriquecerse, el perjuicio que con ello pueda irrogar a otros le trae completamente sin cuidado, raramente lo pretende de un modo directo y, a veces, le es penoso causarlo. Pero ello en ningún caso excluye el ánimo de lucro». Muñoz Conde, F., *Derecho penal. Parte*

lizar todos los elementos propios del engaño y acepta como muy probable el éxito del resultado delictivo.

Es cuando menos peculiar la posición de Pastor Muñoz y Coca Vila[109], que remarcan que el elemento subjetivo de esta conducta típica solamente exige la concurrencia de dolo, y no la de un ánimo de lucro.

No podemos estar más en desacuerdo con esta tesis, pues entendemos que el sujeto activo lo que persigue con la utilización fraudulenta fundamentalmente es lucrarse o que un tercero se lucre, de lo contrario, ¿qué es lo que perseguiría la acción típica?

Por otra parte, en la estafa podemos hablar de dolo eventual si nos referimos al dolo con carácter defraudatorio, de forma que:

> «[...] la estafa admite la modalidad de dolo eventual. Existe también dolo defraudatorio cuando se lleva a cabo el negocio con propósito de cumplir solo si se dan las condiciones necesarias para ello, pero asumiendo y consintiendo la alta probabilidad de que eso no suceda y traspasando por tanto a la víctima el riesgo. Es lo que de forma indudable puede decirse que ha acaecido en este supuesto. Eso es dolo eventual»[110].

Eso sí, hay que remarcar que entendemos que ha de existir una alta probabilidad del suceso defraudatorio.

Ab initio entendemos que se excluye el error[111] en este tipo por lo comentado *ut supra*, sin embargo, no podemos soslayar la existencia de una pujante inteligencia artificial que irrumpe en nuestros días con gran fuerza siendo ya una realidad que podrá comportar situaciones de engaños en incluso maniobras para dañar a terceros con desplazamientos patrimoniales delictivos mediante algoritmos muy bien elaborados por expertos. Y como bien señala la Sentencia del Tribunal Supremo Sala 2.ª n.º 194/2017, de 27 de marzo[112], ha de ser precisamente una maquinación del autor la que ha de provocar el error origen del desplazamiento patrimonial.

Especial. 22.ª edición, revisada y puesta al día conforme a las Leyes Orgánicas 1/2019 y 2/2019 con la colaboración de Carmen López Peregrín, Tirant lo Blanch, Valencia, 2019, p. 398.

[109] Pastor Muñoz, N. y Coca Vila, I., «Delitos contra el patrimonio II», VV. AA: *Lecciones de Derecho penal parte especial*, Atelier, Barcelona, 2021, p. 271.

[110] STS, n.º 691/2013, de 3 de julio, ECLI:ES:TS:2013:4501.

[111] En relación con el error es muy representativa la Sentencia del Tribunal Supremo n.º 369/2007, de 9 de mayo (ECLI:ES:TS:2007:3258) que señala que: «No obstante ya un sector doctrinal, ante esta tesis de que el engaño causa del error debe proyectarse sobre una persona lo que no era posible en los supuestos considerados, argumentó que, aunque los datos se proporcionan a la máquina, ésta opera como está programada y por ello, usando los datos adecuados, la persona que no está habilitada para hacerlo, engaña a quien programó la máquina».

[112] ECLI: ES:TS 2017:1067.

Si bien el dolo y la imprudencia son dos formas de imputación subjetiva del delito, y al tratarse de dos modalidades que se incardinan en una sola categoría, podríamos esperar la existencia de una estructura básica compartida, sin embargo, si realizamos una comparación, podríamos llegar a concluir que existen notables distinciones que pueden llegar a ser incluso chocantes, como bien asevera MOLINA FERNÁNDEZ[113].

En la utilización fraudulenta de tarjetas y otros medios similares es complejo encontrar casos cometidos por imprudencia, si bien alguno existe[114], ya que se trata de una categoría gradual, que puede ser más o menos grave, puesto que siempre se ha admitido que la acción imprudente tenga una gradación. Por contra, el dolo se concibe en la ley, la jurisprudencia y la doctrina como una categoría plana y se define de modo unitario, no existe más o menos dolo, no hay una gradación, como apunta DÍAZ PITA[115]. Por el contrario, en caso de error si tenemos en cuenta que puede ser vencible, sí que podría existir tal gradación.

6. *Iter criminis*

Como hemos indicado *ut supra* este delito puede ser cometido de múltiples formas, y algunas de ellas las vamos a comentar sin ánimo de exhaustividad.

En cuanto a su naturaleza jurídica, es un delito de resultado material que para que pueda concretarse se precisa de una disminución patrimonial ajena, una traslación de activo patrimonial que genere un daño a la víctima de carácter económico, y además requiere la existencia de un perjuicio evaluable económicamente, consumado o en grado de tentativa. En relación con la posibilidad de la tentativa es poco frecuente encontrarla en nuestra jurisprudencia, ya que los casos de inidoneidad del engaño suelen fracasar por sí mismos y ni tan solo podrán llegar a constituir una tentativa precisamente porque

[113] MOLINA FERNÁNDEZ, F., *Op. cit.* pp. 737 y ss.

[114] Como es el caso de Alejandro Fernández, el joven granadino condenado a cinco años de prisión por pagar 80 € con una tarjeta falsa en 2016 cuando tenía 18 años. Alejandro ingresó en prisión cuando tenía 24 años, una familia y trabajo estable. El dramático caso conmocionó a la opinión pública española porque se ponía en serio entredicho el derecho a la reinserción ex art. 25.2 CE que tiene todo ciudadano, con una sentencia que recayó firme seis años después de los hechos y un montante económico nimio comparado con la pérdida de la libertad que iba a sufrir Alejandro. *Vid.* EUROPA PRESS., disponible en: https://www.europapress.es/andalucia/noticia-joven-encarcelado-granada-pagar-80-euros-tarjeta-falsa-pide-gobierno-resuelva-peticion-indulto-20170610111534.html. (Última consulta: 5 de enero de 2023).

[115] DÍAZ PITA, M. M., *El dolo eventual*, Tirant lo Blanch, Valencia, 1994, pp. 290 y ss.

faltan las condiciones esenciales para una imputación objetiva que no han podido servir ni tan solo para el inicio de la ejecución. La tentativa solamente cabría en casos de engaño idóneo en los que la víctima no llega a realizar el acto de disposición por una serie de causas que pueden ser sobrevenidas.

Esta tipología de estafa requiere para que se consume la existencia de un perjuicio patrimonial, solamente podrá estimarse la tentativa en los casos en que hay un fracaso por razones ajenas a la voluntad del sujeto activo, por ejemplo, cuando se introducen los datos de la tarjeta para efectuar una compra y se envía un código de seguridad a un móvil, que no está al alcance y no se puede finalizar la operación con éxito, como bien ejemplifica Pastor Muñoz[116].

Llegados aquí hemos de hacer especial referencia al intento de extracción de efectivo de cajeros sin el conocimiento de la contraseña, que se protegerá normalmente con dispositivos que lo que hacen es reducir las probabilidades de que alguien que no esté autorizado pueda lesionar el bien jurídico del patrimonio de una posible víctima con un desplazamiento económico de forma ilegal. Acertar una contraseña de una tarjeta que no conocemos, *a priori* es algo imposible en condiciones de normalidad, dependiendo el acierto de la suerte del sujeto activo, como aquel que juega a la lotería o a las quinielas. Habitualmente la situación se concreta en acertar cuatro dígitos que con frecuencia tienen relación con el número del Documento Nacional de Identidad, fecha de nacimiento, algún número anotado que queda en una cartera, etc., y es así como las posibilidades de acierto van *in crescendo*.

En estos casos nuestros tribunales se han posicionado en dos sentidos: por una parte, han apreciado que existe la posibilidad de tentativa inidónea no punible, ya que el acierto de un código de una tarjeta si no se utilizan procedimientos técnicos harto complejos para el descifrado es prácticamente imposible y despreciable técnicamente. Por otra parte, la otra posición que se ha adoptado apunta que la tentativa no es absolutamente idónea, ya que, aunque la probabilidad de acierto sea muy baja, ello no es del todo imposible, y además existe la posibilidad de llevar a cabo varios intentos antes de que se produzca un bloqueo por parte de la entidad emisora en aras de conseguir la máxima seguridad posible. Aquí estamos de acuerdo con Molina Fernández[117] en que la situación ha de ser tutelada por parte del Derecho Penal por-

[116] Pastor Muñoz, N., *Op. cit.* pp. 272 y 273.

[117] Molina Fernández, F., «Intentos de extraer dinero de un cajero sin tener la clave: el problema del dolo directo con baja probabilidad y su trascendencia para la dogmática del dolo y la imprudencia», en Gómez Martín, V., Bolea Bardon, C., Gallego Soler, J.I., Hortal Ibarra, J.C., Joshi Jubert, U. (Dirs.); Valiente Ivañez, V., Ramírez Martín, G. (Coords.) *et al., Un modelo integral de derecho penal. Libro homenaje a la profesora Mirentxu Corcoy Bidasolo.* B.O.E., Madrid, 2022, pp. 737 y ss.

que se genera una situación de riesgo en relación con el bien jurídico protegido del patrimonio, pues pensemos que las tarjetas bancarias tienen una probabilidad de acierto en relación con su código de aproximadamente (3/10.000), proporción realmente muy baja, pero no imposible, y la probabilidad de acierto dependerá y se incrementará también en relación con las veces que se permita el intento.

El tiempo también es un factor que ha de resolver nuestro ordenamiento jurídico en relación con este ámbito de la criminalidad, ya que se plantean incógnitas sobre cuándo se ha de entender que se ha cometido el delito, y posteriormente el perjuicio que se haya podido irrogar hasta la consumación delictiva, ya que los daños en la esfera de los delitos cometidos mediante la informática puede suceder que no se puedan cuantificar hasta pasados varios años, con la problemática añadida de una posible prescripción generadora de una impunidad indeseable.

¿En qué momento el hecho irrelevante penalmente ofrece un riesgo real que se convierte en típico? Por el momento no podemos tener una respuesta cierta, ni tan solo acudiendo a la paradoja del montón de arena de Eubúlides de Mileto[118].

7. *Concursos*

Hay autores como Núñez Castaño que son del parecer que este tipo penal no se precisaba, puesto que los supuestos que recoge ya están previstos en otros tipos y ello puede generar una problemática en materia de concursos con otros delitos ya existentes, y más concretamente señala los supuestos en los que el sujeto activo utilice las tarjetas de crédito o débito para efectuar operaciones en un establecimiento comercial o de otro tipo, que quedan sancionados en la estafa genérica del artículo 248 del CP, existiendo un supuesto

[118] La paradoja del montón de arena se establece de la siguiente manera: Tenemos mucha arena. Si quitamos una partícula de un montón de arena, no hacemos que el montón de arena desaparezca. Si repetimos la misma operación, todavía nos quedará mucha arena. Pero un montón de arena no es más que un conjunto finito de granos de arena. Entonces, si continuamos con esta operación, algún día no tendremos más granos, lo que significa que el montón desaparecerá. Esta pequeña historia muestra lo difícil que es reconciliar los siguientes dos argumentos: sacar un grano de arena de un montón no lo hace desaparecer. Un montón consiste en un número finito de partículas. En la antigua Grecia, la paradoja era un arma principal cuando los escépticos luchaban por demostrar que la razón no podía conducir al conocimiento absoluto. La paradoja de los montones o *sorites* se atribuye a Eubúlides de Mileto, filósofo griego de la escuela de Megara y autor de la famosa paradoja del mentiroso, paradoja que surge cuando se utiliza el sentido común para oscurecer conceptos, que en definitiva son ataques a los supuestos de la lógica aristotélica.

de lo que se ha denominado estafa triangular, donde el sujeto engañado es distinto del sujeto pasivo o perjudicado.

En otro orden, la relación existente entre el delito de estafa y la apropiación indebida es una cuestión muy debatida, y encontramos que en algunas calificaciones se aprecia el concurso de normas entre la falsedad y la estafa. No es una cuestión menor, y la doctrina, si bien tiende en su mayoría a apreciar el concurso de normas, la jurisprudencia del Tribunal Supremo, de las diferentes audiencias provinciales, y Fiscalía suelen calificar como concurso de delitos.

La doctrina científica sigue la línea de la consunción entre las falsedades instrumentales y el delito de estafa, siendo una cuestión muy diferente la relación existente entre la estafa y la falsificación de documento público.

No han sido pocas las veces que se ha castigado la acción delictiva que proviene de la falsificación de una tarjeta y también la estafa, con lo que se produce una situación de doble castigo, que sería del todo incompatible con el principio fundamental del *non bis in idem.*

No podemos obviar que la maniobra de engaño intrínseca de la estafa puede precisar de forma necesaria del documento que se ha falsificado para poder conseguir que la víctima sufra un error, y por consiguiente se genere un desplazamiento patrimonial en una relación de causa y efecto.

Un sector de la doctrina entiende que ese desplazamiento patrimonial es cuestionable, pues puede darse el caso de un viajero que no remunera un servicio de transporte con su billete y que produce solamente una pérdida en la empresa, hecho muy cotidiano[119]. Incluso se ha llegado a discutir si una falsificación de títulos de viaje, por ejemplo, como los de transporte público, constituyen un delito de estafa si existe la finalidad de engañar a quien ha de realizar el control de estos. La Fiscalía[120] y la jurisprudencia han entendido

[119] *Vid.* entre otras, SAP V 20 marzo 2002 (ECLI:ES:APV:2002:1539), SAP V 20 noviembre 2002. (ECLI:ES:APV:2002:6485) y SAP M 30 enero 2012 (ECLI:ES:APM:2012:129).

[120] Según la Fiscalía General del Estado, «estimula en quienes realizan funciones de vigilancia la errónea representación de estar utilizando una tarjeta válida, por lo que confluyen los elementos del engaño y el error que exige el tipo de la estafa, a los que se añaden el acto de disposición patrimonial, consistente en la conducta omisiva del vigilante que tolera el acceso, y el consiguiente perjuicio, consistente en el disfrute de un servicio por parte de quien no lo ha pagado». Ello según Consulta 3/2001, de 10 de mayo, de la Fiscalía General del Estado, sobre la calificación jurídico-penal de la utilización, en las cabinas públicas de teléfonos, de instrumentos electrónicos que imitan el funcionamiento de las legítimas tarjetas prepago, citando la Consulta 4/1993, específicamente dedicada a la calificación jurídico-penal de las manipulaciones fraudulentas de las tarjetas multiviaje en los transportes públicos urbanos. *Vid*. Consulta de la Fiscalía General del Estado n.º 3/2001, de 10 de mayo, sobre la calificación jurídico-penal de la utilización, en las cabinas públicas de teléfonos, de

que existe estafa incluso cuando la manipulación es de carácter grosera y bruta, cuando la falsificación consigue generar incluso un sonido igual en el torno de control y se llega a consumar la acción delictiva[121]. En este punto no podemos estar más en desacuerdo, pues no podemos olvidar el principio de intervención mínima del Derecho penal y de *ultima ratio.*

Sobre la polémica cuestión de los concursos es preciso traer a colación el Acuerdo del Pleno no Jurisdiccional de la Sala 2.ª del Tribunal Supremo de 18 de julio de 2007, que cuando abordó la cuestión del tipo de concurso que existe entre la estafa y la falsedad documental señaló que la firma del tique de compra simulando la firma del verdadero titular de una tarjeta de crédito no queda absorbida por el delito de estafa. Dicho esto, puede existir la posibilidad de que se aprecie un concurso medial entre el delito de falsedad y la estafa, pues un documento falseado puede conducir y ser elemento esencial para conseguir el fin último de engañar y por ende, estafar. Y es por lo que, entendemos que se impone la máxima cautela en la apreciación de la estafa y la falsedad de documento siempre teniendo en cuenta la gravedad del caso, pues puede producirse un castigo desproporcionado.

Trayendo a colación la Sentencia del Tribunal Supremo n.º 971/2011, de 21 de septiembre[122] vemos que indica:

> «La solución impuesta por la reforma de la LO 5/2010, 22 de junio, con la consiguiente aplicación del art. 399 bis, apartado 3º, conduce de forma obligada a un concurso entre el delito de falsedad y el delito de estafa. Y es que la misma reforma ha introducido en el art. 248.2 c) del CP una nueva modalidad de estafa, castigando con la pena de prisión de 6 meses a 3 años, a "los que utilizando tarjetas de crédito o débito o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero"».

En este caso entendemos que la situación aúna todas las características para considerarse un concurso aparente[123] de normas y no un concurso de

instrumentos electrónicos que imitan el funcionamiento de las legítimas tarjetas prepago. Mediante esta consulta se interpretan los siguientes artículos del CP: 255.1.º, 623,4.º, 273.3, 270, 287.1. Modificaciones legislativas posteriores que le afectan: Modificación del art. 287.1 CP, 270 por Ley Orgánica 15/2003, de 25 de noviembre. Modificación del art. 273 por LO 15/2003, de 25 de noviembre, que modifica la pena de multa. Modificación de los arts. 255 y 623 CP por LO 15/2003, de 25 de noviembre para actualizar las cuantías (400 €). Modificación del art. 270 por Ley Orgánica 5/2010, de 22 de junio.

[121] *Vid*. al respecto, Faraldo Cabana, P., *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*, Tirant lo Blanch, Valencia, 2009, *passim*.

[122] ECLI:ES:TS:2011:5955.

[123] Tribunal Supremo, Sala Segunda, de lo Penal, Sentencia 330/2014 de 23 Abr. 2014, Rec. 1772/2013, ECLI: ES:TS:2014:1486, FD 7.º Resolución con base en el principio de alternatividad.

delitos, pues el mismo permite llevar a cabo la apreciación de una unidad valorativa ante los hechos típicos perpetrados, siendo preciso que se aplique solo un tipo.

Hay que tener en cuenta que si no se toma una especial cautela en la valoración unitaria de los hechos y su calificación con un solo tipo que recoja todo el desvalor penal de la acción típica, corremos el riesgo de incurrir en el quebranto inadmisible del principio del *non bis in idem*, conculcándose asimismo el principio de proporcionalidad en detrimento de la seguridad jurídica.

Quintero Olivares[124] entiende que, entre la estafa, la falsedad documental que no verse en documentos públicos, y la apropiación indebida debe apreciarse el concurso de normas y no de delitos.

Si acudimos al Acuerdo de la Sala de lo Penal de 28 de junio de 2022[125], sobre la falsificación de tarjetas de crédito como falsificación de moneda y resoluciones sobre clasificación de penados no recurribles apreciamos que se equipara el llamado «dinero de plástico», objeto de un posible delito, la moneda *ex* arts. 386 y 387 CP, existiendo por ello una posible calificación de falsificación de moneda y timbre. También se incluye como núcleo central de este delito la posibilidad de una falsificación de la banda magnética, elemento esencial de la inmensa mayoría de las tarjetas actuales, si bien, ya se imponen en su gran mayoría las que incorporan un microchip, que consigue ofrecer una mayor seguridad.

Es de destacar que, con la reforma del CP operada por Ley Orgánica 14/2022, de 22 de diciembre, que entró en vigor el 12 de enero de 2023, el art. 399 bis 4.ª CP ha quedado modificado y castiga la falsificación de tarjetas de crédito, débito, cheques de viaje, e introduce «cualquier otro instrumento de pago distinto del efectivo». Este mismo artículo incorpora un apartado cuatro que castiga al que:

> «…para su utilización fraudulenta y a sabiendas de su falsedad, posea u obtenga, para sí o para un tercero, tarjetas de crédito o débito, cheques de

[124] Quintero Olivares, G., *Op. cit*. págs., 248 y ss.

[125] Acuerdo: «las tarjetas de crédito o débito son medios de pago que tienen la consideración de «dinero de plástico», que el artículo 387 del código penal equipara a la moneda, por lo que la incorporación a la «banda magnética» de uno de estos instrumentos de pago, de unos datos obtenidos fraudulentamente, constituye un proceso de fabricación o elaboración que debe ser incardinado en el art. 386 del Código penal». *Vid.* CGPJ: Acuerdo sobre: 1º Falsificación de tarjetas de crédito como falsificación de moneda; 2º Resoluciones sobre clasificación de penados son recurribles. Disponible en: https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunal-Supremo/Jurisprudencia-/Acuerdos-de-Sala/Acuerdo-sobre--1--Falsificacion-de-tarjetas-de-credito-como-falsificacion-de-moneda--2--Resoluciones-sobre-clasificacion-de-penados-son-recurribles. (Fecha de consulta: 15 de junio de 2022).

viaje o cualquier otro instrumento de pago distinto del efectivo será castigado con pena de prisión de uno a dos años».

Entendemos que esta reforma es procedente para dejar abierta la posibilidad a nuevas formas de pago que provienen de las nuevas tecnologías sobre las que hemos ido haciendo referencia en el presente artículo.

Aquí se hace preciso realizar una distinción entre el concurso de normas y el concurso ideal o instrumental. El concurso aparente de normas comporta que se lleve a cabo una valoración unitaria en relación con el hecho presuntamente típico, y sería suficiente que se aplicase uno solo de los tipos que comportan la calificación.

Si entramos a comentar la relación entre el delito de estafa y el delito de falsedad en documento oficial o mercantil, el Tribunal Supremo *ex* art. 390 CP entiende que se trata de un tipo de estafa que tiene como fundamento el documento falsificado que está destinado a una finalidad delictiva y que se identifica con el engaño.

El documento falsificado ya de por sí constituye el engaño y se entiende que existe una consunción de conceptos[126].

Por otra parte, entre el delito de falsedad y el de denuncia falsa, existe un concurso ideal instrumental, puesto que el primero es un medio para cometer el segundo, y así también lo entiende el Tribunal Supremo en la Sentencia 254/2011, de 29 de marzo[127]. En otro orden, entre los delitos de falsedad en documento mercantil y la estafa procesal entendemos que no existe una relación de consunción, ya que ninguno de los dos tipos penales dispone de la amplitud que pueda permitir recoger el contenido del otro[128].

8. *Penalidad*

A nivel internacional para castigar estos crímenes que cada vez son más frecuentes y complejos, fundamentalmente se ha optado por las siguientes

[126] De esta forma queda reflejado en la sentencia del Tribunal Supremo n.º 1126/2011, de 12 de noviembre. «Desde antiguo, la doctrina científica consideró al documento falsificado, funcionalmente destinado a cometer una estafa (estafas documentales), como identificable con el engaño. El engaño es el propio documento, entendiendo fundidos ambos conceptos por consunción, ya que la alteración documental no es un ingrediente más del ardid, sino su misma esencia. De esta idea solo deben quedar excluidas las falsedades cometidas por funcionarios públicos en el ejercicio de sus cargos, en cuanto suponen una dimensión adicional del injusto». ECLI:ES:TS:2011:8023.

[127] STS, n.º 254/2011, de 29 de marzo, ECLI:ES:TS:2011:1861.

[128] STS, n.º 232/2014, de 25 de marzo, ECLI:ES:TS:2014:1220.

vías: elaborar leyes penales especiales[129], crear nuevos tipos penales[130], o elaborar nuevas leyes internacionales[131].

[129] Aquí se han prodigado países como España, Francia, Gran Bretaña, Holanda, Estados Unidos, Chile o Venezuela, que han elaborado Leyes penales *ad hoc*. En Europa, Francia dispone de una Ley relativa al fraude informático desde 1988 y Reino Unido promulgó en 1991 la *Computer Misuse Act* como consecuencia de un grave caso de hacking. Estados Unidos promulgó en 1994 el Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030), que modificó al Acta de Fraude y Abuso Computacional de 1986, y en Latinoamérica hay que destacar la Ley chilena contra los delitos informáticos de 1993.

[130] En Europa, Alemania, Austria, Italia, España y Portugal, y en Latinoamérica, Argentina y México son los principales países que han adoptado esta solución.

[131] Desde las Naciones Unidas es preciso traer a colación el Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos, de 1977. En cuanto al Consejo de Europa, hemos de destacar el Convenio sobre el Cibercrimen, aprobado en Budapest en 2001 y vigente desde julio de 2004. Asimismo, es fundamental el Tratado de Lisboa en 2007. Destaca especialmente el Convenio sobre la Ciberdelincuencia, adoptado en Budapest el 23 de noviembre de 2001. Este convenio surgió del trabajo de expertos de 45 países miembros del Consejo de Europa, pero además se incorporaron países como los Estados Unidos de América, Canadá y Japón. España ratificó este convenio el 20 de mayo de 2010, entrando en vigor el 1 de octubre de 2010. Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. BOE» n.º 226, de 17 de septiembre de 2010, pp. 78847 a 78896. En el Preámbulo del Convenio de referencia se indica expresamente: la necesidad de aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional; se reconocen los profundos cambios provocados por la digitalización, la convergencia y la globalización continua de las redes informáticas; se reconoce el riesgo de las redes informáticas y la información electrónica; se reconoce la necesidad de una cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los legítimos intereses en la utilización y el desarrollo de las tecnologías de la información y que es precisa una lucha efectiva contra la ciberdelincuencia que requiere una cooperación internacional en materia penal reforzada, rápida y operativa. Es de destacar en España la transposición de la Directiva Europea 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión Marco 2005/222/JAI del Consejo. Ya en el primer considerando de la Directiva se hace expresa referencia a la necesidad de homogeneizar la legislación penal de la UE y fomentar la cooperación también desde los distintos cuerpos policiales. «Los objetivos de la presente Directiva son aproximar las normas de Derecho penal de los Estados miembros en materia de ataques contra los sistemas de información, mediante el establecimiento de normas mínimas relativas a la definición de las infracciones penales y las sanciones aplicables, y mejorar la cooperación entre las autoridades competentes, incluida la policía y los demás servicios especializados encargados de la aplicación de la ley en los Estados miembros, así como los organismos especializados de la Unión, como Eurojust, Europol y su Centro Europeo contra la Ciberdelincuencia y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)».

En nuestro país, en relación con la penalidad, recordemos que todas sus modalidades participan del sistema de determinación y cualificación de la pena prevista en los artículos 249[132] y 250 CP[133].

Ya que se trata de una defraudación patrimonial, ha de existir una operación que produzca a la víctima un perjuicio patrimonial que tenga correlato con el beneficio patrimonial conseguido por el autor, y según su cuantificación, atendiendo a la reforma del CP de 22 de diciembre de 2022 *ex* art. 248:

> «Los reos de estafa serán castigados con la pena de prisión de seis meses a tres años. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre este y el defraudador, los medios empleados por este y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción. Si la cuantía de lo defraudado no excediere de 400 euros, se impondrá la pena de multa de uno a tres meses».

Nótese que desde la reforma del Código Penal de 2010[134], la utilización fraudulenta pasó a estar tipificada en el artículo 248.2 c) CP cambiando mucho la penalidad, puesto que para el robo con fuerza en las cosas se preveía prisión de uno a tres años *ex* art. 240 CP, mientras que para la estafa se prevé una pena de prisión de seis meses a tres años *ex* art. 249 CP, con un castigo sustancialmente distinto.

También en referencia a la penalidad, Blanco Lozano[135] es muy crítico y entiende que la estafa informática, teniendo en cuenta la enorme cuantía de las sumas que se pueden defraudar resulta excesivamente benigna si la comparamos con la que se atribuye, por ejemplo, al robo, con lo que parece que

[132] En un plano más «concreto» el art. 249 CP añade pautas para la individualización judicial de las penas, de manera adecuada al principio de culpabilidad: el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre este y el defraudador, los medios empleados por este y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción. En el presente caso la cuantía de lo defraudado no ha sido reputada de gran magnitud, por lo que la Audiencia no ha apreciado la circunstancia 6ª del art. 250 CP. Pero el medio de engaño utilizado sí reviste extrema gravedad por su persistencia y por cuanto ha consistido en que el acusado se hizo pasar por miembro de la Guardia Civil, con la facilitación que ello supone en el trance de derribar las normales barreras que adopta el perjudicado para preservar su patrimonio. (STS 1217/2005, de 4 de octubre).

[133] En el Pleno no jurisdiccional de la Sala Penal del Tribunal Supremo celebrado el 26 de abril de 1991 se deliberó sobre las cuantías que permiten apreciar la agravante de especial gravedad atendido el valor de la defraudación prevista en el número 6.º del artículo 250 del Código Penal de 1995 (ahora 250.1.5 CP que se cuantifica en 50.000 euros, o afecte a un elevado número de personas).

[134] La LO 5/2010, de 22 de junio, modifica el art. 248 CP, en su art. único. 61.

[135] Blanco Lozano, C., *Tratado de Derecho penal español*, parte especial, tomo II, Vol. I, J.M. Bosch, Barcelona, 2007, p. 537.

una vez más, en este ámbito deambula la endémica tendencia de la mayoría de los sistemas penales a tratar con mayor vehemencia a los delincuentes de cuello blanco en un claro «Derecho penal del amigo»[136].

9. *Responsabilidad civil*

La cuestión de la responsabilidad civil es un tema harto complejo y especialmente cuando nos encontramos ante estafas multimillonarias, escándalos que han golpeado a millones de bolsillos de la ciudadanía y que ya hemos comentado con anterioridad. Estamos de acuerdo con Queralt Jiménez[137] en que los grandes estafadores saben muy bien cómo ocultar los beneficios obtenidos mediante grandes estafas, pues son delincuentes dotados de una gran especialización y formación. Además, incluso encontramos casos de personajes ratificados por universidades tan importantes y grandes como «ciegas». Aquí podemos recordar el caso de Mario Conde, que fue nombrado doctor honoris causa y que con su gestión provocó la desaparición de Banesto, previa intervención del Gobierno de España.

La pieza de responsabilidad civil en la mayoría de las ocasiones se instruye poco y mal, puesto que se sabe que la gran mayoría de casos nada patrimonial se encontrará, y ello comporta dar paso a una instrucción paralela tan intensa como la de la pieza principal en que se ahonde en el patrimonio que se está encubriendo.

IV. CONCLUSIONES Y PROPUESTAS

Como ya hemos apuntado en la introducción del presente artículo, nos encontramos en un momento histórico en el que todo va muy deprisa, y los cambios acontecen de forma vertiginosa. Estos cambios raudos están afectando de forma directa a colectivos muy vulnerables, como los y las trabajadores y trabajadoras, que suelen ser jóvenes, que desempeñan labores de reparto y que dependen de sueldos caquécticos que pagan grandes multinacionales que presionan cada vez con mayor agresividad para obtener los mayores beneficios al menor coste, incluso vulnerando los derechos más básicos mediante formas de contratación fraudulentas en una situación además, de clara explotación[138].

[136] Concepto que de forma muy acertada acuñó por primera vez Prieto del Pino en Prieto del Pino, A. M.ª., «La armonización del Derecho penal español», *Boletín de información del Ministerio de Justicia*, Madrid, 15 de junio de 2006, pp. 101 y ss.

[137] Queralt Jiménez, J., *Derecho penal español. Parte especial*. Tirant lo Blanch, Valencia, 2015, p. 523.

[138] Sería el caso de un falso autónomo, que es quien trabaja para una empresa como si fuera un autónomo, pero en realidad es un empleado encubierto, ya que su empleador

Pero hay más colectivos vulnerables, como pueden ser las personas que por cuestión de edad no están al día en relación con las nuevas tecnologías, convirtiéndose en presa fácil de diferentes tipos de estafa, incluida la que se comete mediante las tarjetas de crédito, débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo.

Los medios utilizados por la llamada «ingeniería social[139]» tienen como característica esencial el aprovechamiento de la mínima o nula formación e información (veraz) de que disponen la mayor parte de las víctimas, como es el caso de personas de edad avanzada y/o los llamados «inmigrantes digitales», que junto a los menores[140], se encuentran en una situación de clara desventaja ante la criminalidad cibernética. En el caso de esta tipología de víctimas, en muchas ocasiones existen tipos de estafas informáticas que se

tiene el control sobre su trabajo, su horario y sus condiciones laborales, pero no lo trata como tal, y se ahorra los costes laborales asociados a tener empleados. Esto genera tensiones porque los empleados tienen derechos y protecciones laborales que los trabajadores autónomos no tienen. Los falsos autónomos, por otro lado, pueden estar sujetos a una gran inseguridad laboral, ya que su trabajo no tiene las mismas garantías ni protecciones laborales que un trabajador por cuenta ajena.

[139] La ingeniería social es un conjunto de técnicas utilizadas por ciberdelincuentes para obtener información confidencial o realizar actividades maliciosas a través de la manipulación de las personas. Consiste en persuadir a un individuo para que revele información personal o confidencial, como contraseñas o datos bancarios, o para realizar acciones que beneficien al atacante, como abrir un enlace malicioso o descargar un archivo infectado. Los ingenieros sociales utilizan diferentes técnicas para manipular a las personas, como la persuasión, el engaño, la intimidación o la simpatía. También pueden hacer uso de la ingeniería social en línea, utilizando técnicas como el *phishing* o el *spear phishing*, que consisten en enviar correos electrónicos falsificados para engañar a las personas y obtener información confidencial. Se revela como muy importante estar alerta y educar a los usuarios sobre las técnicas utilizadas por los ingenieros sociales. También es ide gran relevancia tener políticas de seguridad sólidas y un entrenamiento en seguridad cibernética para el personal de las empresas y así establecer medidas de seguridad efectivas, como por ejemplo el uso de contraseñas seguras y la autenticación.

[140] Puede verse al respecto la obra de Abadías Selma, A., Fernández Albesa, N. y Leal Ruíz, R., *Ciberdelincuencia: temas prácticos para su estudio*, Colex, A Coruña, 2021, donde se hace una especial referencia en el capítulo 1 en relación con la ciberdelincuencia en la infancia y contra las libertades, y en el capítulo 11 sobre los ciberdelitos contra colectivos vulnerables: con discapacidad, edad avanzada, y víctimas de la radicalización. La Constitución española tiene previsto en su artículo 51.1 que: «Los poderes públicos garantizarán la defensa de los consumidores y usuarios, protegiendo, mediante procedimientos eficaces, la seguridad, la salud y los legítimos intereses económicos de los mismos», y en virtud de este mandato constitucional, las diferentes administraciones no pueden soslayar la desprotección que sufren algunos colectivos vulnerables a los que ya hemos hecho referencia y que merecen el máximo apoyo y tutela para no terminar siendo víctimas de las diferentes tipologías de estafas informáticas.

detectan mayormente por lo inverosímil de su proceder y el envío masivo de información perversa con el objetivo de conseguir el máximo beneficio con las estafas que se perpetran mediante los medios de pago, que cada vez son más y más diversas[141].

En relación con el bien jurídico protegido por esta reforma del delito de estafa, es el patrimonio, pudiendo tratarse de bienes muebles o inmuebles, derechos o servicios, siempre y cuando haya la posibilidad de la conversión en dinero. Pero además del patrimonio, entendemos que es fundamental que se proteja la buena fe y/o las relaciones de confianza que han de presidir una economía de mercado segura que promueva el progreso económico.

Ya en sede de la acción típica, como no podía ser de otra forma, los tiempos corren y las formas de estafa lo han hecho de consuno. Hemos pasado de aquel *Stellionatus*, por el timo de la estampita, estafas piramidales con una amplia victimización, y hoy en día estamos ante un panorama en el que las posibilidades de la criminalidad en relación con medios de pago, tarjetas de crédito, débito, cheques de viaje u otros medios de pago materiales e inmateriales distintos del efectivo podríamos decir que son infinitas. Como dice el adagio popular, no es posible «poner puertas al campo», y es por esto que la autoprotección de la ciudadanía ha de hacerse más presente que nunca, y entendemos que las distintas administraciones públicas han de colaborar en este cometido de forma decidida ayudando a la prevención con formación, transparencia y lucha contra el delito con medios materiales y humanos especializados acordes a los tiempos, pues si bien los cheques de viaje ya prácticamente no se usan, las tarjetas[142] y los llamados «otros medios de pago materiales e inmateriales distintos del efectivo» están cada vez más en auge y en diversos formatos.

También queremos hacer referencia a las entidades financieras, pues pueden aportar mucho en materia de transparencia, información e incluso pedagogía hacia sus usuarios, que en muchas ocasiones utilizan medios de pago distintos del efectivo que ni tan solo comprenden poniendo en grave riesgo

[141] Como muy bien señala Fernández Teruelo en Fernández Teruelo, J.G., «Clásicas y nuevas conductas fraudulentas ejecutadas en la red y su subsunción en los tipos de estafa y estafa informática contenidos en el Código penal». Gómez Martín, V., Bolea Bardon, C., Gallego Soler, J.I., Hortal Ibarra, J.C., Joshi Jubert, U. (Dirs.); Valiente Ivañez, V., Ramírez Martín, G., (Coords.) *et al.; Un modelo integral de derecho penal. Libro homenaje a la profesora Mirentxu Corcoy Bidasolo*. B.O.E., Madrid, 2022, pp. 1136 y 1137.

[142] *Vid.* Banco de España., *Departamento de Sistemas de Pago División de Vigilancia y Análisis de Infraestructuras.* Disponible en: https://www.bde.es/f/webbde/SPA/sispago/ficheros/es/estadisticas.pdf. (Fecha de última consulta: 1 de mayo de 2023). Aquí puede verse en gráficos la evolución de la utilización de las tarjetas en España desde 2002 hasta 2022.

su patrimonio mediante transacciones de diversa índole y tipología. No sirven solamente los códigos de de buenas prácticas de las entidades, y sí se precisan departamentos de defensoría del cliente que sean externos, ello amén de la necesidad de disponer de un servicio de reclamaciones del Banco de España[143] más cercano a la ciudadanía y con más medios para actuar de forma ágil, eficiente y eficaz.

No podemos soslayar que los avances en las tecnologías abren más oportunidades a la comisión delictiva, pero también disponemos de medios mucho más sofisticados para la prevención y lucha contra el delito que se habrán de ir actualizando sin pausa, como algo totalmente normal[144].

Al albur del paso del tiempo y del acontecer del día a día era inevitable una reforma del articulado que ya demandaba la legislación europea, y que se ha traducido en una fórmula que podríamos denominar «abierta» para evitar la «obsolescencia programada» a la que hemos aludido con anterioridad. Esta fórmula más abierta o flexible seguramente permitirá recoger la casuística que se genere por las tarjetas de compra de centros comerciales, de transporte, de teléfono, tarjetas virtuales, Pay Pal, Bizum, etc., que juntamente con los cheques, talones y letras de cambio no se contemplaban.

También es relevante mencionar la esfera de los delitos cibernéticos[145], donde los hechos delictivos que se perpetran mediante medios de pago de forma fraudulenta se avanzan de forma cada vez más rápida al legislador, y

[143] *Vid.* Banco de España., *Memoria de Reclamaciones.* Disponible en: https://www.bde.es/bde/es/secciones/informes/informes-y-memorias-anuales/memoria-de-reclamaciones/. (Fecha de última consulta: 29 de abril de 2023). La memoria anual de Reclamaciones presenta un análisis estadístico de los expedientes tramitados cada ejercicio. Se indican, entre otras cuestiones, las materias sobre las que versan las reclamaciones presentadas, así como las entidades afectadas por las mismas, y se expone la normativa de transparencia y criterios de buenas prácticas aplicados en las resoluciones emitidas durante el año correspondiente. El 1 de septiembre de 2022, se cumplieron 35 años de la puesta en marcha del Servicio de Reclamaciones del Banco de España, uno de los pioneros y de mayor actividad a nivel europeo.

[144] Oficina de Seguridad del Internauta. Disponible en: https://www.incibe.es/ciudadania (Fecha de última consulta: 29 de abril de 2023). Donde se presentan una serie de talleres de ciberseguridad, dirigidos a personas mayores de 14 años, totalmente gratuitos. Con ellos se aprende a navegar por Internet con la mayor seguridad, poniendo en práctica los consejos y conocimientos que se facilitan. Gracias a estos contenidos se puede ser capaz de configurar dispositivos y conseguir una protección óptima, que preserve la seguridad y privacidad, reduciendo y neutralizando los diferentes riesgos que puede suponer navegar en Internet.

[145] *Vid.* Ortega Dolz, P., «Los ciberdelitos aumentan un 72% en España», en El País. Disponible en: https://elpais.com/espana/2023-02-08/los-ciberdelitos-aumentan-un-72-en-espana.html. (Fecha de última consulta: 29 de abril de 2023). Marlaska advirtió que los datos aportados son provisionales, ya que están pendientes de consolidación, yseñaló

pensamos que es por este motivo que se ha dejado una especie de «fórmula abierta» que tendrá que ir perfilando nuestra jurisprudencia a medida que vaya sucediéndose la práctica, en una tarea de interpretación silogística harto compleja. Hay que tener en cuenta que en 2022, las Fuerzas y Cuerpos de Seguridad del Estado contabilizaron 375.506 infracciones penales, un 72% más que en 2019, antes de la pandemia, tomado como año de referencia.

Dicho esto, no han faltado críticas a la citada reforma por la posible vaguedad y/o insuficiencia de esta. En este punto, entendemos que no podemos confiar en una solución solamente mediante el Derecho penal, pues este ha de ir acompañado de normativa extrapenal que constituya un verdadero apoyo y una auténtica barrera de contención del posible delito. Aquí es fundamental que el Derecho penal disponga de apoyo de la normativa reguladora de medios de pago del Banco de España, de consuno con la legislación europea e internacional[146].

Disponemos de otras disciplinas del Derecho para la tutela del patrimonio de las posibles víctimas, y somos del parecer que el Derecho Penal es imprescindible, todo y respetando que se ha de actuar siempre bajo los principios de *ultima ratio*, fragmentariedad e intervención mínima atendiendo a la gravedad de los hechos y a las necesidades de la sociedad que cada vez son más cambiantes[147].

Dada la complejidad de las acciones delictivas que provienen del uso fraudulento de medios de pago, el *ius puniendi* del Estado se ve muy seriamente comprometido por circunstancias como: la apreciación de donde se ha llevado a cabo la comisión del delito[148], el lugar en el que se encuentra el cri-

que la inmensa mayoría de estos ciberdelitos son fraudes o estafas informáticas, tipología en la que encajan 336.778 de las infracciones registradas, casi el 90% del total.

[146] *Vid.* Banco de España., *Eurosistema.* Disponible en: https://www.bde.es/bde/es/secciones/normativas/Regulacion_de_En/Estatal/sistemas_de_pago.html. (Fecha de última consulta: 29 de abril de 2023).

[147] Como bien afirma Ferrajoli, es fundamental el respeto de los principios antedichos, si bien habrá que tener en cuenta sobre todo en la criminalidad cibernética el máximo garantismo, máxime cuando en la mayor parte de las veces existe una macrovictimización *Vid*. Ferrajoli, L., *Derecho y razón. Teoría del garantismo penal,* Trotta, Madrid, 2001, passim.

[148] Es necesario traer a colación el principio de territorialidad, *ex* art. 23.1 LOPJ. Además, la solución puede buscarse también a través de esclarecer en qué lugar se entiende cometido el delito. Respecto del *locus comissi delicti* existen tres construcciones jurídicas que posibilitan la solución de este problema: a) La teoría de la actividad, según la cual el delito se entiende cometido donde el sujeto lleva a cabo externamente la conducta delictiva; b) La teoría del resultado: según ésta el delito se comete donde tiene lugar el resultado externo; y c) La teoría de la ubicuidad: de acuerdo con ella, el delito se entiende cometido donde se lleva a cabo la actividad o se manifiesta el resultado. En este punto, Barrio Andrés señala como doctrina dominante esta última, si bien se inclina porque la

minal, el lugar en el que se ha causado el daño, el lugar en el que se identifica a la víctima, cuál es el ordenamiento penal que se ha de aplicar, o la competencia jurisdiccional.

En relación con el sujeto activo de esta tipología de delitos, podemos extraer que normalmente se precisa de una infraestructura para su comisión, una estabilidad de esta y una pericia específica que hace que estemos en un ámbito muy proclive a la actuación de organizaciones y grupos criminales a los que se tendrá que hacer frente con legislación y acciones que se tendrán que tomar entre diversas naciones para conseguir en lo posible un mayor éxito en la lucha contra el delito[149, 150].

---

solución a esta cuestión de competencia debería solventarse a través del principio de personalidad, es decir, de entre todos los estados en principio competentes, sería competente aquel del que sea nacional el autor. *Vid*. Barrio Andrés, M., «Hacking, Cracking, Grooming y otras conductas ilícitas en internet en el Código Penal español», en *La Ley Penal*, n.º 121, Sección Legislación aplicada a la práctica, del 1 de julio al 1 de agosto de 2016. Por nuestra parte, entendemos que la cuestión es mucho más compleja, y la nacionalidad del autor en este tipo de criminalidad transfronteriza no puede ser el único parámetro para tener en cuenta, pues podría darse el caso de un sujeto activo que buscase ser nacional de un país sin tratados de extradición o con una tutela penal mínima en este punto. Tampoco es nada fácil la cuestión de la cesión de la soberanía en materia procesal penal, pues la gran mayoría de países lo ven como una injerencia. Los tratados de cooperación internacional se revelan como algo muy necesario y que ha de poder implementarse con agilidad para la persecución de la criminalidad cometida mediante medios informáticos, pues es muy frecuente que diversos países se vean afectados por un mismo delito informático cometido por diversos intermediarios de diversas nacionalidades, *ad exemplum*. Tampoco podemos soslayar que, junto al principio de territorialidad, los principios de universalidad, de protección de intereses y de personalidad habrán de actuarse en esta materia tan compleja. En esta materia puede verse Climent Barberá, J., «La justicia penal en Internet. Territorialidad y competencias penales», en *Cuadernos de derecho judicial*, n.º 10, 2001, pp. 645 y ss.

[149] Pero este tipo de criminalidad no es único y exclusivo de los medios de pago, pues la criminalidad cibernética es un fenómeno transnacional que precisa de políticas que ultrapasen fronteras y se centren en la prevención, persecución y castigo del delito. Como bien afirma Muñoz Machado la descentralización, la deslocalización de los operadores y la transnacionalidad de las operaciones hace que se imponga la imperiosa necesidad de cooperación entre autoridades de distintas naciones, pues este es el camino para seguir, que no está exento de complejidad y que precisa de la necesaria implicación de diversas instancias internacionales, nacionales y locales. Muñoz Machado, S., *Op. cit*., p. 42.

[150] La transnacionalidad del delito también existe en el tráfico de drogas, órganos y personas y tiene similar problemática en cuanto a su persecución, además, la dinámica blanqueadora es paradigmática en cuanto fenómeno supranacional y transfronterizo. La homogeneización de las políticas criminales a nivel internacional ha de implementarse con firmeza, y sobre todo, en este ámbito es de especial relevancia la cooperación policial y el establecimiento de cláusulas de extraterritorialidad. En relación con esto último, hay que indicar que la extraterritorialidad se ha previsto en el CP en el art. 189 para la corrup-

En otro orden, las transacciones mediante criptomonedas, que han irrumpido con gran fuerza en los últimos años, si se usan para la comisión de estafas, tendrán que encontrar cabida en la reforma del articulado que aquí comentamos, si bien, no sabremos si esto tendrá una auténtica efectividad, o bien se tendrá que ampliar y redefinir el tipo. Dicho esto, se abre una luz con la nueva regulación de este tipo de monedas con el Reglamento «MICA», *Markets in Crypto Assets*[151]. La directiva pretende armonizar la legislación europea, que desde 2008 ha intentado dar respuestas unilaterales al auge de las monedas digitales. Por una parte, se intenta aportar una información

---

ción de menores. *Vid*. García Mexía, P., *Derecho europeo de Internet,* Netbiblo, A Coruña, 2009, pp. 131 y ss.

[151] *Vid*. Comisión Europeo, *Reglamento del Parlamento Europeo y del Consejo*. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020PC0593 (Fecha de última consulta: 29 de abril de 2023). Relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937. De la Exposición de motivos podemos extraer «Una de las prioridades que se señalan en la Estrategia es la de asegurar que el marco normativo de los servicios financieros de la UE sea favorable a la innovación y no suponga obstáculos para la aplicación de nuevas tecnologías» (…) «Los criptoactivos son una de las principales aplicaciones de la tecnología de cadena de bloques en las finanzas. Desde la publicación de su Plan de Acción en materia de Tecnología Financiera, en marzo de 2018, la Comisión ha estado estudiando las oportunidades y los problemas que presentan los criptoactivos». Y en relación con el fraude y la ciberdelincuencia: «Los distintos enfoques adoptados por los Estados miembros dificultan la prestación transfronteriza de servicios relacionados con los criptoactivos. Asimismo, la proliferación de enfoques nacionales pone en peligro la igualdad de condiciones en el mercado único desde el punto de vista de la protección de los consumidores y los inversores, la integridad del mercado y la competencia. Además, mientras que en los Estados miembros que han introducido regímenes a medida para los criptoactivos se han reducido algunos de los riesgos, en otros Estados miembros los consumidores, los inversores y los participantes en el mercado siguen estando desprotegidos frente a algunos de los riesgos más importantes que plantean los criptoactivos (por ejemplo, el fraude, los ciberataques o la manipulación de mercado)»(…) «La presente propuesta va acompañada de una evaluación de impacto, remitida al Comité de Control Reglamentario (CCR) el 29 de abril de 2020 y aprobada el 29 de mayo de 2020.El CCR recomendó que se introdujeran mejoras en algunos aspectos con vistas a: i) encuadrar la iniciativa en los esfuerzos normativos que se están llevando a cabo en la UE y a escala internacional, ii) aportar más claridad en cuanto al modo en el que la iniciativa reducirá los riesgos de fraude, piratería informática y abuso de mercado, y explicar, además, la coherencia con la futura revisión de la legislación en materia de lucha contra el blanqueo de capitales». Y en el capítulo 3 «Los proveedores de servicios de criptoactivos autorizados para prestar el servicio de custodia y administración de criptoactivos por cuenta de terceros establecerán una política de custodia que incluya normas y procedimientos internos para garantizar la guarda o el control de dichos criptoactivos, o de los medios de acceso a los criptoactivos, tales como claves criptográficas. Estas normas y procedimientos garantizarán que el proveedor de servicios de criptoactivos no pueda perder los criptoactivos de los clientes o los derechos relacionados con estos activos debido a fraudes, amenazas cibernéticas o negligencias».

transparente y fiable a los usuarios y evitar crisis como las de FTX, BlockFi o TerraLuna[152], que pueden comportar colapsos y disfunciones muy graves en los mercados con riesgos de alcance sistémico, y por otra, se espera que una regulación que fomente el control, la transparencia y la solvencia evite la perpetración de delitos, como las estafas y el blanqueo entre otros, al socaire de estos medios.

Siguiendo con el sujeto activo, como hemos señalado, el tipo analizado se encuentra con la figura de los llamados «Muleros», que hoy en día no tienen un tratamiento armonizado por parte de la jurisprudencia ni la doctrina científica. No se trata de una cuestión menor, pues afecta directamente a una forma de participación delictiva muy concreta y que, de seguir al alza, entendemos que es muy posible que en futuras reformas tenga que recogerse en el tipo penal del art. 249.

En relación con el sujeto pasivo del delito, es doctrina unánime que se exige un deber de autoprotección en la estafa y que las características de la víctima van a ser decisivas para aquilatar la situación jurídica tratando el asunto *ad casum*. Dicho esto, con la fórmula abierta que dispensa la reforma del art. 249 CP esperamos que recoja estafas masa con víctimas difuminadas y que se cuentan por miles, como en los casos precitados de Forum Filatélico y AFINSA. Y lo que consideramos más relevante es que la reforma pueda servir para castigar y de esta forma proteger a colectivos muy vulnerables, como lo fueron las personas de edad avanzada que caían en manos de estas organizaciones criminales que actuaron con impunidad durante años con una apariencia de solvencia contrastada. Sin embargo, entendemos que la reforma del delito de estafa del art. 249 CP resultará insuficiente si no va acompañada de legislación, medidas de apoyo, control y fomento de la transparencia por parte de instituciones como la Comisión Nacional del Mercado de Valores, *ad exemplum*.

Pasando a comentar el *iter criminis,* la doctrina es unánime al considerar que se trata de un delito de resultado material que para su concreción requiere una disminución patrimonial de la víctima, una traslación del activo patrimonial, y un daño que ha de ser posible que se evalúe económicamente en grado consumado o tentativa idónea e incluso inidónea no punible. Dicho esto, entendemos que, si bien la tentativa es cuestión polémica entre la doctrina, es un estadio de la comisión delictiva que precisará de próximas reformas que puedan contribuir a proteger *ad exemplum* a posibles víctimas de la estafa por apoderamiento de contraseñas en aras de que se responsabilicen quienes verdaderamente tienen y pueden con medios suficientes velar por la seguridad

[152] *Vid*. El País, «Criptomonedas en crisis». Disponible en: https://elpais.com/opinion/2022-11-18/criptomonedas-en-crisis.html. (Fecha de última consulta: 1 de mayo de 2023).

del patrimonio del usuario de los medios de pago. Legislación como el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera[153] tendrán de ir de consuno a la reforma del CP en materia de estafas mediante tarjetas de crédito, pues el orden penal, es obvio que solamente debe actuar como la última de las soluciones.

Entendemos que la protección de estos medios de pago materiales e inmateriales distintos del efectivo van a precisar de un plus de protección por parte de los operadores financieros para evitar apoderamientos de contraseñas de forma ilícita que habrá de ir actualizándose con el devenir de los tiempos y los imparables avances tecnológicos.

Ya comentando el elemento subjetivo, entendemos que nos encontramos ante un delito doloso que admite el dolo eventual con carácter defraudatorio cuando hay, eso sí, una probabilidad considerable de que acontezca el hecho defraudatorio.

Como hemos comentado con anterioridad, se excluye en un principio el error, sin embargo, a tenor del texto literal de la reforma, entendemos que se abren nuevas y cuantiosas posibilidades de comisión delictiva si no se toman las debidas precauciones que deberán llegar por la vía del legislador con normativa específica de protección para quienes utilicen esos medios de pago que podríamos considerar «nuevos», cuanto menos por su indefinición.

En relación con la imprudencia es difícil encontrar casuística, pero algunos casos se han hallado, pues la dificultad en su apreciación estriba en que estamos ante una categoría gradual, con mayor o menor gravedad, ya que, por ende, en este elemento existe una gradación.

En materia de concurso, de lo investigado, a pesar de que hay algún autor que no aprecia la necesidad de un tipo como el que aquí estamos analizando, entendemos que sí procede su existencia y puesta al día siempre acorde con los cambios sociales y tecnológicos, pues las posibilidades de estafa cada vez son mayores, máxime en el ámbito de los delitos cibernéticos.

[153] Y a mayor abundamiento, *ad exemplum* y sin ánimo de exhaustividad: Real Decreto-ley 6/2013, de 22 de marzo de protección a los titulares de determinados productos de ahorro e inversión y otras medidas de carácter financiero. (BOE de 23 de marzo de 2013) DA 1ª; Resolución de 6 de noviembre de 2018 de la Comisión Ejecutiva del Banco de España, de modificación de las cláusulas generales relativas a las condiciones uniformes para la apertura y el funcionamiento de una cuenta del módulo de pagos y una cuenta dedicada de efectivo en TARGET2-Banco de España. (BOE de 28 de noviembre de 2018); Orden ECE/1263/2019, de 26 de diciembre, sobre transparencia de las condiciones y requisitos de información aplicables a los servicios de pago y por la que se modifica la Orden ECO/734/2004, de 11 de marzo, sobre los departamentos y servicios de atención al cliente y el defensor del cliente de las entidades financieras, y la Orden EHA/2899/2011, de 28 de octubre, de transparencia y protección del cliente de servicios bancarios. (BOE de 30 de diciembre), entre otras.

Asimismo, también se ha explicitado la problemática que existe en la relación concursal entre delitos como la falsedad, la apropiación indebida y la estafa, y en relación con lo analizado, podemos apreciar que hay que proceder con extrema cautela para su delimitación para no conculcar los principios *del non bis in idem*, de proporcionalidad, y siempre para preservar la seguridad jurídica que debe imperar en la aplicación de nuestro ordenamiento. Dicho esto, es de suma importancia tener en cuenta el Acuerdo de la Sala de lo Penal del Tribunal Supremo de 28 de junio de 2022, que aporta claridad y actualiza la comprensión de las nuevas formas de falsificar tarjetas. También apreciamos muy conveniente la reforma del CP operada por Ley Orgánica 14/2022, de 22 de diciembre en relación con el art. 399 bis 4.ª CP que recoge de forma específica la falsificación de tarjetas de crédito, débito, cheques de viaje, y cualquier otro instrumento de pago distinto del efectivo, ello de consuno con el art. 249 CP que de esta forma será de más concisa aplicación.

Ya en la esfera de la penalidad, coincidimos con Blanco Lozano[154] en que, en la estafa informática, habida cuenta del gran perjuicio y la fuerza expansiva que puede generar el daño con posible afectación de gran cantidad de víctimas, sería óptima una detenida valoración criminológica para evitar el trato más benigno que se dispensa a la delincuencia de cuello blanco, por ejemplo, si realizamos una comparación con el robo. Hay que valorar que a la estafa que aquí analizamos del art. 249 CP le corresponde una pena de prisión de seis meses a tres años, mientras que el culpable de robo con fuerza en las cosas será castigado con la pena de prisión de uno a tres años ex art. 240 CP, y si concurren alguna de las circunstancias previstas en el artículo 235 CP, correspondería una pena de prisión de dos a cinco años.

Como hemos comentado, la responsabilidad civil *ex delicto*, comportará sin duda un trabajo de investigación arduo que en la mayoría de las veces no tendrá fruto, pero una sociedad avanzada como la española no puede permitirse que grandes estafadores no paguen económicamente por lo que han hecho y aquí no pueden escatimarse recursos en las correspondientes fases de instrucción.

Para finalizar, entendemos que es preciso que el legislador se base en estudios criminológicos longitudinales a lo largo del tiempo para conseguir aquilatar la problemática existente con la cuestión de la utilización fraudulenta de medios de pago distintos del efectivo, pues las nuevas formas de delincuencia están siempre prestas para burlar a la justicia y perjudicar a las víctimas, sobre todo a las que son más vulnerables.

[154] Blanco Lozano, C., *Op. cit.* p. 537.

V. REFERENCIAS BIBLIOGRÁFICAS

Abadías Selma, A., Fernández Albesa, N., Leal Ruíz, R., *Ciberdelincuencia: temas prácticos para su estudio*, Colex, A Coruña, 2021.

Abadías Selma, A., *Justicia juvenil e inteligencia artificial en la era de la cultura «touch»*, Tirant lo Blanch, Valencia, 2022.

Agreda, M., «Amazon se suma a los despidos masivos, 18 mil trabajadores se quedarán sin empleo», en MSV. Disponible en: https://mvsnoticias.com/mundo/2023/1/5/amazon-se-suma-los-despidos-masivos-18-mil-trabajadores-se-quedaran-sin-empleo-578594.html. (Fecha de última consulta: 5 de enero de 2023).

Agudo Fernández, E., Jaén Vallejo, M. y Perrino Pérez, Á. L., *Derecho penal aplicado. Especial. Delitos contra el patrimonio y contra el orden socioeconómico,* Dykinson, Madrid, 2019.

Alberto Royo, A., *La sociedad gaseosa*, Tusquets, Barcelona, 2009.

Antón Oneca, J. y Rodríguez Muñoz, J.A., *Derecho penal Parte especial*, tomo – II, Reus, Madrid, 1949.

Antón Oneca, J., «Voz "Estafa"», *Nueva Enciclopedia Jurídica*, Seix, Barcelona, 1958.

Banco de España, *Departamento de Sistemas de Pago División de Vigilancia y Análisis de Infraestructuras.* Disponible en: https://www.bde.es/f/webbde/SPA/sispago/ficheros/es/estadisticas.pdf. (Fecha de última consulta: 1 de mayo de 2023).

Barja De Quiroga, J. y Granados Pérez, C., *Manual de Derecho penal parte especial,* tomo II, Aranzadi, Pamplona, 2018.

Barrio Andrés, M., «Hacking, Cracking, Grooming y otras conductas ilícitas en internet en el Código Penal español», en *La Ley Penal*, n.º 121, Sección Legislación aplicada a la práctica, del 1 de julio al 1 de agosto de 2016.

Bauman, Z., *Modernidad líquida,* Fondo de cultura económica, México, 2009.

——— *¿La riqueza de unos pocos nos beneficia a todos?* (Traducción de Alicia Capel Tatjer). Paidós Estado y Sociedad, Barcelona, 2014.

Beck, U., *La sociedad del riesgo: hacia una nueva modernidad*, Editorial Planeta, Barcelona, 1998.

Benítez Ortúzar, I., «Delitos contra el patrimonio y el orden socioeconómico (V)», en Morillas Cueva, L., (Dir.), Del Rosal Blasco, B., Olmedo Cardenete, M., Peris Riera, J., Sáinz-Cantero Caparrós, J.E., *Sistema de derecho penal. Parte especial*, Dykinson, Madrid, 2021.

Benito Sánchez, D., «Exclusión social y gobierno de la pena. Un análisis sobre la legitimidad de la producción penal de la exclusión», Benito Sánchez, D. y Gómez Lanz, J. (Dirs.), VV.AA., *Sistema penal y exclusión social*, Aranzadi, Pamplona, 2020.

Bustos Rubio, M., «La reforma de la ciberestafa y la incorporación de los medios de pago digitales en el Código Penal», en *Revista de Internet, Derecho y Política*, n.º 38, 2023.

Blanco Lozano, C., *Tratado de Derecho penal español*, parte especial, tomo II, Vol. I, J.M. Bosch, Barcelona, 2007.

Boletín Oficial del Estado del viernes 23 de diciembre de 2022, pp. 1-3. Disponible en: https://www.boe.es/boe/dias/2022/12/23/pdfs/BOE-A-2022-21800.pdf. (Fecha de última consulta: 31 de dic. de 22).

Choclán Montalvo, J.A., «Infracciones patrimoniales en los procesos de transferencia de datos», en Morales García, Ó., (Dir.), *Delincuencia informática. Problemas de responsabilidad, Cuadernos de Derecho Judicial IX-2002*, CGPJ, Madrid.

Climent Barberá, J., «La justicia penal en Internet. Territorialidad y competencias penales», en *Cuadernos de derecho judicial*, n.º 10, 2001.

Coleman, G., *Las mil caras de Anonymous*, Arpa Editores, Barcelona, 2016.

Comella Solans, A., «Ignorancia profunda, ignorancia conocedora e internet», *El profesional de la información*, Vol. 8, n.º 4, 1999.

Comisión Europeo, *Reglamento del Parlamento Europeo y del Consejo.* Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020PC0593 (Fecha de última consulta: 29 de abril de 2023).

Corcoy Bidasolo, M., «Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos», en *Eguzkilore*: *Cuaderno del Instituto Vasco de Criminología*, n.º 21, 2007.

Davara Rodríguez, M.Á., *Derecho Informático*, Editorial Aranzadi, Pamplona, 1993.

Díaz Guijarro, R. «Twitter despide al 83% de su plantilla en España», en *Cinco días*, disponible en: https://cincodias.elpais.com/cincodias/2023/01/24/companias/1674591010_214512.html. (Fecha de última consulta: 28 de enero de 2023).

Díaz Pita, M. M., *El dolo eventual*, Tirant lo Blanch, Valencia, 1994.

Dopico Gómez-Aller, J., «Estafas y otros fraudes en el ámbito empresarial», De La Mata Barranco, N. J., Lascuraín Sánchez, J. A., Nieto Martín, A., *Derecho penal económico y de la empresa*, Dykinson, Madrid, 2018.

El País, «Criptomonedas en crisis». Disponible en: https://elpais.com/opinion/2022-11-18/criptomonedas-en-crisis.html. (Fecha de última consulta: 1 de mayo de 2023).

Europa Press, disponible en: https://www.europapress.es/andalucia/noticia-joven-encarcelado-granada-pagar-80-euros-tarjeta-falsa-pide-gobierno-resuelva-peticion-indulto-20170610111534.html. (Última consulta: 12 de julio de 2022).

Expansión.com, «IBM anuncia 3.900 despidos tras ganar un 71% menos en 2022», disponible en: https://www.expansion.com/economia-digital/companias/2023/01/26/63d29e27e5fdeace7a8b45ef.html., (Fecha de última consulta: 26 de enero de 2023).

Faraldo Cabana, P., *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico,* Tirant lo Blanch, Valencia, 2009.

Fernández Bermejo, D., «El phishing y la responsabilidad penal de los muleros o cibermulas a la luz del artículo 248.2 A) del Código Penal». VV.AA. *Tratado de delincuencia cibernética*, Aranzadi, Pamplona, 2021.

Fernández-Salinero San Martín, M.A., *Las estafas piramidales y su trascendencia jurídico penal*, Dykinson, Madrid, 2019.

Fernández Teruelo, J.G., «Respuesta penal frente a fraudes cometidos en internet: estafa, estafa informática y los nudos de la red», en *Revista de Derecho Penal y Criminología,* 2.ª Época*,* n.º 19, 2007.

——— «Clásicas y nuevas conductas fraudulentas ejecutadas en la red y su subsunción en los tipos de estafa y estafa informática contenidos en el Código Penal». Gómez Martín, V., Bolea Bardon, C., Gallego Soler, J.I., Hortal Ibarra, J.C., Joshi Jubert, U. (dirs.); Valiente Ivañez, V., Ramírez Martín, G., (Coords.) *et al.; Un modelo integral de derecho penal. Libro homenaje a la profesora Mirentxu Corcoy Bidasolo*. B.O.E., Madrid, 2022, pp. 1136 y 1137.

Ferrajoli, L., *Derecho y razón. Teoría del garantismo penal,* Trotta, Madrid, 2001.

Fiscalía General del Estado, Consulta de la Fiscalía General del Estado n.º 3/2001, de 10 de mayo, sobre la calificación jurídico-penal de la utilización, en las cabinas públicas de teléfonos, de instrumentos electrónicos que imitan el funcionamiento de las legítimas tarjetas prepago.

Gallego Soler, J. I., «Delitos contra bienes jurídicos patrimoniales defraudatorios», Corcoy Bidasolo, M. (dir.); Santana Vega, D. M.ª (coord.); Gómez Martín, V.; Bolea Bardon, C., Cardenal Montraveta, S., Joshi Jubert, U., Hortal Ibarra, J.C., Fernández Bautista, S., Carpio Briz, D., Díaz Morgado, C., Vera Sánchez, J.S., Valiente Ivañez, V., Castellví Monserrat, C., Ramírez Martín, G., Bages Santacana, J., Miranda, G., Rogé Such, G., *Manual de Derecho penal parte especial*, Tirant lo Blanch, Valencia, 2019.

García Mexía, P., *Derecho europeo de Internet*, Netbiblo, A Coruña, 2009.

Gil Nobajas, M.ª S., «Respuesta penal a la criminalidad empresarial en supuestos de explotación laboral», en Benito Sánchez, D., Gómez Lanz, J. (Dirs.), VV.AA., *Sistema penal y exclusión social,* Aranzadi, Pamplona, 2020.

Gómez Rivero, M.ª C. (Dir.)., «Delitos patrimoniales de enriquecimiento mediante defraudación (I): estafa», Nieto Martín, A., Cortés Bechiarelli, E., Núñez Castaño, E., Pérez Cepeda, A. M.ª., *Nociones fundamentales de derecho penal parte especial*, Tecnos, Madrid, 2020.

Himanem, P., *La ética del hacker y el espíritu de la era de la información*, Editorial Destino, Madrid, 2002.

Instituto Nacional de Ciberseguridad (INCIBE), Disponible en: https://www.incibe.es/protege-tu-empresa/blog/e-skimming-y-proteger-tu-tienda-esta-tecnica-maliciosa. (Fecha de última consulta: 2 de enero de 2023).

Jiménez Bravo, R., «La Unión Europea gastó casi 400,000 euros en una fiesta programada en el metaverso y tuvo solamente 6 asistentes», *COINTELEGRAPH*, disponible en: https://es.cointelegraph.com/news/the-european-union-spent-nearly-400-000-euros-on-a-party-scheduled-in-the-metaverse-and-had-only-6-attendees, (fecha de última consulta: 7 de diciembre de 2022).

Kern, L., *La gentrificación es inevitable y otras mentiras*, Bellaterra, Barcelona, 2022.

Laforet Díaz, C., *Nada,* Ediciones Destino, Barcelona, 1969.

Luzón Cuesta, J.M.ª, *Compendio de Derecho penal. Parte Especial*, Dykinson, Madrid, 2022.

Marshall, T. H., *Citizenship and social class, and other essays*, Cambridge University Press, Londres, 1950.

Martín, R., *Diccionario de la mitología clásica*, Espasa Calpe, México, 1998.

Martínez Cañadas, E., *El mito de la infoxicación,* UOC, Barcelona, 2021.

Mcluhan, M. & Powers, B. R., *La aldea global*, GEDISA, Barcelona, 2015.

Mcluhan, M., *La guerra y la paz en la aldea global,* La Marca, Buenos Aires, 2018.

Mestre Delgado, E., «Delitos contra el patrimonio y el orden socioeconómico». Lamarca Pérez, C., Alonso de Escamilla, A., Rodríguez Núñez, A., *Delitos. La parte especial del Derecho penal*, Dykinson, Madrid, 2022.

——— «El phishing y la responsabilidad peal de los muleros o cibermulas a la luz del artículo 248.2 A) del Código Penal». Abadías Selma, A., Bretones Alcaraz, F.J., Cámara Arroyo, S., Carou García, S., Fernández Bermejo, D., García Valdés, C., Gil Gil, A., Marcos Ayjón, M., Martínez Atienza, G., Martínez Galindo, G., Pérez López, X., Roca De Agapito, L., Romero Jaime, D.J., Sanz Delgado, E., Téllez Aguilera, A., Tejada De La Fuente, E., de Urbano Castrillo, E., *Tratado de delincuencia cibernética*, Aranzadi, Pamplona, 2021.

Ministerio de Sanidad, Disponible en: https://www.sanidad.gob.es/profesionales/saludPublica/ccayes/alertasActual/nCov/situacionActual.htm. (Fecha de última consulta: 26 de enero de 2023).

Molina Fernández, F., «Intentos de extraer dinero de un cajero sin tener la clave: el problema del dolo directo con baja probabilidad y su trascendencia para la dogmática del dolo y la imprudencia». Gómez Martín, V., Bolea Bardon, C., Gallego Soler, J.I., Hortal Ibarra, J.C., Joshi Jubert, U. (dirs.); Valiente Ivañez, V., Ramírez Martín, G. (coords.) *et al.; Un modelo integral de derecho penal. Libro homenaje a la profesora Mirentxu Corcoy Bidasolo.* B.O.E., Madrid, 2022.

Molist Ferrer, M., *Hackstory.es: La historia nunca contada del underground hacker en la Península Ibérica,* Editorial Amazon, Madrid, 2015.

Muñoz Conde, F., *Derecho penal. Parte Especial. 22ª edición, revisada y puesta al día conforme a las Leyes Orgánicas 1/2019 y 2/2019 con la colaboración de Carmen López Peregrín*, Tirant lo Blanch, Valencia, 2019.

——— *Derecho penal parte especial*, Tirant lo Blanch, Valencia, (24.ª Ed.), 2022.

Muñoz Machado, S., *La regulación de la red. Poder y Derecho en Internet*, Editorial Taurus, Madrid, 2000.

Núñez Castaño, E., «Estafas realizadas mediante tarjetas de crédito o débito y cheques de viaje (art. 248.2 c CP)», en Núñez Castaño, E., Galán Muñoz, A., *Manual de derecho penal económico y de la empresa*, Tirant lo Blanch, Valencia, 2018.

Observatorio de la Discapacidad, disponible en: https://www.observatoriodeladiscapacidad.info/ (Fecha de última consulta: 12 de enero de 2023).

Oficina de Seguridad del Internauta, Disponible en: https://www.incibe.es/ciudadania (Fecha de última consulta: 29 de abril de 2023).

Ortega Dolz, P., «Los ciberdelitos aumentan un 72% en España», en *El País*. Disponible en: https://elpais.com/espana/2023-02-08/los-ciberdelitos-aumentan-un-72-en-espana.html. (Fecha de última consulta: 29 de abril de 2023).

Pastor Muñoz, N., «El delito de estafa», en Silva Sánchez, J.M.ª (Dir.)., *et al. Lecciones de Derecho penal económico y de la empresa. Parte general y especial*, Atelier, Barcelona, 2020.

Pastor Muñoz, N. y Coca Vila, I., «Delitos contra el patrimonio II», *VV.AA: Lecciones de Derecho penal parte especial*, Atelier, Barcelona, 2021.

Pérez López, X., «Introducción», en: Fernández Bermejo, D. (Dir.), *Blanqueo de Capitales y TIC: Marco Jurídico Nacional y Europeo, Modus Operandi y Criptomonedas. Ciberlaundry. Informe de situación*., Aranzadi, Pamplona, 2019.

Prados García, C., «La inaccesibilidad digital como supuesto de discriminación de las personas con discapacidad», García Goldar, M. y Núñez Cerviño, J. (dirs.). Andrés Segovia, B., Prados García, C., Gil Otero, L., Merchán Murillo, A., Martínez Calvo, A., Gonçalves de Sousa, A., Ramón Fernández, F., Castillo Olano, A., Argelich Comelles, C., Castillo Parrilla, A., Navas Navarro, S., Marchal Escalona, N., Pazos Sierra, A., Guerra, S., López-Barajas Perea, I., Castro Corredoira, M., Zolea, S., *El derecho ante la tecnología: innovación y adaptación*, Colex, A Coruña, 2022.

Prensky, M., *Enseñar a nativos digitales,* Ediciones SM, Madrid, 2011.

Prieto del Pino, A. M.ª, «La armonización del Derecho penal español», *Boletín de información del Ministerio de Justicia*, Madrid, 15 de junio de 2006.

Queralt Jiménez, J., *Derecho penal español. Parte espe*cial. Tirant lo Blanch, Valencia, 2015.

Quintero Olivares, G., «De las defraudaciones», en Morales Prats, F., Morón Lerma, E., Tamarit Sumalla, J Mª., Ramón Ribas, E., Villacampa Estiarte, C., Hernández García, J., Ortega Lorente, J. M., Aguilar Romo, M., Camarena Grau. S, Torres Rosell, N., García Albero, R., Llarena Conde, P., Demetrio Crespo, E., Bañeres Santos, F., Ramírez Ortiz, J. L., Calvo López, Mª., Navarro Blasco, E., Rueda Soriano, Y., Cugat Mauri, M., Ramos Rubio, C., De la Peña Oliete, M., Portilla Contreras, G., García Rivas, N., Salat Paisal, M., Ortega Gutiérrez-Maturana, M., en Quintero Olivares, G., (Dir.), *Comentarios a la parte especial del Derecho penal*, Aranzadi, Navarra, 2016.

Ramos Portero, R., «Los delitos informáticos», en *Revista Latinoamericana de Derecho Penal y Criminología*, n.º 6, 1989.

Rey Huidobro, L.F., «La estafa informática: relevancia penal del *phishing* y el *pharming», en Diario La Ley*, n.º 7926, sección Doctrina, 19 de septiembre de 2012, Ref. D-322, LALEY 16076/2012.

Romeo Casabona, C., «De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal», en AA.VV. (Coord.: Romeo Casabona, C.)., *El cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Editorial Comares, Granada, 2006.

Roso Cañadillas, R., «Algunas reflexiones sobre los nuevos fenómenos delictivos, la teoría del delito y la ignorancia deliberada», en: *Dogmática del Derecho penal material y procesal y política criminal contemporáneas. Homenaje a Bernd Schünemann por su 70 aniversario*, Tomo I, Lima (Gaceta Penal & Procesal Penal, Gaceta Jurídica), 2014.

Sequera Fernández, J., *Gentrificación: Capitalismo cool, turismo y control del espacio urbano*, Los libros de la catarata, Madrid, 2020.

Serrano Gómez, A. y Serrano Maíllo, A., *Derecho penal parte especial*, Dykinson, Madrid, 2011.

Stiglitz, J.E., (Trad. Pradera Sánchez, A.) *El precio de la desigualdad*, De bolsillo, Madrid, 2015.

Suárez-Mira Rodríguez, C., (Dir. y coord.)., Judel Prieto, Á., y Piñol Rodríguez, J. R., *Manual de Derecho penal parte especial*, tomo II, Aranzadi, Pamplona, 2020, p. 376.

Terradillos Basoco, J.M.ª, *Aporofobia y plutofilia: la deriva jánica de la política criminal contemporánea*, Bosch, Barcelona, 2020.

Urra Portillo, J., *El pequeño dictador crece: padres e hijos en conflicto*, La Esfera de los libros, Madrid, 2015.

Vázquez González, C., «Estafa», en Serrano Gómez, A., Serrano Maíllo, A., Serrano Tárraga, M.ª D., *Curso de Derecho penal parte especial*, Dykinson, Madrid, 2019.

Vázquez Iruzubieta, C., *Código Penal Comentado,* Atelier, Barcelona, 2015.

Velasco Núñez, E., *Delitos cometidos a través de Internet. Cuestiones procesales,* La Ley, Madrid, 2010.

——— *Delitos tecnológicos, definición, investigación y prueba en el proceso penal,* Sepín, Madrid, 2016.