EL DELITO DE ESTAFA INFORMÁTICA. ¿ES POSIBLE DETERMINAR LA RESPONSABILIDAD CIVIL DE LA ENTIDAD FINANCIERA EN BASE AL ARTÍCULO 120.3 DEL CÓDIGO PENAL COMO CONSECUENCIA DEL «PHISHING»?[1]

Francisco Rodríguez Almirón

Profesor Sustituto interino en la Universidad de Granada

Title: *The crime of computer scam. Is it possible to determine the civil liability of the financial institution based on article 120.3 of the penal code as a consequence of «phishing»?*

Resumen: Sin duda las nuevas tecnologías, y principalmente el uso de internet, ha supuesto una revolución en todos los aspectos de la vida de las personas. A su vez, esa forma de relación de los ciudadanos con la Administración, con las empresas y entre los individuos ha provocado nuevos problemas y retos hasta este momento desconocidos. Las nuevas tecnologías también están siendo aprovechadas por la criminalidad organizada, cada vez más especializada y sofisticada, para sus propósitos criminales. Este trabajo trata de abordar el fenómeno del *phishing* y conectarlo con la reparación a la víctima. Para ello partimos del análisis de las diferentes técnicas utilizada por los delincuentes y de la descripción de este fenómeno delictivo. Se analizarán las principales características del delito de *phishing* y la posible responsabilidad civil subsidiaria de las entidades financieras cuando el delito se ha cometido en sus establecimientos y ha existido una infracción de la normativa que regula su actividad. Esta responsabilidad subsidiaria surgiría del artículo 120.3 CP, y es diferente a la responsabilidad *ex lege* contenida en el Real Decreto-Ley 19/2018, de 23 de noviembre que regula los medios de pago.

[1] El presente trabajo ha sido realizado dentro del Proyecto de investigación sobre «La ciberdelincuencia en el presente y futuro andaluz (CAPF PRY 056/22)» del que es IP el Dr. D. Miguel Olmedo Cardenete.

Palabras clave: Indemnización; reparación de las víctimas; *phishing*; estafa informática.

Abstract: *Undoubtedly, new technologies, and mainly the use of the Internet, have brought about a revolution in all aspects of people's lives. In turn, this way of relating to the Administration, with companies and among individuals has caused new problems and challenges unknown up to now. New technologies are also being used by organized crime, which is increasingly specialized and sophisticated, for their criminal purposes. This work tries to address the phenomenon of phishing and connect it with the reparation to the victim. To do this, we start from the analysis of the different techniques used by criminals and the description of this criminal phenomenon. The main characteristics of the crime of phishing and the possible subsidiary civil liability of financial institutions are analyzed when the crime has been committed in their establishments and there has been a violation of the regulations. This responsibility would arise from article 120.3 CP, and is different from the ex lege direct responsibility contained in Royal Decree-Law 19/2018, of November 23, which regulates the means of payment.*

Keywords: *compensation; victim reparation; phishing; computer scam.*

1. Introducción

Como dice VALLS PRIETO[2] la relación de la tecnología con las personas siempre ha sido disruptiva. Ha sido una relación positiva en cuanto ha supuesto una mejora de las condiciones de vida debido a la innovación, pero también negativa al cambiar nuestra forma de vivir y nuestras libertades.

Actualmente nos encontramos en puertas de lo que se denomina la cuarta revolución industrial. En estos últimos años se ha producido un aumento exponencial de la tecnología, lo que plantea al hombre nuevos retos y genera nuevas oportunidades. Y, si bien es cierto que esta nueva forma de relacionarse entre las personas y en los negocios ha traído consigo mejoras a la sociedad, también ha provocado nuevas amenazas antes inimaginables. Sin duda, hoy en día el uso de las nuevas tecnologías

[2] Cfr. VALLS PRIETO, J. «Sobre la responsabilidad penal por la utilización de sistemas inteligentes», *Revista Electrónica de Ciencia Penal y Criminología,* 2022, p. 34.

plantea un reto al derecho penal debido a la aparición de nuevos fenómenos delictivos cada vez más especializados y organizados. Como señala MIRÓ LLINARES[3] el traslado de las oportunidades delictivas del espacio físico al ciberespacio es algo que viene ocurriendo desde hace tiempo, pero que se ha agudizado y hecho más evidente a partir de la pandemia.

La delincuencia evoluciona y los criminales constantemente están perfeccionando y adaptando sus métodos, siendo cada vez más sofisticados, organizados y profesionales. Un ejemplo lo tenemos en el *phishing*, donde es común el uso por parte de los criminales de complejos programas informáticos para conseguir sus fines delictivos. Por si fuera poco, las nuevas herramientas de inteligencia artificial pueden facilitar en un futuro, sino es ya en el presente, aún más esta labor a los delincuentes, por lo que es necesario implementar medidas de control que ayuden a prevenir los peligros de estas nuevas herramientas.

Sin duda el *phishing* es uno de los fenómenos delictivos más actuales, estando en pleno auge[4]. Es suficiente con leer la prensa diaria para darse cuenta de la importancia creciente de este fenómeno, y como nadie está a salvo de esta amenaza. En este delito, aunque reviste diversas modalidades, los atacantes utilizan técnicas de ingeniería social —principalmente correos electrónicos, llamadas de teléfono fraudulentas, o réplicas de páginas web— con el fin de conseguir datos confidenciales de las víctimas para ser usados posteriormente por los propios criminales, o bien ceder esos datos a terceros. En este sentido, es primordial conocer las diferentes técnicas con las que operan estos delincuentes para así poder alertar a la población y que puedan tomar medidas de autoprotección, así como las empresas puedan implementar medidas de seguridad y desarrollar herramientas para impedir o reducir estos delitos. La magnitud de estas estafas es tal, que en la actualidad ya existen empresas que se dedican a formar a empleados y particulares en las técnicas necesarias para protegerse de esta práctica.

La ciberdelincuencia tiene consecuencias no solo económicas en las personas afectadas por el delito o en las que deben de responder civilmente por este —seguros, responsables civiles subsidiarios etc.—, sino que también puede provocar otros daños, como el daño moral a nivel reputacional[5]. Así ocurre, por ejemplo, en aquellos casos donde los *hackers* sustraen datos personales de los clientes de las empresas, lo que sin duda

---

[3] Cfr. MIRÓ LLINARES, F. «Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos». *IDP: revista de Internet, derecho y política*, N.º 32, 2021, p. 12.

[4] Según la página unodecadacincodelitos.com en España se cometieron 375.506 ciberdelitos, lo que supone un aumento del 352,1% desde 2015: https://unodecadacincodelitos.com/ (fecha consulta 03/04/2023).

[5] Ver sobre los diferentes conceptos de responsabilidad civil ROCA TRÍAS, E. / NAVARRO MICHEL, M. *Derecho de Daños*. Tirant Lo Blanch. 2020.

afecta al buen nombre de la organización. Situación que se torna aún más grave cuando lo que se sustraen son datos personales que disponen de una alta protección, como son los datos médicos, como ha ocurrido en alguna ocasión, datos que quedan expuestos en la red a la mirada de cualquiera. Para DE LA CUESTA ARZAMENDI la cibercriminalidad es un fenómeno criminógeno de extensa y elevada lesividad, desde el punto de vista económico-patrimonial, y desde el prisma de la intensa afección a cualquier bien jurídico que no ostente una naturaleza económica[6].

Si bien existen diferentes técnicas forenses que ayudan a la averiguación de estos delitos, uno de los principales problemas que se plantea en la práctica es que en la mayoría de las ocasiones este delito tiene un carácter transnacional que va más allá del lugar de comisión, lo que dificulta no solo la averiguación de este, sino también la persecución de sus autores. Es por ello necesario potenciar los lazos colaborativos entre los distintos países. Y es que, el *phishing* no es un fenómeno exclusivo que afecte a España, sino que afecta a todos los Estados. No se escapan de estos ataques ni la Administración[7], ni las empresas, ni los particulares[8], pudiendo proceder los ataques desde cualquier ubicación del mundo. No hay tampoco un sector que pueda librarse de estas irrupciones, ya que los delincuentes atacan donde pueden y siempre que pueden. Últimamente se han recrudecido, por ejemplo, los ataques contra infraestructuras críticas, hospitales o universidades, lo que ha obligado a estas instituciones a adoptar mayores medidas de protección, como doble autenticación, redes inalámbricas separadas etc.[9]. Como señala SÁNCHEZ-ESCRIBANO[10], la nota común de todos ellos es que almacenan una gran cantidad de datos de los usuarios.

Partimos de que tanto empresas como particulares tienen una obligación de autoprotección. No obstante, el deber exigible a una entidad financiera que oferta un determinado medio de pago no puede ser el

---

[6] Cfr. DE LA CUESTA ARZAMENDI, J.L. / PÉREZ MACHÍO, A.I. / SAN JUAN, C. «Aproximaciones criminológicas a la realidad de los ciberdelitos», en Monografías, Civitas, Derecho penal informático. BIB 2010\1677, p. 3.

[7] Así, por ejemplo, encontramos el supuesto fraude a través de una compleja operación de phishing al Departamento de Defensa de EE.UU. https://www.escudodigital.com/ciberseguridad/californiano-estafo-235m-dolares-departamento-defensa-eeuu_51621_102.html (fecha consulta 20/03/2023).

[8] Últimamente es fácil encontrar noticias de ataques con malware para robar credenciales de tarjetas de crédito y minar ilegalmente la criptomonedas https://es.cointelegraph.com/news/us-justice-dept-convicts-two-romanians-of-cybercrimes-including-cryptojacking (fecha consulta 20/03/2023).

[9] https://cybersecuritynews.es/aumentan-los-ataques-de-phishing-a-universidades/ (fecha consulta 20/03/2023).

[10] SÁNCHEZ-ESCRIBANO, M. «Tendencias actuales en materia de cibercrimen: la respuesta penal al Phishing, Ransomware y Dos, las tres principales amenazas cibernéticas a plataformas digitales desde la pandemia». *Estudios. Aportaciones jurídicas a la economía de plataformas*. Aranzadi, S.A.U., 2022, p. 3.

mismo que se le puede exigir al usuario. En estos casos en los que se produce un pago o una transferencia fraudulenta puede existir una responsabilidad de la entidad financiera por el riesgo que entrañan dichas operaciones. Esa responsabilidad puede derivar de dos ámbitos: la legislación sobre medios de pago —salvo que exista una negligencia grave por parte del usuario— o la responsabilidad civil subsidiaria en base al artículo 120.3 CP., siempre y cuando se cometan en sus establecimientos y no se hayan implementado todas las medidas necesarias para prevenir el delito y otorgar seguridad a la operación, facilitando con ello la comisión de este.

En relación con este tipo de ciberdelincuencia encontramos diversas modalidades de conductas delictivas[11]. Sin ánimo de ser exhaustivos, las principales amenazas en la red son:

— *Phishing*: En la actualidad, como señala MIRÓ LLINARES[12] no hay un único *phishing*, sino múltiples modalidades de este. La modalidad típica de tipo de fraude consiste en provocar un engaño a la víctima para que proporcione información confidencial sobre sus contraseñas, datos personales u otras credenciales. Existen diferentes modalidades de *phishing*, siendo la más habitual el envío de correos electrónicos y SMS generalizados. La inventiva de los delincuentes no tiene límites a la hora de intentar conseguir los datos de sus víctimas. Así, no dudan en lanzar falsos mensajes que suplantan no solo a empresa sino que incluso usurpan la identidad de los propios Cuerpos y Fuerzas de Seguridad del Estado[13]. Es interesante como en las últimas semanas hemos conocido como un grupo de investigadores han conseguido servirse de una Inteligencia Artificial (en adelante, IA) para intentar perfeccionar estos ataques[14].

---

[11] Ver la SAP de Barcelona, sentencia núm. 151/2013 de 7 de marzo. ECLI:ES:APB:2013:2625, que relaciona las tipologías más comunes y que afectan a las entidades financieras como «Siendo conocido o debe serlo en una entidad como la demandada, los distintos fraudes, como clonación de tarjeta en comercio o en un banco 'Pisica' o gato en lengua rumana, el lazo libanés o falsa boca en cajero en que se introduce la tarjeta, skimming o carcasa superpuesta que tiene diferentes variantes, y el phising que aquí se alega por la Caixa como utilizado, que también pudiere ser el Pharming en que similar a aquel, pero consiste en introducirse en un servidor ya sea local o ISP, a través de hackers. O, ya bien, a través de la introducción de virus o spyware en los ordenadores, o keyloogers que registra todas las teclas que el usuario oprime en el teclado para capturar claves, contraseñas, etc..., o el hacking o variantes del hijacking o secuestro o modificación de (IP, o page, o módem, o browser, etc...)».

[12] MIRÓ LLINARES, F. «La respuesta penal al ciberfraude: Especial atención a la responsabilidad de los muleros del phishing», *Revista electrónica de ciencia penal y criminología*, N.º 15, 2013, p. 8.

[13] Ver Audiencia Nacional núm. 14/2016, de 3 de marzo. ECLI:ES:AN:2016:704.

[14] Según informa la web https://www.forbesargentina.com/innovacion/el-esperado-gpt-4-openai-materializa-inedito-peligro-inteligencia-artificial-escala-global-n30877 (fecha consulta 20/03/2023) los investigadores lograron que una inteligencia artificial les ayudara a crear un software que recopilaba archivos PDF y los enviaba a un servidor remoto. Como señala la información, la Inteligencia Artificial proporcionó consejos a

La mayoría de los casos de *phishing* se detectan por lo poco profesional de los envíos, ya que es frecuente encontrar faltas de ortografía, o una mala redacción del contenido del mensaje. También ayuda a su detección comprobar la dirección de emisión —de donde proceden—. En este sentido, las nuevas IA pueden facilitar mucho la labor de los delincuentes, principalmente ayudando a dar apariencia de veracidad a sus mensajes[15].

El *phishing* actualmente se castiga a través del artículo 249 CP (anteriormente estaba tipificado en el 248.2 CP) cuando se consigue una transferencia no consentida en perjuicio de otro y concurre ánimo de lucro. Si el delincuente, sin estar autorizado, se limita a apoderarse, utilizar o modificar, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado cometería un delito de descubrimiento y revelación de secretos del artículo 197.2 CP

— *Malware*: Es el uso de un software que infecta el dispositivo de la víctima con virus, troyanos etc., lo que posibilita que el delincuente pueda sustraer la información. El acceso al equipo se realiza normalmente por correos electrónicos fraudulentos o por correos que incorporan ficheros adjuntos que, tras ser abiertos, infectan el equipo de la víctima[16].

— *Ransomware*: (Secuestro de datos). Proviene de la unión de las palabras *ransom* (rescate) y *ware* (software o datos)[17]. La dinámica es parecida a la anterior, pero con la salvedad de que, una vez infectado el equipo, el delincuente se hace con él de forma remota mediante un cifrado de los datos del disco duro, bloqueando el acceso al dispositivo o a determinados archivos de forma que, si la víctima quiere recuperar los datos debe de pagar, como si de un rescate se tratara, una determinada cantidad económica.

Estos ataques van dirigidos a empresas[18], a particulares, o a la Administración. En el caso de la Administración suelen atacar frecuentemente lo que se denominan infraestructuras críticas, cómo hospitales, plantas energéticas,[19] etc., lo que da una idea de la capacidad de estos *hackers*,

---

los investigadores sobre actuar para que el programa tuviera menos posibilidades de ser detectado por el software de seguridad.

[15] Es muy interesante el cómo se puede perfeccionar ese lenguaje y enseñar a la IA a imitarlo. https://research.checkpoint.com/2022/opwnai-ai-that-can-save-the-day-or-hack-it-away/.

[16] Ver https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime (fecha consulta 25/04/2023).

[17] https://www.abogacia.es/wp-content/uploads/2017/07/Guia_Ransomware.pdf pág., 7 (fecha consulta 14/04/2023).

[18] https://www.businessinsider.es/fabricante-alarmas-amazon-sufre-ciberataque-ransomware-1214668 (fecha consulta 20/03/2023).

[19] https://theobjective.com/economia/2023-03-12/empresas-ciberataques-hospital-clinic/ (fecha consulta 20/03/2023).

ya que son infraestructuras que gozan generalmente de una protección reforzada para prevenir estos ataques. El rescate del equipo se realiza usualmente mediante el pago en criptomonedas, lo que dificulta el seguimiento del dinero sustraído.

Existe otra modalidad, donde los delincuentes en lugar de bloquear el sistema lo que hacen es amenazar con filtrar en caso de impago documentos, fotos, o material sensible de la víctima o de los usuarios de la empresa o institución atacada a la web [20]. El castigo de estos delitos suele realizarse a través del delito de daños que castiga al que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos. En caso de que el resultado producido fuera grave está prevista una mayor pena, así como aquellos casos en los que los ataques recaen sobre infraestructuras críticas[21], el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad. El tipo aplicable en el supuesto de un ataque que solo produce daños sería el delito de daños del 264.2.3.ª y 4.ª CP. No obstante, si el delincuente consigue una transferencia patrimonial a través de dicho ataque *ransomware*, estaríamos ante una estafa del 249 CP[22].

— Suplantación o robo de identidad en la web: Se trata de suplantar a la víctima. Para ello el delincuente previamente se apodera de la información de esta. Esta información es obtenida, bien directamente en la *dark web*, o mediante técnicas de *phishing, malware*, etc., para, posteriormente, con esa información llevar a cabo la correspondiente actividad defraudadora.

— *Hackeo*: Consiste en el acceso no consentido mediante el uso de diferentes técnicas a determinados soportes informáticos o redes a fin de obtener información reservada o confidencial. Actualmente se ha puesto de moda una nueva modalidad como es el *hacktivismo* con fines políticos o sociales, y donde el *hacker* ataca una página web de una determinada institución o empresa con una finalidad política o social[23]. Las razones de

[20] Robó imágenes de pacientes sometidos a tratamiento de oncología: https://es.digitaltrends.com/tendencias/paciente-cancer-demanda-hospital-por-ransomware-que-filtro-sus-fotos-medicas-desnudas/ (fecha consulta 20/03/2023).

[21] Según el artículo 264.2.4.ª del CP una es infraestructura crítica es «un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones».

[22] Ver sentencias de la Audiencia Nacional, Sala de lo Penal, Sección 4.ª, núm. 14/2016, de 3 de marzo. ECLI:ES:AN:2016:704; y núm. 28/2016, de 4 julio. ECLI:ES:AN:2016:2639.

[23] Ver informe sobre hacktivismo y Ciberyihadismo: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6594-ccn-cert-ia-03-22-informe-anual-2021-hacktivismo-y-ciberyihadismo-1/file.html (fecha consulta 25/04/2023).

estas prácticas no siempre son económicas, a veces solo constituyen un reto para los *hackers* poder acceder a determinadas instituciones como Agencias de Inteligencia, de Defensa etc.[24].

— Espionaje corporativo: Consiste en la intromisión ilegítima y la sustracción de información de una empresa, generalmente por una competidora por razones puramente comerciales.

— Encontramos otra serie de conductas como los ataques DDos o de denegación de servicio, donde el delincuente satura mediante diferentes herramientas el acceso a una determinada página web, aplicación etc.[25]. Una variedad de estos ataques es el denominado *smurf* o pitufo, donde el atacante localiza la dirección IP de la víctima y, tras crear un paquete de datos falsificado, hace que todos los dispositivos conectados dentro de la misma organización respondan, dejando el servidor de la víctima inoperativo[26].

— Existen, además, otros delitos que pueden ser cometidos a través de medios informáticos como la pornografía infantil, *ciberbullying*, *sexting*[27], *stalking*[28], etc.

En todos los supuestos, si además, se opera como una organización criminal se aplicaría el artículo 570 bis CP. No obstante, como señala SÁNCHEZ-ESCRIBANO en la Dark Web es posible comprar kits de ciberataque a un precio muy reducido[29].

2. Modalidades de *phishing*

Etimológicamente *phishing* proviene del inglés «fishing» (pescar) y hace referencia al hecho de intentar pescar usuarios en la red mediante

[24] Ver https://www.elmundo.es/tecnologia/2019/08/30/5d6997c0fc6c83235b8b4647.html.

[25] Especialmente llamativo es el sufrido por una empresa el 1 de junio de 2022 donde, según señala la noticia, alcanzo a los 46 millones de solicitudes por segundo. https://www.mundodeportivo.com/urbantecno/seguridad/asi-sobrevivio-google-al-mayor-ataque-ddos-de-la-historia-con-46-millones-de-solicitudes-por-segundo

[26] https://www.pandasecurity.com/es/mediacenter/seguridad/ataque-smurf/.

[27] Consiste en difundir revelar o ceder a terceros sin autorización de la persona afectada, imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.

[28] Consiste, entre otras cosas en utilizar la imagen de la víctima para realizar anuncios o abrir perfiles falsos en redes sociales, páginas de contacto o cualquier medio de difusión pública, ocasionándole a la víctima una situación de acoso, hostigamiento o humillación. Está regulado en el 172 CP.

[29] SÁNCHEZ-ESCRIBANO, M. «Tendencias actuales en materia de…», *op. cit*., p. 6.

anzuelos, cada vez más sofisticados, para obtener información financiera o contraseñas[30].

Como señala la SAP de Barcelona, núm. 151/2013 de 7 de marzo[31] dentro de los distintos fraudes informáticos sobre las cuentas de los clientes de entidades crediticias, el *phishing* es la contracción de «password harvesting fishing: cosecha y pesca de contraseñas». Las razones por las que se cometen estos hechos obedecen a razones diversas (robar las contraseñas de acceso al correo, bancarias, sustracción de secretos e información confidencial, afán de notoriedad, buscar una vulnerabilidad en el sistema informático que permita un ataque posterior[32], etc.).

El *phishing* también ha ido evolucionando, de manera que encontramos diferentes técnicas utilizadas por los delincuentes. Así encontramos:

— El *phishing* por correo electrónico. El delincuente generalmente remite un correo electrónico a la víctima en el que simula ser su entidad financiera, o una empresa con la que tiene una relación comercial, o bien la propia Administración. Se trata de correos que se mandan de forma generalizada y donde a través de diferentes tretas (fingen un acceso no consentido a la cuenta del cliente, una trasferencia pendiente de confirmación, un envío retenido, etc.) se induce a la víctima a que pinche en un enlace que lo lleva a una página «clonada», para que introduzca sus claves, lo que esta hace en la creencia de su veracidad. Introducidas las contraseñas el delincuente obtiene la información que precisa, y ordena al instante una o varias trasferencias desde la cuenta de la víctima a la cuenta de los muleros. Estos muleros o mulas, son terceros que han sido captados previamente, generalmente por internet, bajo falsas ofertas de trabajo y, tras recibir en sus cuentas el dinero sustraído de forma ilegítima por los delincuentes, lo transfieren a otras cuentas utilizando para ellos herramientas o sistemas de pago de difícil seguimiento, cobrando por su labor una comisión.

Otras veces los correos tienen por finalidad sustraer los datos personales de las víctimas para ser cedidos a terceros. Estos correos electrónicos normalmente llevan aparejados mensajes que simulan un lucro para el sujeto. Recientemente se ha utilizado una campaña que prometía una nevera gratis por rellenar un cuestionario, para lo que se usaba como

---

[30] RODRÍGUEZ-MAGARIÑOS, J. «Nuevos delitos informáticos: *phising, pharming, hacking y cracking*», disponible en línea en: https://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20%20Nuevos%20delitos%20inform% C3%A1ticos.pdf (fecha consulta 30/03/2023).

[31] SAP de Barcelona, sentencia núm. 151/2013 de 7 de marzo. ECLI:ES:APB:2013:2625.

[32] TORRES KEENLYSIDE, A. / CONTRERAS SOLER, B. / GARROS FONT, I. «Análisis criminológico, técnico y legal del phishing», *Revista Aranzadi Doctrinal*, núm. 9, 2021, p. 4.

gancho unas conocidas marcas de cerveza, La intención no era otra que captar los datos personales de las víctimas[33].

— *Spear phishing*. A diferencia del anterior se personalizan los correos de forma que se estos posean una mayor credibilidad. Así, por ejemplo, si se consigue infectar un terminal de un empleado se pueden remitir correos al resto de la organización. Al provenir los correos de un correo corporativo o de una persona conocida es más fácil que la víctima caiga en el engaño.

— *Whaling phishing* o caza ballenas. En esta modalidad los ataques van dirigidos a los ejecutivos de una corporación. Es más sofisticada y difícil de detectar, ya que es más personal y, en ocasiones el delincuente suele incorporar algún tipo de información previamente estudiada para hacer caer a la víctima en el engaño.

— *Phishing* por SMS o *smishing*: Últimamente se ha puesto de moda esta modalidad delictiva. En ella, la víctima recibe un SMS, normalmente con un aviso revestido de cierta urgencia instándole a clicar en el enlace[34].

— *Pharming*. La víctima, cuando accede a internet, es redirigida, en lugar de a la página legítima, a una copia de esta a fin de que introduzca sus claves. Para facilitar el engaño se utilizan determinadas técnicas muy sofisticadas que hacen creer al usuario que se encuentra ante la fuente legítima. Para ello se corrompen determinados protocolos de seguridad. Las técnicas más usuales son la corrupción del servidor DNS, el ataque de secuestro de sesión, o la interceptación de la comunicación.

— *Phishing* de voz o *vishing*. En este caso, en lugar de un correo o SMS, la víctima recibe una llamada de teléfono convencional donde se le alerta de una trasferencia no consentida, o de algún cargo, para a continuación solicitarle las claves y los códigos remitidos al móvil. El estafador se hace pasar por un trabajador de la empresa o institución y actúa con el aparente fin de solventar y ayudar al usuario a resolver el problema. A partir de ese momento la dinámica difiere, o bien se realizan trasferencias no consentidas o se instala una tarjeta asociada etc.

[33] https://www.europapress.es/portaltic/ciberseguridad/noticia-campana-phishing-anima-usuarios-completar-formularios-datos-conseguir-cerveza-gratis-20230315160539.html (fecha consulta 20/03/2023).

[34] Recientemente se han recibido mensajes con el logotipo de una empresa de paquetería en la que le informa al cliente de que un envío a su nombre no le ha sido entregado al estar pendiente de un pago de aproximadamente dos euros. Para desbloquear dicho envío el mensaje insta al usuario a pinchar en el enlace adjunto que lo redirige a una página que simula ser la auténtica. Ciertamente, esperar un envío de un paquete postal, máxime en determinadas fechas, y con el auge de las compras por internet, no es nada inusual, lo que es aprovechado por el delincuente para engañar a su víctima.

— *SIM swapping* (o intercambio de SIM). Como señala CANO TERUEL, consiste en la utilización de un duplicado de la tarjeta SIM de la víctima para acceder a desbloquear sistemas de autentificación de doble factor de sus cuentas de usuario. La operativa consiste en que el delincuente solicita un duplicado de la tarjeta SIM en nombre del usuario para posteriormente realizar trasferencias aprovechando el código de verificación mandado al teléfono[35].

La preparación en este tipo de delitos pasa generalmente por diferentes fases: organización de la operación; captación de los «muleros» y apertura de cuentas; confección de los correos electrónicos, de las webs dobladas, y planificación de las llamadas; el envío a los usuarios; la infestación de los equipos y acceso a los datos de la víctima; el uso de los datos sustraídos mediante las trasferencias y posterior retirada de los fondos —normalmente en efectivo en los cajeros automáticos por los muleros— [36]. En otras ocasiones el delincuente no solo despoja a la víctima de lo que tiene en la cuenta sino que contrata a su nombre créditos personales instantáneos o preconcebidos, dejándolo endeudado. Habitualmente lo sustraído termina invertido en criptomonedas que son depositadas en *wallet* frías para evitar su decomiso.

Para conseguir sus fines, señala TORRES KEENLYSIDE como las principales estrategias que utilizan los delincuentes son[37]: correos electrónicos con mensajes enfocados al lucro; enlaces a páginas web fraudulentas[38]; correos electrónicos con mensajes que potencian la toma de decisiones rápidas[39]; o uso de spam, cuya finalidad sería poner a prueba la seguridad.

Se trata normalmente de mensajes sencillos, cotidianos, que cualquiera puede recibir, y que la víctima abre, por curiosidad, por lucro, o

---

[35] CANO TERUEL, Q. «Phishing: definición, tipos y cómo protegerse» [Cibercrim]. Disponible en: https://cibercrim.com/phishing-definicion-tipos-y-como-protegerse/ Fecha de consulta: 12/04/2023.

[36] Sobre la operativa Vid. TORRES KEENLYSIDE, A. *op. cit.*, pp. 5 y 6.

[37] Entre otras que señala el autor como el *Spear phishing* y el *vishing*. Cfr. TORRES KEENLYSIDE, A. *op. cit*., p. 7.

[38] A través de un enlace se accede a esas páginas que son una réplica de la web legítima. El usuario pincha en el enlace y rellena los datos que se le solicitan bajo la creencia de que se encuentra en la página auténtica, datos que son utilizados por los delincuentes para su uso o posterior venta a terceros.

[39] Podemos encontrar ejemplos en aquellos en los que se conmina a la víctima a dar sus credenciales para evitar una trasferencia no consentida, o bajo la amenaza de bloqueo de la cuenta. Recientemente se ha desarticulado una banda liderada por un menor de edad y cuya operativa, presuntamente, consistiría en llamar a las víctimas, haciéndose pasar por empleados de las entidades financieras de las víctimas para solventar una supuesta brecha de seguridad. Les solicitaban los códigos de verificación por teléfono lo que facilitaba las transacciones fraudulentas que eran realizadas en tiempo real. https://elpais.com/economia/2023-02-26/la-policia-desarticula-una-red-de-cibercriminales-liderada-por-un-menor.html (Fecha de consulta: 12/04/2023).

por temor, como ocurre con aquellos cuyo origen parece ser la policía o el juzgado[40].

Para ver el nivel de especialización que alcanza este tipo de delincuencia es suficiente con analizar la sentencia de la Audiencia Nacional núm. 8/2020 de 15 septiembre[41] donde se nos señala como la organización criminal tenía un carácter trasnacional y estaba formada por un número elevado de miembros con una alta especialización en la realización de engaños a través de internet y una cualificación técnica considerable. Se trataba de una organización con un alto grado de coordinación que, como señala la sentencia, estaba organizada como una gran compañía, y estructurada en diferentes departamentos. Así disponía de un departamento de planificación que se ocupaba de diseñar las operaciones; un departamento de informática, encargado de realizar los *phishing*; un departamento que se encargaba de confeccionar documentos; y un departamento de logística, que se encargaba de gestionar la «mulas». De idéntica manera dentro de la organización, enormemente jerarquizada, existían diferentes figuras y categorías (miembro relevante, creadores de documentación, captador, testaferro, colaboradores y mulas).

3. La regulación del *phishing* en el Código Penal español

La Ley Orgánica 14/2022, de 22 de diciembre ha modificado el tipo penal de la estafa informática, no solo cambiando su ubicación sino también incorporando nuevas conductas típicas. Como recoge el Preámbulo de la Ley, en estos últimos años se ha producido un crecimiento exponencial de los delitos informáticos como consecuencia «(…) del incremento del denominado ciberespacio y el consecuente aumento de la ciberpoblación en el ámbito de Internet». El legislador según han ido apareciendo nuevas formas comisivas ha ido introduciendo nuevas figuras penales junto a las ya tradicionales, de forma que los tipos penales se adapten a las nuevas tecnologías. Existe una necesidad, como señala el preámbulo, de facilitar la integración de las exigencias normativas derivadas de la Directiva (UE) 2019/713, de 17 de abril.

Según señala el preámbulo de la Ley el ámbito de protección de la reforma se extiende también a las monedas de carácter virtual, que son las nuevas realidades. Así, se señala como «quedan incluidos, por tanto, todos los instrumentos de pago distintos del efectivo, incluidas las monedas virtuales y otros criptoactivos que se utilicen como medio de pago y

[40] https://www.europapress.es/nacional/noticia-policia-nacional-advierte-envio-correo-spam-policiagobernoes-contiene-virus-20101211093952.html (Fecha de consulta: 12/04/2023).

[41] SAN núm. 8/2020 de 15 septiembre, confirmada por STS (Sala de lo Penal, Sección1.ª) núm. 291/2021 de 7 abril. ECLI:ES:TS:2021:1601.

los monederos electrónicos en una definición lo suficientemente abierta como para permitir la flexibilidad necesaria para adecuarse a los rápidos avances tecnológicos».

Recoge FERNÁNDEZ TERUELO como los elementos caracterizadores del delito de estafa común son el engaño precedente o concurrente, que ha de ser bastante, o suficiente para poder conseguir la finalidad propuesta por el estafador, lo que obliga a tener en cuenta las condiciones subjetivas del sujeto pasivo, y las objetivas que concurran en el caso. Señala el autor como esa maniobra defraudatoria ha de estar envuelta en un halo de apariencia de realidad suficiente para que una persona de mediana perspicacia y diligencia pueda ser engañada. El engaño, ya sea implícito, explícito, activo u omisivo, es lo que llevaría al sujeto a tener un conocimiento inexacto de la realidad y es la causa de la subsiguiente disposición patrimonial en perjuicio de quien realiza la misma o de un tercero. Además, es necesario que concurra el ánimo de lucro[42].

NÚÑEZ CASTAÑO, tras señalar como fue la insuficiencia del tipo genérico de estafa para hacer frente a determinados comportamientos de desapoderamiento a través de las nuevas tecnologías lo que llevó al legislador a la introducción de este tipo penal, refiere como en estas nuevas modalidades faltan dos de los requisitos clásicos de la estafa: el engaño y el error, ya que la conducta no va dirigida a una persona sino que el destinatario es la máquina o sistema informático, que no puede ser engañado. No obstante, como señala la autora sí que existe un comportamiento fraudulento que causa un perjuicio patrimonial[43]. Para FARALDO CABANA la regulación de la estafa informática equipara a la estafa a efectos penológicos conductas que adolecen de algunos de los elementos de la estafa común, pero que implican una actuación subrepticia, astuta, que el legislador equipara al engaño característico de la estafa[44].

Señala SÁNCHEZ-ESCRIBANO en los delitos de estafa informática nos encontramos ante un tipo de estafa por asimilación, ya que el legislador se refiere a la estafa informática con la expresión «también se consideran reos de estafa»[45]. Si bien el tipo de estafa genérico refiere la necesidad de ánimo de lucro y la utilización del engaño bastante para producir error en la otra persona, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno, lo cierto es que en determinadas modalidades de

---

[42] FERNÁNDEZ TERUELO, J. «Respuesta penal frente a fraudes cometidos en internet: estafa, estafa informática y los nudos de la red», *Revista de Derecho Penal y Criminología*, 2.a Época, núm. 19, 2007, p. 231 y ss.

[43] NÚÑEZ CASTAÑO, E. «Delitos patrimoniales de enriquecimiento mediante defraudación (I) estafa», En *Nociones fundamentales de derecho penal*. Gómez Rivero (dir.) Tecnos, 2019, p. 119.

[44] FARALDO CABANA, P. «Estrategias legislativas en las reformas de los delitos informáticos contra el patrimonio». *Revista Aranzadi de Derecho y Nuevas Tecnologías,* núm. 42, 2016, p. 5.

[45] SÁNCHEZ-ESCRIBANO, M. «Tendencias actuales en materia de…», *op. cit*., p. 9.

estafa informática se presentan peculiaridades. Así, señala FERNÁNDEZ TERUELO como en los fraudes donde el defraudador introduce un software malicioso en el dispositivo de la víctima para captar las credenciales que le permitan realizar las transacciones posteriores no hay ningún mensaje dirigido a la víctima para que ésta haga algo. Igualmente, señala el autor, presenta dificultades de subsunción en la estafa común los supuestos de *phishing,* donde es la víctima la que hace llegar al defraudador los datos necesarios para realizar las transacciones, no existiendo necesariamente en el momento ulterior un engaño para llevar a cabo la disposición patrimonial, sino que es el defraudador quien realiza la disposición patrimonial. Para dar respuesta a estas situaciones el legislador creó la llamada estafa informática[46].

El *phishing,* en su modalidad más habitual, se encuadraría dentro del artículo 249.1 letra a) del CP que castiga 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*. Para el TS[47] sentencia núm. 379/2019 de 23 julio, el tipo penal exige un ánimo de lucro, una manipulación informática o artificio semejante y un acto de disposición económica en perjuicio de tercero que se concreta en una transferencia no consentida.

Como señala la sentencia aludida, en este tipo de estafa subsiste la defraudación, siendo el engaño propio de la relación personal, sustituido por la manipulación informática o artificio semejante en el que lo relevante es, a juicio del Tribunal, «que la máquina, informática o mecánica, actúe a impulsos de una actuación ilegítima que bien puede consistir en la alteración de los elementos físicos, de aquéllos que permite su programación, o por la introducción de datos falsos». Respecto al error, como recoge la STS en los aparatos electrónicos no existe un error idéntico al exigido por el tipo tradicional de la estafa, en el sentido de una representación falsa de la realidad[48].

A diferencia de la redacción anterior que solo hacía referencia a la obtención de una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro *valiéndose de cualquier otra manipulación informática o artificio semejante*, en la redacción actual se ha aumentado el elenco de las conductas típicas, lo que viene a coincidir con el núcleo

[46] FERNÁNDEZ TERUELO, J. «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». En un modelo integral de derecho penal. En *Libro homenaje a la profesora Mirentxu Corcoy Bidasolo,* Agencia Estatal Boletín Oficial Del Estado, 2022, Madrid, p. 1142.

[47] STS núm. 379/2019 de 23 julio. ECLI:ES:TS:2019:2606.

[48] STS núm. 509/2018 de 26 octubre. ECLI:ES:TS:2018:3666.

de la conducta típica de otros tipos penales, siendo el elemento diferenciador, la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro[49].

Respecto a los elementos configuradores del tipo penal, la palabra «artificio» hemos de entenderla como cualquier artimaña, doblez, enredo o truco[50]. NÚÑEZ CASTAÑO se refiere a ella como «toda manipulación operada sobre ficheros o soportes informáticos, electrónicos o telemáticos (…)»[51]. Señala la STS núm. 509/2018 de 26 octubre[52] cómo la cuestión de cuáles son los artificios semejantes debe ser determinada por la aptitud del medio informático empleado para producir el daño patrimonial. En este sentido, señala la sentencia como «es equivalente, a los efectos del contenido de la ilicitud, que el autor modifique materialmente el programa informático indebidamente o que lo utilice sin la debida autorización o en forma contraria al deber». En definitiva, señala la sentencia, el hecho de identificarse ante el sistema informático mendazmente o de introducir datos en el sistema que no se corresponden con la realidad, es una manipulación informática que integra el tipo de la estafa. Refiere REY HUIDOBRO como la doctrina penal mayoritaria, maneja un concepto más adecuado y restringido, que considera la manipulación informática o artificio semejante a la que directamente ocasiona el traspaso patrimonial ilícito y causa el perjuicio de tercero[53]. Para el autor la manipulación informática o el artificio semejante, no se dará en la primera fase, donde el defraudador obtiene las credenciales de acceso a la cuenta bancaria, ya que no existe ningún traspaso patrimonial ilícito. Para el autor dichas manipulaciones quedarían fuera del concepto de estafa aunque podrían dar lugar a otras responsabilidades penales como falsedad documental o descubrimiento y revelación de secretos Diferente es la segunda fase, donde si existe esa trasferencia patrimonial y un perjuicio[54].

La reforma introduce nuevas conductas típicas, como obstaculizar o interferir indebidamente en el funcionamiento de un sistema de información lo que daría soporte a la punición de aquellas acciones cuyo fin es perturbar el servicio (por ejemplo, mediante ataques a los equipos provocando respuestas masivas de estos para bloquearlos). Dentro de la expresión sistema de información se incluirían «plataformas, hardware y software especializados que centralizan un conjunto de datos sobre el dominio, el proceso, o las actividades específicas de una empresa, para ges-

[49] Vid. MARTÍNEZ GARCÍA, K. Conferencia impartida en el Paraninfo de la Facultad de Derecho de la Universidad de Granada con el título «Estafas en el metaverso», (18 de abril de 2023).

[50] Cfr. STS núm. 379/2019 de 23 julio. ECLI:ES:TS:2019:2606.

[51] NÚÑEZ CASTAÑO, E. «Delitos patrimoniales de enriquecimiento…», *op. cit*., p. 120.

[52] STS núm. 509/2018 de 26 octubre. ECLI:ES:TS:2018:3666.

[53] REY HUIDROBRO, L. «La estafa informática:…», *op. cit*., p. 5.

[54] *Ibidem*. p. 6.

tionarlos y proporcionar orden, visibilidad, interpretación y análisis»[55]. Respecto al uso del término «indebidamente» hemos de entenderlo referido a de forma ilícita.

Otra de las conductas incorporadas en la última reforma consiste en introducir, alterar, borrar, transmitir o suprimir indebidamente datos informáticos de forma indebida. Introducir consistiría en incorporar nuevos datos, lo que afectaría a la fiabilidad del sistema, mientras que alterar equivaldría a modificar estos datos informáticos. Por su parte, borrar implicaría una destrucción de los datos contenidos en ese sistema de información, hacerlos desaparecer. Respecto al borrado, hemos de recordar que también el artículo 264 CP, relativo a los daños informáticos, castiga al que sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos. Por su parte, el 264 bis castiga obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno. El 249 CP exige dos elementos clave para diferenciar ambas figuras, el ánimo de lucro, y la finalidad conseguir una transferencia no consentida de cualquier activo patrimonial en perjuicio de terceros.

Respecto a la trasferencia, no puede ser realizada por el propio usuario, como ocurre con las famosas cartas nigerianas, donde se incita a depositar un dinero para compartir una cuantiosa cantidad de dinero que el estafador supuestamente tiene en su país. Esa modalidad se integraría, como señala Miró Llinares, dentro de la estafa clásica[56].

Refiere Rey Huidobro como en el *phishing* los denominados scammers crean o modifican documentos informáticos, o electrónicos, simulando documentos normalmente mercantiles[57]. La clonación de páginas web plantea el dilema de si nos encontramos ante un delito de falsedad documental. Como refiere Sánchez-Escribano, se colman los requisitos en cuanto la página web es un documento electrónico que incorpora información, lo que iría además en consonancia con la interpretación extensa que del término documento ha realizado la jurisprudencia[58].

Junto al castigo del *phisher,* la otra cuestión interesante es el castigo de los muleros, donde la jurisprudencia es vacilante. Se trata de personas que son captadas por la organización y a las que se les ofrece una cantidad de dinero, normalmente un 8 o 10% del monto recibido, para que colaboren abriendo una cuenta, y recibir en ella las cantidades sustraídas. Estas personas posteriormente transfieren ese dinero a la organización,

[55] https://negociosyempresa.com/sistemas-de-informacion-empresas/ (fecha consulta 03/04/2023).

[56] Miró Llinares, F. «La respuesta penal al ciberfraude: …», *op. cit*., p. 14.

[57] Rey Huidrobro, L. «La estafa informática:…», *op. cit*., p. 11.

[58] Sánchez-Escribano, M. «Tendencias actuales en materia de…», *op. cit.*, p. 10.

descontada la comisión, mediante trasferencias o medios de pago difícilmente rastreables. Respecto a ellos se plantea si cometen un delito de estafa, de blanqueo imprudente, o incluso de receptación[59].

Para la SAP de Asturias (Sección 2.ª) núm. 27/2023 de 26 enero[60], abrir una cuenta corriente cuya única finalidad es ingresar el dinero que previamente otros han sustraído a la víctima integra el delito de estafa. Como señala la SAP, esa cuenta también es necesaria para el buen fin del delito, por lo que la contribución del «mulero», quien se presta de forma interesada a convertirse en depositario momentáneo de los fondos sustraídos es un acto que integra la cooperación necesaria al tratarse de actos de relevancia, y no una conducta meramente accesoria o irrelevante, ni periférica.

En esta cuestión se torna de gran importancia la teoría de la ignorancia deliberada. Así, si el mulero conoce o sospecha, y se sitúa ante esa ignorancia deliberada comete el delito de estafa, mientras que si desconoce por completo el origen delictivo se podría hablar de un blanqueo por imprudencia[61]. La SAP ha venido a recoger el estado de esta cuestión al señalar como:

> «1.ª) Si el 'mulero' interviene y participa dolosamente en el delito cuya secuencia inicial —la obtención de las claves secretas y la transferencia del dinero de esas cuentas a la abierta por el 'mulero'— ejecuta un tercero, pero a la que el 'mulero' coopera de forma decisiva, cometería delito de estafa;
>
> 2.ª) Si el 'mulero' no interviene ni participa dolosamente en esas primeras secuencias iniciales, limitándose a abrir una cuenta a su nombre y poner ésta a disposición de quienes sí lo hicieron, para acto seguido transferir el producto del dinero en ella ingresado a cuentas de terceros, estaríamos ante un delito de blanqueo de capitales , bien en su modalidad dolosa, bien en su modalidad imprudente, tipificación ésta más ajustada que la manejada por algún sector de la doctrina relativa al delito de receptación».

Por su parte las STS núm. 51/2020, de 17 de febrero[62] hace referencia a como desconocer la estructura de la organización cuando se conoce el origen ilícito del dinero colma los requisitos del delito de estafa, mientras

---

[59] Ver Audiencia Provincial de Tarragona (Sección 2.ª), sentencia núm. 197/2018 de 20 abril. ECLI:ES:APT:2018:637. Como señala la SAP una parte de la doctrina entiende que «(…) la colocación del dinero en países con los que no existen mecanismos jurídicos de cooperación judicial, forma parte ya de la fase de agotamiento del delito, de forma que la captación de éstos puede llegar a producirse cuando ya la estafa se habría cometido. De ahí que estaríamos en presencia de una participación postdelictiva o postconsumativa, con un evidente contenido lucrativo, notas definitorias del delito de receptación)».

[60] SAP de Asturias (Sección 2.ª) núm. 27/2023 de 26 enero. ECLI: ECLI:ES:APO:2023:131.

[61] Cfr. STS núm. 51/2020 de 17 febrero. ECLI:ES:TS:2020:2017.

[62] STS núm. 51/2020, de 17 de febrero. ECLI:ES:TS:2020:2017.

que la STS núm. 253/2020, de 27 de mayo interpreta como el hecho de ofrecer un medio de recepción del dinero es una aportación importante para el delito de estafa «(…) la recepción del dinero desplazado pro el engaño, al tiempo que establece un elemento de dificultad en la identificación del delito, de su persecución y de los autores. El conocimiento de los hechos de la estafa, como elemento subjetivo, se infiere con racionalidad de los hechos externos realizados por el recurrente quien recibe una cantidad importante económica de una fuente, para él desconocida, y le proporciona una documentación en contabilidad deliberadamente falsa, disponiendo de la cantidad indebidamente realizada. Deducir de esa conducta un conocimiento de los hechos que dan lugar a la tipicidad de la estafa, y la colaboración con el artificio, es razonable y así lo explica la sentencia».

4. El Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera y de la legislación de consumidores y usuarios

La utilización masiva de internet y la implantación de medios de pago electrónicos ha facilitado la vida diaria de los usuarios, pero a su vez ha supuesto una serie de peligros y riesgos que son inherentes a su uso, lo que ha obligado a llevar a cabo una regulación de estos servicios. Fruto esta necesidad surgió el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera y de la legislación de consumidores y usuarios. El RD establece una suerte de responsabilidad cuasi objetiva de la entidad que presta los servicios de pago, y que solo permite excluir la responsabilidad en los supuestos de negligencia grave o fraude por parte del cliente.

En este RD se establecen determinadas pautas a seguir por usuarios y servicios de pago a fin de evitar fraudes en el uso de estos medios. En primer lugar, el artículo 36 de dicho RD se refiere al consentimiento. Así, establece como para que una operación se pueda autorizar es preciso el consentimiento del ordenante, y como a *falta de tal consentimiento la operación de pago se considerará no autorizada.* En los supuestos de *phishing* el delincuente no dispone de un consentimiento por parte del titular de la cuenta, sino que se vale del engaño o mecanismos para obtener las claves. Es cierto que la víctima ingresa en la página o facilita las claves de forma voluntaria, pero no con ánimo de autorizar la operación fraudulenta.

El usuario de servicios de pago tiene derecho a que una operación no autorizada sea rectificada siempre y cuando lo comunique sin demora a la entidad. La Ley establece una inversión de la carga de la prueba de forma que, si el usuario niega haber autorizado una operación de pago

ya ejecutada habrá de ser el proveedor de servicios quien demuestre 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 de servicios de pago». Como refiere el RD no es suficiente para enervar la prueba el uso del instrumento de pago.

Por otro lado, el usuario está obligado conforme al artículo 41 del RD a tomar todas las medidas razonables a fin de proteger sus credenciales de seguridad, y en caso de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada, a notificar a la entidad ese incidente sin demora, —tan pronto haya tenido conocimiento—. Desde el momento en que se comunique esta circunstancia la entidad debe de impedir cualquier utilización posterior del instrumento de pago.

Es importante señalar como el RD 19/2018 pone énfasis en el riesgo que ha de soportar la entidad en determinados supuestos distintos al uso, como son, por ejemplo, el envío de un instrumento de pago al usuario o el envío de los elementos de seguridad personalizados del mismo, esto se basa en el aforismo latino «cuius commoda eius incommoda», el que se beneficia de una determinada actividad debe de soportar los riesgos que ella lleva aparejada.

Conforme al artículo 45 del RD, en caso de que se ejecute una operación de pago no autorizada la entidad ha de devolver al usuario el importe de la operación de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente desde la notificación de la operación, salvo sospecha de la existencia de fraude, debiendo en este caso de comunicar las razones por escrito al Banco de España.

Si la víctima ha contribuido a la pérdida o ha actuado de manera fraudulenta o ha incumplido deliberadamente o por negligencia grave, una o varias de las obligaciones que establece el artículo 41 del RD será esta la que deba de asumir la pérdida. No obstante, deberá ser la entidad quien pruebe que el usuario del servicio de pago cometió ese fraude o actuó con negligencia grave.

Existe una obligación general por parte de la entidad financiera de reintegrar al cliente el dinero sustraído en estos casos. Se trata de una responsabilidad *ex lege*. La entidad deberá de reintegrar directamente esa cantidad a su cliente, si bien podrá personarse en el juicio y reclamar las cantidades satisfechas, actuando como perjudicado, subrogándose en la acción de responsabilidad civil que tenía el ofendido[63]. En relación a esta

[63] SAP de Barcelona (Sección 9.ª) núm. 842/2017 de 6 noviembre. ECLI:ES:APB:2017:13366.

última cuestión, en la SAN núm. 7/2022 de 28 junio[64]se planteaba por la defensa del acusado si el otorgar una indemnización al banco subrogado en la reclamación no podría constituir un supuesto de enriquecimiento injusto, —en el supuesto de que el Banco fuera indemnizado por el acusado y dispusiera a su vez de un seguro—. En este caso, como señala la SAN, legitimados serían tanto la Entidad financiera como la propia Aseguradora, pudiéndose corregir en cualquier caso esa situación entre los legitimados afectados, que se podrían reclamar entre ellos, por lo que no da la razón al apelante.

La Directiva 2015/2366/UE, de 25 de noviembre del Parlamento Europeo y del Consejo, sobre servicios de pago en el mercado interior recoge, en su Considerando 72, como a la hora de determinar si nos encontramos ante un comportamiento negligente del usuario es necesario tener en cuenta todas las circunstancias «No obstante, si el concepto de negligencia supone un incumplimiento del deber de diligencia, la negligencia grave tiene que significar algo más que la mera negligencia, lo que entraña una conducta caracterizada por un grado significativo de falta de diligencia. Un ejemplo sería el guardar las credenciales usadas para la autorización de una operación de pago junto al instrumento de pago, en un formato abierto y fácilmente detectable para terceros. Se deben considerar nulas las cláusulas contractuales y las condiciones de prestación y utilización de instrumentos de pago mediante las cuales aumente la carga de la prueba sobre el consumidor o se reduzca la carga de la prueba sobre el emisor. Además, en situaciones específicas y, más concretamente, cuando el instrumento de pago no esté presente en el punto de venta, como en el caso de los pagos en línea, resulta oportuno que el proveedor de servicios aporte pruebas de la presunta negligencia, puesto que los medios a disposición del ordenante son limitados en esos casos»[65].

A la hora de deslindar los conceptos de negligencia y negligencia grave la jurisprudencia menor es vacilante. En la SAP de Valladolid (Sección 1.ª) núm. 74/2010 de 10 marzo[66], se nos indica como el facilitar claves al usuario tiene como finalidad proteger al cliente de las injerencias de terceros. En el supuesto enjuiciado, la víctima facilitó sus claves tras acceder al enlace, lo que para la AP suponía un incumpliendo de una elemental medida de seguridad, dándose la circunstancias de que dicha advertencia aparecía en la pantalla auténtica del banco y que, además, se había remitido por parte de la entidad a los clientes una carta en la que se advertía expresamente de las oleadas de *phishing*, razones que llevaron a la AP a desestimar la demanda del usuario.

[64] SAN núm. 7/2022 de 28 junio. ECLI:ES:AN:2022:3186.

[65] Vid. SAP de Pontevedra núm. 539/2021 de 21 diciembre. ECLI:ES:APPO:2021:3078.

[66] SAP de Valladolid (Sección 1.ª) núm. 74/2010 de 10 marzo. AC 2010\368. ECLI: ECLI:ES:APVA:2010:226.

En la SAP de A Coruña (Sección 3.ª) núm. 17/2023 de 25 enero[67] , la víctima tras recibir un mensaje de texto pichó en el link, introdujo sus claves, y posteriormente recibió un mensaje a su teléfono en el que le advertía de la realización de la trasferencia, procediendo a trasladar el código de verificación a su interlocutor. Destaca aquí la sentencia la existencia de tres tipos de negligencias de distinta entidad: «No es una negligencia, son tres. Y si la primera aún pudiera ser más o menos comprensible (pinchar en un enlace), la segunda ya es grave (facilitar usuario y contraseña), y la tercera es totalmente temeraria (informar de la confirmación)».

Por el contrario, otras resoluciones, como la SAP de Madrid (Sección 10.ª) núm. 24/2023 de 13 enero[68], no han calificado como grave la negligencia de un cliente víctima de *phishing* que introdujo sus claves, realizándose varias trasferencias no consentidas. Para la SAP se trata de un fraude muy específico del que es fácil ser víctima, «sin que ello implique una actuación negligente del cliente, dado lo bien articulada en su ejecución que está esta modalidad de fraude». En este caso se da, además, la circunstancia de que el cliente acudió al banco al día siguiente, y el empleado de la entidad no detectó ninguna irregularidad. La Sala entendió que la entidad bancaria actuó sin tomar las medidas de diligencia y seguridad exigidas, sin que el hecho de haber avisado a las víctimas por web y otros medios de las campañas masivas de phishing sirviera de eximente. Así, señala como «tampoco sirve de excusa a la entidad apelada la inclusión de avisos en web y otros medios de la entidad sobre el comportamiento seguro que en el uso de la plataforma había de tener el cliente, sino que la entidad bancaria debe dotar a la banca electrónica de las medidas de seguridad necesarias para prevenir unos tipos de fraude ya muy extendidos y que, como lo prueba el supuesto que nos ocupa, siguen produciéndose por falta de una medida adecuadas por la entidades bancarias, que ponen a disposición de sus clientes la banca online y la contratación electrónica como dotados de una seguridad que no garantizan».

Tampoco apreció esta circunstancia la SAP de Pontevedra (Sección 6.ª) núm. 539/2021 de 21 diciembre[69], en un supuesto donde el Banco alegaba que la víctima debía de soportar las pérdidas, al haber actuado con grave negligencia, ya que tras recibir un correo fraudulento de *phishing* que simulaba ser de Correos, pinchó en el enlace que la redirigió a una página fraudulenta donde introdujo las claves de la tarjeta para pagar un envío pendiente. Tras esto, el defraudador instaló la tarjeta de la víctima en la aplicación Samsung Pay de su terminal, para así poder realizar

[67] SAP de A Coruña (Sección 3.ª) núm. 17/2023 de 25 enero. ECLI:ES:APC:2023:196.

[68] SAP de Madrid (Sección 10.ª) núm. 24/2023 de 13 enero. ECLI:ES:APM:2023:249.

[69] SAP de Pontevedra (Sección 6.ª) núm. 539/2021 de 21 diciembre. ECLI:ES:APPO:2021:3078.

pagos con esta. El banco remitió a la víctima un mensaje de verificación que decía: «¡Atención! Usa el código NUM000 para instalar tu tarjeta acabada en NUM001 en Samsung Pay. Válido 30min. No lo compartas. Si tienes dudas llama al (…)». Una vez instalada la tarjeta volvió a mandar otro mensaje «Tu tarjeta acabada en xxx ha sido activada en Samsung Pay. Si no es correcto llámanos al teléfono». La SAP tras recordar el contenido del artículo 2 del Reglamento delegado 2018/389/UE, de 27 de noviembre que obliga a los proveedores de servicios de pago a disponer de mecanismos de supervisión de las operaciones que les permitan detectar operaciones de pago no autorizadas o fraudulentas a efectos de la aplicación de las medidas de seguridad establecidas en el Reglamento, principalmente en lo referido al procedimiento de autenticación reforzada de clientes, señala como:

> «El deber de diligencia de la demandada para asegurar la correcta autenticación de las operaciones de pago exigía de dotarse de mecanismos de supervisión que permitieran detectar operaciones de fraudulentas a cuyo efecto habría de considerar los supuestos del fraude conocidos en la prestación de servicios de pago (artículo 2 del Reglamento Delegado 2018/389. Es por ello que conocido que la técnica del phishing incluye, a menudo, la creación y puesta en la red de páginas que clonan las del sitio oficial de las entidades emisoras de instrumentos de pago, el deber de diligencia de la entidad demandada exigía dotarse de la tecnología antiphishing precisa para detectar las páginas clonadas de las oficiales propias y cerrarlas o eliminarlas, lo que, de producirse, impediría que el defraudador pudiera hacerse con las credenciales del usuario del instrumento de pago por ella emitido, pues la rotura del enlace del correo electrónico haría ya ineficaz cualquier conducta que frente al mismo pudiera observar el usuario receptor».

Para la SAP la entidad financiera no había acreditado la observancia de los deberes de diligencia exigibles con respecto a la autenticación de la operación, al no especificar en el mensaje el número de teléfono en que se activaría dicha tarjeta. Por otro lado, tampoco quedó demostrado que la entidad hubiera implementado un mecanismo *antiphising* de protección de los usuarios de los instrumentos de pago para hacer frente a los posibles fraudes. Termina la sentencia señalando como no cabría observar negligencia grave de los deberes de conducta de la afectada al usar del instrumento de pago y al introducir las credenciales de uso personal en una página que imitaba las del sitio oficial de la entidad emisora de su tarjeta. Razones que llevan a condenar a la demandada —la entidad financiera— al pago.

En la SAP de Barcelona núm. 151/2013 de 7 marzo[70] la Sala utiliza una frase muy relevante «no puede ofrecerse es un sistema on line sin

[70] SAP de Barcelona núm. 151/2013 de 7 marzo. ECLI:ES:APB:2013:2625.

adoptar las medidas de seguridad necesarias». En este caso, si se conocen los riesgos, y la existencia de estas prácticas fraudulentas se debe de exigir al proveedor de pagos que conozca esas operativas e instaure medidas de protección adecuadas. Para el Tribunal, no constaba ningún filtro de seguridad adicional. Se hicieron en este caso varias trasferencias por un importe superior al límite diario estipulado, lo que se burló al no existir un límite entre cuentas de la misma entidad. Por otro lado, el destino de las diferentes trasferencias, inusuales y, además, nombres de personas de origen extranjero, como puso de manifiesto por el Tribunal, podían haber servido para establecer alertas informáticas.

Muy interesante es la sentencia de la AP de Vizcaya núm. 429/2016 de 10 noviembre[71], donde el hecho de que se alegara por el banco que se había llamado al cliente —sin localizarlo— al detectar unos movimientos sospechosos y no haberse bloqueado las cuentas, suponía una falta de diligencia achacable al banco. Como recoge la SAP «a la entidad bancaria demandada le incumbe proteger a sus clientes de cuantas conductas se realicen a través de la banca electrónica y ello en cuanto que precisamente este tipo de fraude comienza con la posibilidad de que los defraudadores interesan las claves de acceso a los clientes de los bancos (en este incide la mecánica delictiva). Téngase en cuenta que el fraude se comete creando los delincuentes una página web similar a la del Banco, que se realizan a través de la línea bancaria reiteradas operaciones en la misma semana (hasta 30 movimientos) y por cantidades elevadas, lo cual no era propio de estos clientes; que no solo se efectuaron transferencias de cuentas sino que se emitieron órdenes de venta de valores de los que el Banco tiene suscrito un contrato de guarda y custodia y cobrando por dicha prestación que resulta obvia que ha sido burlada fácilmente sin ninguna comprobación exhaustiva; por el Banco no se realizó ninguna comprobación cuando además tras obtener la cantidad de la venta, dicha cantidad se transmitía a cuentas de terceros y de éstas a cuentas en el extranjero por las que recibían una comisión (en tal extremo recuérdese que esta cuenta de valores hasta ese momento no había tenido actividad alguna; se trataba de parte de la herencia de la Sra. Guillerma). El propio Banco, en el informe que aporta en el procedimiento penal y al realizar las investigaciones tras tener conocimiento de los hechos ya admite que ha sido objeto de un fraude en la superlínea y que no ha sido detectado; se dice en dicho informe que se llamó al cliente pero que no fue hallado, lo cual viene a ratificar que los movimientos de resultaron sospechosos, lo cual permite sostener la falta de diligencia que ante la sospecha no se bloquearan los movimientos (además de que no consta cual fue la conducta para hallar al cliente o a qué número telefónico se le llamó)». También la SAP de Madrid núm. 178/2015 de 4 de mayo[72], entendió que

[71] SAP de Vizcaya núm. 429/2016 de 10 noviembre. ECLI:ES:APBI:2016:2070.
[72] SAP de Madrid núm. 178/2015 de 4 de mayo. ECLI:ES:APM:2015:6240.

existía una falta de implementación de medidas de seguridad en el momento en el que la entidad sufrió el ataque, por lo que no se puede hablar de negligencia de la víctima.

Hoy en día, con las IA, que pueden servir para perfeccionar los ataques de *phishing* haciendo que los mensajes recibidos sean casi idénticos a los remitidos por las entidades financieras, o donde la clonación de las páginas web hace que estas sean casi indetectables para un ciudadano medio, debemos de replantear el concepto de negligencia grave. Este concepto de negligencia grave debería de reservarse para aquellos supuestos en los que la víctima guarda de forma incorrecta las claves, —por ejemplo, guarda el instrumento de pago junto con la credencial—, o se produce una tardanza injustificada en avisar a la entidad una vez conocido el fraude, o no adopta las medidas de autoprotección. Pero, en el resto de supuestos estimo que, a lo sumo, existiría una negligencia leve.

Señala PÉREZ GUERRA como la responsabilidad del banco va a existir cuando la entidad no aplique protocolos de seguridad efectivos; cuando ignore evidencias de fraude (movimientos sospechosos); cuando, denunciado el hecho por el usuario, la entidad se mantiene pasiva sin detener las transferencias o reacciona tarde; cuando, ante operaciones sospechosas, no realiza comprobaciones eficaces con los usuarios[73]. Para REY HUIDOBRO en caso de negligencia grave por phising de la entidad, la víctima no será responsable de las consecuencias del fraude, si no tiene disponibles medios adecuados y gratuitos para que pueda notificarse en todo momento la sustracción[74].

5. La responsabilidad civil *ex delito* de las entidades financieras consecuencia del articulo 120.3 CP

La revolución operada por internet, y la posibilidad de operar a través de la banca virtual han proporcionado comodidad al usuario, que puede operar desde cualquier sitio y a cualquier hora, pero también una fuente de peligros, principalmente para las personas mayores menos familiarizadas con las nuevas tecnologías. Para las entidades financieras ha supuesto un ahorro de costes, ya que han sustituido en muchas ocasiones el espacio físico por un establecimiento virtual. De hecho, existen entidades financieras que operan exclusivamente por internet. El artículo 120.3 CP establece la responsabilidad civil subsidiaria de «las personas naturales o

[73] Cfr. PÉREZ GUERRA, M. «Ciberdelitos y responsabilidad civil de las entidades financieras a la luz de la jurisprudencia», *En Revista de Derecho del Mercado de Valores*, Nº 29, Sección Mercados y Praxis Negocial, Segundo semestre de 2021, Wolters Kluwer, LA LEY 13822, 2021.

[74] Cfr. REY HUIDROBRO, L. «La estafa informática: relevancia penal del phising…», *op. cit.* p. 6.

jurídicas, en los casos de delitos cometidos en los establecimientos de los que sean titulares, cuando por parte de los que los dirijan o administren, o de sus dependientes o empleados, se hayan infringido los reglamentos de policía o las disposiciones de la autoridad que estén relacionados con el hecho punible cometido, de modo que éste no se hubiera producido sin dicha infracción».

Se trata de una responsabilidad cuasi objetiva[75] donde el obligado responde en base a cuatro criterios, tres de carácter positivo —que el delito se haya cometido en el establecimiento del que son titulares las personas naturales o jurídicas; que se haya producido por parte de sus titulares o empleados una infracción de unas normas, alcanzando esta infracción incluso al mero incumplimiento del deber objetivo de cuidado; que este incumplimiento haya facilitado el delito, de forma que este no se hubiera cometido sin esa infracción— y uno de carácter negativo, que el delito sea cometido por un tercero ajeno a ese establecimiento, ya que en caso contrario se estaría ante una responsabilidad del artículo 120.4 CP. Es una ampliación de la teoría clásica de la *culpa in eligendo y la culpa in vigilando*, en favor de postulados más modernos fundamentados en la teoría del riesgo[76].

Cuando el legislador se refiere a personas naturales o jurídicas no distingue entre personas jurídicas de carácter público o privado, por lo que deben de entenderse incluidas ambas categorías.

En relación con estas entidades financieras la primera cuestión sería determinar qué entendemos por establecimiento, y si nos referimos exclusivamente al espacio o sede física donde se desarrolla la actividad o si por el contrario nos encontramos ante un concepto amplio que abarca también el medio web o, como se conoce coloquialmente, la banca virtual. Está claro que internet ha supuesto una auténtica revolución en estos años dando paso a situaciones inimaginables en el año 1995, lo que obliga a actualizar estos conceptos y mirarlos desde la mirada actual. En mi opinión el concepto de establecimiento es un concepto amplio que abarca no solo el concepto de institución, sino también al *lugar donde habitualmente se ejerce una actividad*[77].

No podemos limitar el concepto de establecimiento a aquellos lugares que solo tengan previsto un uso comercial. Así, por ejemplo dentro de ese concepto pueden englobarse no solo comercios o entidades financie-

---

[75] Vid. San José Arévalo, X. «De la responsabilidad civil subsidiaria ex delicto de los arts. 120 y 121 del Código Penal». De La Fuente Hondarrubia, F. (Dir.). En *Estudios sobre la responsabilidad civil ex delicto*, Madrid, Sepín, 2022, p. 381. Vid. Quintero Olivares, G. *La responsabilidad civil «ex delicto»*. Aranzadi. 2002.

[76] Vid. Rodríguez Almirón, F. *Aspectos jurídico-dogmáticos y jurisprudenciales en torno a la responsabilidad civil ex delicto*, Madrid, Dykinson, 2022, pp. 127 y ss.

[77] Ver acepción de la RAE.

ras, sino también otras instituciones como una parroquia, un hospital[78], un centro educativo, o cualquier otro lugar donde se desarrolla una actividad[79]. Se trata de implantar en estas personas naturales o jurídicas una conciencia de que hay que velar por el cumplimiento de las normas que regulan las diferentes actividades u oficios[80].

En relación con el fenómeno delictivo por internet son varias las sentencias que, en sede penal, se han pronunciado sobre la responsabilidad civil subsidiaria de las entidades financieras. El primer problema es determinar cuando no encontramos ante un establecimiento. La STS núm. 49/2020 de 12 febrero[81] ha señalado como «(…) el entorno digital que el banco crea como plataforma y medio de prestación de los servicios esenciales que suministra, y de los que obtiene su lógico beneficio, colman los presupuestos de lugar a los que se refiere el artículo 120.3 CP (…)». En este caso, el acusado aprovechando que la víctima estaba de viaje solicitó a una amiga que le facilitara las llaves de la vivienda con la excusa de darle una sorpresa. Una vez en el interior se apoderó de la tarjeta de coordenadas y realizó una serie de trasferencias a su favor. Además, posteriormente hizo unos supuestos ingresos a través de un sobre vacío lo que no fue apercibido por el banco inmediatamente, sino 24 horas más tarde. Como señala la sentencia, la operativa online tiene riesgos, uno de ellos es el de la suplantación de identidad y la realización de operaciones no autorizadas, pero corresponde a la entidad el establecer mecanismos para que el cliente pueda operar seguro «(…) Es claro también que, excluyendo actuaciones dolosas o gravemente negligentes por parte de los clientes, la entidad bancaria es responsable de ofrecer y poner en práctica un sistema seguro, de manera que las consecuencias negativas de los fallos en el mismo no deberán ser trasladados al cliente».

La responsabilidad civil subsidiaria del artículo 120.3 CP exige que dentro del establecimiento se haya producido una vulneración los reglamentos de policía o de las disposiciones de la autoridad por parte de los directivos o trabajadores de la persona natural o jurídica, de forma que, a consecuencia de esta vulneración, se haya podido cometer el delito. Cuando la jurisprudencia de refiere a esa infracción de reglamentos se está refiriendo no solo a una violación reglamentaria, sino que hemos de entenderlo en su sentido amplio, es decir, referido también cualquier violación de la ley, de los reglamentos, o de otras disposiciones normativas de rango inferior «(…) incluso el deber objetivo de cuidado que afecta a toda actividad para no causar daños a terceros (…)»[82].

[78] STSJ de Murcia núm. 28/2021 de 17 noviembre ECLI:ES:TSJMU:2021:2262.
[79] STSJ de Cataluña, núm. 290/2021 de 14 septiembre ECLI:ES:TSJCAT:2021:9069.
[80] STS núm. 53/2020 de 17 febrero ECLI:ES:TS:2020:530.
[81] STS núm. 49/2020 de 12 febrero ECLI:ES:TS:2020:332.
[82] STS núm. 768/2009 de 16 julio ECLI:ES:TS:2009:4829.

El delito ha de ser cometido por un tercero ajeno a esa persona natural o jurídica, pues de cometerse el delito por sus empleados o dependientes, representantes o gestores en el desempeño de sus obligaciones o servicios, se aplicaría la responsabilidad subsidiaria del artículo 120.4 CP. Por otro lado, tampoco puede tratarse de delitos cometidos por autoridades, agentes y contratados por la Administración o funcionarios públicos en el ejercicio de sus cargos o funciones, ya que estos se rigen por el artículo 121 CP que establece la responsabilidad civil subsidiaria de la Administración.

La redacción del precepto solo exige que se haya cometido un delito y un nexo causal, que se haya producido una infracción por parte de los empleados o dependientes, sin que exista una obligación concreta de determinar la persona o personas que han infringido esa normativa, y cuyo quebrantamiento ha permitido que se cometa el delito. La STS núm. 372/2020 de 3 julio ha referido como para que opere la responsabilidad del artículo 120.3 CP es preciso un nexo de causalidad operativo, eficaz y eficiente con el daño causado. Por su parte la STS núm. 53/2020 de 17 febrero[83] ha establecido respecto al nexo causal como no es necesario que exista una relación de causalidad absoluta entre la infracción de la norma y el delito, como ocurriría en el ámbito estrictamente penal. Lo relevante es que exista un incumplimiento de una norma, que como señala la sentencia tiene un carácter preventivo, y el acaecimiento de la infracción penal, de tal forma que, desde un punto de vista *ex post*, se pueda afirmar que si no se hubiera infringido la norma no se hubiera podido cometer el delito.

Como incide el TS no se puede confundir causalidad civil y penal, ya que se rigen por criterios distintos. En el supuesto del artículo 120.3 CP la causalidad es diferente a la aplicable al resto de la responsabilidad civil[84] debido a que en este caso el delito lo comete un tercero y es una responsabilidad civil subsidiaria. Esta responsabilidad surgiría, por tanto, de la falta o insuficiencia de medidas de prevención obligatorias que, como señala el TS, se centrarían en los deberes de vigilancia y control exigibles.

Las normas buscan prevenir un riesgo, y si esa inobservancia ha creado el riesgo que se pretende evitar «se identificará el fundamento de este tipo de responsabilidad civil, que requiere no una directa relación de causalidad entre la infracción y la comisión del ilícito, sino una relación simplemente adecuada entre la infracción y el ilícito que se quiera prevenir por la norma infringida». Así, el incumplimiento vendría referido a la prevención *ex ante*, y no la represión *ex post*. Señala la sentencia como no es necesario que la falta de diligencia sea la causa eficiente del delito sino que, esa falta de diligencia o de observancia de las normas, haya hecho posible este, es decir, ha favorecido el resultado.

[83] STS núm. 53/2020 de 17 febrero ECLI:ES:TS:2020:530.
[84] Relación entre delito cometido y daño soportado.

Como recoge la SAP de Asturias núm. 406/2020 de 27 noviembre las medidas de seguridad han de ser las adecuadas en cada momento para así evitar situaciones de peligro innecesarias, por lo que han de valorarse en su conjunto, y desde una perspectiva *ex ante,* las diferentes circunstancias. Por ejemplo, la SAP de Baleares núm. 109/2018 de 14 marzo[85] conoció un supuesto donde un fedatario público a pesar de advertir el poco parecido entre la figura que aparecía en el DNI y el firmante del documento, autorizó la escritura, lo que favoreció la usurpación de personalidad. En este caso el fedatario público no comete el delito, pero sí que lo favorece desde el momento en que no realiza otros actos tendentes a asegurarse de la verdadera personalidad del otorgante. Aquí, es ese deber de diligencia el que es transgredido. En otros casos, como el conocido por el TSJ de Madrid núm. 271/2020 de 5 octubre[86] respecto de un delito de fraude a la Seguridad Social, lo infringido es la normativa, así una persona percibió de forma indebida una pensión tras el fallecimiento de un familiar, sin que la Seguridad Social se apercibiera de esta situación, debido a que la entidad financiera no cumplió de forma correcta con su obligación de realizar el control anual de supervivencia.

Respecto a la infracción de los reglamentos o disposiciones, en la STJ del País Vasco núm. 82/2021 de 29 de septiembre[87], se analizaba un supuesto donde el acusado, trabajador de una aseguradora, detraía en nombre de estos cantidades que estos previamente habían ingresado, sin su consentimiento, para invertirlas en fondos de inversión de mayor riesgo que los contratados por el cliente, para así poder recuperar las pérdidas de estos sin que se enteraran o bien compensar las pérdidas sufridas por otros clientes. Para llevar a cabo su plan cobraba los cheques que la entidad emitía a nombre de los clientes, y que venían nominativos, barrados y no a la orden, mediante su entrega en otra entidad distinta a la de cobro. El Tribunal plantea como, podría considerarse una violación de reglamentos la trasgresión de la propia normativa interna del propio banco. El Tribunal entiende que no se acredita la infracción de ninguna norma que implicara una desatención de las cautelas necesarias para evitar el delito o reducir el riesgo de su comisión.

De todo lo anterior podemos concluir que mientras el Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera y de la legislación de consumidores y usuarios establece una responsabilidad *ex lege* de la entidad financiera, que es directa respecto al cliente, siempre y cuando no exista una actitud defraudadora ni una negligencia grave por parte del cliente, en el su-

[85] SAP de Baleares núm. 109/2018 de 14 marzo ECLI:ES:APIB:2018:502.
[86] STSJ de Madrid núm. 271/2020 de 5 octubre ECLI:ES:TSJM:2020:12132.
[87] STJ del País Vasco núm. 82/2021 de 29 de septiembre ECLI:ES:TSJPV:2021:2244.

puesto del artículo 120.3 CP, este requisito de negligencia «grave» no es necesaria, ya que no lo impone la norma.

En el artículo 120.3 CP nos encontramos ante una responsabilidad civil subsidiaria consecuencia del delito, por la que la entidad responde en defecto del responsable civil directo, y que no exige una negligencia grave, sino una mera inobservancia de las normas, o de ese deber de cuidado. Esto significa que incluso cualquier inobservancia de la normativa interna de la entidad, o incluso del propio programa de cumplimiento normativo[88] daría lugar a esta responsabilidad. El principal problema es la imposibilidad de identificar en muchas ocasiones al responsable de este delito al cometerse de forma telemática.

6. Competencia judicial

Conforme establece la jurisprudencia en los delitos de estafa informática la competencia vendría determinada por varios criterios que tienen un carácter complementario. Normalmente se ha utilizado el criterio de la ubicuidad, si bien las nuevas líneas optan por complementarlo con el criterio del lugar donde la instrucción pueda ser más eficaz. Así, por ejemplo, se ha determinado como más eficaz el lugar de residencia de los investigados, o donde se ha podido operar con los medios informáticos, o donde se encontraba la página web. Como recoge el ATS núm. 20131/2023 de 16 febrero «el lugar donde la investigación pueda tener algún éxito, o donde se hayan realizado algunos de los elementos del delito, criterio del lugar del comisión del delito, que debe ser acompañada por el de mayor eficacia en la investigación y respecto a este último criterio es en Valencia donde se han desarrollado elementos del delito o donde en principio reside la persona objeto de investigación»[89].

No se impone ese criterio de la ubicuidad, por tanto, cuando nos encontramos con otros lugares donde existan datos relevantes que puedan propiciar que la investigación llegue a buen término «el criterio de la ubicuidad no se impone cuando los datos son relevantes para la determinación a limine de la competencia y en este caso resulta la conveniencia de que se profundice en la investigación no solo de los titulares de las cuentas a las que parecen ordenadas las transferencias, sino también de quién podía manejar la página»[90].

---

[88] En este caso, el delito no puede ser cometido por los empleados o directivos, pues de lo contrario nos encontraríamos ante una responsabilidad también subsidiaria pero del artículo 120.4 CP.

[89] Tribunal Supremo (Sala de lo Penal, Sección1.ª), Auto núm. 20131/2023 de 16 febrero. ECLI:ES:TS:2023:1896A.

[90] Tribunal Supremo (Sala de lo Penal, Sección1.ª), Auto núm. 20019/2023 de 18 enero. ECLI:ES:TS:2023:789A.

Se trata por tanto de una teoría no contrapuesta sino complementaria a la teoría de la ubicuidad, como recoge el ATS núm. 20045/2023 de 25 enero «Esta es la doctrina de esta Sala que, frente a la teoría de la ubicuidad a la hora de atribuir la competencia cuando de delitos de estafa se trata, ha ganado terreno y se ha consolidado un nuevo criterio que lo complementa, como es el de la eficacia, de manera que, la competencia vendría determinada por el lugar donde la investigación policial pudiera tener, en el momento actual, algún éxito, donde se hayan realizado los elementos del delito, donde pueda operarse sobre los elementos informáticos y en definitiva donde la instrucción pueda ser eficaz»[91].

7. Reflexión final

Es una triste realidad como la delincuencia organizada es cada vez más profesional y su forma de operar más sofisticada. Los ataques de *phishing* son desgraciadamente habituales, y en muchos casos no es fácil de detectar incluso para personas que están familiarizadas con las nuevas tecnologías.

El delincuente utiliza múltiples artimañas, que provocan que sus víctimas muerdan el anzuelo. En este sentido, se ha de exigir de las entidades que proveen de esos servicios unas medidas preventivas adecuadas que disminuyan e intenten evitar estas prácticas, y que hagan de la operativa online medios seguros, sobre todo para aquellas personas menos familiarizadas con las nuevas tecnologías.

El Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera y de la legislación de consumidores y usuarios establece una obligación de la entidad de asumir el riesgo y de reintegrar al cliente esas cantidades defraudadas salvo que se haya producido una negligencia grave o exista por parte de este de un fraude. Se trata de una responsabilidad que nace *ex lege*. El problema está en determinar que se entiende por negligencia grave, y en esto la jurisprudencia menor es vacilante como hemos visto. En mi opinión, si se ofrece una actividad como segura la entidad debería de soportar esos riesgos, incluso cuando el cliente acceda a un enlace fraudulento.

En cualquier caso, fuera de esa responsabilidad directa *ex lege*, también puede surgir otra responsabilidad, pero en este caso subsidiaria cuya acción puede ser ejercitada dentro del procedimiento penal, y como consecuencia del delito que se ha cometido en ese establecimiento. Este concepto de establecimiento alcanza no solo al bien inmueble físico sino también a la plataforma o establecimiento virtual.

[91] Tribunal Supremo (Sala de lo Penal, Sección1.ª), Auto núm. 20045/2023 de 25 enero. ECLI:ES:TS:2023:942A.

La responsabilidad civil *ex delicto* del artículo 120.3 CP no exime a la entidad en caso de negligencia grave, es diferente. A lo sumo podría plantearse una compensación de culpas si se entiende que la persona ha contribuido con su conducta a la producción del daño. Lo relevante en este supuesto es que se haya cometido un delito en ese establecimiento y que, por parte de la persona natural o jurídica, se haya producido una infracción de los reglamentos o de la normativa que regula esa actividad. Esa infracción incluiría cualquier negligencia por pequeña que sea, incluso de las normas de conductas exigibles. Esa transgresión puede ser incluso de las normas o directrices internas, de las normas de compliance, etc. Eso sí, su inobservancia debe de haber posibilitado la comisión del hecho delictivo. Hecho delictivo que ha de ser cometido por un tercero ajeno a la entidad, pues de lo contrario operaría el artículo 120.4 CP.

8. Bibliografía

DE LA CUESTA ARZAMENDI, J.L. / PÉREZ MACHÍO, A.I. / SAN JUAN, C. *Aproximaciones criminológicas a la realidad de los ciberdelitos*, Civitas, Derecho penal informático. BIB 2010\1677.

FERNÁNDEZ TERUELO, J. «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». En un modelo integral de derecho penal. En *Libro homenaje a la profesora Mirentxu Corcoy Bidasolo,* Agencia Estatal Boletín Oficial Del Estado, 2022, Madrid.

— «Respuesta penal frente a fraudes cometidos en internet: estafa, estafa informática y los nudos de la red», *Revista de Derecho Penal y Criminología*, 2.a Época, núm. 19, 2007.

MIRÓ LLINARES, F. «Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos». *IDP: revista de Internet, derecho y política*, N.º 32, 2021.

— «La respuesta penal al ciberfraude: Especial atención a la responsabilidad de los muleros del phishing», *Revista electrónica de ciencia penal y criminología*, N.º 15, 2013.

PÉREZ GUERRA, M. «Ciberdelitos y responsabilidad civil de las entidades financieras a la luz de la jurisprudencia», *Revista de Derecho del Mercado de Valores*, Nº 29, Sección Mercados y Praxis Negocial, Segundo semestre de 2021, Wolters Kluwer, *La Ley* 13822, 2021.

QUINTERO OLIVARES, G. *La responsabilidad civil «ex delicto»*. Dir. QUINTERO OLIVARES, G. Navarra. Aranzadi. 2002.

REY HUIDROBRO. «La estafa informática: relevancia penal del phising y el pharming», *La Ley Penal*, Nº 101, 2013, Editorial Wolters Kluwer.

ROCA TRÍAS, E. / NAVARRO MICHEL, M. *Derecho de Daños*. Tirant Lo Blanch. 2020.

RODRIGUEZ ALMIRÓN, F. *Aspectos jurídico-dogmáticos y jurisprudenciales en torno a la responsabilidad civil ex delicto*, Madrid, Dykinson, 2022.

RODRÍGUEZ-MAGARIÑOS, J. «Nuevos delitos informáticos: *phising, pharming, hacking y cracking*».

SAN JOSÉ ARÉVALO, X. «De la responsabilidad civil subsidiaria ex delicto de los arts. 120 y 121 del Código Penal». DE LA FUENTE HONDARRUBIA, F. (Dir.), *Estudios sobre la responsabilidad civil ex delicto*, Madrid, Sepín, 2022.

SÁNCHEZ-ESCRIBANO, M. «Tendencias actuales en materia de cibercrimen: la respuesta penal al Phishing, Ransomware y Dos, las tres principales amenazas cibernéticas a plataformas digitales desde la pandemia». *Estudios. Aportaciones jurídicas a la economía de plataformas*. Aranzadi, S.A.U., 2022.

TORRES KEENLYSIDE, A. / CONTRERAS SOLER, B. / GARROS FONT, I. «Análisis criminológico, técnico y legal del phishing», *Revista Aranzadi Doctrinal*, núm. 9, 2021.

VALLS PRIETO, J. «Sobre la responsabilidad penal por la utilización de sistemas inteligentes», *Revista Electrónica de Ciencia Penal y Criminología,* 2022.