Máster en Abogacía y Procura

La responsabilidad bancaria en supuestos de phishing por SMS

Presentado por:

Eduardo Mongil Garzón

Tutelado por:

Marina Echebarría Sáenz

Valladolid, julio de 2024

Índice

1. Introducción y justificación

El uso del teléfono móvil se ha generalizado totalmente en España. Concretamente, el dispositivo está presente en el 99,5% de los hogares españoles con al menos un miembro de 16 a 74 años. A ello se suma que más del 95% de las personas en ese rango de edad ha accedido a Internet en los últimos tres meses[1]. Mediante estas herramientas se llevan a cabo actividades cotidianas como informarse, comprar, o realizar trámites, por lo que surgen ventanas de oportunidad muy grandes para los delincuentes.

Ahora mismo, uno de cada cinco delitos que se denuncian en España son ciberdelitos, y, de ellos, el 90% son estafas informáticas. Según datos oficiales, en 2023 esas estafas informáticas registradas son un 509,1% más en comparación con las registradas en 2016[2]. Un aumento tan espectacular como preocupante. Y muchas de ellas se llevan a cabo a través de la modalidad de smishing (o phishing por SMS).

Asimismo, el Banco de España, asegura que casi una de cada tres reclamaciones que recibe es por operaciones presuntamente fraudulentas realizadas con tarjeta o mediante transferencia, una cifra que también va en aumento, ya que se ha duplicado su volumen con respecto a años pretéritos [3]. Queda claro que estamos ante un problema de plena actualidad y que puede afectar a cualquier persona.

Al tratarse de prácticas en las que es muy difícil determinar la identidad de los autores materiales, gran parte de las víctimas pueden sentir una sensación de indefensión, lo que desincentiva la denuncia e investigación de estos fraudes. En este contexto surge la figura del banco, que debería

[1] Datos del Instituto Nacional de Estadística. Consultado en: https://www.ine.es/prensa/tich_2023.pdf

[2] Balance de criminalidad cuarto trimestre de 2024. Disponible en: https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2024/Balance-de-Criminalidad-Primer-Trimestre-2024.pdf

[3] Memoria de reclamaciones del Banco de España 2022. Disponible en: https://www.bde.es/f/webbe/Secciones/Publicaciones/PublicacionesAnuales/MemoriaServicioReclamaciones/22/MSR2022.pdf

garantizar que el dinero y los datos de sus clientes están en buenas manos, algo que no siempre es así.

El supuesto de hecho de este TFM es una situación totalmente real que viven cada vez más ciudadanos en su día a día. Mediante este trabajo se pretende hacer un acercamiento sobre la responsabilidad que tendría la entidad bancaria en estos casos, y estudiar algunas de las opciones por las que podrían optar los particulares para reclamar la recuperación de su dinero.

2. Descripción del supuesto de hecho

Don Gabriel Alonso Fernández, de 31 años edad y residente en Aranda de Duero (Burgos), es cliente del Banco Cantabria, donde tiene suscrito un contrato de cuenta corriente bancaria desde marzo del año 2012.

El 25 de noviembre de 2023 a las 11:31 horas recibe un SMS en su teléfono móvil personal por parte de un remitente que dice ser el Banco Cantabria. En el mensaje se incluye una advertencia de que tiene que mejorar la seguridad de sus claves electrónicas y se le emplaza a que confirme sus datos a través de un enlace externo que se incluye en el SMS. Al leerlo, don Gabriel pincha en el enlace, que le lleva a una pasarela con la apariencia del sitio web del Banco Cantabria, aunque con algunas diferencias visibles en su diseño. Don Gabriel introduce los datos solicitados, entre ellos sus claves para acceder a su área privada online.

Al acceder al enlace, don Gabriel ignoró también las advertencias de su navegador sobre la posible falta de seguridad del sitio web, procediendo a ingresar sus credenciales sin verificar la autenticidad del sitio.

Además, aunque el Banco Cantabria ofrece la opción de habilitar la autenticación en dos pasos (2FA), don Gabriel decidió no utilizarla meses atrás porque le parecía engorrosa.

Horas después de introducir los datos solicitados, a las 11:31, decide hacer unas comprobaciones en su cuenta bancaria y no observa ningún tipo de movimiento o cargo extraño. Un día después, en la mañana del 26 de

noviembre, recibe una llamada de su entidad bancaria informándole de que tiene movimientos que pudieran ser fraudulentos.

A partir de esta llamada, don Gabriel confirma que tiene en su cuenta varios cargos no autorizados por él con destino Malta. Concretamente, se le han efectuado dos cargos, uno de 950 euros, y otro de 10 euros. Además, puede ver que el propio Banco Cantabria ha rechazado otros 5 movimientos de la misma naturaleza durante esa misma mañana.

Ante esta situación, don Gabriel decide informar a su banco, que le entrega un formulario específico para este tipo de supuestos, y le indica que mande un correo electrónico describiendo el caso concreto a su servicio de reclamaciones junto con el citado formulario, y adjuntando la denuncia de fraude presentada ante la Policía Nacional, si la hubiere.

Don Gabriel decide esa misma tarde acudir a la oficina de denuncias de la Policía Nacional de Aranda de Duero, sita en la calle San Francisco 92 de la ciudad burgalesa. A las 15:34 horas del 26 de noviembre de 2023 queda constancia de la denuncia realizada por don Gabriel por fraude informático a través de SMS (smishing).

Esa misma tarde envía un correo electrónico al servicio de reclamaciones del Banco Cantabria en el que detalla estos hechos a través del formulario requerido y adjunta la denuncia efectuada en comisaría. Le entregan acuse de recibo emplazándole a una respuesta.

Después de dos meses sin obtener contestación, don Gabriel decide enviar otro correo electrónico al servicio de reclamaciones del Banco Cantabria, sin recibir respuesta una vez más. Un mes después volvió a hacerlo con idéntico resultado. Ante esto, decide acudir a una sucursal física, donde vuelve a interponer la reclamación, aunque le indican que seguramente el Banco no se haga responsable de los cargos debido a una negligencia por su parte.

Después de otros cuatro meses más sin noticias del Banco, se presenta en el despacho de un abogado para pedir ayuda sobre el procedimiento a seguir en este momento.

3. Conceptos previos

3.1. ¿Qué es el el 'smishing' (phishing por SMS)?

El concepto principal que hay que acotar en este Trabajo de Fin de Máster es el de smishing o phishing por SMS. La definición base que podemos usar es la aportada por el Instituto Nacional de Ciberseguridad (INCIBE), que dice que el phishing "es una técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico"[4].

El smishing sería lo mismo, pero los archivos infectados se adjuntarían al teléfono móvil y no al correo electrónico. El INCIBE lo define como "una técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima -red social, banco, institución pública, etc. -con el objetivo de robarle información privada o realizarle un cargo económico. Generalmente el mensaje invita a llamar a un número de tarificación especial o acceder a un enlace de una web falsa bajo un pretexto"[5].

Otra definición que se puede aportar del smishing es considerarlo como "la suplantación de la identidad de empresas o terceros de confianza a través del envío de un mensaje de texto (SMS) con objeto de objeto de obtener la información personal (usuario, contraseñas, domicilio, número de teléfono, correo electrónico…) y bancaria de la víctima para el desarrollo de un fraude".[6]

---

[4] INCIBE, disponible en: https://www.incibe.es/aprendeciberseguridad/phishing#:~:text=El%20phishing%20es%20una%20t%C3%A9cnica,econ%C3%B3mico%20o%20infectar%20el%20dispositivo

[5] INCIBE, disponible en: https://www.incibe.es/aprendeciberseguridad/smishing

[6] RIBÓN SEISDEDOS, E. (2024). 'Fraudes bancarios y defensa del afectado. Nuevas tendencias defraudatorias especial referencia al phishing bancario'. Tirant lo Blanch: Ilustre Colegio de Abogados de Madrid. Pág. 44

Este tipo de conductas delictivas las llevan a cabo individuos o bandas con el fin de obtener lucro de la víctima, llegando al punto de solicitar, en nombre del particular, capital de su cuenta corriente bancaria. En estas situaciones, la víctima queda en una situación de desamparo, porque no tiene cómo identificar al autor del fraude, por lo que la opción que se le plantea es reclamar a la entidad bancaria con la que tiene suscrito el contrato[7]. Los bancos son organismos con una acreditada solvencia, por lo que podrían responder perfectamente por las cantidades sustraídas, siempre que estos supuestos entren dentro de sus responsabilidades, algo que analizaremos en este Trabajo Fin de Máster.

3.2. Aproximación al contrato de cuenta corriente bancaria en el medio electrónico

El contrato de cuenta corriente se puede definir como un acuerdo por el cual una entidad bancaria se compromete a recibir depósitos de dinero por parte de un particular, a mantenerlos seguros y a permitir al cliente disponer de ellos en cualquier momento, mediante operaciones como ingresos, reintegros, transferencias y pagos. Este contrato implica también que, en algunos supuestos, el banco podría abonar intereses por ese dinero, y cargar las comisiones y gastos derivados de la gestión de la cuenta.

La cuenta corriente sirve, por tanto, para contabilizar y liquidar las transacciones de un cliente con una entidad de crédito, incluyendo depósitos, pagos y cobros, mediante un sistema de compensación continua. Además, ofrece un servicio de caja, actuando como agente de cobros y pagos y administrando el dinero del cliente [8]. Además, el abrir una cuenta corriente en

[7] CALVO SAN JOSE, M. J. (2023) 'La responsabilidad civil de los bancos en los delitos de estafa por "phishing"'. Actualidad Jurídica Iberoamericana Nº 18, febrero 2023, ISSN: 2386-4567, págs. 1788-1809 (1790-1791)

[8] PABLO-ROMERO GIL-DELGADO, M. C. (2015), 'El contrato de cuenta corriente bancaria'. Operaciones bancarias de activo y pasivo en el contexto de crisis económica: hacia la unificación de la contratación privada / coord. por María Ángeles Egusquiza Balmaseda Árbol

una entidad bancaria es una forma de poder operar económicamente en un día a día en el que cada vez se utiliza menos el dinero físico.

Respecto a la banca electrónica, el alcance del acuerdo es simplemente una ampliación y modificación del concepto del contrato. Se permite al cliente gestionar su cuenta corriente y realizar operaciones bancarias a través de medios electrónicos como aplicaciones móviles y plataformas web conectadas a Internet. Este contrato incluye tanto las obligaciones y derechos tradicionales de la cuenta corriente como las disposiciones específicas para garantizar la seguridad y eficiencia de las operaciones electrónicas.

Esas obligaciones están recogidas en varios preceptos. Es relevante señalar el artículo 68 del Real Decreto-ley 19/2018,[9] que establece la obligación de las entidades de pago de aplicar la autenticación reforzada del cliente "cuando el ordenante: a) acceda a su cuenta de pago en línea; b) inicie una operación de pago electrónico; c) realice por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos".

Para el supuesto de hecho de este Trabajo de Fin de Máster es importante también el artículo 66 del Real Decreto-ley, que indica que "los proveedores de servicios de pago establecerán un marco, de conformidad con lo que disponga el Banco de España, con medidas paliativas y mecanismos de control adecuados para gestionar los riesgos operativos y de seguridad relacionados con los servicios de pago que prestan. Como parte de ese marco, los proveedores de servicios de pago establecerán y mantendrán procedimientos eficaces de gestión de incidentes, en particular para la detección y la clasificación de los incidentes operativos y de seguridad de carácter grave".[10] Del precepto se deduce que la entidad bancaria está obligada a desarrollar sistemas de seguridad para evitar todo tipo de riesgos a sus clientes cuando operen a través de Internet.

---

académico, Rafael Lara González Árbol académico, 2015, ISBN 978-84-9059-935-8, págs. 347-397

[9] Artículo 68 del Real Decreto-ley 19/2018 de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera

[10] Artículo 66 del Real Decreto-ley 19/2018 de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera

Sobre esto merece la pena hacer una pequeña mención al Reglamento general de protección de datos de la UE, que según expone en su introducción "ejerce de marco de protección de los datos de los particulares en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior" [11]. El artículo 32 del Reglamento hace referencia a la obligación que los responsables de custodiar los datos que un particular les ceda tienen de prevenir peligros en la seguridad "el responsable y el encargado del tratamiento -en este caso será el banco- aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo".[12]

Además, las entidades bancarias también tienen establecidas más obligaciones en la Orden EHA/2899/2011, de transparencia y protección del cliente de servicios bancarios. En este texto se consagran compromisos como el de comunicar de manera clara los términos en los que se desarrollan todos los servicios que se ofrecen al particular[13]; la obligación de dar explicaciones adecuadas y suficientes para comprender los términos esenciales de todos esos servicios, así como de informar al cliente de las consecuencias derivadas de solicitarlos, para que pueda tomar la mejor decisión para sus intereses[14], y el deber de diligencia de corregir de forma inmediata los errores detectados por la entidad o por los propios clientes,[15] entre otras cuestiones.

En conclusión, el contrato de cuenta corriente bancaria en el ámbito de la banca electrónica en España incluye no solo los elementos tradicionales del contrato típico, sino también disposiciones específicas para garantizar la

[11] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016

[12] Artículo 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016

[13] Artículo 8 de la Orden EHA/2899/2011, de transparencia y protección del cliente de servicios bancarios

[14] Artículo 9 de la Orden EHA/2899/2011, de transparencia y protección del cliente de servicios bancarios

[15] Artículo 13 de la Orden EHA/2899/2011, de transparencia y protección del cliente de servicios bancarios

seguridad y la protección del cliente en las operaciones electrónicas, motivado por la singularidad de la prestación de servicios a través de Internet.

Conviene señalar, además, que las entidades bancarias están sometidas a un régimen especial de regulación y supervisión mucho más fuerte que el de otras industrias. “Esto se debe a la captación de importantes cantidades de fondos del público, al intermediar entre el ahorro y el crédito, y al efecto positivo que tiene un sistema financiero solvente y bien gestionado sobre la estabilidad financiera y la actividad económica general”.[16]

El artículo 7.6 de la Ley de Autonomía del Banco de España establece que le corresponde al Banco de España esa labor. Esta entidad debe promover el cumplimiento de la normativa específica de las entidades de crédito y velar por el buen funcionamiento de todo el sistema bancario.[17]

3.3. Pequeña delimitación del delito de estafa electrónica

El smishing podría ser una conducta encajable en un tipo delictivo, concretamente en el de la estafa electrónica. El artículo 248 del Código Penal[18] indica que 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.

Por su parte, el Convenio de Budapest, firmado el 21 de noviembre de 2001 por miembros del Consejo de Europa, es la principal herramienta europea para regular los delitos informáticos. La mayoría de los países lo han ratificado, y gracias a este convenio se han definido varios delitos informáticos. España lo ratificó en 2010 [19].

[16] Web oficial del Banco de España. Consultado en: https://www.bde.es/wbe/es/areas-actuacion/supervision-entidades-financieras/funcion-supervisora-banco-espana/modelo-supervision-espana/

[17] Artículo 7.6 de la Ley 13/1994 de Autonomía del Banco de España

[18] Artículo 248 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

[19] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

El artículo 8 habla de fraude informático, y dice que se ajustarán a este supuesto “los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante cualquier introducción, alteración, borrado o supresión de datos informáticos; o cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona”. [20]

El Código Penal español establece una modalidad que se ajusta aún mejor al smishing que el de la estafa tradicional. La Ley Orgánica 14/2022 decidió incluir el delito de estafa informática en el artículo 249[21], ya que antes de esta reforma era el apartado 2 del art. 248 el que regulaba este tipo de conductas. En él se indica que “cometerán estafa 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”.

En estas notas se ven elementos que coinciden con el concepto de smishing. Está incluido el ánimo de lucro, la utilización de un engaño para producir error en otro, y la inducción a la víctima de estas técnicas para realizar un acto en favor de un tercero. También es relevante la falta de consentimiento para que la estafa sea tal. Podríamos hablar, por tanto, de que el smishing es un tipo de estafa electrónica que incluye los elementos del artículo 249 del CP, pero para ello tiene que estar presente siempre, además, un medio electrónico o un sistema informático[22], y este caso se utilizarían los SMS a través del teléfono móvil. “Es un ciberataque que se dirige a las personas a través de SMS (servicio de mensajes cortos) o mensajes de texto”.[23]

[20] Artículo 8 del Convenio sobre Ciberdelincuencia del Consejo de Europa de Budapest 2001

[21] Artículo 249 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

[22] FLORES PRADA, I (2012), ‘Criminalidad informática, aspectos sustantivos y procesales’. Editorial Tirant lo blanch, Valencia, 2012, pág. 202.

[23] Sentencia de la Audiencia Provincial de Lleida, a 19 de abril de 2024 - ROJ: SAP L 349/2024

3.4. La negligencia como elemento fundamental de los casos de smishing

En los supuestos de smishing en los que se reclama la responsabilidad al banco, como el de este TFM, el concepto de negligencia aparece como un factor totalmente clave. Si se demuestra que el cliente ha actuado negligentemente, la entidad bancaria podría no tener que verse a obligada a responder de nada, aunque se le reclamasen las cantidades.

Conviene, en primer lugar, acotar el concepto de negligencia. Según la doctrina, la negligencia se puede definir como la falta de cuidado, el descuido intencional y, en general, la actuación sin el nivel adecuado de precaución. Esta puede derivar en delitos o infracciones que se regirán por las normas del Código Penal, o en actos u omisiones que, aunque no constituyen infracción, representan un acto ilícito y generan responsabilidad contractual o extracontractual[24]. Según Goldsteind, la negligencia se caracteriza porque el autor, a raíz de su falta de cuidado, no ha previsto, debiendo hacerlo[25].

La negligencia también se puede definir como la infracción de los deberes de precaución o de cuidado o como un incremento irrazonable del riesgo[26]. Serán la ley, los reglamentos o los tribunales quienes aclaran cuáles son los niveles exigidos para que el perjudicado pueda reclamarlos y tenga derecho a la compensación de los daños que haya sufrido.

La anterior referencia al debido nivel de cuidado se podría equiparar a la diligencia debida. El artículo 1104 del Código Civil hace una aproximación. “La culpa o negligencia del deudor consiste en la omisión de aquella diligencia que

[24] https://guiasjuridicas.laley.es/

[25] HERNÁNDEZ, P. P. (2018). Responsabilidad civil: (ed.). Santiago de los Caballeros, Universidad Abierta para Adultos (UAPA), pág. 186. Recuperado de https://elibro-net.ponton.uva.es/es/lc/uva/titulos/175610

[26] SALVADOR CODERCH, P. (Ed.), GÓMEZ LIGÜERRE, C., RAMOS GONZÁLEZ, S., RUBÍ PUIG, A., LUNA YERGA, Á. (2022) ‘Derecho de daños (DdD). Análisis, aplicación e instrumentos comparados’, 11ª edición, 2022, InDret, pág. 74

exija la naturaleza de la obligación y corresponda a las circunstancias de las personas, del tiempo y del lugar".[27]

También toca hablar, además, de la culpa. Históricamente, se ha equiparado la culpa lata al dolo. El origen de ello está en el Derecho Romano, y la definición más relevante se ha atribuido a Ulpiano, aunque donde de manera más clara se ve la equiparación es en el Derecho justinianeo, que también usa la palabra negligencia: "magna negligencia culpa est, magna culpa dolus est".[28]

Los autores contribuirán a explicar esta conexión, porque definen la culpa lata como "una desviación del grado mínimo de diligencia exigible". Y la razón de la equiparación "puede hallarse en la significación desfavorable que, al igual que el dolo, merece para el Derecho la máxima negligencia que esta culpa comporta; lo que hace que funcione como mínimo de responsabilidad. Como consecuencia se responde al menos por ella en todos los contratos, sin perjuicio de que, en algunos, por la utilidad que de ellos obtiene el deudor, le sea exigible un mayor grado de diligencia."[29] Por tanto, de la definición doctrinal se deduce que de la culpa se deriva responsabilidad en todos los contratos.

El Tribunal Supremo equipara el concepto de negligencia al de culpa, y asegura que esta "se apoya invariablemente como elemento indispensable en la omisión de la diligencia exigible al agente. La posición moderna, en cambio, caracteriza la culpa por notas distintas de esa falta de diligencia y llega a hablar de una culpa social o culpa sin culpabilidad. El sentido clásico de la culpa civil parte de identificarla con negligencia, concepto que se opone al de diligencia; basado todo ello en un criterio subjetivo. La culpa es desviación de un modelo ideal de conducta: modelo representado, unas veces por la "fides" o "bona fides", y otra por la "diligentia" de un "pater familias" cuidadoso".[30]

---

[27] Artículo 1104 del Código Civil

[28] MORALES MORENO, A. M. (1982), 'El dolo como criterio de imputación de responsabilidad al vendedor por los defectos de la cosa'. Anuario de derecho civil, ISSN 0210-301X, Vol. 35, Nº 3, 1982, págs. 591-684, pág. 604

[29] MORALES MORENO, A. M. (1982), 'El dolo como criterio de imputación de responsabilidad al vendedor por los defectos de la cosa'. Anuario de derecho civil, ISSN 0210-301X, Vol. 35, Nº 3, 1982, págs. 591-684, pág. 607.

[30] Sentencia del Tribunal Supremo, a 10 de julio de 2003 - ROJ: STS 4880/2003

En el Código Civil podemos ver que una actuación negligente lleva aparejada el nacimiento de responsabilidad, como se puede ver en el artículo 1101. “Quedan sujetos a la indemnización de los daños y perjuicios causados los que en el cumplimiento de sus obligaciones incurrieren en dolo, negligencia o morosidad, y los que de cualquier modo contravinieren al tenor de aquéllas”. [31] El artículo 1103 asegura que esa responsabilidad procedente de la negligencia se podrá moderar por los tribunales según los casos.[32]

La responsabilidad civil se puede definir como un deber de indemnizar en el que concurren un derecho de crédito, del que es titular o acreedor el perjudicado, y un deber de prestación, del que es deudor el responsable. Puede ser que este sea el mismo autor del daño, y exista responsabilidad por hechos propios y cabe que la responsabilidad recaiga sobre una persona distinta y exista “responsabilidad por hechos ajenos”.[33]

Es fundamental señalar que en supuestos como el que analizamos en este Trabajo Fin de Máster, en el que el conflicto se da entre un particular y un banco, se invierte la carga de la prueba, por lo que al contrario de lo establecido en el artículo 217 de la LEC[34], le correspondería al demandado -en este caso el banco- demostrar que el demandante no ha incurrido en negligencia. Esto lo establece el artículo 44.3 del RD-Ley del Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que dice lo siguiente: “corresponderá al proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación

[31] Artículo 1101 del Código Civil

[32] Artículo 1103 del Código Civil

[33] GONZÁLEZ HERNÁNDEZ, R. (2013). Responsabilidad extracontractual y contractual: barrera entre ambas. Anuario Jurídico Y Económico Escurialense, (46), págs. 203–214, pág 205. Recuperado a partir de https://publicaciones.rcumariacristina.net/AJEE/article/view/152

[34] El artículo 217.2 de la LEC establece que “corresponde al actor y al demandado reconviniente la carga de probar la certeza de los hechos de los que ordinariamente se desprenda, según las normas jurídicas a ellos aplicables, el efecto jurídico correspondiente a las pretensiones de la demanda y de la reconvención”:

de pagos, probar que el usuario del servicio de pago cometió fraude o negligencia grave".[35]

4. Cuestiones planteadas. Análisis y fundamentación jurídica

4.1 ¿El Banco Cantabria es responsable en supuestos de smishing (phishing por SMS) como el sufrido por don Gabriel?

Como hemos mencionado, la norma principal a la que habría que acudir es el Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que adapta la normativa española a la Directiva PSD2 que refuerza las medidas de seguridad y autenticación y derogó la Ley 16/2009, de 13 de noviembre, de servicios de pago. Autores como Heras Hernández o Martínez de Salazar Bascuñana, referenciados por Ribón, indican que "la mayor diligencia exigida a las entidades de crédito, puesta en relación con las exigencias de buena fe, acorde con la naturaleza de las relaciones contractuales bancarias, dan como resultado una especial responsabilidad, muy cercana a la responsabilidad por riesgo del profesional, por los hechos que las entidades de crédito realicen dentro del ámbito de su actividad y que únicamente cesará en los supuestos de negligencia probada del cliente".[36]

El Banco de España, en su Memoria de Reclamaciones de 2018, apuntó que "corresponde a la entidad demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico o por cualquier otra anomalía. No obstante, el registro por parte del proveedor de servicios de pago de la utilización del instrumento de pago no bastará necesariamente para demostrar que la operación fue autorizada por el ordenante ni que este actuó de manera fraudulenta o

[35] Artículo 44.3 del RD-Ley del Real Decreto-Ley 19/2018, de servicios de pago y otras medidas urgentes en materia financiera

[36] Heras Hernández y Martínez de Salazar Bascuñana en RIBÓN SEISDEDOS, E. (2024). 'Fraudes bancarios y defensa del afectado. Nuevas tendencias defraudatorias especial referencia al phishing bancario'. Tirant lo Blanch: Ilustre Colegio de Abogados de Madrid. Págs. 61-62

incumpliendo deliberadamente o por negligencia grave una o varias de las obligaciones que le incumben como usuario del servicio de pago, a saber i) utilizar el instrumento de pago de conformidad con las condiciones que regulen su emisión y utilización; ii) tomar todas las medidas razonables a fin de proteger los elementos de seguridad personalizados de los que vaya provisto, y iii) en caso de extravío, sustracción o utilización no autorizada del instrumento de pago, notificarlo sin demoras indebidas a la entidad, en cuanto tenga conocimiento de ello, debiendo la entidad adoptar las medidas necesarias para evitar, desde que se produce dicha comunicación, la utilización ilegítima del instrumento de pago por terceros no autorizados, debiendo contar esta con medios adecuados y gratuitos a fin de posibilitar, en todo momento, que el titular efectúe la comunicación de la operación de pago cuya autoría no reconoce".[37]

Los tribunales también se han pronunciado debidamente sobre esta cuestión, y establecen una responsabilidad cuasi objetiva a la entidad bancaria. Esta se puede definir como la "imputación de los daños al causante de los mismos, con abstracción de si ha incurrido o no en culpa, quedando exonerado únicamente en los casos de fuerza mayor o culpa exclusiva del perjudicado"[38]. Esto está conectado al artículo el artículo 147 del Texto Refundido de la Ley para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, que dispone: "Los prestadores de servicios serán responsables de los y perjuicios causados a los consumidores o usuarios, salvo que prueben que han cumplido las exigencias y requisitos reglamentariamente establecidos y demás cuidados y diligencias que exige la naturaleza del servicio".[39]

La jurisprudencia ha mencionado la responsabilidad cuasi objetiva en varias ocasiones. La SAP de Alicante de 12 de marzo de 2018 afirma que

[37] Memoria de Reclamaciones del Banco de España 2018, págs. 364-365

[38] Extraído de https://dpej.rae.es/lema/responsabilidad-cuasi-objetiva#:~:text=Civ.,CC%2C%20arts.

[39] Artículo 147 del del Texto Refundido de la Ley para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre

“conforme a la doctrina jurisprudencial en materia de phishing la responsabilidad de la titular de la banca online es de naturaleza cuasi objetiva, derivada de la exigencia a la entidad titular del servicio online de adoptar medidas de seguridad necesarias y renovables ante los distintos modos de fraude informático, en modo tal que salvo que se acredite la negligencia grave por parte del usuario de la banca electrónica, la entidad financiera debe responder del reintegro de los importes obtenidos de forma fraudulenta”.[40]

La Audiencia Provincial de Salamanca, en una sentencia reciente, hace referencia a la SAP de Alicante y establece que “se ha de partir de la consideración de que, con arreglo al marco jurídico en el que se desenvuelve la actividad de servicios de pago a través de banca online, el régimen de la responsabilidad de la prestadora del servicio ha de reputarse cuasi objetiva, en la medida en que sólo se excluye en unos casos por culpa grave del cliente y en otros por únicamente por fraude imputable al mismo”.[41]

También es relevante ver lo que ha indicado acerca de la responsabilidad bancaria en los supuestos de phishing la Sala de lo Penal del Tribunal Supremo[42], que considera que "no debe desplazarse indebidamente sobre los perjudicados la responsabilidad de comportamientos en los que la intención de engañar es manifiesta, y el autor ha conseguido su objetivo, lucrándose en perjuicio de su víctima", algo que parece evidente que ha sucedido en el supuesto de hecho de este TFM, ya que el cargo económico ha acabado en un tercero no identificado.

Además, la Audiencia Provincial de Lleida hace referencia a la Sentencia nº 88/2023 dictada por el Juzgado de 1ª Instancia nº 7 de Cerdanyola del Vallés, que afirma que “siendo Internet una red pública de comunicaciones, la seguridad de las operaciones bancarias precisa de soluciones tecnologías avanzadas a los efectos de garantizar tanto la autenticidad como la integridad y

[40] Sentencia de la Audiencia Provincia de Alicante, a 12 de marzo de 2018 - ROJ: SAP A 632/2018

[41] Sentencia de la Audiencia Provincial de Salamanca, a 18 de abril de 2024 - ROJ: SAP SA 255/2024

[42] Sentencia del Tribunal Supremo, a 17 de febrero de 2020 - ROJ: STS 2017/2020

la confidencialidad de los datos… Consecuencia derivada de la omisión, insuficiencia o defectuoso funcionamiento de las adoptadas es que han de ser las entidades bancarias las que asuman las consecuencias derivadas de los fallos de seguridad del sistema".[43]

En la misma sentencia de la Audiencia Provincial ilerdense se hace alusión al aumento de estafas como el smishing, "cuyas cifras de criminalidad rebasan las de otros sectores, de actividades peligrosas, y siendo la finalidad de la DSP2, que los usuarios gocen de la debida protección frente a los riesgos inherentes a los medios de pago digitales, la doctrina jurisprudencial establece que quien tiene las ventajas de un negocio por el que obtiene un lucro, debe soportar los inconvenientes de ese negocio como contraprestación por el lucro obtenido"[44]. Esta postura daría a entender que el Banco Cantabria, al ser una empresa que se beneficia del contrato suscrito con el cliente debería también correr con los riesgos asociados del negocio en sí.

Más contundente aún se muestra la Audiencia Provincial de La Coruña[45], que establece que existe una presunción de culpa o responsabilidad cuasi objetiva de la entidad bancaria que "tan solo se destruye cuando se demuestra que hubo una actitud dolosa o imprudente grave por parte del cliente, pues caso contrario la culpa recaería inexcusablemente sobre el Banco y de forma única".

Volviendo al Real Decreto-ley 19/2018, el artículo 36.1 del mismo establece que "Las operaciones de pago se considerarán autorizadas cuando el ordenante haya dado el consentimiento para su ejecución. A falta de tal consentimiento la operación de pago se considerará no autorizada. El consentimiento para la ejecución de una operación de pago podrá darse también por conducto del beneficiario o del proveedor de servicios de iniciación

[43] Sentencia de la Audiencia Provincial de Lleida, a 19 de abril de 2024 - ROJ: SAP L 349/2024, que hace referencia a la Sentencia 88/2023, de 7 de junio de 2023, dictada por el Juzgado de 1ª Instancia nº 7 de Cerdanyola del Vallés

[44] Sentencia de la Audiencia Provincial de Lleida, a 19 de abril de 2024 - ROJ: SAP L 349/2024

[45] Sentencia de la Audiencia Provincial de A Coruña, a 09 de enero de 2024 - ROJ: SAP C 12/2024

de pagos”[46]. Por tanto, habrá que aclarar el concepto de consentimiento para determinar si ha existido o no la autorización a la que se hace referencia.

El artículo 45.1 de ese texto legal indica qué ocurre cuando no media consentimiento: “en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago -el banco- del ordenante devolverá a éste el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación”.[47]

En el supuesto de hecho analizado en este trabajo, don Gabriel informó a su banco el mismo día que se efectuaron los cargos que se considerarían fraudulentos, además de acudir a comisaria para interponer una denuncia. Por lo que hay pruebas documentales que apoyan la actuación del ordenante en este sentido.

El artículo 1265 del Código Civil indica que “será nulo el consentimiento prestado por error, violencia, intimidación o dolo”[48]. El Tribunal Supremo indica que “hay error vicio cuando la voluntad del contratante se forma a partir de una creencia inexacta… Es decir, cuando la representación mental que sirve de presupuesto para la realización del contrato es equivocada o errónea”.[49]

Se podría determinar que la creencia inexacta existiría en el momento en el que don Gabriel pensó que quien le mandaba el SMS era el Banco Cantabria, por lo que se deduce que sin ese error o engaño jamás habría introducido sus datos en el enlace fraudulento. Por lo tanto, según lo apuntado previamente, nos inclinamos a pensar que el Banco Cantabria sería responsable de restituir las cantidades, siempre y cuando se considerase que detrás de las operaciones no ha existido el consentimiento de don Gabriel.

[46] Artículo 36.1 del Real Decreto-ley 19/2018 de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera

[47] Artículo 45.1 del Real Decreto-Ley 19/2018 de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera

[48] Artículo 1265 del Código Civil

[49] Sentencia del Tribunal Supremo, a 21 de noviembre de 2012 - ROJ: STS 7843/2012

Para acabar de concretarlo, habría que atender a lo dispuesto en el artículo 46.1.b. del Real Decreto-Ley 19/2018, que indica que don Gabriel estaría exento de toda responsabilidad si no se ha producido fraude o negligencia grave, algo que vamos a analizar en el siguiente subapartado, y que ya apunta la jurisprudencia: “Este sistema de responsabilidad civil solo cesa cuando, conforme a lo establecido en el artículo 46, el cliente ha actuado fraudulentamente o con negligencia grave a la hora de aplicar los medios razonables de protección de seguridad personalizados de que haya sido provisto, o en el caso de que no haya comunicado a la entidad el pago no autorizado, en cuanto tenga conocimiento del mismo”.[50]

4.2. ¿Ha actuado don Gabriel negligentemente?

El artículo 44 del Real Decreto-ley 19/2018 establece la inversión de la carga de la prueba, por lo que le correspondería al Banco Cantabria demostrar que don Gabriel no ha actuado negligentemente. [51]

En este supuesto de hecho, la negligencia podría darse en varias actuaciones de la víctima. Es posible que don Gabriel no hubiese actuado con la diligencia que se menciona en el artículo 1104 del Código Civil al no percatarse de las diferencias que se veían en la web fraudulenta en comparación con la real del Banco Cantabria. Además, al acceder a este sitio web, don Gabriel ignoró las advertencias de su navegador sobre la posible falta de seguridad de la página, procediendo a ingresar sus credenciales sin verificar correctamente su autenticidad.

Hay que tener en cuenta que el Banco de España establece algunas recomendaciones a los particulares con el ánimo de evitar ser víctimas de este tipo de estafas. Según indican, “los usuarios de servicios de pago que deben extremar las precauciones a la hora de dar credibilidad a comunicaciones de ese tipo que pudieran recibir en sus dispositivos —teléfono fijo, móvil,

[50] Sentencia de la Audiencia Provincial de Badajoz, a 06 de marzo de 2024 - ROJ: SAP BA 332/2024

[51] Artículo 44 del Real Decreto-ley 19/2018 de servicios de pago y otras medidas urgentes en materia financiera

ordenadores—, siendo recomendable consultar con sus entidades financieras, o con las presuntas empresas o entidades remitentes, la veracidad de estas (sin utilizar para ello los enlaces incluidos en los mensajes), pues no suelen pedir datos bancarios ni personales por ninguna de esas vías".[52]

Aun así, en supuestos similares al de este TFM, los tribunales se han inclinado hacia proteger los derechos de los particulares, en especial recientemente. La Audiencia Provincial de Oviedo admitía que una lectura detenida y pausada de un SMS podría servir para darse cuenta del intento de fraude, "pero el nerviosismo cuando y precipitación que produce en cualquier persona esta clase de alerta" puede inducir a no actuar de una manera diligente. En este caso era crucial que se introdujeran las claves para activar la estafa que don Gabriel pretendía evitar. Las advertencias como la del propio navegador podrían resultar inocuas cuando un particular actúa fundado en la creencia "de que estaba interactuando con el propio Banco y no con un tercero. En estas circunstancias difícilmente podrá atribuirse la calificación de negligencia grave" [53].

La Audiencia Provincial de Pontevedra se pronunció en un mismo sentido en un caso similar. Este tribunal indicó que "partiendo de que la autorización propiciada por el cliente se funda en comportamiento fraudulento de tercero -extremo admitido por la demandada-, deberá entenderse que la negligencia plasmada en la cesión de datos personales producida se debió al complejo engaño recibido, y no a la iniciativa o acción directa personal del usuario, que, en definitiva, cumple con las obligaciones señaladas en el artículo 41 de la LSP - Real Decreto-ley 19/2018-, excluyéndose razonablemente la gravedad en el reproche por falta de custodia de claves y, con ello, la responsabilidad con arreglo a art. 46.1 de la Ley y art. 1104 CC, persistiendo el

[52] Memoria de Reclamaciones del Banco de España 2022, pág. 225

[53] Sentencia de la Audiencia Provincial de Asturias, a 03 de abril de 2024 - ROJ: SAP O 1253/2024

incumplimiento por la prestadora del servicio del deber esencial de facilitar un sistema de banca telemática seguro".[54]

En el supuesto de hecho de este TFM se puede dilucidar que el Banco Cantabria asume efectivamente el carácter fraudulento del tercero si se atiende a que rechazó varios pagos sospechosos después de autorizar los dos que sí se cargaron a la víctima, por lo que tampoco cabría entender que hay negligencia grave de don Gabriel si nos apoyamos en esta valoración.

La Audiencia Provincial de Madrid en su Sentencia 184/2022 indicaba que "no cabe apreciar en el demandante un comportamiento negligente de la gravedad y entidad para con base en el mismo hacerle responsable, ni siquiera de la primera disposición de efectivo realizada con la tarjeta usada de manera fraudulenta por un tercero. Como se indica en la Directiva 2015/2036 la negligencia que le hace responder al cliente es la que se deriva de una conducta caracterizada por un grado significativo de falta de diligencia, lo que supone que la misma surge o se produce por iniciativa del usuario, no como consecuencia del engaño al que ha sido inducido por un delincuente profesional [55]. En este caso, resulta evidente que don Gabriel actúo fruto del engaño que derivado del SMS recibido.

Precisamente a esa Sentencia de la Audiencia Provincial de Madrid hace referencia el Juzgado de Primera Instancia de Ferrol, que asegura que “no puede tacharse de gravemente negligente la conducta de quien, tras recibir en el mismo canal en el que recibe habitualmente las comunicaciones procedentes de su banco un mensaje de texto en el que se le informa de la aceptación de una operación por un importe de tres cifras facilitándole un enlace para poder cancelarla, decide pulsar en ese enlace e introducir su usuario y contraseña, dado que, para una persona no experta, no es fácil detectar que el mensaje

[54] Sentencia de la Audiencia Provincial de Pontevedra, a 01 de diciembre de 2022 - ROJ: SAP PO 2845/2022

[55] Sentencia de la Audiencia Provincial de Madrid, a 20 de mayo de 2022 - ROJ: SAP M 7327/2022

recibido es fraudulento o que la web a la que ha accedido a través del enlace facilitado es falsa” [56].

El caso que analiza el juzgado gallego es análogo al del supuesto de hecho de este Trabajo de Fin de Máster, ya que, si bien no se le pedía su contraseña para cancelar ninguna operación concreto, sí que se le requería confirmar las claves para mejorar su seguridad.

Hay algunas sentencias más antiguas de la Audiencia Provincial de Sevilla[57] o la de la Audiencia Provincial de Valencia[58] que deciden desestimar las demandas contra las entidades bancarias por entender que los clientes sí actuaron con negligencia grave. En el primer caso se estableció que existió dicha negligencia debido a que el banco ya avisaba en su página que nunca pediría claves dos veces, ni por correo ni por la web. Además, se añadió que la cliente llevaba muchos años operando con dicho banco, por lo que esa advertencia bastó para entender la desestimación.

Por su parte, la Audiencia valenciana vio negligencia grave en un supuesto similar, porque la web del banco también aconsejaba que no se facilitasen contraseñas mediante e-mails o llamadas, ya que la entidad nunca lo pediría a través de estos medios.

No obstante, estas son sentencias que la posterior jurisprudencia ha ido dejando atrás, y que se dictaron antes de que entrase en vigor la Directiva 2015/2366, que en su preámbulo aclaraba que existe “la obligación de preservar la seguridad de las credenciales personalizadas es de extrema importancia para proteger los fondos del usuario de servicios de pago y limitar los riesgos de fraude y el acceso no autorizado a la cuenta de pago”.[59]

---

[56] Sentencia del Juzgado Primera Instancia de Ferrol, a 03 de julio de 2023 - ROJ: SJPI 1022/2023

[57] Sentencia de la Audiencia Provincial de Sevilla, a 26 de mayo de 2014 - ROJ: SAP SE 1891/2014

[58] Sentencia de la Audiencia Provincial de Valencia, a 31 de enero de 2013 - ROJ: SAP V 457/2013

[59] Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior

4.3. ¿Ha actuado el Banco correctamente para proteger a su cliente?

Teniendo en cuenta que es probable que no exista negligencia grave por parte de don Gabriel, cabe analizar ahora si el Banco Cantabria ha actuado correctamente en este supuesto de hecho. Y encontramos varios puntos en los que no lo ha hecho.

El primero de ellos tiene que ver con la autenticación reforzada (2FA). Ya hemos indicado que el artículo 68 del Real Decreto-ley 19/2018 establece la obligación de que se incluya para pagos electrónicos, pero ese mismo precepto permite una serie de exenciones que los bancos pueden hacer en algunos casos: “no obstante, no será preciso aplicar la autenticación reforzada de clientes a la que se refiere el apartado 1 a los supuestos indicados en el artículo 98.1.b) de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015”, indica el citado artículo 68.

Concretamente, es el Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017 que complementa la Directiva (UE) 2015/2366 del Parlamento Europeo[60] y define exactamente las exenciones. En dicha norma se observan supuestos libres de la autenticación reforzada como son pagos sin contacto en punto de venta por debajo de 50 euros, pagos a beneficiarios de confianza, operaciones frecuentes, u otras en las que el importe de la operación remota de pago electrónico no exceda de 30 euros.

El artículo 16.c del Reglamento también establece la posibilidad de exención siempre y cuando “el número de las operaciones remotas de pago electrónico previas iniciadas por el ordenante desde la última aplicación de la autenticación reforzada de clientes no exceda de cinco operaciones remotas de pago electrónico individuales consecutivas”. [61]

[60] Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017 que complementa la Directiva (UE) 2015/2366 del Parlamento Europeo

[61] Artículo 16.c del Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017 que complementa la Directiva (UE) 2015/2366 del Parlamento Europeo

En el supuesto de hecho de este TFM se observa que el Banco Cantabria efectivamente frenó varias operaciones, pero no dos de ellas. También se señala que don Gabriel decidió prescindir de la autenticación 2FA con el consentimiento de la entidad bancaria, pero esta opción no queda al arbitrio del cliente en todos los casos, sino que únicamente podría alcanzar las exenciones del Reglamento 2018/389. El cargo de 950 euros autorizado no entra jamás en ninguno de los supuestos que podrían estar exentos de la autorización reforzada, y el de 10 euros tampoco. El Banco Cantabria no habría actuado correctamente al permitirlos, aunque posteriormente cancelase los otros pagos que se intentaron hacer.

Por otro lado, el artículo 45 del RD-ley 19/2018 habla de la responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas. En el precepto se especifica lo siguiente: “Sin perjuicio del artículo 43 de este real decreto-ley, en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devolverá a éste el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación, salvo cuando el proveedor de servicios de pago del ordenante tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España, en la forma y con el contenido y plazos que éste determine. En su caso, el proveedor de servicios de pago del ordenante restituirá la cuenta de pago en la cual se haya efectuado el adeudo al estado en el que se habría encontrado de no haberse efectuado la operación no autorizada”.[62]

Consideramos que el Banco Cantabria no tendría la obligación de restituir cantidad alguna al cliente hasta que no se demostrase fehacientemente que la operación no estaba autorizada por el mismo, porque podría tener motivos para sospechar la existencia de una estafa. Ahora bien, en el supuesto de hecho no se indica en ningún momento que el Banco Cantabria haya

[62] Artículo 45 del Real Decreto-ley 19/2018 de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera

informado al Banco de España de absolutamente nada, por lo que aquí ha incumplido la obligación mínima de notificación del artículo 45.

La jurisprudencia también sirve para apoyar que la actuación del Banco ha sido claramente incorrecta, por no haber actuado con diligencia en la protección de la seguridad de su cliente.

El Tribunal Supremo estableció en 2016 que "con carácter general debe señalarse que, conforme a la naturaleza y función del contrato de cuenta corriente bancaria, el cercioramiento o comprobación de la veracidad de la firma del ordenante constituye un presupuesto de la diligencia profesional exigible a la entidad bancaria con relación a sus obligaciones esenciales de gestión y custodia de los fondos depositados por el titular de la cuenta, cuyo incumplimiento da lugar a la indemnización de daños y perjuicios, conforme a lo dispuesto en los artículos 1101 y 1106 del Código Civil".[63] En este supuesto de hecho la entidad bancaria no fue capaz de comprobar que el titular de la cuenta, don Gabriel, no era quien efectuaba los pagos, algo que podía inferirse de la naturaleza de los mismos y el destino de ellos, ya que Malta es un país donde se ha demostrado que existen operadores de phishing.[64] [65]

Por su parte, la Sentencia de la Audiencia Provincial de Navarra 203/2023, en un supuesto parecido al de este TFM, condenaba a una entidad bancaria por dos operaciones no autorizadas y que fueron realizadas porque el propio cliente recibió un SMS informándole de que debía actualizar los datos de su tarjeta bancaria y, al acceder al enlace que le remitía a la propia aplicación de la entidad, se realizaron dos cargos económicos en su tarjeta. La sentencia indica que en estos supuestos “compete a la entidad bancaria que pone a disposición de su cliente instrumentos de pago y contratación electrónica el adoptar las medidas de seguridad necesarias para garantizar la plena autenticación de la operación, que ha de incluir la efectiva identidad del

[63] Sentencia del Tribunal Supremo, a 12 de mayo de 2016 - ROJ: STS 2124/2016

[64] Extraído de: https://www.interior.gob.es/opencms/ca/detalle/articulo/La-Guardia-Civil-detiene-a-un-centenar-de-personas-por-estafar-mas-de-un-millon-de-euros-mediante-los-SMS-fraudulentos/

[65] Sentencia de la Audiencia Provincial de Madrid, a 15 de marzo de 2024 - ROJ: SAP M 4197/2024

ordenante, debiendo asegurar y garantizar que la autorización de la operación provenía efectivamente del cliente titular de la tarjeta, lo que no demuestra haber supervisado ni verificado debidamente en este caso". [66]

Al ser un caso similar al analizado en este trabajo podemos determinar que se debe aplicar la misma doctrina y afirmar que el Banco Cantabria no ha efectuado la labor de verificación de forma correcta.

4.4. ¿Cuáles son los pasos a seguir más recomendables para reclamar el dinero al Banco Cantabria?

El artículo 43.1 RD-Ley 19/2018 establece la obligación al cliente de informar de las operaciones incorrectas sin dilaciones indebidas y en cuanto tenga conocimiento de que se han producido. En este supuesto de hecho, don Gabriel ha comunicado al Banco Cantabria los cargos fraudulentos el mismo día, por lo que ha actuado debidamente en ese sentido. Además, ha denunciado los hechos ante la Policía Nacional, y posteriormente ha registrado una reclamación ante el servicio de reclamaciones de la entidad bancaria. Y, en varias ocasiones, sin obtener respuesta.

Ese hecho es presupuesto esencial para poder efectuar una reclamación ante el Banco de España. Como hemos señalado anteriormente, este organismo tiene encomendadas las labores de supervisión de la actividad en las entidades bancarias en nuestro país.[67]

La entidad bancaria tiene 15 días hábiles para responder desde que se presentó la reclamación, pero como no ha obtenido esa respuesta por parte de su banco, don Gabriel puede acudir al Departamento de Conducta de Mercado y Reclamaciones del Banco de España, ya que no se ha cumplido aún el plazo máximo de 1 año para acudir a este organismo. [68]

---

[66] Sentencia de la Audiencia Provincial de Navarra, a 09 de marzo de 2023 - ROJ: SAP NA 493/2023

[67] Portal web del Banco de España

[68] Consultado en: https://www.bde.es/wbe/es/para-ciudadano/gestiones/reclamaciones/

La reclamación al Banco de España es recomendable para el cliente porque es un proceso gratuito, sencillo y que se resuelve de forma ágil, ya que esta entidad tiene 90 días de plazo para emitir un dictamen motivado. Existe el problema de que sus informes no son vinculantes, pero eso no significa que no sirvan para nada. Según los datos de la Memoria de Reclamaciones del Banco de España de 2022, en ese año, en las reclamaciones por fraude -las más habituales-, el 43,8% de ellas se han resuelto con allanamiento o desistimiento, siendo el porcentaje de satisfacción global del cliente del 84,4%. [69]

Por tanto, es muy aconsejable llevar a cabo este paso antes de interponer una demanda judicial, porque, como acabamos de ver, en muchos casos los bancos asumen los dictámenes del Banco de España, aunque no tengan la obligación de hacerlo.

Además, si la entidad bancaria no se allanase, los tribunales suelen tener en cuenta[70] el informe del Banco de España a la hora de deliberar, y el demandante, que en este caso sería don Gabriel, podría aportarlo como prueba al proceso.[71]

Si al final el Banco de España no diera la razón a don Gabriel, o dándosela, el Banco Cantabria continuase sin allanarse, el paso a seguir sería demandar a la entidad bancaria, ya que habría muy buenas perspectivas para que las pretensiones del cliente prosperasen a tenor de lo analizado.

El Juzgado de Primera Instancia de Aranda de Duero sería competente si se atiende al artículo 51.1 de la LEC. Ese precepto establece que “salvo que la Ley disponga otra cosa, las personas jurídicas serán demandadas en el lugar de su domicilio. También podrán ser demandadas en el lugar donde la situación o relación jurídica a que se refiera el litigio haya nacido o deba surtir efectos, siempre que en dicho lugar tengan establecimiento abierto al público o

---

[69] Memoria de Reclamaciones del Banco de España 2022. Disponible en: https://www.bde.es/f/webbe/Secciones/Publicaciones/PublicacionesAnuales/MemoriaServicioReclamaciones/22/MSR2022.pdf

[70] Extraído de:

https://clientebancario.bde.es/pcb/es/blog/Sirve_para_alg_3a2a736dffadb61.html

[71] Artículo 381 de la Ley de Enjuiciamiento Civil

representante autorizado para actuar en nombre de la entidad". Como la entidad bancaria tiene sucursal en Aranda de Duero, se podría demandar ante el Juzgado de Primera Instancia de esta ciudad, que sería la opción más cómoda para don Gabriel debido a que es vecino del municipio burgalés.

El artículo 10 de la LEC concreta la legitimación activa y pasiva de don Gabriel y el Banco Cantabria ya que indica que "serán considerados partes legítimas quienes comparezcan y actúen en juicio como titulares de la relación jurídica u objeto litigioso".[72]

Según el artículo 250.2 y siguientes de la LEC, este conflicto se decidiría a través del juicio verbal, más rápido y sencillo que el juicio ordinario, ya que la cuantía del procedimiento no excede de 15.000 euros: "Se decidirán también en el juicio verbal las demandas cuya cuantía no exceda de quince mil euros y no se refieran a ninguna de las materias previstas en el apartado 1 del artículo anterior".[73]

Como otra opción antes de iniciar un procedimiento contencioso también se podría utilizar la herramienta de la conciliación, que "es tramitada por lo común, con aceptable agilidad".[74] El artículo 139 de la Ley de Jurisdicción Voluntaria indica que se podrá intentar la conciliación para alcanzar un acuerdo con el fin de evitar un pleito.[75] Lo convenido tendrá el valor y eficacia de un convenio consignado en documento público y solemne.[76]. No obstante, en un supuesto como este, en el que el Banco Cantabria no quiere reconocer ningún tipo de responsabilidad, resulta complicado pensar que la entidad aceptase acudir al acto de conciliación.

[72] Artículo 10 de la Ley de Enjuiciamiento Civil

[73] Artículo 250.2 de la Ley de Enjuiciamiento Civil

[74] RIBÓN SEISDEDOS, E. (2024). 'Fraudes bancarios y defensa del afectado. Nuevas tendencias defraudatorias especial referencia al phishing bancario'. Tirant lo Blanch: Ilustre Colegio de Abogados de Madrid. Pág. 202

[75] Artículo 139 de la Ley de Jurisdicción Voluntaria

[76] Artículo 147 de la Ley de Jurisdicción Voluntaria

5. CONCLUSIONES

PRIMERA: Del análisis se extrae que la postura de los tribunales es la de proteger de manera general los derechos de los particulares que son víctimas de smishing. El artículo del Real Decreto-Ley 19/2018 ya establece un elemento importante al invertir la carga de la prueba y obligar al banco a demostrar que el particular ha cometido una negligencia para liberarle de responsabilidad. Y la jurisprudencia se muestra partidaria de ponerse del lado de los clientes.

Es muy complicado encontrar nuevas sentencias que tomen por buena la versión de las entidades bancarias, ya que, como hemos visto repetidamente, los órganos jurisprudenciales consagran en sus sentencias la obligación de que sean las entidades bancarias quienes asuman las consecuencias derivadas de los fallos de seguridad que desembocarían en el posterior phishing.

Por las características de este delito, resulta muy complicado conseguir que los autores materiales del delito puedan ser juzgados, ya que en muchos casos actúan desde otros países a través de IPs de difícil seguimiento y obtienen el dinero sin dejar apenas rastro. Ante esto, las víctimas de los engaños quedan en una situación de desamparo para recuperar las cantidades que les han sido sustraídas, por lo que resulta lógico que se busque su protección de forma reforzada.

SEGUNDA: En ese sentido, podemos ver claramente que las entidades bancarias tienen una responsabilidad cuasi objetiva para este tipo de supuestos. Por ello, y al tener que responder por los fallos de seguridad, los bancos deberían ser proactivos en la implementación de medidas de protección avanzadas, en el seguimiento constante de las transacciones sospechosas y en la actualización periódica de sus sistemas de seguridad para adaptarse a las nuevas amenazas electrónicas. De lo contrario, los tribunales penalizarán su actuación.

Se puede deducir que esta posición está inspirada en la idea de que los beneficios que el progreso tecnológico aporta al tráfico económico y a los

proveedores de servicios deben ser equilibrados con, como hemos señalado anteriormente, una protección adecuada para los usuarios que están expuestos a los riesgos de fraude.

Los bancos son beneficiarios últimos de la relación contractual con el cliente, y cuentan con un músculo financiero suficiente para hacer frente a estas reclamaciones, así que resulta entendible que la jurisprudencia eleve los estándares de la negligencia grave de los clientes, por un principio de equidad.

TERCERA: Falta regulación específica para supuestos de este tipo. Es cierto que el artículo 249 habla de las estafas informáticas, en las que se pueden encuadrar los supuestos de smishing, pero la actual legislación quizá sea insuficiente para abordar de manera específica los riesgos asociados a estas prácticas.

La normativa vigente, como el Real Decreto-ley 19/2018, no aborda en detalle las particularidades del smishing, lo que deja a los consumidores potencialmente desprotegidos frente a estas amenazas emergentes, aunque es cierto que la jurisprudencia está tratando de llenar esos vacíos. Una regulación más concreta serviría para establecer estándares uniformes que ayudasen más a la identificación, prevención y respuesta a los ataques de phishing.

Además, al ser fraudes que usualmente se realizan desde países distintos al lugar efectivo de la estafa, establecer mecanismos de compensación a nivel internacional para las víctimas de phishing podría ser una buena idea para fortalecer la confianza en el sistema bancario global.

CUARTA: La diligencia de las partes ayudaría a la solución de los conflictos. En los casos de phishing vemos a veces que los clientes no siguen las recomendaciones que los bancos les hacen porque no las leen en sus canales informativos. Aunque estas faltas de atención puedan no ser consideradas como negligencias graves, una mayor concienciación del usuario podría evitar muchos de estos casos.

Esto no es óbice para que las entidades bancarias, al tener los medios y beneficiarse económicamente de la relación contractual, deban hacer mayores

esfuerzos en comunicar a sus clientes los riesgos asociados a la actividad bancaria en Internet. Se ha visto que con avisos genéricos puede no ser suficiente, por lo que es recomendable que implementen mecanismos y herramientas de vigilancia activa que de verdad sirvan para detectar intentos de phishing y smishing de manera temprana.

La adopción por parte de los bancos de medidas de autenticación fuertes pero sencillas de usar, combinándolas con la educación del cliente, deberían ser estrategias fundamentales para que este tipo de supuestos se produzcan cada vez menos con el paso de los años.

QUINTA: Para el cliente siempre sería recomendable denunciar a su entidad bancaria, ya que el proceso para resarcir sus daños suele ser rápido, barato y sencillo. De lo analizado se observa que, por lo general, las perspectivas de resarcimiento del daño son muy positivas para las víctimas. Y, además, se podría llegar a esa solución desde diversas vías.

Si el banco no acepta directamente la reclamación del cliente, surge la opción de acudir al Banco de España, que es un procedimiento gratuito y fácil de llevar a cabo. Ya hemos visto que en muchos casos es suficiente con acudir a este organismo para obtener el reembolso debido a un allanamiento de la entidad bancaria. Y este tipo de resoluciones son relativamente rápidas, ya que en menos de 90 días debería estar listo el dictamen. También se podría recurrir, antes de iniciar un procedimiento contencioso, como hemos visto, a la conciliación.

No obstante, si tras estos pasos, el banco sigue sin aceptar las pretensiones de su cliente, la demanda judicial es una alternativa que está dando buenos resultados. De forma generalizada, la jurisprudencia se muestra a favor del cliente y no de la entidad bancaria, y en supuestos como el de don Gabriel, de poca cuantía, el proceso se desarrollaría mediante juicio verbal, un procedimiento mucho menos engorroso que el juicio ordinario. Además, en el caso concreto de este Trabajo de Fin de Máster, habría menores impedimentos económicos para el cliente, ya que don Gabriel no necesitaría de forma

obligatoria los servicios de abogado y procurador para interponer la demanda, aunque, evidentemente, su contratación fuera lo más aconsejable.

6. BIBLIOGRAFÍA

Webgrafía:

Balance de criminalidad cuarto trimestre de 2024:
https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2024/Balance-de-Criminalidad-Primer-Trimestre-2024.pdf

Banco de España:
https://www.bde.es/wbe/es/

Boletín Oficial del Estado;
https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

Clientes bancarios – Banco de España:
https://clientebancario.bde.es/pcb/es/blog/Sirve_para_alg_3a2a736dffadb61.html

INCIBE:
https://www.incibe.es/

Instituto Nacional de Estadística:
https://www.ine.es/prensa/tich_2023.pdf

Memoria de Reclamaciones del Banco de España 2018:
https://www.bde.es/f/webbde/Secciones/Publicaciones/PublicacionesAnuales/MemoriaServicioReclamaciones/18/00_Memoria_reclamaciones_completa.pdf

Memoria de reclamaciones del Banco de España 2022:
https://www.bde.es/f/webbe/Secciones/Publicaciones/PublicacionesAnuales/MemoriaServicioReclamaciones/22/MSR2022.pdf

Ministerio del Interior:
https://www.interior.gob.es/opencms/ca/detalle/articulo/La-Guardia-Civil-detiene-a-un-centenar-de-personas-por-estafar-mas-de-un-millon-de-euros-mediante-los-SMS-fraudulentos/

La Ley:
https://guiasjuridicas.laley.es/

Noticias jurídicas:
https://noticias.juridicas.com/

Libros, revistas y manuales:

CALVO SAN JOSE, M. J. (2023), 'La responsabilidad civil de los bancos en los delitos de estafa por "phishing"'. Actualidad Jurídica Iberoamericana Nº 18, febrero 2023, ISSN: 2386-4567. Págs. 1788-1809

FLORES PRADA, I (2012), 'Criminalidad informática, aspectos sustantivos y procesales'. Editorial Tirant lo blanch, Valencia, 2012. Pág. 202

GONZÁLEZ HERNÁNDEZ, R. (2013). Responsabilidad extracontractual y contractual: barrera entre ambas. Anuario Jurídico Y Económico Escurialense, (46), págs. 203–214. Pág. 205. Recuperado a partir de https://publicaciones.rcumariacristina.net/AJEE/article/view/152

HERAS HERNÁNDEZ y MARTÍNEZ DE SALAZAR BASCUÑANA en RIBÓN SEISDEDOS, E. (2024). 'Fraudes bancarios y defensa del afectado. Nuevas tendencias defraudatorias especial referencia al phishing bancario'. Tirant lo Blanch: Ilustre Colegio de Abogados de Madrid. Págs. 61-62

HERNÁNDEZ, P. P. (2018). 'Responsabilidad civil': (ed.). Santiago de los Caballeros, Universidad Abierta para Adultos (UAPA). pág. 186. Recuperado de https://elibro-net.ponton.uva.es/es/lc/uva/titulos/175610

MORALES MORENO, A. M. (1982), 'El dolo como criterio de imputación de responsabilidad al vendedor por los defectos de la cosa'. Anuario de derecho civil, ISSN 0210-301X, Vol. 35, Nº 3, 1982, págs. 591-684

PABLO-ROMERO GIL-DELGADO, M. C. (2015), 'El contrato de cuenta corriente bancaria'. Operaciones bancarias de activo y pasivo en el contexto de crisis económica: hacia la unificación de la contratación privada / coord. por María Ángeles Egusquiza Balmaseda Árbol académico, Rafael Lara González Árbol académico, 2015, ISBN 978-84-9059-935-8. Págs. 347-397

RIBÓN SEISDEDOS, E. (2024). 'Fraudes bancarios y defensa del afectado. Nuevas tendencias defraudatorias especial referencia al phishing bancario'. Tirant lo Blanch: Ilustre Colegio de Abogados de Madrid.

SALVADOR CODERCH, P. (Ed.), GÓMEZ LIGÜERRE, C., RAMOS GONZÁLEZ, S., RUBÍ PUIG, A., LUNA YERGA, Á. (2022) 'Derecho de daños (DdD). Análisis, aplicación e instrumentos comparados', 11ª edición, 2022. Pág.74

Jurisprudencia:

Sentencia del Tribunal Supremo, a 17 de febrero de 2020 - ROJ: STS 2017/2020: https://www.poderjudicial.es/search/AN/openDocument/54a1aff4683d8f63/20200707

Sentencia del Tribunal Supremo, a 12 de mayo de 2016 - ROJ: STS 2124/2016: https://www.poderjudicial.es/search/AN/openDocument/9dc54dfb165f94c5/20160526

Sentencia del Tribunal Supremo, a 21 de noviembre de 2012 - ROJ: STS 7843/2012: https://www.poderjudicial.es/search/AN/openDocument/fe1f876cd914c8db/20121217

Sentencia del Tribunal Supremo, a 10 de julio de 2003 - ROJ: STS 4880/2003: https://www.poderjudicial.es/search/AN/openDocument/48b85ae4a418119b/20030808

Sentencia de la Audiencia Provincial de Lleida, a 19 de abril de 2024 - ROJ: SAP L 349/2024: https://www.poderjudicial.es/search/AN/openDocument/64f7f14647c6999da0a8778d75e36f0d/20240620

Sentencia Audiencia Provincial de Salamanca, a 18 de abril de 2024 - ROJ: SAP SA 255/2024: https://www.poderjudicial.es/search/AN/openDocument/b06dd240c7bd0113a0a8778d75e36f0d/20240627

Sentencia de la Audiencia Provincial de Asturias, a 03 de abril de 2024 - ROJ: SAP O 1253/2024: https://www.poderjudicial.es/search/AN/openDocument/a31c5b8030ac7899a0a8778d75e36f0d/20240618

Sentencia de la Audiencia Provincial de Madrid, a 15 de marzo de 2024 - ROJ: SAP M 4197/2024: https://www.poderjudicial.es/search/AN/openDocument/ebfdb6ceb24e3a58a0a8778d75e36f0d/20240606

Sentencia de la Audiencia Provincial de Badajoz, a 06 de marzo de 2024 - ROJ: SAP BA 332/2024: https://www.poderjudicial.es/search/AN/openDocument/80a98cc7c349b8f6a0a8778d75e36f0d/20240529

Sentencia de la Audiencia Provincial de A Coruña, a 09 de enero de 2024 - ROJ: SAP C 12/2024: https://www.poderjudicial.es/search/AN/openDocument/e7207435413ef3e9a0a8778d75e36f0d/20240318

Sentencia de la Audiencia Provincial de Navarra, a 09 de marzo de 2023 - ROJ: SAP NA 493/2023: https://www.poderjudicial.es/search/AN/openDocument/98e2f1418a39ff66a0a8778d75e36f0d/20230727

Sentencia de la Audiencia Provincial de Madrid, a 20 de mayo de 2022 - ROJ: SAP M 7327/2022: https://www.poderjudicial.es/search/AN/openDocument/a13754bb45b5eae1a0a8778d75e36f0d/20220812

Sentencia de la Audiencia Provincial de Pontevedra, a 01 de diciembre de 2022 - ROJ: SAP PO 2845/2022: https://www.poderjudicial.es/search/AN/openDocument/513dd3def7a460e0a0a8778d75e36f0d/20230111

Sentencia de la Audiencia Provincia de Alicante, a 12 de marzo de 2018 - ROJ: SAP A 632/2018: https://www.poderjudicial.es/search/AN/openDocument/9718501a458ca5d7/20180613

Sentencia de la Audiencia Provincial de Sevilla, a 26 de mayo de 2014 - ROJ: SAP SE 1891/2014: https://www.poderjudicial.es/search/AN/openDocument/833db869f268e75a/20140905

Sentencia de la Audiencia Provincial de Valencia, a 31 de enero de 2013 - ROJ: SAP V 457/2013: https://www.poderjudicial.es/search/AN/openDocument/ad54b0f28d67c639/20130521

Sentencia del Juzgado Primera Instancia de Ferrol, a 03 de julio de 2023 - ROJ: SJPI 1022/2023: https://www.poderjudicial.es/search/AN/openDocument/cae5df274e9d12cca0a8778d75e36f0d/20230821

Legislación:

Española:

Real Decreto-Ley 19/2018, de servicios de pago y otras medidas urgentes en materia financiera

Orden EHA/2899/2011, de transparencia y protección del cliente de servicios bancarios

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

Código Civil

Ley de Enjuiciamiento Civil

Ley 13/1994 de Autonomía del Banco de España

Ley 15/2015, de 2 de julio, de la Jurisdicción Voluntaria

Texto Refundido de la Ley para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre

Internacional:

Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo sobre servicios de pago en el mercado interior

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

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Convenio sobre Ciberdelincuencia del Consejo de Europa de Budapest 2001