Centro de Estudios de Consumo

**PUBLICACIONES JURÍDICAS**
http://centrodeestudiosdeconsumo.com

# ¿DEBE RESPONDER EL BANCO CUANDO UN CLIENTE ES VÍCTIMA DE 'PHISHING'?*

***Blanca Aparicio Araque***
*Doctoranda del Departamento de Derecho civil*
*Universidad de Castilla la Mancha*

*Fecha de publicación: 12 de noviembre de 2024*

El '*phishing'* es un tipo de ciberataque en el que se utilizan correos fraudulentos, llamadas, mensajes de texto, etc., con la intención de obtener los datos bancarios de las víctimas a través de un consentimiento viciado, para después sustraer la mayor cantidad de dinero posible de sus tarjetas de crédito[1]. Es en el año 1996 cuando se le da nombre por primera vez a este ciberataque, y su mención tuvo lugar en el seno del primer proveedor de Internet: America Online (AOL). En el año 2022, el Ministerio del Interior español notificó casi 375.000 ciberdelitos en nuestro país, un 22% más que en el

* Este trabajo es parte del Proyecto de I+D+i PID2021-128913NB-I00, titulado "Protección de consumidores y riesgo de exclusión social: seguimiento y avances", financiado/a por MICIU/AEI/10.13039/501100011033/ y "FEDER Una manera de hacer Europa" dirigido por Ángel Carrasco Perera y Encarna Cordero Lobato, del Proyecto de Investigación SBPLY/23/180225/000242 "El reto de la sostenibilidad en la cadena de suministros y la defensa del consumidor final" cofinanciado por el Fondo Europeo de Desarrollo Regional, en el marco del Programa Operativo de Castilla-La Mancha 20212027, dirigido por Ángel Carrasco Perera y Ana Carretero García y de las Ayudas para la realización de proyectos de investigación aplicada, en el marco del Plan Propio de investigación, cofinanciadas en un 85% por el Fondo Europeo de Desarrollo Regional (FEDER), para el proyecto titulado "Modelos jurídicos eficientes de consumo sostenible", con Ref.: 2022-GRIN- 34487 dirigido por Ángel Carrasco Perera y Ana I. Mendoza Losana.

[1] La Audiencia Provincial de Madrid definió el phising como: *"la suplantación de la identidad de un banco por parte del phiser con la finalidad de adquirir información confidencial sobre contraseñas de cuentas bancarias, tarjetas de crédito o cualquier otra información en relación con el banco, que permita entrar en las cuentas de los usuarios en internet de banca electrónica. El internauta recibe un correo electrónico o cualquier mensaje instantáneo, a través del cual se le informa de que debe cambiar sus claves bancarias, proporcionándole un link a través del cual pueda acceder a la página Web de la supuesta entidad bancaria y allí realizar la modificación aconsejada. En la mayoría de los métodos de phishing se utilizan técnicas de engaño, a través de las cuales el phiser utiliza contra la víctima el propio código de programa del banco o servicio similar, adquiriendo la página Web la verdadera apariencia de la entidad bancaria. Igualmente, resulta muy habitual que el internauta reciba un correo en el que se le informe de que debe verificar sus cuentas, seguido por un enlace que parece la página Web oficial de la entidad bancaria."*, véase la sentencia de la Audiencia Provincial de Madrid, Sección 9ª, núm. 178/2015 de 4 de mayo de 2015, rec. 661/2013.

año anterior[2]. España se encuentra en el top 10 de países que más ataques informáticos sufre y, además, los casos de phishing se encuentran en primera posición entre las ciberamenazas detectadas durante el último semestre, tal y como reflejan los análisis realizados[3]. Además, los datos oficiales de ciberseguridad arrojan un crecimiento exponencial y preocupante de los delitos de estafa informática, que acaparan más del 90% del total de los hechos criminales cometidos en las redes, con un incremento porcentual de 3 puntos en al año 2023 respecto al anterior, teniendo como principales víctimas, por su escasa cultura tecnológica, a las personas de edad avanzada[4].

Como medidas de protección ante la inseguridad con la que se encontraban los consumidores en la era digital, se publica en el año 2018 el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera[5]. En el preámbulo del mismo se indica que tiene como principales objetivos facilitar y mejorar la seguridad en el uso de sistemas de pago a través de internet, reforzar el nivel de protección al usuario contra fraudes y abusos potenciales, respecto del previsto en la Ley 16/2009, de 13 de noviembre, así como promover la innovación en los servicios de pago a través del móvil y de internet. En este sentido, destaca el artículo 45, que habla de la responsabilidad del proveedores de servicios de pago en caso de operaciones de pago no autorizadas, indicando lo siguiente: "*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" (...).* Todo ello condicionado a lo que se establece en el artículo 43, en el que se indica que es deber el usuario de servicios de pago comunicar que la operación no fue autorizada correctamente sin demora justificada en cuanto tenga conocimiento de las mismas. Ahora bien, también se indica en el artículo 46 del referido texto lo siguiente: "*El ordenante soportará todas las pérdidas derivadas de operaciones de pago no autorizadas si el ordenante ha incurrido en tales pérdidas por haber actuado de manera fraudulenta o por haber incumplido, deliberadamente o por negligencia grave, una o varias de las obligaciones que establece el artículo 41(...)".* Por tanto, lo que se instaura con esta normativa es la responsabilidad cuasi-objetiva de las entidades bancarias cuando se cometen este tipo de fraudes, y solo quedarán exoneradas de dicha responsabilidad, y liberadas de la carga de restituir el dinero que haya sido extraviado, en el caso de que puedan probar que el ordenante actuó de manera fraudulente o que la apropiación de

[2] Fuente: https://www.channelpartner.es/seguridad/principales-ciberataques-espana-2023-lockbit ransomware-hospital-clinic/

[3] Fuente: https://cincodias.elpais.com/smartlife/lifestyle/2024-06-28/espana-en-el-top-10-de-paises-que-mas-ataques-informaticos-sufren-a-nivel-mundial.html

[4] GÓMEZ LINACERO, D. *Responsabilidad de los bancos frente a la estada informática: preguntas y respuestas en clase práctica,* Diario LA LEY, nº 10590, Sección Tribuna, 17 de octubre de 2024, pág. 4.

[5] El acuerdo de convalidación se llevó a cabo por Resolución de 13 de diciembre de 2018 (Ref. BOE-A-2018-177.

fondos se produjo a causa de su propia culpa o dolo por incumplir, deliberadamente o por negligencia grave, alguno de los deberes de diligencia impuestos por la norma al ordenante[6].

Una vez expuesta la normativa con la que nos encontramos en el derecho español que protege al consumidor, hemos de plantear cuál es la problemática actual, que nos lleva persiguiendo algunos años. Si bien es cierto que en un primer momento las entidades bancarias respetaban la normativa establecida, devolviendo el dinero sustraído a sus clientes, con el paso de los años, y con la aparición de estafas mucho más sofisticadas y novedosas, gracias al uso de diversos sistemas desarrollados con inteligencia artificial, los bancos han ido desdibujando esta garantía que se establecía para sus clientes, negándose en algunas ocasiones a la devolución de las cuantías que habían sido sustraídas. El principal motivo que oponen es que el cliente no ha actuado de manera diligente, puesto que ha cedido las claves de su cuenta o ha facilitado a los hackers los códigos de autenticación que les hayan solicitado, olvidando por completo que, cuando los clientes prestan su consentimiento en estas situaciones (entre las que se encuentran mensajes que aparecen en el mismo buzón en que el que reciben los clientes las notificaciones habituales de los bancos, que derivan a aplicaciones bancarias ficticias que son idénticas a las reales) lo hacen de una manera viciada[7], puesto que consideran que los datos que están cediendo van dirigidos a otro fin completamente distinto.

Habiendo trazado con este breve resumen el panorama actual, analicemos la jurisprudencia más reciente, que puede presentar matices dependiendo del caso concreto, pero en la mayoría de las resoluciones encontraremos puntos de inflexión que nos ayudarán a sacar conclusiones claras respecto a la responsabilidad del banco en este tipo de delitos. Las cuestiones que más se repiten y que son resueltas por la jurisprudencia son las siguientes: (i) que el demandado plantee la prejudicialidad penal por haberse presentado una denuncia ante la Policía, (ii) alegar falta de legitimación pasiva al pertenecer la entidad bancaria a un grupo de empresas, (iii) rechazar cual tipo de responsabilidad, entendiendo que el cliente debe asumir la culpa al haber cedido los datos a los estafadores.

En aras a dilucidar la primera cuestión, nuestros Tribunales[8] han aclarado que la decisión que pueda adoptarse en un futuro proceso penal, en orden a la eventual condena a un

[6] Sería el caso de los usuarios que, con desprecio a las más elementales reglas de ciudad, exponen ses credenciales por diferentes vías a los demás (apuntándolas en lugares visibles, facilitándolas a terceros, dejándolas al descuido). Véase en este sentido, GÓMEZ LINACERO, D., ob. cit., pág. 10.

[7] Recordemos que la falta de consentimiento, aunque no esté incluida expresamente en la redacción literal del artículo 36.1 del RD 19/2018, debe completarse con este consentimiento viciado, según los principios básicos de nuestro derecho contractual y obligaciones, erigidos sobre el consentimiento como piedra angular del acto perfeccionador del negocio. En este sentido, véase GÓMEZ LINACERO, D. ob. cit., pág. 6.

[8] Véase la SAP Madrid (10ª) núm. 501/2019, de 28 de octubre de 2019, rec. 313/2019.

tercero por estafa (por conducir mediante engaño al deudor a realizar los actos de disposición que se investigan) no afecta a la decisión del Tribunal civil sobre la cuestión a dilucidar, que en este caso es la procedencia del pago al verdadero acreedor. La resolución que se tome en el procedimiento penal no tendrá una influencia decisiva para el tribunal civil y su decisión sobre la extinción o no de la deuda, por lo que no existiría prejudicialidad penal[9]. Centrándonos en la alegación de prejudicialidad penal por parte de la defensa del demandado en este tipo de casos, resulta ilustrativa la sentencia del Juzgado de 1ª Instancia Nº4 de Torremolinos núm. 331/2021, de 30 de noviembre de 2021, rec. 97/2021, en la que se indica lo siguiente: "*TERCERO.- Centrado el debate en estos términos, y comenzando por la petición de suspensión por prejudicialidad penal, el artículo 40.2 LEC establece que en los casos en los que en un proceso civil se ponga de manifiesto un hecho que ofrezca apariencia de delito o falta, no se ordenará la suspensión de las actuaciones del proceso civil sino cuando concurran las siguientes circunstancias: 1.ª Que se acredite la existencia de causa criminal en la que se estén investigando, como hechos de apariencia delictiva, alguno o algunos de los que fundamenten las pretensiones de las partes en el proceso civil. 2.ª Que la decisión del tribunal penal acerca del hecho por el que se procede en causa criminal pueda tener influencia decisiva en la resolución sobre el asunto civil. En el presente caso la petición de suspensión debe desestimarse de plano: según los términos en los que está planteado el debate, el resultado de la acción penal, una vez comprobada y asumida la realidad de los hechos, es irrelevante a los efectos de determinar si la entidad emisora de la tarjeta debe responder de los efectos del uso inconsentido de la misma. Las diligencias penales, en su caso, serían de interés a la hora de identificar a los posibles responsables y la eventual repetición o reclamación frente a ellos en caso de una condena estimatoria, que pudiera permitir a la emisora de la tarjeta resarcirse de las resultas de este procedimiento. En consecuencia, como queda dicho, la petición no puede prosperar."* También merece ser citado por su carácter ilustrativo la SAP Pontevedra (3ª) núm. 177/2023, de 23 de marzo, cuya fundamentación aboga por una respuesta negativa a la prejudicialidad penal.

Respecto a la segunda cuestión, como es la falta de legitimación pasiva, el hecho de que el banco se valga de sociedades filiales para la gestión de emisión de tarjetas no debe perjudicar al emisor. En este sentido destaca la sentencia de la Audiencia Provincial de Girona (2ª) núm. 62/2024, de 31 de enero de 2024, rec. 724/2023, en la que se indica lo siguiente: *'"El hecho que CaixaBank se valga de sociedades filiales (en este caso, CaixaBank Payments) por la gestión de emisión de tarjetas u otras actuaciones relacionadas con el contrato celebrado entre el cliente y CaixaBank es algo que no tiene que perjudicar al consumidor quién, lógicamente, confía en su relación contractual con CaixaBank, con independencia de la actuación de cariz interno que esta entidad haga a través de filiales suyas, directamente vinculadas a ella. Pero es que, además, la*

[9] CUAIRÁN GARCÍA, J., FERNÁNDEZ HUERTAD P., *El fraude «man in the middle». Un análisis dual en los órdenes penal y civil,* Diario LA LEY, Nº 81, Sección Ciberderecho, 1 de marzo de 2024.

*demandante concertó los contratos bancarios que se encuentran en la base de la reclamación formulada con CaixaBank. Es CaixaBank quien es suplantada en la actuación de terceros, y es el número de atención al cliente de CaixaBank el que es empleado por terceros para cometer el fraude informático que es objeto de este procedimiento. Es también el servicio de atención al cliente de CaixaBank quien responde a las reclamaciones extrajudiciales que se formulan por razón de los hechos que enjuiciamos. Y es CaixaBank quién en este procedimiento facilita y aporta todos los contratos y datos del demandante en relación a su relación contractual bancaria, poniendo de manifiesto que tiene acceso a toda la documentación que, en parte, dice que corresponde a una tercera entidad con personalidad jurídica propia de la que mira de desvincularse. Los motivos expuestos en los dos párrafos anteriores llevan a concluir, sin ningún tipo de duda, que la acción ejercitada por el consumidor ante CaixaBank era plenamente correcta, y alcanza la totalidad de operaciones que le han comportado el perjuicio por el cual reclama.*[10]"

Respecto a la tercera cuestión, en cuanto a la responsabilidad por parte de la entidad bancaria analizaremos la jurisprudencia a lo largo de los años. En primer lugar, las Audiencias Provinciales comparten el mismo criterio en cuanto a la responsabilidad cuasi objetiva de las entidades bancarias, y más en aquellos casos en los que incumplen los deberes de diligencia debidos en la autenticación de operaciones de pago, así como en la prevención del fraude mediante phising. En este sentido, destaca la sentencia núm. 184/2022 de la Audiencia Provincial de Madrid, Sección 20ª, de 20 de mayo de 2022, rec. 945/2021. en la que se indica lo siguiente: "(…) *la demandada incurrió en un incumplimiento de los deberes de diligencia en la prevención del fraude mediante phising, que le hace ser responsable del perjuicio total sufrido por el demandante, pues no podía la entidad desconocer que frecuentemente mediante esa técnica el tercero defraudador utiliza los datos de la tarjeta para activarla en una aplicación de pago de la que tiene dominio (...). No habiendo quedado acreditado que la entidad demandada cumplió en la forma que le es exigible los deberes de diligencia en la autenticación de las operaciones de pago, pues ni habría probado haber implementado un mecanismo antiphising de protección de los usuarios de los instrumentos de pago por ella emitidos frente al uso fraudulento por un tercero de páginas imitativas de las propias para hacerse con las credenciales del instrumento, ni habría puesto en conocimiento del usuario los datos necesarios para que este conociera que se trataba de instalar su tarjeta en una aplicación de pago de un terminal de un tercero y no apreciándose que el demandante incurrió en negligencia grave en el cumplimiento de sus deberes de custodia y uso de la*

[10] De la misma manera se pronuncia el tribunal en las sentencias: SAP Huelva (2ª) núm. 97/2024, de 8 de febrero de 2024, rec. 142/2024; SAP Madrid (25ª) núm. 133/2024, de 15 de marzo de 2024, rec. 42/2023; SAP Barcelona (16ª) núm. 11/2019, de 22 de enero de 2019, rec. 227/2017.

*tarjeta ".* En este mismo sentido se pronuncian las Audiencias Provinciales de Vizcaya, Asturias, Valladolid, Pontevedra y Alicante, entre otras[11].

En segundo lugar, los Tribunales de 1ª instancia, a través de sus resoluciones, han dado respuesta una serie de interrogantes muy cuestionados a la hora de dilucidar la responsabilidad de la entidad bancaria en este tipo de estafas. Respecto al nivel de conocimiento por parte del demandado, resulta interesante como, antes de la entrada en vigor del el Real Decreto-ley de servicios de pago del año 2018, era un hecho determinante si la persona estafada podía llegar a tener ciertos conocimientos informáticos o en el manejo de estas aplicaciones. Véase en este sentido la sentencia del Juzgado de 1ª Instancia Nº9 de Valladolid núm. 362/2009, de 10 de marzo de 2009, proc. 884/2007 , que indica lo siguiente: "*De todo lo anterior se deduce que existió en la actora una actitud negligente pues proporcionó datos a terceros sin atender a las más elementales normas de seguridad de la banca on-line, puesto que la actora no es quien busca el portal de Banco de Santander, sino que recibe un correo electrónico en el que le invita a entrar en una página, lo cual hace, y una vez dentro, entrega las claves de seguridad sin cerciorarse que está en la página correcta, y más en el caso de autos en el que se trata del director financiero del "Grupo El Árbol", que es una importante empresa de supermercados, lo cual hace que se le presuponga cierta destreza en el manejo de esta situaciones, a lo que hay que añadir que usaba con cierta frecuencia la banca on-line del Banco de Santander (...)".* Sea como fuere, tampoco en este caso entiende que sea culpa del demandante, sino que existe una concurrencia de culpas puesto que el banco no fue diligente al permitir disposiciones por encima de lo que constaba en el contrato de banca por internet.

Respecto a la exoneración por parte de la entidad bancaria alegada en ocasiones por la defensa del demandado, es interesante destacar que los tribunales han mantenido que, el hecho de que se proporcionen por parte de los estafados una serie de códigos de autenticación, no se traduce en una actuación gravemente negligente por defecto[12], pues los proporcionan engañados, bajo la apariencia de que los aportan a su entidad bancaria. En este sentido véase la sentencia del Juzgado de 1ª Instancia Nº5 de Ferrol núm. 128/2023, de 3 de julio de 2023, rec. 92/2023, en la que se indica lo siguiente: *"No cabe apreciar negligencia grave por parte de la demandante en el cumplimiento de su*

[11] Véase al respecto las siguientes sentencias: SAP Valladolid (1ª) núm. 74/2010, de 10 de marzo de 2010, rec. 280/2009; SAP Asturias (1ª) núm. 351/2012, de 18 de septiembre de 2012, rec. 594/2011; SAP Vizcaya (3ª) núm. 429/2016, de 10 de noviembre, rec. 386/2016; SAP Pontevedra (6ª) núm. 539/2021, de 21 de diciembre de 2021, rec. 346/2021; SAP Alicante (9ª) núm. 371/2023, de 23 de junio de 2023, rec. 172/2023.

[12] Véase en este sentido la SAP Ourense (1ª) núm. 369/2023, de 9 de junio, en la que se indica lo siguiente: *"Ahora bien, no puede afirmarse que la aplicación de este sistema de autenticación implique por sí misma la exclusión de responsabilidad de la entidad bancaria, sino que, como se ha visto, ésta únicamente se producirá en caso de fraude o negligencia grave del usuario del servicio de pago. Está obligación de autenticación, impuesta a las entidades bancarias con el objetivo de reducir el riesgo de fraude, no agota su responsabilidad en el ámbito civil".*

*obligación de proteger sus credenciales de seguridad. 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 (en este caso, 499 euros), 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 recibido es fraudulento o que la web a la que ha accedido a través del enlace facilitado es falsa"*[13]. En este mismo sentido se pronuncia también el tribunal en la sentencia del Juzgado de 1ª Instancia Nº5 de Pamplona/Iruña núm. 172/2023, de 3 de abril de 2023, rec. 1566/2022, indicando lo siguiente: "*Los sistemas de autenticación se establecen por los proveedores de servicios de pago y si un banco no ha sido capaz de limitar el acceso al canal de banca electrónica no puede pretender que el presunto ordenante víctima de esta práctica fraudulenta sea el único responsable, pues es el banco quien tiene responsabilidad respecto del buen funcionamiento y la seguridad del mismo. Por tanto, en el caso de órdenes de pago y transferencias fraudulentas puede afirmarse que sin dicha declaración de voluntad la operación de pago o transferencia de fondos, presuntamente realizada por la titular de los fondos, se considerará no autorizada".*

También resulta de gran importancia la rapidez con la que se avise por parte del estafado, considerando los tribunales que la celeridad con la que se actúe por su parte se traduce en un comportamiento diligente y debido. En este sentido, véase la sentencia del Juzgado de Primera Instancia e Instrucción Nº1 de Avilés núm. 162/2023, de 27 de julio de 2023, proc. 59/2022, que indica lo siguiente: "*la actora tan pronto como pudo conocer que se habían sustraído las mencionadas cantidades de dinero lo puso en inmediato conocimiento de la demandada, cumpliendo de esta manera con las obligaciones legales que al respecto se impone a todo cliente que sufre un perjuicio como el tratado en el presente asunto. Desde que lo puso en conocimiento de la entidad demandada no se le devolvió la llamada sino hasta transcurridos aproximadamente unos 30 minutos, momento en el que se confirmó a la actora que había sido víctima de fraude y que de los cinco operaciones que se intentaron, dos de ellas pudieron ser rechazadas, sin haberse explicado, tanto en los trámites de reclamación interna previa a este procedimiento como en el seno del mismo, porque las otras tres operaciones no se pudieron bloquear por el sistema de seguridad del banco."*

Por último, pero como aspecto más importante a considerar, cobran especial importancia las medidas de seguridad que hubiera adoptado el banco antes de producirse el incidente. En este sentido destaca la sentencia del Juzgado de 1ª Instancia Nº3 de Toledo núm.

[13] En este mismo sentido se pronuncian en las sentencias núm. 126/2012 del Juzgado de Primera Instancia e Instrucción nº4 de Majahonda, de 8 de noviembre de 2012, rec. 50/2012; así como la sentencia núm. 310/2022, del Juzgado de Primera Instancia Nº7, de Logroño, de 3 de noviembre de 2022, rec. 413/2022.

136/2024, de 8 de marzo de 2024, proc. 426/2023, en la que se indica: *"A tal efecto, aparte el uso de protocolos seguros de cifrado de información que permite establecer una conexión cifrada entre el usuario y la entidad de crédito impidiendo con ello el que terceras personas no autorizadas puedan acceder a la información confidencial que viaja a través de la Red, los sistemas de seguridad empleados por las entidades de crédito en sus operaciones electrónicas deben estar basados en última instancia en infraestructuras de claves públicas que garantizan la autentificación del usuario mediante el uso de claves de firma digital».*

En efecto, este debería ser el aspecto más relevante a considerar, pues no en vano constituye una práctica abusiva en relación con los consumidores y usuarios trasladar a estos las consecuencias económicas de los errores en los sistemas y mecanismos de gestión y administración que quedan bajo el control del prestador del servicio y que no sean imputables a aquellos (art. 89.2 TRLCU aprobado por del RD Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias).

En conclusión, como ha quedado reseñado en el presente artículo, pese a que en ocasiones las entidades bancarias rechacen la devolución del dinero que ha sido sustraído a los clientes, nos encontramos con una normativa tuitiva en la que poder resguardarnos en aquellas ocasiones en las que hayamos picado en el anzuelo con este tipo de mensajes que nos llegan haciéndose pasar por nuestro banco de confianza. No es cierto, como alegan en ocasiones, que el deber de diligencia del consumidor deba verse aumentado, aunque lo recomendable es advertir cuanto antes de la incidencia acontecida. De hecho, el sistema con el que contamos es lógico, coherente y proteccionista con el eslabón más débil (que es el consumidor y descansa en la máxima de que *"el riesgo operacional y las fugas del sistema deben ser asumidos por los bancos en virtud de su posición de garante al ser una pieza clave para evitar la comisión del fraude"*[14]. No podemos negar que, ante la gran oleada de delito cibernéticos que nos abruma actualmente, debamos estar atentos y pensemos con cuidado en qué sitios web estamos accediendo. Pero esto no puede traducirse en un estado de alerta constante, y menos aún en una desprotección cada vez mayor para el consumidor, que debe comprobar cada instante si su navegación por la red estará siendo correcta o no. Apelemos a la cautela y a la atención, mas no al estrés constante y la sensación de inseguridad absoluta provocada por déficits de protección de los sistemas y mecanismos utilizados por la propia entidad bancaria.

[14] Véase SAP Madrid, Sección 11ª, 74/22 (LA LEY 33893/2022).