06/07/2025

Bruselas tramita una nueva regulación que obligará a las entidades financieras a mejorar sus medidas contra el fraude

La Directiva PSD3 introduce mejoras para luchar contra el 'phishing', que en nuestro país ha crecido de forma notable estos últimos años



"El usuario financiero necesita un marco legislativo protector, que delimite de forma suficiente el grado de responsabilidad, en los casos de ciberfraude, y que tenga en cuenta el contexto en el que se produce", así ha transmitido Patricia Suárez, presidenta de la Asociación de Usuarios Financieros (ASUFIN), el sentir de los consumidores españoles al europarlamentario René Repasi, del grupo Socialista en la cámara europea, y ponente responsable de la Regulación de Servicios de Pago, que se debate en estos momentos en Bruselas, conocida como PSD3.

El encuentro, se organizó en la oficina de BEUC, ha contado con la asistencia de numerosas organizaciones de consumidores europeas.

Suárez ha transmitido al político datos sobre el ciber fraude en nuestro país, que choca con una consideración del problema por parte del máximo regulador, el Banco de España, muy alejada a la realidad que sufren los usuarios, expuestos cada vez más a la ingeniería social de los ciberdelincuentes, que va muy por delante de la seguridad que despliegan las entidades. Así, en el 47% de los casos, se considera que el usuario ha cedido sus datos y, por tanto, no hay causa que defender. Y del resto de asuntos, se concluye que, en la gran mayoría, el usuario lleva razón.

La PSD3 introduce mejoras clave para hacer frente a estos desafíos como es la verificación del IBAN: se exigirá que los proveedores de servicios de pago (PSP) verifiquen que el IBAN del destinatario coincide con el nombre del titular de la cuenta antes de procesar una transferencia. Si hay discrepancias, el pagador será notificado y podrá decidir si procede o no con el pago.

Otra cuestión que se plante son nuevas medidas de autenticación: se refuerzan los requisitos de Autenticación Reforzada del Cliente (SCA), haciendo que sean más accesibles para usuarios con dificultades tecnológicas o discapacidades. Será obligatoria en la incorporación de nuevos métodos de pago en billeteras digitales y se establecen excepciones específicas.

Un tercer elemento son los derechos de reembolso: se amplían los derechos de reembolso para víctimas de fraude online, permitiendo que los usuarios puedan recuperar su dinero en determinados casos de suplantación de identidad o transferencias erróneas.

Por último, también se mejora en el intercambio de información sobre fraudes: impulsa la creación de redes de intercambio de información en tiempo real entre entidades financieras para detectar patrones de fraude con mayor rapidez.

En nuestro país, las Audiencia provinciales y los juzgados de primera instancia están dando la razón a las personas consumidoras en caso de fraude, señalando que deben ser los bancos quienes deben acreditar la negligencia grave de los usuarios y que ser engañado por un defraudador profesional no puede considerarse negligencia grave. Además, apuntan a que las entidades financieras deben adoptar las medidas necesarias para prevenir el fraude.

La sentencia del Tribunal Supremo (sentencia 571/2025, de 9 de abril de 2025) de la que E&J hizo un análisis importante con el propio abogado de Zaragoza, Miguel Ángel Marqués, que logró este fallo, el cual marca un antes y un después en materia de phishing porque en el fallo el magistrado Manuel Almenar cuestiona las medidas de seguridad del banco.

Auge del phishing en Europa

Para Eugenio Ribón, decano del Ilustre Colegio de la Abogacía de Madrid (ICAM) y presidente de la Asociación Española de Derecho de Consumo (AEDS), la digitalización de los servicios bancarios ha traído consigo innumerables ventajas para los consumidores. Y por supuesto, también para las entidades financieras. Sin embargo, también ha abierto la puerta a nuevas formas de criminalidad que aprovechan las vulnerabilidades tecnológicas para defraudar a los usuarios.

En los últimos años, España ha experimentado un aumento significativo en los delitos informáticos, en particular los relacionados con operaciones bancarias no autorizadas. Las últimas estadísticas ofrecidas en el Sistema Estadístico de Criminalidad elaborado por Dirección General de coordinación y Estudios, dependiente de la Secretaría de Estado de Seguridad del Ministerio del Interior, informa de la existencia de 472.125 hechos conocidos en 2023 referidos a ciberdelincuencia, de los cuales 427.448 correspondieron a fraudes informáticos.

Por lo tanto, del conjunto de las actividades delictivas en el “espacio ciber” aproximadamente un 90 % corresponden a fraudes informáticos, en su mayoría vinculados a suplantaciones de identidad y accesos no consentidos a cuentas bancarias digitales. El crecimiento es exponencial y seriamente preocupante con un incremento del 60,81% respecto de 2021. Una de cada cuatro denuncias presentadas, ya se refiere a ciberdelincuencia.

Ribón indica que “este fenómeno no es exclusivo del ámbito nacional. A nivel europeo, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) advierte del incremento exponencial de ataques de phishing, los cuales representaron la técnica de entrada más utilizada en incidentes de seguridad en 2023”.

Frente a las sofisticadas técnicas de ciberdelincuencia, las entidades financieras no han adaptado suficientemente sus sistemas de seguridad, como si lo hicieron en sus oficinas físicas, exponiendo con ello a sus clientes a una situación de vulnerabilidad en la banca electrónica que estas mismas diseñaron y potenciaron.

Para Ribón, el régimen jurídico de la responsabilidad por operaciones bancarias no autorizadas encuentra su pilar fundamental en la Directiva (UE) 2015/2366 (PSD2), transpuesta al ordenamiento jurídico español mediante el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago. Esta normativa establece una obligación general de seguridad para las entidades bancarias, así como una presunción de no autorización en beneficio del usuario cuando este alega que no consintió la operación controvertida.

“En su artículo 45, el RD-ley 19/2018 consagra expresamente el derecho del usuario a la devolución inmediata del importe de la operación no autorizada, salvo que la entidad pruebe que el cliente actuó con fraude o negligencia grave. La exigencia de la concurrencia de una diligencia grave, y por tanto, más allá de la simple negligencia, viene corroborada por la lectura del artículo 46 del Real Decreto-ley 19/2018, de 23 de noviembre”, subraya.

A su juicio, “este tipo de fraudes suele ir ligado a su vez a operaciones anómalas desde la perspectiva de los usos, costumbres y perfil del cliente, lo que exigiría hoy en día la implantación de un sistema de alertas preventivo capaz de detectar estas conductas, con frecuencia desarrolladas desde IPs ubicadas en otros países, con compras de criptomonedas u otras contrataciones ajenas al usuario”.

Desde hace decenas de años se viene aplicando en países de nuestro entorno, tanto en los de corte anglosajón bajo la máxima “KYC” (Know your customer —conoce a tu cliente—), que exige indagar en los conocimientos y experiencia financiera del cliente, su intención y su predisposición a la asunción de riesgos.

Para Ribón, “no puede olvidarse de hecho, que dentro de las condiciones generales de la contratación a las que se adhiere el usuario suele predisponerse que el usuario autoriza a la entidad financiera a la realización de estudios, comportamientos de riesgos mediante modelos de scoring, sistemas de información integrados u otros de similar naturaleza”.

A su juicio, la sentencia del Tribunal Supremo 571/2025, de 9 de mayo, marca un hito interpretativo al declarar que no puede imputarse automáticamente negligencia grave al cliente que haya sido víctima de una estafa sofisticada mediante técnicas de phishing con apariencia verosímil y sin defectos de custodia evidentes”.

En este sentido destaca que “el Alto Tribunal exige a las entidades bancarias no solo la implementación de sistemas de autenticación reforzada, sino también mecanismos de detección de operaciones anómalas o inusuales. En este sentido, el incumplimiento de estas obligaciones preventivas constituye una infracción del deber de diligencia que activa el deber de indemnizar”.

Lo que dicen los tribunales

Por su parte Alicia Visitación, magistrada del Juzgado de Primera Instancia número 89 de Madrid y juez de refuerzo del Juzgado 104 Bis, indica que “nadie duda de los beneficios de la tecnología, pero el aumento en su utilización conlleva un aumento de las estafas en dicho ámbito. La Ley 16/2009, de 13 de noviembre, fue el resultado de la trasposición de la Directiva 2007/64/CE, incluyéndose innovaciones y creando un entorno más seguro y fiable la Directiva 2105/2366, que ha sido traspuesta por el RD-ley 19/2018, de 23 de noviembre de servicios de pago y otras medidas urgentes en materia financiera”.

En el Congreso del ICAM de Derecho de Consumo coincidieron el decano Eugenio Ribón con la magistrada Alicia Visitacion. (Imagen: ICAM)

La norma acude a una responsabilidad cuasiobjetiva de la entidad bancaria, y es que, siendo ésta la directa y claramente beneficiaria de la imposición de las nuevas tecnologías a los clientes, han de responder, salvo que se pruebe que, además de que la orden de pago no se vio afectada por fallo técnico u otra deficiencia del servicio, concurre actitud fraudulenta o de negligencia grave en el cliente (SAP Oviedo n.º 158/24, 18 marzo).

Como recogen nuestros tribunales, se potencia la utilización por clientes y usuarios y el banco “tiene y debe implementar todas las medidas de seguridad necesarias para evitar fraudes”. (sentencia de la Audiencia Provincial de Ourense n.º 369/23, de 9 junio).

Recoge la sentencia de la Audiencia Provincial (AP) de Jaén n.º 202/24, de 16 febrero que: “mientras los terceros soportan la amenaza eventual de sufrir daños significativos, con la única ventaja de obtener a cambio, en el mejor de los casos, un beneficio meramente difuso, el titular de la actividad, por el contrario, se beneficia de las ganancias generadas de su explotación en su particular provecho”. La sentencia de la Audiencia Provincial de Bilbao, n.º 124/24, de 4 marzo, haciendo alusión a la sentencia de la AP Madrid, n.º 178/15, 4 mayo, recuerda que el riesgo debe soportarlo quienes se benefician con tal forma de plantear un negocio.

Recientemente se ha pronunciado el Tribunal Supremo (TS) en su sentencia de 9 de abril de 2025. Aunque en la ley no se recoge una definición de lo que puede entenderse por negligencia grave, y podemos encontrar resoluciones dispares de nuestros tribunales, sí puede tenerse una idea o concepción de lo que puede considerarse como tal a partir de la solución dada en cada caso concreto. En ese caso concreto se puede determinar si hay una negligencia grave, lo que sí queda claro es que la mera cesión de

datos por parte del cliente al “estafador”, no puede por sí solo servir para exonerar a la entidad bancaria de responsabilidad (entre otras, la SAP Oviedo n.º 158/24, 18 marzo y de Málaga de 30 noviembre de 2021).

Esta magistrada, estudiosa de esta jurisprudencia indica que “el banco ha de adoptar las medidas necesarias para evitar el phishing, sin olvidar que ante cualquier conducta anómala o inusual del cliente, habrá de adoptar medidas extras para evitar la estafa; su diligencia va más allá del buen padre de familia, sino reforzada; habiendo quedado resuelto, igualmente, por nuestros Tribunales que la doble autenticación no es suficiente para la exoneración de la entidad” (entre otras, la SAP Madrid n.º 184/22, de 20 mayo y la SAP Oviedo n.º 236/23, de 10 mayo).

Fuente: https://www.economistjurist.es/

LINK DE LA NOTICIA