1.5. Obligaciones y contratos

Responsabilidad civil del proveedor de servicios de pago en casos de fraude y phishing

Civil liability of the payment service provider in cases of fraud and phishing

por

ROBERT REINHART SCHULLER

Investigador predoctoral en formación FPI-UR/CAR 2022

Universidad de La Rioja

RESUMEN: La normativa europea y nacional posibilita, ante determinadas situaciones, que un prestador de servicios de pago llegue a responder por hechos de terceros. A lo largo del presente comentario se analizará la normativa, la jurisprudencia, para extraer la posición actual respecto a tal tipo de responsabilidad. Se valorará el concepto de negligencia, la autenticación reforzada y los diferentes deberes de seguridad, así como la diligencia de los participantes en la relación contractual.

ABSTRACT: European and national regulations allow, in certain situations, a payment service provider to be held liable for acts commited by third parties. Throughout this commentary, the legislation and case law will be analyzed to outline the current position regarding this type of liability. The concepts of negligence, strong authentitcation, and various seciruty obligations will be assessed, as well as the diligence of the parties involved in the contractual relationship.

PALABRAS CLAVE: prestadores de servicios de pago, diligencia, negligencia grave, usuario, responsabilidad, carga de la prueba.

KEYWORDS: payment service providers, diligence, gross negligence, user, liability, burden of proof.

https://doi.org/10.36151/rcdi.2025.810.10

I. INTRODUCCIÓN

Los llamados delitos informáticos, concepto que engloba una multitud de actos llevados a cabo gracias a los medios tecnológicos, no solo cuentan con una respuesta penal, sino que también se han ido creando normas *ad hoc*. El claro ejemplo de ello es la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) nº 1093/2010 y se deroga la Directiva 2007/64/CE[1].

La Directiva 2015/2366, entre otras cosas, contempla la responsabilidad de las entidades bancarias por defectos de seguridad. Quiere decir esto, al menos en lo que a consumidores se refiere, que esta norma desplaza el régimen de la responsabilidad por bienes o productos defectuosos, del libro tercero del TRLGDCU. En otras palabras, se trata de una norma específica que establece unos requisitos específicos en materia de responsabilidad y carga de la prueba.

Aunque el objeto del comentario se centre en el estudio jurisprudencial de la responsabilidad civil de las entidades bancarias, por phishing y otras prácticas análogas, no deben obviarse una serie de estadísticas. Para ello resulta útil aportar un gráfico del Ministerio del Interior, en el cual se pone de manifiesto la evolución de la cibercriminalidad en los últimos años en España. A continuación, se expone el gráfico[2]:

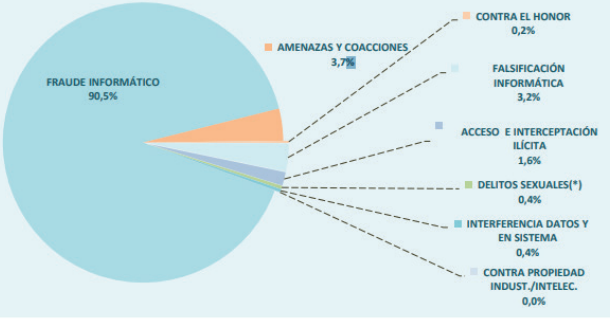
INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA

3.- DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD (Fuente de datos: Sistema Estadístico de Criminalidad)

>> 3.1. Evolución de hechos conocidos por categorías delictivas

HECHOS CONOCIDOS	2019	2020	2021	2022	2023
ACCESO E INTERCEPTACIÓN ILÍCITA	4.004	4.653	5.342	5.578	7.367
AMENAZAS Y COACCIONES	12.782	14.066	17.319	15.982	17.472
CONTRA EL HONOR	1.422	1.550	1.426	1.191	1.174
CONTRA PROPIEDAD INDUST./INTELEC.	197	125	137	114	64
DELITOS SEXUALES(*)	1.774	1.783	1.628	1.646	1.804
FALSIFICACIÓN INFORMÁTICA	4.275	6.289	10.476	12.569	15.137
FRAUDE INFORMÁTICO	192.375	257.907	267.011	335.995	427.448
INTERFERENCIA DATOS Y EN SISTEMA	1.473	1.590	2.138	1.662	1.659
Total HECHOS CONOCIDOS	**218.302**	**287.963**	**305.477**	**374.737**	**472.125**

(*)Excluidas las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



Como habrá podido observarse, sin contar con datos actualizados en relación con el año 2025, desde el año 2019 hasta el 2023[3] los casos de fraude informático se duplicaron.

En lo que aquí interesa, del considerando sexto de la Directiva 2015/2366 se extrae que el objetivo consiste en garantizar una elevada protección al consumidor en los servicios de pago[4]. Este considerando debe interpretarse de forma conjunta con el séptimo, que enfatiza la necesidad de asegurar la seguridad en los pagos electrónicos. Todo ello, a pesar de la pluralidad de sujetos intervinientes[5] según los casos.

La utilización de diferentes instrumentos que permiten facilitar la adquisición de diferentes bienes o servicios conllevan una serie de riesgos, entre los cuales están el potencial *hackeo* de dichos terminales. Los consumidores cada vez son más vulnerables, a pesar de que en muchas ocasiones emplean una gran diligencia en la custodia de sus claves, ya que los avances tecnológicos permiten burlar, de diferentes formas, la seguridad tanto de las entidades como de los usuarios.

Se pretende, por tanto, poner de manifiesto la postura jurisprudencial en materia de responsabilidad civil cuando el usuario hubiera sufrido perjuicio económico, como consecuencia del *phishing* y otras prácticas análogas. Para ello, resulta pertinente adelantar que se valorarán dos conductas: la del usuario y, por otro lado, la de la entidad. En cuanto a las entidades[6], en parte, su diligencia se debe reconducir a las medidas de seguridad adoptadas para evitar fenómenos que supongan un perjuicio patrimonial, a causa por terceros, a sus clientes[7].

II. AUTENTICACIÓN REFORZADA

Si bien se distingue entre dos conceptos, autenticación y autenticación reforzada del cliente, este último tiene una gran relevancia para garantizar la legitimidad del usuario ordenante en los pagos por internet. El concepto de autenticación se recoge en el art.4.29 de la Directiva 2015/2366, donde se establece que:

"autenticación: procedimiento que permita al proveedor de servicios de pago comprobar la identidad del usuario de un servicio de pago o la validez de la utilización de determinado instrumento de pago, incluida la utilización de credenciales de seguridad personalizadas del usuario[8]".

Conviene subrayar y tener en cuenta el objetivo, el cual se centra en la comprobación de la identidad del usuario. Esta precisión, como se verá más adelante, cuenta ya con ciertos matices jurisprudenciales.

Por otro lado, se entiende por autenticación reforzada del cliente:

"la autenticación basada en la utilización de dos o más elementos categorizados como conocimiento (algo que solo conoce el usuario)[9], posesión (algo que solo posee el usuario[10]) e inherencia (algo que es el usuario[11]), que son independientes —es decir, que la vulneración de uno no compromete la fiabilidad de los demás—, y concebida de manera que se proteja la confidencialidad de los datos de autenticación[12]".

La autenticación reforzada tiene como objetivo paliar y minimizar situaciones de riesgo. Según el considerando noventa y cinco de la Directiva 2015/2366, se busca que el usuario tenga pleno conocimiento, en todo momento, del importe que vaya a autorizar y del beneficiario de la orden. Este hecho, que implica la uti-

lización de códigos dinámicos de un solo uso, permite que no sea necesario que el sujeto esté físicamente localizado, atribuyendo la confianza en un sistema que permite, en principio, identificar al sujeto con derecho a realizar transferencias. Sin embargo, este objetivo no se cumple únicamente con el empleo de la autenticación reforzada, sino que, para cerciorarse, en la medida de lo posible, de que la solicitud proviene de un usuario legitimado, será también necesario implementar mecanismos de supervisión[13].

En lo que aquí interesa, la autenticación reforzada se menciona en los arts.97 y 98 de la Directiva 2015/2036, y cuenta con una regulación exhaustiva en el Reglamento Delegado 2018/389. No obstante, existen una serie de factores a tener en cuenta, pues en ciertas ocasiones la autenticación reforzada no será necesaria. Estas exenciones se encuentran reguladas en el Capítulo III del Reglamento Delegado 2018/389 y se refieren principalmente a operaciones que no excedan un determinado importe, a un importe concreto tras realizar varias operaciones, o a un número concreto de operaciones. Sin embargo, estas exenciones no constituyen una obligación, sino que corresponde al proveedor de servicios de pago decidir si las aplica y, en consecuencia, si exige o no la autenticación reforzada en dichas situaciones.

Sin embargo, la autenticación reforzada desempeña un papel relevante a la hora de modular, o no, la responsabilidad del ordenante en caso de operaciones no autorizadas. Conviene tener en cuenta que el art.74.2 de la Directiva 2015/2036 establece:

"*2. Si el proveedor de servicios de pago del ordenante no exige autenticación reforzada*[14] *de cliente, el ordenante solo soportará las posibles consecuencias económicas en caso de haber actuado de forma fraudulenta. En el supuesto de que el beneficiario o el proveedor de servicios de pago del beneficiario no acepten la autenticación reforzada del cliente, deberán reembolsar el importe del perjuicio financiero causado al proveedor de servicios de pago del ordenante*".

A su vez, el art.97 de dicha Directiva contempla una serie de supuestos en los cuales se exige la autenticación reforzada. Sin embargo, este precepto y el anterior deben interpretarse conforme al Reglamento Delegado 2018/389. Es decir, se debe entender que el prestador de servicios de pago, aunque hubiera habido negligencia grave, deberá responder ante el usuario en aquellas situaciones en las que la autenticación reforzada no se hubiera aplicado cuando la norma la exigía de forma imperativa.

Ciertas dudas pueden surgir respecto a los supuestos que abarcan excepciones, ya que el Reglamento Delegado establece estas excepciones como una facultad discrecional del prestador de servicios para decidir su aplicación o no. Resulta sugestivo preguntarse si dicho prestador debería responder en un supuesto contemplado como excepción. En principio, al no tratarse de una obligación, el riesgo de no aplicar la exención, siendo una potestad en tales situaciones, deberá asumirlo el usuario. De este modo, le correspondería responder incluso por negligencia grave, a pesar de no haberse llevado a cabo una autenticación reforzada, pues esta constituía una mera facultad a favor del prestador de servicios de pago.

III. CONSENTIMIENTO

El primer paso para analizar una orden consiste en determinar si hubo consentimiento por parte del ordenante. Para ello, según el art.64 de la Directiva

2018/389, será necesario que el consentimiento se hubiera prestado conforme a la forma acordada entre el ordenante y el proveedor de servicios de pago. En la normativa española, el consentimiento, así como su forma y procedimiento de notificación quedan recogidos en el art.36 del RD-Ley 19/2018. Desde un punto de vista jurisprudencial, la prestación del consentimiento se ha relacionada con el procedimiento de autenticación e identidad del ordenante[15].

El consentimiento supone, según la jurisprudencia, que la manifestación de voluntad se haya llevado a cabo no solo conforme a la forma y procedimiento establecidos, sino también por el verdadero sujeto con derecho de disposición respecto a un instrumento de pago[16]. Asimismo, conforme al art.64 de la Directiva 2015/2036, la falta de este supone que la operación de pago se considerará no autorizada[17]. Además, el consentimiento puede verse modulado y, por tanto, está relacionado con los propios límites de gasto, aplicables al instrumento de pago aplicables al instrumento de pago en virtud del contrato marco. Este aspecto es relevante, ya que el proveedor de servicios de pago podrá reservarse el derecho a bloquear el instrumento de pago, por ejemplo, en caso de un aumento significativo, del límite de gasto[18].

IV. DILIGENCIA Y RIESGOS

Desde un punto de vista subjetivo, es importante tener en cuenta que la jurisprudencia y la normativa objeto de estudio establecen un reparto de riesgos que se relaciona de manera inherente con la diligencia esperada de las partes, conforme al marco normativo establecido. Se observará que la diligencia esperada cuenta con un régimen propio, lo cual permite no tener que acudir a soluciones genéricas del Derecho común.

Uno de los supuestos de hecho más frecuentes donde se valora esta situación consiste en el *phishing* y sus distintas modalidades. Como se verá, antes situaciones en las cuales el cliente recibe un mensaje de correo electrónico o SMS, según el contenido y la situación de hecho, la jurisprudencia ha analizado cuál es la diligencia y riesgo asumido por el cliente y el proveedor de servicios de pago.

1. Contenido de los mensajes

Lo habitual es que, tanto por correo electrónico como por SMS, el contenido de la comunicación indique que un tercero está intentando acceder a la cuenta bancaria del usuario, y que este debe ingresar al enlace proporcionado por motivos de seguridad. En muchas ocasiones, se alega que el motivo se basa en la vinculación de un nuevo dispositivo. La efectividad de estos contenidos radica en su notable parecido con los oficiales que normalmente envían las entidades bancarias.

Ante estas situaciones, las posiciones adoptadas por ambos sujetos se centran, por parte de los prestadores de servicios de pago, el cumplimiento de los requisitos de seguridad y en su diligencia al haber identificado y autentificado que la orden proviene del usuario. Por otro lado, de forma resumida, el usuario sostiene que existió alguna falla en el sistema de identificación del prestador de servicios

de pago. Asimismo, afirma que no obró de manera negligente, y mucho menos fraudulenta o con negligencia grave.

2. Jurisprudencia

La jurisprudencia atribuye a las entidades financieras el papel de custodios y depositarios[19]. Desde un punto de vista jurisprudencial se ha puesto de manifiesto que la responsabilidad, en situaciones como el *phishing* y análogas, al entenderse no autorizadas las operaciones por parte del cliente, es de carácter cuasi-objetiva[20]. Es decir, el prestador de servicios de pago responderá, salvo que demuestre que hubiera habido negligencia grave o actuación fraudulenta por parte del cliente. La carga de la prueba recae en el prestador de servicios de pago, debido a que dispone de la facilidad probatoria[21].

De esta forma, una de las cuestiones esenciales es: ¿se considera negligencia grave por parte del usuario el haber confiado en la apariencia de un enlace aparentemente verídico?

3. Diligencia del usuario

Desde un punto de vista de la diligencia del usuario, se ha valorado su actuación una vez que tuvo conocimiento del fraude cometido por tercero. En este sentido, en la SJPI VALLADOLID, 8/2023 de 11 de enero, se tuvo en cuenta que el cliente acudió a la sucursal al día siguiente de enterarse de lo acaecido. Que contractualmente se estableció, a favor del usuario la facultad de revocar ciertas operaciones. Sin embargo, pese a dicha facultad, la entidad rechazó la solicitud de anulación. Para el Juzgado, este hecho supuso un incumplimiento contractual y una falta de diligencia por parte del prestador de servicios de pago[22].

En la SAP LA RIOJA 49/2023 de 17 de febrero se llega a manifestar que, los diferentes tipos de ataques que captan los datos del cliente son situaciones que poco tienen poca relación con el comportamiento del usuario y que, además, suelen pasar desapercibidos.

1.A. Sustracción

En ocasiones, la posibilidad de uso proviene de una sustracción, que puede haberse perpetrado mediante robo o hurto. En la SAP MADRID 484/2024 de 14 de noviembre, se analiza un supuesto de esta naturaleza. A un sujeto le sustraen sus pertenencias y, mientras tanto, el autor se presenta en varias entidades, logrando en la primera de ellas extraer una cantidad de dinero, presentando el DNI del y realizando su firma[23]. Desde el punto de vista de la actuación del cliente, este, tras sufrir la sustracción, procedió inmediatamente a denunciar. Posteriormente, un día después, al percatarse de la extracción realizada en sucursal por parte del tercero, presentó una nueva denuncia.

Lo relevante de este supuesto de hecho consiste en la interpretación del art.41 del RD-Ley 19/2018. En relación con la diligencia del usuario, el Tribunal sostiene que el precepto se refiere a los instrumentos de pago y no al medio de identificación de este, es decir, el DNI. Esta distinción resulta relevante respecto a la omisión de comunicación por parte del usuario, ya que se infiere que el cliente no incumplió, dado que no está obligado a comunicar la sustracción de su documento de identidad.

El detalle es importante, ya que lo que se utilizó para proceder a la extracción de capital fue del DNI y no del instrumento de pago. De este mod, el tercero aprovechó dicho documento para extraer dinero de dos cuentas en las cuales el afectado era autorizado. Respecto a la negligencia de la entidad, se considera que en otras dos sucursales comenzaron a sospechar del sujeto y lograron detener dos reintegros. Conviene apuntar que de la sentencia citada no se extrae cómo el tercero supo la entidad, que el afectado era beneficiario de dos cuentas, ni otros detalles que pudieran tener interés.

2.B. Factores personales

Puede aseverarse que las circunstancias del cliente pueden valorarse en dos sentidos: tanto en la diligencia esperada de este como en la diligencia que debe de llevar a cabo la entidad. En la SAP LA RIOJA 49/2023 de 17 de febrero, se llega a manifestar: *"Y queremos destacar que, para quedar exento de responsabilidad, el Banco deberá acreditar no sólo que la orden de pago no se vio afectada por un fallo técnico que es en lo que se centra el recurrente, sino tampoco por "otra deficiencia del servicio prestado por el proveedor de servicios de pago." Esto quiere decir que el banco debe actuar con la diligencia exigible, que no es sólo la reglamentariamente prevista sino la adecuada a las circunstancias de personas, lugar y tiempo. Entre estas, cobran especial relevancia datos tales como, el perfil del cliente, los movimientos inusuales, los importes dispuestos, la hora en que se hace la operación, etc"*.

Existe jurisprudencia que, para valorar la diligencia de la entidad y, por ende, la ausencia de negligencia grave del cliente, tiene en cuenta la dirección de IP del atacante. Esto sucedió en la SAP TERUEL 74/2023 de 30 de junio, donde se observó que la dirección de IP desde la que se realizó la orden no coincidió con la IP del domicilio del cliente. Del mismo modo, se tuvo en cuenta que se solicitó a través de SMS la generación de unas claves nuevas, todo ello a través de un dispositivo que no se corresponde con el del titular de la cuenta[24].

Entre los factores personales que se han tenido en cuenta hay que destacar la confianza generada por el tercero hacia el cliente. Cabe mencionar un caso de *caller ID spoofing*[25]. En la SAP CÁCERES 555/2023 de 18 de diciembre[26], un tercero se hizo pasar por la entidad del cliente, ganándose su confianza. Todo comenzó con una llamada en la que se le comunicó que se había realizado una transferencia desde su cuenta hacia la de un tercero[27]. Al aceptar el cliente la ayuda para revertir la transferencia, el supuesto comercial obtuvo acceso a su instrumento de pago al vincular la cuenta de la clienta con otro dispositivo. La AP no aprecia negligencia grave, dado que no se observó la iniciativa del usuario y se valoró la complejidad del método empleado para generar confianza.

En ocasiones, no solo se ha atendido al contenido del mensaje, sino también a los factores personales y circunstancias del sujeto afectado. En la SAP LLEIDA 303/2024 de 19 de abril, se enjuicia un supuesto en el cual el cliente recibe un mensaje en relación con un paquete. Al ser este encargado de un taller mecánico, la AP aprecia que normalmente este recibe muchos paquetes[28]. Es más, se tuvo en cuenta por parte de la AP que el remitente del paquete era una empresa con la que habitualmente trabajaba el encargado del taller, y que también estaba esperando un pedido en ese momento.

Cabe destacar que la entidad no probó si realmente su cliente esperaba un paquete, ni si el cebo fue para apreciar una negligencia grave. Según esta sentencia, los usuarios suelen confiar más en mensajes que en correos electrónicos, de modo que tras hacer *click* y seguir otras pautas, se manifiesta que se instaló un troyano en el terminal.

Nuevamente, se recurre a la iniciativa del usuario como requisito jurisprudencial asentado[29], pero también se añade, teniendo en cuenta el Derecho penal, que estas estafas bancarias, por su naturaleza, conllevan un engaño bastante. Aunque se recurra al Derecho penal, cabe recordar que la jurisprudencia en Derecho penal no sería vinculante en el ámbito de lo civil.

Por último, el llamado deber de supervisión preventivo, según esta AP, supone: "*Pero es que, además, los proveedores de servicios de pago no sólo están obligados a rastrear las páginas web que suplantan su identidad, también están obligados a realizar un análisis de riesgo de las operaciones y a implementar medidas de seguridad acorde a los riesgos presentes*[30]".

4. Supuestos complejos

Existen ciertos supuestos en los que valorar la diligencia del usuario resulta más complicado. Uno de estos ejemplos es el llamado *SIM swapping*. El llamado *SIM swapping* consiste en la duplicación de una tarjeta *SIM*[31]. Para ser más precisos, esta duplicación permite que el defraudador obtengo el control sobre la línea telefónica del usuario sin necesidad de sustraer físicamente la tarjeta. Supondría lo anterior anular la tarjeta del cliente, de modo que podría decirse que se quedaría como un recipiente vacío.

Esto posibilita que el defraudador reciba los mensajes y llamadas destinadas al usuario, así como restablezca las contraseñas en diferentes programas y plataformas. Esta situación representa una vulnerabilidad en el sistema, especialmente cuando muchas entidades utilizan un procedimiento de autenticación reforzada basado en un segundo factor, que suele enviarse en forma de códigos de confirmación vía SMS. En este caso, el defraudador sería quien recibe dichos códigos, poniendo en riesgo la seguridad del instrumento de pago del usuario[32].

La doctrina de la STS 571/2025 de 9 de abril, resulta relevante por cuanto confirma la jurisprudencia menor y aclara una serie de aspectos. De los antecedentes de hecho, interesa destacar que el sujeto afectado compartía la titularidad de dos cuentas bancarias. Que recibió un aviso de *Google*[33], donde se le informaba que había un posible acceso no autorizado. Ese mismo día, recibió en su teléfono móvil mensajes con códigos para realización de diversas órdenes[34]; al no haber

solicitado dichas operaciones, contactó inmediatamente con su entidad bancaria. Sin embargo, la entidad no procedió a realizar ninguna medida.

Posteriormente, el cliente constató que los defraudadores habían conseguido transferir más de ochenta mil euros; cabe mencionar que se consiguieron recuperar casi treinta mil euros. Quien había alterado de las anomalías, debido a un ingreso, fue otra entidad bancaria y no la perteneciente al cliente.

Cabe subrayar que transcurrieron casi dos meses desde que el afectado contactó con su por primera vez con su entidad para informar del percance hasta que esta actuó, y fue únicamente a petición expresa del cliente.[35]

El argumento de la entidad bancaria, con el fin de defender su diligencia, consistió en que las operaciones sean realizaron conforme a la forma y el procedimiento. Es decir, que se cumplió con una autenticación de carácter reforzada[36]. Hecho este que daría lugar a una autenticación de la identidad del cliente, puesto que al prestador no le correspondería verificar si se hizo por un cliente o un tercero, sino comprobar que se realizó conforme a la forma y procedimiento pactado.

Debe destacarse también una cláusula que presenta interés y, si se recuerda la naturaleza de las normas examinadas, sería nula por vulnerar una norma de carácter imperativo. Se dice en la cláusula: "*En última instancia, en los contratos de banca digital y de cuenta corriente y/o depósitos se prevé expresamente (cláusula 8ª) que la demandada queda exenta de los perjuicios que se pudieran derivar por intromisiones ilegítimas de terceros en el sistema elegido por el cliente, fuera del control de Ibercaja Banco*".

Desde el punto de vista de la normativa nacional, el recurso de casación se funda en el art.36 y los arts.41 a 46 del RD-Ley 19/2018. El TS dilucida el significado del concepto operaciones de pago no autorizadas; las opciones eran: las realizadas por un tercero sin consentimiento del titular o, solo las que no siguiesen el procedimiento legal y contractualmente fijado. De este modo, el TS procede a interpretar la normativa nacional conforme a la Directiva 2015/2366 y el Reglamento Delegado 2018/389.

El TS establece, en lo que aquí interesa, que el marco normativo prevé un régimen de responsabilidad conformado por tres factores vinculados: el deber de notificación por parte del usuario, la atribución de la carga de la prueba al proveedor y, en caso de que no demostrara que hubiera negligencia grave o actuación fraudulenta, la asunción de responsabilidad por hecho ajeno. No obstante, no debe olvidarse la diligencia del usuario, la cual se valora a efectos de determinar si hubo o no negligencia grave o actuación fraudulenta.

El TS manifiesta que el mero hecho de que una operación haya quedado contabilizada la, es decir, registrada cumpliendo la forma y procedimiento de manifestación del consentimiento, no constituye prueba plena de que el ordenante autorizara tal operación, pero tampoco implica que hubiera actuado de forma fraudulenta o con negligencia grave.

De ese modo, una vez notificado, en plazo, que la operación no fue autorizada, el proveedor debe probar, de forma cumulativa, lo siguiente: "*que la operación de pago que no se vio afectada por un fallo técnico u otra deficiencia del servicio*[37]*, sin que el simple registro de la operación baste para demostrar que fue autorizada nique el usuario ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave fue autenticada, registrada con exactitud y contabilizada, y que no se vio*

afectada por un fallo técnico u otra deficiencia del servicio, sin que el simple registro de la operación baste para demostrar que fue autorizada nique el usuario ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave[38]".

Entonces serían operaciones no autorizadas aquellas en las cuales se hubiere cumplido con la forma y procedimiento de manifestación de consentimiento, pero que no fueron autorizadas por su titular, siempre que lo niegue. De forma que, si lo negase, corresponderá a la entidad probar la negligencia grave o fraude del cliente, en una operación que desde un punto de vista técnico se registro conforme a la forma y procedimiento.

Concluye el TS que, desde el punto de vista de los hechos, el prestador de servicios de pago no solo no demostró negligencia grave o fraude, sino que actuó de manera negligente una vez que le comunicaron los hechos. Además, pone de manifiesto el TS la necesidad de supervisar operaciones, conforme a diferentes criterios[39], potencialmente anómalas.

5. Diligencia del prestador de servicios de pago

La diligencia de los prestadores se relaciona con su labor de autentificar la operación y la entidad del ordenante, tarea que puede llevarse a cabo mediante diferentes procedimientos. Sin embargo, existe un matiz relevante: la normativa atribuye el riesgo de la falsedad de una transferencia realizada por un ordenante no titular de la cuenta al propio prestador de servicios. Desde el punto de vista del Derecho común, el argumento y sustento de la normativa se encontraría en que: *"el deudor sólo se libera pagando al verdadero acreedor por lo que, si el banco cumple una orden falsa, habrá de reintegrar en la cuenta correspondientes las cantidades cargadas*[40]". Presunción esta *iuris tantum*, que se desvirtuará si el prestador probara la negligencia o actuación grave por parte de su cliente. Asimismo, se ha dicho que los prestadores asumen ese riesgo porque el sistema digital implica un ahorro de costes y representa un negocio rentable para las entidades bancarias[41].

La complejidad de este asunto, como se evidenciará en sentencias posteriores, consiste en que, salvo que exista negligencia grave o actuación fraudulenta por parte del cliente, cuando un defraudador consigue obtener acceso al instrumento de pago, se establece una presunción que casi tiene una naturaleza *iuris et de iure*. Esto significa que, más que en problemas de seguridad del sistema, lo que debe demostrar el prestador es un factor conductual del cliente, es decir, que este haya actuado con negligencia grave o de forma fraudulenta. Si bien es cierto que el factor seguridad tiene su relevancia, ningún sistema es infalible. Si se observan las cosas con detenimiento, para que un tercero realice su propósito, en ciertas ocasiones, debe buscar al cliente como sujeto vulnerable, puesto que la acción directa contra el proveedor sería harta complicada, obviamente, debido a las capas de seguridad existentes.

Si bien es cierto que el cliente, al igual que la entidad, tiene unas obligaciones de custodia, su falta de diligencia se reconduce por la norma a la presencia de una negligencia grave[42]. Es decir, bien puede probar que cuenta con un sistema robusto, pero al haber conseguido un tercero llevar a cabo operaciones, sin consentimiento del titular, se presupone, salvo que se probara la negligencia grave o actuación fraudulenta, que hubo un fallo en el sistema de seguridad[43].

En otras ocasiones ha de atenderse a la diligencia del proveedor, pero esta puede resultar insuficiente a efectos de eximirse de la responsabilidad por hecho ajeno. El supuesto de hecho enjuiciado por la SAP ISLAS BALEARES 132/2023 de 17 de febrero permite observar tal hecho. En la configuración del sistema de seguridad de la entidad, al producirse una serie de operaciones se preveía un bloqueo preventivo[44]. Si bien en Primera Instancia se otorgó la razón a la entidad, la AP revoca dicho pronunciamiento. El motivo de fondo tiene que ver con uno de los principales argumentos de estos proveedores. Es decir, estima la AP que no es suficiente, conforme a la normativa, que la entidad hubiera probado que los movimientos fueran autenticados, registrados con exactitud y contabilizados sin fallos técnicos ni deficiencias[45]. Para no responder por un hecho ajeno, sumado a lo anterior, debió de probar la negligencia grave o actuación fraudulenta de su cliente.

A veces, para valorar la diligencia del prestador de servicios se han valorado una serie de hechos[46]. En la SAP LA RIOJA 49/2023 de 17 de febrero se analiza una situación en la cual, una vez que la clienta se percató de que su instrumento de pago se encontraba comprometido, contactó con la entidad bancaria. Esta consiguió revertir dicha orden, conceptuando la reversión como: "devolución posible fraude". Sin embargo, a pesar de tal actuación, sí que se consolidaron unos pagos. La AP aprecia una inconsistencia en la actuación, pues primeramente se reconoce el fraude, pero llegado el procedimiento se niega debido a la consolidación del pago[47]. Sumado a lo anterior, la falta de diligencia también se aprecia porque se tiene en cuenta, que una vez que accedió el tercero a la cuenta del cliente este elevó el límite de gasto en un trescientos por cien.

Una falta de diligencia se apreció, por parte del prestador de servicios de pago, en la SAP CÁCERES, 29/2024 de 24 de enero. Se pondera y tiene en cuenta la actitud del cliente, quien al percatarse del fraude contacta inmediatamente con la entidad para proceder al bloqueo de la cuenta. Sin embargo, una hora después, se extrae dinero mediante la tarjeta supuestamente bloqueada[48]. Hay que tener en cuenta que dicho proveedor incumplió con la obligación del art.42.1.e (RD-Ley 19/2018[49]), precepto en el cual se dice que, una vez recibida la notificación del supuesto ilícito, debe impedir la utilización del instrumento de pago. La notificación al proveedor de servicios de pago también tiene un efecto en cuanto al alcance de responsabilidad del cliente. Es decir, se minoran las exigencias de diligencia cuando el usuario hubiera notificado, pero la entidad no hubiera impedido la utilización del instrumento de pago. La norma establece que, ante tal inacción, el usuario no responderá si posteriormente se utilizara el instrumento de pago aunque hubiera habido negligencia grave por su parte. La norma reduce la responsabilidad posterior del cliente, dejando a salvo su responsabilidad posterior solo cuando hubiera actuado de manera fraudulenta[50].

Respecto de la prueba de la falta de diligencia, la jurisprudencia se ha pronunciado sobre la necesidad de esta, y no que la entidad aporte unas meras conjeturas. Esto último resultaría insuficiente para demostrar una negligencia grave[51].

6. Valor de los avisos y advertencias

Las entidades suelen remitir avisos y advertencias relacionados con diversos instrumentos de pago, cuyo objetivo es minimizar los riesgos de fraude. Sin

embargo, la jurisprudencia ha mostrado reticencia a otorgar a estos mensajes un valor suficiente, manifestando en multitud de ocasiones la necesidad de implementar medidas de control y seguridad efectivas. Puesto que no son suficientes las medidas genéricas, mediante las cuales se remiten mensajes y avisos estereotipados de cuidado, de modo que se ha llegado a decir que tales avisos son: *"fórmulas predispuestas vacías de contenido*[52]". De esta forma, si se atribuyera el valor que las entidades alegan, el riesgo se trasladaría hacia los clientes, y no son estos quienes tiene que prevenir o averiguar las diferentes modalidades de riesgos de su sistema.

7. Valor de los avisos y advertencias

En relación con supuestos de *phishing* y sus derivados, uno de los argumentos traídos por las entidades ha consistido en el contenido del mensaje. En la SAP CÁCERES 531/2023 de 28 de noviembre se enjuicia un supuesto donde se presta atención al contenido del mensaje. La entidad demandada alega que hubo negligencia grave por parte de su cliente debido a que, en el mensaje recibido, de su lectura se deduce que el objeto consistía en el registro de un nuevo dispositivo, y no para poder seguir siendo usuario de banca online[53].

Para la entidad la negligencia grave debe apreciarse por no detenerse a la lectura del mensaje, de cuyo contenido se desprende, de forma sencilla, el objeto de este. Es decir, que de haberlo leído sabría que la introducción de las credenciales tendría por objeto el cambio de dispositivo de confianza.

La AP, refrenda el pronunciamiento de primera instancia y aprecia que no hubo un grado significativo de falta de negligencia. En relación con el concepto de negligencia se dice que: *"la negligencia que determina la responsabilidad del 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 haya podido ser inducido por un delincuente profesional. Pero es más, tomando como parámetro del actuar negligente el artículo 1104 del Código Civil, que exige la diligencia asociada a la naturaleza de la obligación y a las circunstancias personales, de tiempo y lugar, tampoco cabría calificar de negligencia grave la conducta seguida por Dña. Isabel en atención al método fraudulento empleado, de complejidad y grado de perfección difícilmente detectable por un cliente de las características de la demandante, pues el mensaje que recibe el usuario imita perfectamente el diseño utilizado por su entidad bancaria, por lo que ni siquiera el texto del mensaje (vas a registrar un nuevo dispositivo) tiene entidad suficiente para detectar el engaño o fraude, pues una vez generada la confianza en el usuario de que se trata y encuentra ante su entidad bancaria, la propia dificultad del texto (que la propia recurrente subraya) induce a cliquear el enlace*[54]".

Ante un supuesto de hecho idéntico al anterior, una valoración diversa puede encontrarse en SAP A CORUÑA 17/2023 de 25 de enero[55]. El contenido del mensaje era el siguiente: "*Carmelo Un dispositivo no autorizado está conectado a su cuenta online. Si no reconoce este acceso, verifique inmediatamente: https://s.id/EJKaN*". El cliente una vez pulsó en el enlace fue dirigido a una página web que simulaba la correspondiente a ABANCA, introduciendo de este modo sus datos bancarios.

También recibió una llamada, de un sujeto que se hizo pasar por empleado de ABANCA, solicitando los códigos que este recibió mediante SMS. Al cortarle este la llamada de forma abrupta se percató de que algo no andaba bien, de modo que llamó a la entidad bancaria.

El encaje y lectura del supuesto de hecho se hace por remisión a dos preceptos del RD-Ley 19/2018. En concreto, el art.41 sobre obligaciones del cliente y el 46, sobre la responsabilidad del ordenante en operaciones de pago no autorizadas. Se aprecia que en este caso la negligencia grave proviene de una reiteración de una conducta. Es decir, el cliente no adoptó todas las medidas razonables con el fin de proteger sus credenciales de seguridad personalizadas. La clave y la puesta en conexión con esta obligación y el atributo de la gravedad proviene de varios hechos. En primer lugar, no se leyó el mensaje de forma completa. Ahora bien, a lo anterior debe sumarse la llamada del supuesto empleado de la entidad, quien solicitó al cliente los códigos que recibió mediante SMS. En relación con esto último, antes de proceder al envío de las claves, el cliente hubo de leer que la clave tiene por objeto la autorización para una transferencia de 9.132 euros.

En definitiva, en este supuesto de hecho, para apreciar la gravedad, la AP refiere la aparición de tres negligencias. La primera, relativa a pinchar un enlace (cuestión que lo entiende más o menos comprensible), la segunda, que consistió en facilitar el usuario y contraseña (hecho este al cual atribuyen mayor gravedad), y la tercera, la confirmación de la operación (acto este considerado temerario por la AP).

La valoración de la AP merece tener en cuenta el factor del impulso psicológico. Es decir, los ataques de *phishing* y sus variantes, buscan aprovechar impulsos y reacciones rápidas y casi automáticas. La propia configuración del mensaje, tanto en web o correo, mediante su apariencia de realidad dan lugar a un impulso de actuar lo más rápido posible. La supuesta alerta y la apariencia, sin realizar un análisis detallado el cliente, lo empujan a actuar lo antes posible, dada la confianza generada y la dificultad de identificar, en muchas ocasiones, el fraude que se pretende llevar a cabo. De este modo, debe ponderarse hasta qué punto la técnica de ingeniería social ha ido más allá de un mero impulso, de forma que hubiera indicios suficientes para decir que hubo más fases o contenido para no actuar con un mero impulso. Los seres humanos son impulsivos por naturaleza, sin embargo, para contemplar la negligencia grave, no basta con tener en cuenta dicho factor, sino que debe ponderarse junto con otras circunstancias del caso. Circunstancias estas que debe ponerlas de manifiesto y probarlas el proveedor de servicios de pago.

Tal es así, que sin tener en cuenta otros posibles detalles no manifestados, en SAP CÁCERES 267/2024 de 1 de julio o SAP ASTURIAS 372/2024 de 9 de julio[56], se dice que no hubo negligencia grave del cliente por no leer que el contenido del mensaje consistía en la vinculación de un nuevo dispositivo[57].

Respecto a correos electrónicos, también conviene tener en cuenta la valoración, en relación con situaciones en las cuales el mensaje contiene fallos gramaticales. En la SAP PONTEVEDRA 539/2021 de 21 de diciembre, se manifiesta que el usuario a través de una lectura se hubiera dado cuenta o, al menos, podría haber sospechado, con relación a esa imprecisión textual. No obstante, debido a la participación de un tercero, llevando a cabo un engaño previo, ganándose su confianza, sostiene la AP que ese hecho le llevó al cliente a que no llevara a cabo una lectura atenta. Sin embargo, del contenido de la sentencia, se extrae que la participación del tercero únicamente

consistió en el envió del correo. Es decir, a diferencia de otros supuestos de hecho, donde la confianza se va ganando paulatinamente, aquí no sucedió eso.

De la sentencia se extrae también, que la entidad al proporcionar el SMS para la vinculación al sistema de *Samsung pay*, la clienta no pudo prestar atención porque la marca de su terminal coincidía con la del sistema de pago. Es más, se envía el código, pero tampoco se dice desde que terminal se pretendía acceder. Es decir, la ubicación del terminal, la marca, el número de teléfono etc.; datos estos que podrían haber sido útiles para valorar una posible negligencia grave.

8. Supuestos negligentes

Existen, quizás, pocos casos claros en la jurisprudencia donde se manifieste de forma clara que la operación cumplió con todos los requisitos y que hubo negligencia del cliente. Un ejemplo de ello lo constituye la SJPI Nº14 de VALLADOLID 324/2022 de 25 de octubre, en la que para valorar la posible responsabilidad de las entidades bancarias se dice que es necesario ponderar de forma conjunta si existió negligencia grave por parte del cliente, hecho este que deberá probar el proveedor, y, por otro lado, si este último cumplió con todas las exigencias de seguridad que le vienen impuestas. En este caso las operaciones fueron realizadas por la sobrina del titular, el cual se encontraba hospitalizado. Cabe destacar que el mismo le proporcionó la tarjeta y las claves secretas. De este modo, ante tales hechos, la entidad bancaria no tiene responsabilidad alguna.

Con anterioridad se puso de manifiesto que la carga de la prueba corresponde al prestador de servicios de pago. Sin embargo, en determinadas ocasiones, una serie de hechos pueden genera indicios que eximen a la entidad de responsabilidad. En la SAP CUENCA 224/2024 de 30 de septiembre se analiza un caso interesante desde el punto de vista fáctico. Cabe destacar que el cliente exige responsabilidad a su entidad, pero el detalle relevante consiste en que hubo movimientos reiterados en su cuenta con anterioridad a cinco meses de la reclamación. Refiere la AP que hubieron reiterados ingresos a favor del usuario, lo que supondría un conocimiento de este respecto de las entradas y salidas. Además, consta probado que el usuario solicitó la consulta de extractos, lo que indicia que estaba al tanto de los movimientos realizados. De esta forma, para la AP, si bien no hay una prueba exhaustiva de la entidad, los hechos mencionados la conducen a sostener que no hay indicio alguno de actuación fraudulenta por parte de tercero. Los hechos traídos a colación deben suponer, según la AP, un conocimiento del usuario y consentimiento respecto a los movimientos que se fueron realizando durante los últimos cinco meses.

A diferencia de otros supuestos de hecho, en la sentencia mencionada, se observa que el usuario no actuó con la celeridad vista en otros casos. Como bien se dijo antes, es cierto que la norma establece que el usuario cuenta con un plazo de trece meses, desde la fecha del adeudo[58] para notificar una operación no autorizada. Sin embargo, hechos como la consulta de los movimientos[59], mediante petición, supone que este tuvo ya conocimiento. Parece ser que para la AP incluso podría tratarse de una actuación fraudulenta. El supuesto mencionado ha permitido observar una cierta flexibilidad en la interpretación normativa y en la carga de la prueba.

V. CONCLUSIONES

I. La Directiva 2015/2036, el RD-Ley 19/2018 y el Reglamento Delegado 2018/39, establecen un conjunto de normas orientadas a reforzar el mercado único europeo. La utilización de diferentes instrumentos de pago digitales es una realidad consolidada. No obstante, a pesar de la neutralidad tecnológica que caracteriza a la norma, existen otros riesgos frente a los cuales se debe combatir.

II. A pesar de la seguridad implantada por los proveedores de servicios de pago y otros sujetos, persiste la posibilidad de que terceros logren vulnerar dichas medidas, ya sea a través de dicho prestador o de forma indirecta, mediante ataque dirigidos al cliente.

III. La jurisprudencia interpreta el requisito de seguridad de manera amplia, estableciendo que los proveedores no solo han de implantar medidas eficaces y seguras, sino que también están obligados a un deber de seguridad preventiva que les permita detectar situaciones anómalas.

IV. Hoy en día, a gran parte de la población no les es ajeno el concepto *phishing*. Las estafas informáticas se multiplican con el avance tecnológico, ya que, a medida que evoluciona la tecnología, también lo hacen los métodos de los delincuentes. Sin embargo, en numerosas ocasiones surge la pregunta: ¿ante tales situaciones, qué responsabilidad asume el proveedor hacia su cliente?

V. Tal como se ha expuesto a lo largo de este análisis, la jurisprudencia interpreta la responsabilidad de estos proveedores como un supuesto de responsabilidad cuasi-objetiva. Esto significa que corresponderá probar a la entidad ciertos aspectos. Estos aspectos no se limitan únicamente a demostrar que cuenta con herramientas eficaces y que la operación fue registrada conforme a la forma y procedimiento establecidos, en algunos casos empleando un segundo factor de autenticación

La norma establece que, en caso de que el cliente niegue haber autorizado una operación, además de probar esa exactitud de la operación, corresponde a la entidad demostrar la negligencia grave o intención fraudulenta del cliente. Esta interpretación implica que, si el proveedor no logra acreditar lo anterior, deberá responder ante el cliente, al atribuirse el fraude ocurrió debido a un fallo en su sistema de seguridad.

VI. De este modo, existe una doble valoración de la diligencia: más flexible a favor del cliente y más rigurosa respecto al proveedor. La negligencia grave, si bien deberá apreciarse caso por caso, no puede basarse en meras conjeturas ni en una simple falta de diligencia, sino que la gravedad exige algo más. La respuesta no es única, sino que se basa en un sistema casuístico de suma y resta, en función de la diligencia y actuación de ambos sujetos.

VII. La responsabilidad por hecho ajeno implica para los proveedores una necesidad constante de mejorar sus sistemas de seguridad, especialmente en el ámbito preventivo, debido a la más que favorable interpretación jurisprudencial hacia el cliente. Por otro lado, la forma en que se valora la diligencia de ambos partes dificulta que se reconozca una concurrencia de culpas y, por ende, un reparto del riesgo económico derivado del perjuicio.

VI. JURISPRUDENCIA

- STS 571/2025 de 9 de abril
- SAP MADRID 112/2025 de 17 de marzo
- SAP SALAMANCA 173/2025 de 11 de marzo
- SAP ASTURIAS 24/2025 de 28 de enero
- SAP MADRID 484/2024 de 14 de noviembre
- SAP NAVARRA 1217/2024 de 18 de octubre
- SAP ASTURIAS 463/2024 de 1 de octubre
- SAP CUENCA 224/2024 de 30 de septiembre
- SAP LUGO 307/2024 de 10 de septiembre
- SAP CÁCERES 267/2024 de 1 de julio
- SAP BARCELONA 501/2024 de 26 de junio
- SAP ASTURIAS 372/2024 de 9 de julio
- SAP BALEARES 342/2024 de 19 de junio
- SAP LA RIOJA 253/2024 de 30 de mayo
- SAP NAVARRA 702/2024 de 27 de mayo
- SAP MADRID 236/2024 de 21 de mayo
- SAP LLEIDA 303/2024 de 19 de abril
- SAP CÁCERES 64/2024 de 20 de febrero
- SAP CÁCERES, 29/2024 de 24 de enero
- SAP CÁCERES 555/2023 de 18 de diciembre
- SAP CÁCERES 531/2023 de 28 de noviembre
- SAP TERUEL 74/2023 de 30 de junio
- SAP ISLAS BALEARES 132/2023 de 17 de febrero
- SAP LA RIOJA 49/2023 de 17 de febrero
- SAP ZARAGOZA 55/2023 de 17 de febrero
- SJPI PAMPLONA 59/2023 de 6 de febrero
- SAP ZARAGOZA 34/2023 de 1 de febrero
- SAP A CORUÑA 17/2023 de 25 de enero
- SJPI VALLADOLID 8/2023 de 11 de enero
- SAP CÁCERES 555/2023 de 18 de diciembre
- SJPI Nº14 de VALLADOLID 324/2022 de 25 de octubre
- SAP MADRID 184/2022 de 20 de mayo
- SJPI TORRENT 105/2022 de 11 de abril
- SAP PONTEVEDRA 539/2021 de 21 de diciembre

NOTAS

[1] En adelante, Directiva 2015/2366. Por otro lado, esta norma se ha visto transpuesta en el ordenamiento jurídico español a través del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera; en adelante RD-Ley 19/2018. Tampoco cabe olvidar la importancia del 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; en adelante, Reglamento Delegado 2018/389.

[2] Llama la atención que no exista una gran diferencia numérica respecto de los fraudes informáticos, en cuanto a la edad de los perjudicados se refiere. Informe sobre la criminalidad en España (2023). Sistema estadístico de criminalidad, pg.32.

Disponible en:

https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Informe-Cibercriminalidad_2023.pdf.

[3] Por ejemplo, debe tenerse en cuenta que gracias a la IA también están aumentando los casos de *pig butchering*, donde se utilizan personalidades famosas gracias a la IA para entablar una relación de confianza.

Desde un punto de vista terminológico interesa remitirse a la siguiente publicación de INTERPOL: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2024/INTERPOL-insta-a-acabar-con-el-uso-del-termino-pig-butchering-ya-que-ahonda-en-el-dano-que-sufren-las-victimas-en-linea.

Aunque muchos de estos conceptos son susceptibles de un reproche penal, conviene tener en cuenta la posible responsabilidad de la entidad bancaria, según los casos.

[4] La referencia en este comentario, sobre la base del estudio jurisprudencial, se centrará en el concepto de consumidor. Cabe manifestar que la Directiva 2015/2366 prevé diferente alcance según la condición subjetiva del cliente. Puede afirmarse que la protección tiene un contenido imperativo cuando se trata de un consumidor, y un carácter más o menos dispositivo según otros tipos de sujetos. El ejemplo para mencionar lo constituye la posibilidad, según la Directiva 3025/2366, de ampliar la protección de las microempresas. En el considerando cincuenta y tres (así como el art.38) y 61 se menciona la posibilidad de otorgar un nivel de protección equivalente al de los sujetos que son consumidores. En lo que aquí interesa, dicha elevación aparece en el preámbulo del RD-Ley 19/2018, así como también, por ejemplo, el art.28 y 34 de dicha norma.

[5] A lo largo de la Directiva 2015/2366 y el RD-Ley 19/2018 aparecen una pluralidad de sujetos que llevan a cabo diferentes prestaciones. Un ejemplo podría ser los proveedores de servicios de pago y los proveedores de servicios de iniciación de pagos. Los primeros, por ejemplo, se reconduciría, según el caso, a una entidad bancaria (BBVA). Mientras que, a modo de muestra, un proveedor de servicios de iniciación de pagos lo sería, BIZUM. Las diferencias conceptuales establecidas por la normativa son relevantes, puesto que, dependiendo de cada tipo de prestación, el sujeto será responsable únicamente respecto de las partes de la operación que estén bajo su control. Esta mención aparece, por ejemplo, en el considerando setenta y cuatro de la Directiva 2015/2366. Véase también el art.61.1 del RD-Ley 19/2018.

[6] Entiéndase este concepto en sentido amplio, abarcando a todos los sujetos que se designan en la Directiva 2015/2366, en su art.1, como proveedores de servicios de pago.

[7] El término seguridad aparece en multitud de ocasiones en la Directiva 2015/2366, así como también en las otras dos normas objeto de estudio. Véanse, por ejemplo, los considerandos noventa y uno, noventa y cinco y noventa y seis, donde se hace referencia a los responsables de las medidas de seguridad y al objetivo perseguido, que consiste en minimizar el riesgo de fraude.

[8] Concepto este relevante a efectos de realizarse operaciones. Se recomienda consultar los considerandos treinta, noventa y cinco, así como el art.4.31, que se refiere a credenciales de seguridad personalizadas, de la Directiva 2015/2366.

[9] Un PIN.

[10] Un teléfono móvil concreto e identificado.

[11] Por ejemplo, una huella dactilar o un mecanismo que permita el reconocimiento facial.

[12] Los tres elementos contemplados en la definición son relevantes, ya que el art.4 del Reglamento Delegado 2018/389 establece que, para que se considere que existe autenticación reforzada, deben emplearse al menos dos de la definición citada *ut supra*.

[13] Considerando primero del Reglamento Delegado 2018/389, así como el art.2 de dicha norma.

[14] La prueba de que hubo autenticación reforzada corresponde al proveedor de servicios de pago. SAP BALERARES 169/2025 de 10 de marzo.

[15] La SJPI PAMPLONA 59/2023 de 6 de febrero, SJPI TORRENT 105/2022 de 11 de abril, SAP SALAMANCA 173/2025 de 11 de marzo, abordan, respecto del consentimiento, la aparición de tres sujetos dentro del proceso de ordenación de una transferencia. Asimismo, esta última sentencia enfatiza la relación del consentimiento y el deber de identificación de la identidad del cliente, de manera que se entienda autorizada la operación. Por su parte, SAP NAVARRA 702/2024 de 27 de mayo presenta interés por cuanto, en relación con el certificado REDYS, manifiesta que no verifica la identidad real del usuario ordenante. En el mismo sentido: SAP NAVARRA 1217/2024 de 18 de octubre.

[16] Idea esta que se deduce, de forma nítida, de la reciente STS 571/2025 de 9 de abril; sentencia que se analizará con posterioridad.

[17] La misma postura y consecuencia se repite en el art.36 del RD-Ley 19/2018.

[18] Esta facultad respondería a cuestiones de seguridad, así como a la necesidad de cerciorase, en determinadas situaciones, de que es realmente el cliente quien propone una modificación significativa respecto al gasto en operaciones. Véanse, a este respecto, el art.40 del RD-Ley 19/2018 y el art.68 de la Directiva 2015/2036.

[19] SJPI Nº3 de Torrent 105/2022 de 11 de abril. Además, se recuerda en esta sentencia que de la normativa de la UE ser derivan una serie de obligaciones para el prestador de servicios, encaminadas a la detección de transferencias de pago no autorizadas o fraudulentas.

[20] También, dicho de otro modo, una responsabilidad por culpa *in vigilando*, SAP SALAMANCA 173/2025 de 11 de marzo. Por otro lado, el significado atribuido a este tipo de responsabilidad consiste en que se presume que el titular de la cuenta no ha autorizado la operación, SJPI VALLADOLID 8/2023 de 11 de enero.

[21] La jurisprudencia argumenta que el motivo de fondo respecto a dicha distribución establecida por la norma reside en ese hecho. SAP ZARAGOZA 34/2023 de 1 de febrero.

[22] Sobre la exención de responsabilidad, si bien en la sentencia se menciona que constituiría una cláusula abusiva, conviene matizar que su nulidad proviene por vulnerar una norma de carácter imperativo. Sobre la nulidad por vulnerar norma imperativa, véase la SAP ZARAGOZA 34/2023 de 1 de febrero o SAP TERUEL 74/2023 de 30 de junio.

[23] Según parece, el autor se parecía al titular de la cuenta; pero también su firma coincidía.

[24] Supuesto de hecho de *SIM swapping*. Es relevante lo manifestado en esta sentencia por cuanto se otorga importancia a la comprobación de que se trata de un dispositivo de confianza.

[25] Se caracteriza por una situación en la cual un tercero se hace pasar por la entidad del cliente. A continuación, se proporciona un enlace del INCIBE explicando en qué consiste dicho concepto: https://www.incibe.es/ciudadania/blog/spoofing-telefonico-cuando-la-llamada-parece-legitima.

[26] Véase también en la SAP CÁCERES 64/2024 de 20 de febrero.

[27] Por una cantidad cercana a los 5.000 euros. Véase también un supuesto cuyo inicio se dio a través de una llamada en: SAP BALEARES 342/2024 de 19 de junio.

[28] Debe recordarse la protección hacia el microempresario, y que el RD-Ley 19/2018, haciendo uso de la facultad prevista en la Directiva 2015/2036, ha elevado la protección hacia estos sujetos.

[29] Concepto este que aparece en la Directiva 2015/2036 en su considerando setenta y dos. Y a raíz de ello manifiesta la AP: *"Así pues, la negligencia grave debe surgir como consecuencia de la iniciativa del usuario, no como consecuencia de la iniciativa de un delincuente profesional, porque el engaño típico de la estafa excluye la negligencia grave. Si el phishing está caracterizado por el "engaño bastante", que es algo más que un burdo engaño, en el que caen multitud de personas, la víctima nunca puede haber actuado con negligencia grave, que es la más grave falta de diligencia"*.

[30] Con relación a este aspecto, es útil recordar el considerando primero, art.2, art.18 del Reglamento Delegado 2018/389. Se habla en la SAP MADRID 184/2022 de 20 de mayo de la necesidad de implantar tecnología *antiphishing*. En el mismo sentido, SAP PONTEVEDRA 539/2021 de 21 de diciembre. Hecho este que para las AP impediría al defraudador utilizar las credenciales del usuario.

[31] STS 571/2025 de 9 de abril.

[32] De modo que la utilización de alternativas como segundo factor, a través de las cuales el mensaje se envía a la propia aplicación de la entidad o a una aplicación específica de autenticación, dicho riesgo debería reducirse de forma notoria.

[33] Con posterioridad, dicho aviso también lo recibió otro familiar; cuya cuenta, *Google,* la bloqueó.

[34] Resulta extraño que le llegase un SMS de confirmación, por cuanto hay que tener en cuenta que el *sim swapping* da lugar a que la víctima se quede sin servicio telefónico. Véase para ello la explicación de INCIBE: https://www.incibe.es/ciudadania/blog/sim-swapping-como-evitar-esta-estafa. Quizás pudo ser un caso de *phishing*, pero del relato fáctico no queda muy claro que ocurrió desde un punto de vista tecnológico.

[35] Este hecho puede resultar relevante respecto al deber de previsión, diligencia y conocimiento de un potencial problema de seguridad respecto de un cliente concreto, con precedencia, y que ninguna pesquisa se realizó por la entidad. Además de que se comunicó, con anterioridad a los movimientos cuantiosos, otro cargo en *Google Play* y *Google Ads*.

[36] Con mayor precisión, se tuvo acceso a la cuenta, pero también se recibió el segundo factor que consistió en una clave dinámica que se envía al teléfono móvil facilitado por el titular.

[37] Que se refiere a que abarca cualquier falta de diligencia o mala praxis en el servicio prestado, según el tipo de actividad.

[38] Misma idea en: SAP MADRID 112/2025 de 17 de marzo.

[39] Por ejemplo, en SAP MADRID 236/2024 de 21 de mayo, se enjuició un caso de *sim swapping*, donde se probó que la demandante se encontraba en Murcia y que la operación se realizó desde Gibraltar. Cabe manifestar que la entidad bancaria no demostró cómo los autores obtuvieron la duplicación de la tarjeta, lo que pudiera haber incidido en una posible negligencia grave. Aunque se debe reconocer en estos supuestos, que en no pocas ocasiones, será fácil demostrar la falta de diligencia del cliente y el cómo se produjo el duplicado. Véase también SAP BARCELONA 501/2024 de 26 de junio, donde se expone que: *"No pudiendo interpretarse una ingerencia de tercero como negligencia grave de la usuaria, siendo negligente BBVA que no utilizó las medidas de Seguridad adecuadas para asegurar la identidad del ordenante y autenticación de la operación, pues las nueve transferencias se ordenaron desde Varsovia (Polonia)"*. Donde no se acreditó ninguna conexión entre la titular y el tercer sujeto ubicado en Polonia, ni tampoco se hizo un examen del terminal de la afectada, ni solicitado.

[40] SJPI PAMPLONA, 59/2023 de 6 de febrero.

[41] SAP ZARAGOZA 55/2023 de 17 de febrero.

[42] Es el art.41 del RD-Ley 19/2018 el que establece las obligaciones del usuario. Ahora bien, el significado y alcance de esta obligación se completa, por un lado, con el art.43 y, por otro, con el 44 que refiere al concepto de negligencia grave.

[43] Se llega a manifestar en la SAP ZARAGOZA 55/2023 de 17 de febrero: "*Es decir que la seguridad o inseguridad en el canal de comunicación prestador y cliente opera a cargo y riesgo del proveedor*".

[44] Desde el punto de vista de los hechos, puede resultar controversial la SAP LUGO 307/2024 de 10 de septiembre, donde la entidad afirma que realizó de oficio un bloqueo preventivo. Sin embargo, dicho hecho parece contradecirse a través del certificado de la entidad *Redys*.

[45] Obligación esta, en materia de prueba de autenticación, recogida en el art.44.1 del RD-Ley 19/2018. Obligación esta cuyo sentido y significado se tiene que completar con el apartado segundo y tercero de dicha norma.

[46] Es más, se ha dado que una sustracción fraudulenta de los datos de una entidad fuera tenida en cuenta en un posterior supuesto de hecho en el que el titular se ve afectado a raíz de un SMS. SAP ASTURIAS 24/2025 de 28 de enero.

[47] Si bien en el contrato se estipuló: "*otorgar plena validez jurídica a las operaciones realizadas mediante cualquier tipo de claves y/o códigos que permitan la identificación personal del mismo, dando como válidas y propias las operaciones que sean realizadas empleando las claves o códigos previstos en este contrato*". Hay que recordar el carácter imperativo de la norma objeto de estudio, cuando de consumidor se trate.

[48] Hay que tener en cuenta que el cliente cumplió con la obligación prevista en el art.61.1. b de la Directiva 2015/2036, comunicando sin demora indebida en cuanto tuvo conocimiento del ilícito. Obligación esta transpuesta al RD-Ley 19/2018 en el art.41. Sobre el plazo de notificación para operaciones no autorizadas, téngase en cuenta que el art.71 de la Directiva 2015/2036 establece un plazo de notificación, en caso de operaciones de pago no autorizadas, de un plazo máximo de trece meses desde la fecha del adeudo. En el RD-Ley 19/2018, dicho plazo se recoge en el art.43.

[49] Obligación esta que en la Directiva 2015/2036 se encuentra recogida en el art.70.1. e.

[50] RD-Ley 19/2018 art.46.3; Directiva 2015/2036 art.74.3.

[51] SAP LA RIOJA 253/2024 de 30 de mayo.

[52] SAP LA RIOJA 49/2023 de 17 de febrero.

[53] Cabe añadir que en esta sentencia se manifiesta que las entidades gozan de una doble condición, la de beneficiario, pero también de generadoras de riesgo.

[54] El mismo argumento sobre la necesidad de iniciativa se encuentra en: SAP CÁCERES 555/2023 de 18 de diciembre o SAP LLEIDA 303/2024 de 19 de abril.

[55] Compárese esta sentencia con la en SAP CÁCERES 64/2024 de 20 de febrero. Decisión esta última, con cierto parecido, pero en la que no se apreció negligencia grave debido al método empleado, su complejidad y la necesidad de ser un experto en la materia para detectar la ingeniería del fraude del caso.

[56] *Idem* SAP ASTURIAS 463/2024 de 1 de octubre o SAP ASTURIAS 24/2025 de 28 de enero.

[57] En otras sentencias se ha puesto de manifiesto, que si bien se certificó el envió de código mediante SMS, no se hizo así respecto al número que se ha enviado ni tampoco el terminal. SAP NAVARRA 702/2024 de 27 de mayo. Hecho este que también podría servir para probar la identidad real del ordenante.

[58] Art.43 RD-Ley 19/2018.

[59] Movimientos realizados, tanto activos como pasivos.