Uso fraudulento

La LSP regula un sistema común de derechos y obligaciones para proveedores y usuarios de servicios de pago y delimita, con el carácter de estatuto legal irrenunciable, las consecuencias jurídicas de las operaciones de pago no autorizadas, fijando las responsabilidades tanto del usuario como del proveedor de servicios de pago cuando el primero niegue la autoría de las operaciones

Entre las peculiaridades de la ley, cabe destacar:

- Es aplicable a «cualquier mecanismo personalizado [...] utilizado (por el usuario del servicio de pago) para iniciar una orden de pago». Es decir, resulta igualmente aplicable a las libretas de ahorro y a otros instrumentos de pago, además de a las tarjetas de pago.

- La fijación de un plazo máximo general para comunicar a la entidad que se ha producido una operación no autorizada o ejecutada incorrectamente, estableciéndose este en 13 meses desde la fecha de adeudo o abono.

- El límite de responsabilidad se aplicará, ente otros supuestos, cuando el instrumento de pago hubiera sido sustraído, no necesariamente robado, por lo que no se requiere que en la pérdida de la posesión haya intervenido violencia o intimidación.

- No se aplicará el régimen de responsabilidad previsto al dinero electrónico si la entidad emisora no tuviera capacidad para bloquear la cuenta o el instrumento de pago.

- Cuando el usuario no sea un consumidor, las partes pueden convenir que no resulten de aplicación determinados preceptos.

Notificación de operaciones de pago no autorizadas o ejecutadas incorrectamente

Cuando un usuario de servicios de pago —por ejemplo, el titular de una tarjeta— tenga conocimiento de que se ha producido una operación de pago no autorizada o ejecutada incorrectamente, deberá comunicarlo a la entidad, sin tardanza injustificada.

Salvo en los casos en los que el proveedor de servicios de pago no le hubiera proporcionado o hecho accesible al usuario la información correspondiente a la operación de pago, la comunicación a la que se refiere el apartado precedente deberá producirse en un plazo máximo de trece meses desde la fecha del adeudo o del abono, si bien, en caso de que el usuario no sea un consumidor, las partes podrán pactar un plazo inferior (artículo 29 de la LSP).

…/…

Prueba de la autenticación y ejecución de las operaciones de pago

Corresponde a la entidad demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico o por cualquier otra anomalía (artículo 30 de la LSP). No obstante, el registro por el proveedor de servicios de la utilización del instrumento de pago no bastará necesariamente para demostrar que la operación fue autorizada por el ordenante —titular de la tarjeta— ni que este actuó de manera fraudulenta o incumpliendo deliberadamente o por negligencia grave una o varias de las obligaciones que le incumben como usuario del servicio de pago, a saber: i) utilizar el instrumento de pago de conformidad con las condiciones que regulen su emisión y utilización; ii) tomar todas las medidas razonables a fin de proteger los elementos de seguridad personalizados de que vaya provisto, y iii) en caso de extravío, sustracción o utilización no autorizada del instrumento de pago, notificarlo sin demoras indebidas a la entidad, en cuanto tenga conocimiento de ello, debiendo la entidad adoptar las medidas necesarias para evitar, desde que se produce dicha comunicación, la utilización ilegítima del instrumento de pago por terceros no autorizados, debiendo contar esta con medios adecuados y gratuitos a fin de posibilitar, en todo momento, que el titular efectúe la comunicación de la operación de pago cuya autoría no reconoce.

La acreditación de las operaciones variará dependiendo del uso dado a la tarjeta, siendo los más habituales los de reintegros en efectivo y los de pago en comercios. En el primero de los casos, la entidad deberá acreditar mediante sus propios registros internos y/o los del cajero en los que se llevó a cabo la operación que esta fue correctamente registrada y que no se vio afectada por ninguna deficiencia. En el segundo de los casos, esto es, cuando la tarjeta se usa como medio de pago en un comercio, cabe exigir a la entidad emisora de la tarjeta que actúa como intermediaria en el pago lo siguiente:

- Que presente la documentación justificativa de cada operación (la boleta de la operación debidamente firmada, o bien autenticada mediante el tecleo del NIP), ya que, de otro modo, se invertiría la carga de la prueba, de tal forma que el cliente, que no ha creado el sistema, estaría obligado a demostrar que no ha realizado las compras cuestionadas, lo que, obviamente, es inadmisible.

- Que realice una gestión diligente y puntual de la reclamación efectuada por su cliente ante la sociedad propietaria del sistema, para conseguir, en su caso, la devolución de los importes adeudados en cuenta si estos no hubieran sido procedentes de acuerdo con las condiciones en que se realizara la contratación.

…/…

En cuanto a la valoración de la autenticidad de las firmas contenidas en los resguardos de compras, si bien la firma contenida en las boletas constituye, en su caso, un límite a la responsabilidad del titular de la tarjeta, no corresponde al DCMR efectuar dicha valoración, pues únicamente los tribunales de justicia, a través de la práctica de los medios de prueba que estimen necesarios, pueden determinar la falsedad de la firma contenida en los resguardos, así como pronunciarse acerca de la diligencia empleada por todos los sujetos intervinientes en el cumplimiento de sus obligaciones; entre ellos, los establecimientos comerciales. Para demostrar que las operaciones de pago fueron autenticadas, registradas con exactitud y contabilizadas, las entidades financieras aportan con frecuencia copia de sus registros internos en las que se reflejan diferentes datos sobre la ejecución de las distintas operaciones de pago. El DCMR ha venido considerando que, además de la aportación de dichos registros, en caso necesario, deben aportar una explicación de su contenido. Así, en el expediente R-201608322 se consideró que la entidad había quebrantado las buenas prácticas bancarias por cuanto no facilitó explicaciones suficientes relativas a un mensaje que aparecía en las tiras de fondo del cajero en el que se produjo la operación controvertida.

En el expediente R-201609665 también se estimó que la entidad propietaria del cajero se había apartado de las buenas prácticas bancarias al faltar a la colaboración con el DCMR por no aportar explicación de las claves utilizadas en la tira del cajero, lo que impide comprobar que la disposición controvertida hubiese sido autenticada conforme al artículo 30 de la LSP y que no fuera afectada por un fallo técnico o cualquier otra deficiencia.

Fraude con datos de tarjetas

Por lo que respecta a la presentación de la documentación justificativa de las operaciones controvertidas, una dificultad añadida aparece cuando la utilización de la tarjeta se produce a distancia, por Internet, utilizando únicamente los datos de aquella en conjunción, en su caso, con otros dispositivos o códigos de seguridad.

Las entidades emisoras de las tarjetas suelen aportar para acreditar la autenticación del titular (no olvidemos que en operaciones a distancia no se puede realizar una identificación presencial del portador de la tarjeta) y la autorización de la operación copia de los registros internos que, a su vez, les facilitan las redes o las entidades globales. Sin embargo, el DCMR considera que las entidades emisoras de las tarjetas deben estar en condiciones de acreditar extremos tales como la forma de autenticación del instrumento y la autorización de la operación, el exacto registro y contabilización de esta o la forma de prestación del consentimiento a las operaciones de pago. En cualquier caso, desde el punto de vista del cumplimiento de la normativa sobre servicios de pago y de las buenas prácticas con las que se debe proceder con la clientela, resulta imprescindible que la forma de prestar el consentimiento para la realización de las operaciones de pago esté acordada con el cliente y se encuentre debidamente recogida en el contrato, en los términos que señala el artículo 25 de la LSP.

…/…

Además, con respecto a esta cuestión resulta oportuno señalar que la Autoridad Bancaria Europea (ABE) publicó el 19.12.2014 unas directrices definitivas sobre la seguridad de los pagos por Internet, que la Comisión Ejecutiva del Banco de España adoptó como propias en su sesión de 24.3.2015[47]. Estas directrices establecen un conjunto de requisitos mínimos de seguridad en la lucha contra el fraude y su finalidad es aumentar la confianza del consumidor en los servicios de pago por Internet y, así, recomiendan con carácter general —salvo en ciertas excepciones[48]— que los proveedores de servicios de pago, para autorizar las operaciones de pago por Internet o para modificar datos sensibles, usen procedimientos de autenticación fuerte del cliente, que se definen como aquellos basados en el uso de dos o más de los siguientes elementos, clasificados como conocimiento, posesión e inherencia:

i) algo que solo conoce el usuario: por ejemplo, una contraseña, código o número de identificación personal fijos;

ii) algo que solo posee el usuario: por ejemplo, token, tarjeta inteligente, teléfono móvil;

iii) algo que caracteriza al propio usuario: por ejemplo, una característica biométrica, como su huella dactilar.

Tales elementos, según la EBA, deben ser independientes entre sí (es decir, la violación de uno no debe comprometer la seguridad de los otros) y al menos uno de ellos no debe ser reutilizable ni reproducible ni debe resultar posible su sustracción, de manera subrepticia, a través de Internet.

Del contenido de dichas directrices, también interesa destacar su punto 5, que establece que los proveedores de servicios de pago deben contar con procesos que garanticen que todas las operaciones, así como el flujo del proceso del mandato electrónico, quedan adecuadamente registrados.

Por lo tanto, resulta esencial que las operaciones de pago autorizadas por Internet queden adecuadamente explicadas, con especial referencia a la forma en que se autenticó el titular y el modo en que se prestó el consentimiento a la operación realizada, también para poder comprobar si la operativa se ajusta a lo establecido en las directrices. Si la entidad emisora de la tarjeta no dispusiera de documentación suficiente, deberá recabarse de los sistemas de tarjetas, redes o plataformas y/o de los establecimientos comerciales intervinientes.

---

47 Puede consultarse en: https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments %29.pdf/f27bf266-580a-4ad0-aaec-59ce52286af0 y la versión traducida en http://www.bde.es/f/webbde/INF/MenuHorizontal/Normativa/guias/EBA-GL-2014-12.pdf.

48 Pagos de escasa cuantía o a beneficiarios de confianza que el cliente previamente seleccione, pagos a favor de beneficiarios de confianza que estén incluidos en listas blancas que ese cliente haya establecido, operaciones entre dos cuentas del propio cliente dentro de la misma entidad o transferencias dentro de la misma entidad de pago cuando esté justificado por un análisis del riesgo de las operaciones.

Comercio electrónico seguro

Con frecuencia, las entidades emisoras de tarjetas, ante una reclamación de un titular de tarjeta por la que manifiesta no haber autorizado un pago con los datos de aquella por Internet, se limitan a indicar que se ha realizado mediante «Comercio Electrónico Seguro». Con este sistema se trata de garantizar la seguridad de las transacciones de compras con tarjeta a través de Internet, de forma que, al efectuar la compra, la plataforma redirige al cliente a un sitio seguro, en el que, además de los datos de la tarjeta —número, caducidad, los tres dígitos del reverso—, se debe introducir un código de identificación personal (CIP) que solo el titular de la tarjeta debe conocer. Los datos de la tarjeta irán encriptados, de forma que el establecimiento comercial no llega a conocer esos datos.

Responsabilidad del proveedor de servicios de pago por operaciones de pago no autorizadas

En estos supuestos, y con independencia de la obligación de la entidad de demostrar que la operación de pago controvertida fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico, corresponde a esta, en tanto proveedor de servicios de pago del ordenante, devolver a este de inmediato el importe de la operación de pago no autorizada, restableciendo la cuenta de pago al estado que habría tenido de no haberse producido la operación de pago no autorizada, en su caso (artículo 31 de la LSP); ello, claro está, con independencia del derecho que asiste a la entidad a efectuar cuantas actuaciones estime convenientes en defensa de sus legítimos intereses.

Dentro del apartado de uso fraudulento de tarjetas que ahora analizamos, y más concretamente de la responsabilidad del proveedor del servicio de pago por operaciones de pago no autorizadas, que se regula en el artículo 31 de la LSP, cabe incluir, a juicio del DCMR, y con independencia de la mejor opinión de los tribunales de justicia, las operaciones de pago no autorizadas que se hubieran efectuado con tarjeta en las que su titular no ha perdido la posesión de aquella, esto es, los casos en los que se ha llevado a cabo una copia de la tarjeta, o bien la realización de operaciones de pago no autorizadas realizadas a través de Internet, tales como compras, transferencias, etc.

Efectivamente, el DCMR viene entendiendo que, en caso de utilización fraudulenta de una tarjeta derivada de una copia del instrumento de pago, sería de aplicación el artículo 31 de la LSP, en tanto que se trata de una operación de pago no autorizada, debiendo en estos casos la entidad, a juicio del DCMR, llevar a cabo la devolución del importe íntegro de la operación de pago no autorizada, siempre y cuando el titular de la tarjeta no hubiera incumplido deliberadamente o por negligencia grave las obligaciones que incumben a este y a las que hemos hecho referencia con anterioridad, y la entidad así pueda acreditarlo, valorando el DCMR de manera individualizada las circunstancias que concurren en cada caso.

En el expediente R-201609130 se excepcionó la aplicación de lo previsto en el artículo 31 de la LSP, puesto que, aunque la entidad no tramitó el retroceso del importe reclamado se entendió que ello se hallaba justificado por la rápida verificación del buen fin de la operación.

…/…

Responsabilidad del ordenante por operaciones de pago no autorizadas derivadas de la utilización de un instrumento de pago extraviado o sustraído

Cuando la entidad tenga conocimiento de que se ha producido una operación de pago no autorizada derivada de la utilización de un instrumento de pago extraviado o sustraído, deberá demostrar que la operación de pago controvertida fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico. En estos casos, se establece que el ordenante tan solo soportará, hasta un máximo de 150 euros, las pérdidas derivadas de la utilización del instrumento de pago extraviado o sustraído (artículo 32 de la LSP), salvo que la operación de pago no autorizada fuera fruto de una actuación fraudulenta del ordenante o del incumplimiento deliberado o por negligencia grave de sus obligaciones, en cuyo caso el ordenante soportará el total de las pérdidas derivadas de las operaciones de pago no autorizadas.

Por otra parte, el ordenante no soportará consecuencia económica alguna derivada del uso fraudulento de la tarjeta extraviada o sustraída con posterioridad a la notificación a la entidad del extravío, sustracción o utilización no autorizada del instrumento de pago.

En cuanto a la enervación por parte de las entidades del límite de responsabilidad descrito, es criterio reiterado de este DCMR considerar que en última instancia habrán de ser los tribunales de justicia, y no las entidades de crédito como parte interesada, los que deberán valorar y determinar, en su caso, la existencia de una conducta fraudulenta o el incumplimiento, deliberado o con negligencia grave, de las obligaciones que corresponden al titular en relación con el instrumento de pago. No obstante, cuando la entidad acredite la existencia de hechos que, a priori y en nuestra opinión, podrían considerarse suficientes para enervar el límite de responsabilidad, este DCMR, analizando las circunstancias que concurren en cada supuesto, no considera el proceder de la entidad apartado de las buenas prácticas bancarias, indicando, al mismo tiempo, que, dadas las circunstancias, los interesados podrán someter la controversia, si así lo estiman oportuno, a conocimiento y resolución de los tribunales de justicia.

En el expediente R-201601023 se consideró que la actuación de la entidad fue contraria a los buenos usos y prácticas financieras en tanto la redacción del contrato de tarjeta relativa a los límites de responsabilidad en caso de uso fraudulento de esta no se ajustaba a la LSP, debido a que se daba igual tratamiento a los casos en que el instrumento de pago había sido extraviado o sustraído y a aquellos en los que no, y el cliente debía asumir, en todo caso, una pérdida de 150 euros. Ahora bien, de conformidad con el artículo 32 de la LSP, es únicamente en caso de instrumento de pago extraviado o sustraído cuando el ordenante ha de soportar la pérdida máxima de 150 euros. Por otro lado, la actuación de la entidad fue considerada contraria a las buenas prácticas bancarias al no retroceder, al menos de forma interina o provisional, las operaciones denunciadas y no procurar los justificantes de las operaciones controvertidas de la entidad propietaria del cajero.