La Audiencia Provincial de Madrid obligó a una entidad bancaria española a devolver 28.744,21 euros a una clienta a la que habían robado la tarjeta. El banco acusó a la afectada de negligente al no tener activado el sistema de alertas por SMS de los movimientos asociados a su tarjeta.

SENTENCIA

Si los pagos 'contactless' crecen, el banco debe bloquear la tarjeta

Aunque las compras menores de 50 euros y sin contacto no exigen al usuario identificarse, la entidad bancaria debe controlar este tipo de pagos.

Alejandro Galisteo. Madrid

Entre las muchas novedades que llegaron con la pandemia, las entidades financieras acordaron ampliar de forma temporal de 20 a 50 euros el límite del pago *contactless*. Esta medida, tomada para prevenir contagios, facilitaba a los usuarios hacer compras de mayor volumen con sus tarjetas de crédito utilizando la tecnología NFC, que permite realizar operaciones sin contacto y, por tanto, sin introducir el código pin. Algunos expertos en ciberseguridad calificaron esta decisión de arriesgada, ya que, en caso de robo de la tarjeta, los ladrones podían hacer compras de mayor volumen con facilidad.

A un debate similar ha puesto fin el Tribunal de Justicia de la Unión Europea (TJUE). Los magistrados comunitarios han resuelto el litigio que mantenían DenizBank, entidad bancaria austriaca, y VKI, asociación de consumidores del mismo país. La institución denunció las cláusulas que el banco hacía firmar a sus clientes por utilizar las tarjetas que incorporaban la tecnología *contactless*. Entre otras cuestiones, DenizBank señalaba que sus responsables no estaban obligados a autorizar o denegar los pagos inferiores a 25 euros, los que no exigían el uso del código pin, en caso de fallo técnico o de otro tipo. Además, el contrato eximía de responsabilidad a la entidad bancaria y de tener que reembolsar las transacciones no autorizadas por el titular.

Responsabilidad del cliente

Cuando un banco ofrece una tarjeta de crédito a un cliente, este acepta una serie de condiciones de buen uso. Este deber de salvaguarda fue abordado por la Audiencia Provincial de Madrid en 2017. Dos usuarios de un banco español fueron abordados frente a un cajero de la entidad por una persona que les dijo que se les había caído un billete al suelo y les ayudó a volver a introducirlo en la máquina. Se trataba de una estafa, ya que al cabo de unos días vieron que les habían robado más de 6.000 euros. El banco dijo que esto era responsabilidad del cliente por mal uso de la tarjeta pero los jueces no validaron su argumento.

La sentencia del TJUE reconoce que aunque sea imposible identificar a la persona que realiza las operaciones de menos de 25 euros sin contacto, la tarjeta está vinculada a una cuenta bancaria a la que se carga el dinero. "Un movimiento de escasa cuantía realizado sin contacto constituye una utilización anónima del instrumento de pago", señala el fallo.

Los magistrados europeos recuerdan que el banco no puede acogerse a este anonimato y limitarse a afirmar que "resulta imposible bloquear la tarjeta o impedir que se siga utilizando", aclara la sentencia que, además, recuerda a las entidades bancarias que deben disponer de canales gratuitos para denunciar un uso fraudulento de su tarjeta y que no están libres de resarcir económicamente al perjudicado en caso de fraude.

DenizBank señaló que no estaba obligado a autorizar o denegar los pagos inferiores a 25 euros

El banco no puede utilizar el anonimato de las transacciones para no controlarlas

En la misma línea, en 2019, la Audiencia Provincial de Madrid obligó a una entidad bancaria española a devolver 28.744,21 euros a una clienta a la que habían robado la tarjeta y que tardó siete días en denunciar la extracción del dinero en comisaría. El banco acusó a la afectada de negligente al no tener activado el sistema de alertas por SMS de los movimientos asociados a su tarjeta. Pero los jueces señalaron que la empresa conocía estos movimientos y debía haber bloqueado la tarjeta.

TELECOMUNICACIONES

Es ilegal premarcar la casilla de tratamiento de datos en un contrato

A. Galisteo. Madrid

Cuando un usuario firma un contrato con una compañía de telefonía, más allá de la relación entre los datos y el coste de la tarifa, no suele observar las cláusulas del documento. Y a veces, en el texto aparecen algunas que, de comprenderlas, el cliente se pensaría más de un par de veces aceptarlas. Precisamente, un particular fue el que dio la voz de alarma sobre la forma en la que aparecían redactados algunos contratos de Orange en Rumanía.

"Incluía en sus contratos de prestación de servicios de telecomunicaciones móviles una cláusula premarcada (antes de la firma del contrato) a través de la cual se consentía la obtención y conservación de la copia del documento de identidad de los firmantes, con fines de identificación", comenta Salvador Silvestre, socio del área de tecnología de Ecija

Esto provocó que la compañía de telecomunicaciones francesa fuera sancionada por la autoridad de protección de datos rumana (Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal) mediante la imposición de una multa el 28 de marzo de 2018.

Ese mismo día, Orange decidió recurrir esta sanción ante el Tribunal de Distrito de Bucarest, que a su vez solicitó al Tribunal de Justicia de la Unión Europea (TJUE) que precisara las condiciones en las que puede considerarse válido el consentimiento de los clientes para el tratamiento de datos personales.

"Dicho consentimiento debe ser libre, específico, informado e inequívoco", explica Silvestre sobre la sentencia del organismo europeo, que recuerda que no se permite demostrar válidamente el consentimiento del usuario a través de casillas ya marcadas.

Además, los magistrados del tribunal europeo recuerdan que, para que el cliente esté verdaderamente informado, la redacción de las cláusulas deben estar redactadas con un lenguaje sencillo, claro e inteligible.

"Las estipulaciones contractuales de dicho contrato pueden inducir al interesado a error sobre la posibilidad de celebrar el contrato en cuestión pese a negarse a consentir en el tratamiento de sus datos", señala el socio de Ecija sobre una práctica con la que Orange menoscababa la libertad de elección de sus clientes.

10,6

Millones de clientes

Orange tiene más de 10,6 millones de clientes en Rumanía, unos usuarios que pueden verse afectados por la resolución del TJUE.