APM 3.9.

Publicación digital. - Asociación Profesional de la Magistratura

LAURA CRISTINA MORELL ALDANA

MAGISTRADA JAT TSJ COMUNIDAD VALENCIANA

***SIM SWAPPING*, RESPUESTAS DE NUESTROS TRIBUNALES A LA EVOLUCIÓN DE LA CIBERCRIMINALIDAD**

1. Introducción

La evolución de las **modalidades comisivas de la estafa es imparable** y buena muestra de ello, es el surgimiento de una nueva forma de fraude, denominada ***sim swapping* o *sim swap scam*.**

Brevemente, el *sim swapping* consiste en **duplicar**, de manera fraudulenta la tarjeta SIM del teléfono móvil de una persona y consta de dos fases, aunque su traducción literal hace referencia a un '**intercambio**' de una tarjeta SIM por otra. **Preliminarmente,** se han obtenido de forma ilícita datos especialmente sensibles, como nombre y apellidos o números de teléfono, DNI o cuenta corriente. En una **primera fase**, el ciberdelincuente suplanta la identidad del titular de la tarjeta SIM, con el objeto de obtener un duplicado de ésta. A partir de dicho momento, éste queda **sin servicio telefónico**. En una **segunda fase**, caracterizada por su especial **rapidez** con ánimo de no ser descubierto, obtenido el duplicado de la tarjeta, el ciberdelincuente accede y emplea la información personal del perjudicado, principalmente la bancaria, para recepcionar en dicha SIM los SMS de verificación o mensajes de texto de confirmación, con las claves con las que, usualmente, se restablecen los servicios bancarios y así ejecutar algún ciberdelito, como puede ser realizar una operación bancaria y suplantaciones de identidad en redes sociales.

Precisamente, una herramienta especialmente útil para prevenir suplantaciones de identidad, con finalidad de obtener un ilícito desplazamiento patrimonial –y que se puede ver sorteada con el fraude del *sim swapping*- es el **Real Decreto-ley 19/2018, de 23 de noviembre,**

de servicios de pago y otras medidas urgentes en materia financiera[1], que actualiza la derogada Ley 16/2009, de 13 de noviembre, de servicios de pago.

Real Decreto-ley que tiene por objeto, una trasposición más adecuada de 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** –también conocida como **PSD2**-, una trasposición completa de la Directiva de ejecución (UE) 2015/2392 de la Comisión, de 17 de diciembre de 2015 así como en general, diversas Directivas de tipo financiera; abordando además la modificación del Texto Refundido de la Ley del mercado de valores.

El **Capítulo II** del Real Decreto-ley 19/2018 se encuentra dedicado a la autorización de operaciones de pago. El artículo 41 regula **las obligaciones del usuario de servicios de pago** en relación con los instrumentos de pago y las credenciales de seguridad personalizadas, siendo especialmente, a los efectos del *sim swappping*, disponiéndose como obligación que "b) en caso de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada, lo notificará al proveedor de servicios de pago o a la entidad que este designe, sin demora indebida en cuanto tenga conocimiento de ello". El artículo 42 hace referencia a las **obligaciones del proveedor de servicios de pago** en relación con los instrumentos de pago, entre otras, que "Impedirá cualquier utilización del instrumento de pago una vez efectuada la notificación en virtud del artículo 41.b)".

El artículo 44 por su parte, hace reseña a las **normas sobre la carga de la prueba**, sobre la autenticación y ejecución de las operaciones de pago y concretamente en su apartado 1º se dispone que "Cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, corresponderá al proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado por el proveedor de servicios de pago. Si el usuario de servicios de pago inicia la operación de pago a través de un proveedor de servicios de iniciación de pagos, corresponderá a éste demostrar que, dentro de su ámbito de competencia, la operación de pago fue autenticada y registrada con exactitud y no se vio afectada por un fallo técnico u otras deficiencias vinculadas al servicio de pago del que es responsable".

También como una obligación se articula el artículo 45.1, sobre **responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas** según el cual "en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devolverá a éste el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación, salvo cuando el proveedor de servicios de pago del ordenante tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España, en la forma y con el contenido y plazos que éste determine. En su caso, el proveedor de servicios de pago del ordenante restituirá la cuenta de pago en la cual se haya efectuado el adeudo al estado en el que se habría encontrado de no haberse efectuado la operación no autorizada. La fecha de valor del abono en la cuenta de pago del ordenante no será posterior a la fecha de adeudo del importe devuelto".

Por último y en cuanto al marco legal, el artículo 46 dispone una serie de obligaciones, de cuyo incumplimiento puede derivar responsabilidad del ordenante, en caso de operaciones de pago no autorizadas, que excepcionan lo previamente expuesto en el artículo 45

[1] https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16036

El *sim swapping* como modalidad defraudatoria[2] ha irrumpido con fuerza en el panorama español, al que no es ajena nuestra doctrina. Por ejemplo, FORADADA BERMEJO[3], partiendo de la premisa de que "(…) esta modalidad delictiva incide tanto en la esfera patrimonial de los afectados como también en su **intimidad**: el acceso a la información que pudiera almacenarse en estos dispositivos, su posterior difusión o empleo de la misma con finalidades lucrativas son otras de las consecuencias más graves de este tipo de fraude (…)", propone la siguiente **batería de medidas** para paliar los efectos económicos del *sim swapping,* una vez colmada la estafa:

- **Facilitar información a los particulares** sobre este tipo de estafa, ya que "(…) para poder evitar que una persona sea víctima de una estafa es necesario que sea capaz de reconocer los efectos de la misma (…)", por ejemplo, el momento inicial de pérdida de cobertura.

- Mejorar la **trazabilidad de las operaciones fraudulentas** para la persecución e investigación de la estafa, bien sea mediante el uso de IP, bien sea acudiendo a tiendas de telefonía, donde hay una implicación personal del autor de la estafa. "(…) cuantos más datos puedan recabar las operadoras de telefonía, así como las entidades que prestan servicios de banca online mayor respuesta se podrá dar al efecto de averiguar quiénes son los autores de estos delitos (…)".

- Promoción del **resarcimiento** de los particulares que son víctimas de estas transacciones efectuadas fraudulentamente.

Por su parte, CABEZAS BERDIÓN[4], apreciando que la primera fase de esta estafa consiste en la obtención de un "(…) duplicado de una tarjeta SIM consiste en obtener una nueva tarjeta con un IMSI no asociado a ningún MSISDN, esto es, a ningún número teléfono móvil, y modificar los datos en las bases de red de manera que se asocie a ese nuevo IMSI de la nueva tarjeta SIM el número de teléfono (MSISDN) de la antigua tarjeta SIM (…)", establece cuatro formas según la práctica forense de obtención del duplicado SIM:

- **Presentación de documentación falsa**, personándose en una tienda física de la operadora de telefonía suplantando la identidad del titular de la tarjeta SIM.

- **Engaño** al empleado de la operadora de telefonía móvil.

- **Connivencia** con el empleado de la operadora, método que califica de muy residual.

- Finalmente, la que considera la modalidad más habitual**, solicitud de duplicado por vía telemática** sin presencia física, lo que será más o menos factible dependiendo "(…) de las medidas de seguridad y de verificación de la identidad que hayan establecido cada una de las operadoras telefónicas, es decir, de las políticas KYC o *Know Your Client* (…)"

---

[2] La Agencia Estatal de Protección de Datos tiene diversas publicaciones con consejos para el usuario de tarjeta SIM ante éstas prácticas fraudulentas, véase https://www.aepd.es/areas-de-actuacion/recomendaciones/saber-mas

[3] FORADADA BERMEJO, J.A., "Medidas encaminadas a erradicar o a minimizar el impacto en la realidad socieconómica del *sin swapping*", Centro de Estudios Jurídicos, Taller sobre la estafa 2FA mediante el intercambio de tarjeta SIM, formato electrónico, págs. 5, 13-14.

[4] CABEZAS BERDIÓN, L., "El intercambio de tarjeta sim o *sim swapping*. Concepto y formas de ejecución", Centro de Estudios Jurídicos, Taller sobre la estafa 2FA mediante el intercambio de tarjeta SIM, formato electrónico, págs. 19,20-22

Obtenido el duplicado de la SIM, ya se puede quebrar la **verificación en dos pasos** (2FA o *two factor authentication*) que normalmente consiste en 'algo que solo yo sé' (datos también ilegítimamente obtenidos, como el nombre/apellidos, número de teléfono móvil, número de DNI, número de cuenta corriente) y en 'algo que yo solo tengo', en este caso, el terminal telefónico. Recordemos que al obtener un duplicado de la SIM se puede insertar en cualquier terminal telefónico y activar, dejando 'sin línea' al legítimo titular.

PILLADO QUINTAS[5] finalmente estima que hay un momento especialmente relevante para la comisión de una estafa informática por medio del *sim swapping*, como es hacerse previamente con los datos relevantes del titular de la línea telefónica, normalmente, a través del ***phishing,*** el envío de forma masiva de correos maliciosos.

Adiciona como característica relevante del *sim swapping* "(…) la **urgencia o rapidez en el actuar** que ha de adoptar el delincuente, debido a que el usuario detectará que no tiene línea telefónica en su terminal móvil, ya que el duplicado de la tarjeta SIM supone dejar sin operatividad a la tarjeta original, pudiendo incluso recibir un mensaje de su compañía comunicándole que se ha solicitado/expedido un duplicado de su tarjeta SIM. Dichos indicadores provocarán que el perjudicado en un tiempo reducido se percate de que se está acometiendo un fraude y ante ello adopte medidas de seguridad para evitarlo, principalmente llamando a la compañía de telefonía para que bloquee esa tarjeta SIM y así evitar que puedan realizarse operaciones con cargo a su patrimonio, pero también adoptando medidas semejantes con su entidad bancaria (…)".

Podemos afirmar que se trata de una clase de estafa en la que, por una parte, la **inteligencia artificial** puede llegar a minimizar el impacto de la misma e incluso evitar su comisión –por ejemplo con el uso de un segundo factor de verificación biométrico, como el reconocimiento facial- pero también, esa misma inteligencia artificial puede facilitar su comisión.

Sostiene VELASCO NÚÑEZ[6] que "(…) Ya parecen haberse usado aplicaciones de IA para, por ejemplo, estafar al CEO de una empresa energética británica mediante la utilización de una que reunió datos de voz para imitar la del director ejecutivo de su matriz alemana, y haciéndose pasar por él en una llamada telefónica con su voz solicitarle los defraudadores la transferencia inmediata de doscientos veinte mil euros a la cuenta bancaria de un proveedor húngaro, desde la cual el dinero se reenvió a otra mexicana y de ahí a otras, consumando la disposición inconsentida del dinero. Parece por tanto bastante actual y real la subsunción de este tipo de maniobras en el delito de estafa mediante artificios en la programación, que, en el campo comercial, podría convertir en acciones de naturaleza penal, fenómenos como las «obsolescencias programadas», en donde el dolo de extinguir el uso normal de un producto, escaso tiempo después de haberlo adquirido, siempre que no haya sido claramente advertido por el vendedor, constituiría el artificio sin el cual el consumidor medio no habría adquirido una mercancía de habitual uso más prolongado. La IA se puede utilizar como técnica de rastreo y cruce de los datos obrantes en diferentes contratos de seguros, primas, pólizas, siniestros declarados, pagos e indemnizaciones, para averiguar si alguno de sus beneficiarios ha pretendido o conseguido algún cobro indebido, configurando supuestos de posible estafa de defraudación (…)".

---

[5] PILLADO QUINTAS, V., "Investigación Judicial de la modalidad delictiva de *SIM Swapping*. Calificación Jurídica y Cuestiones Prácticas cara el acto de Juicio Oral", Centro de Estudios Jurídicos, Taller sobre la estafa 2FA mediante el intercambio de tarjeta SIM, formato electrónico, págs.10-12.

[6] VELASCO NÚÑEZ, E., "Inteligencia artificial: aspectos penales y procesales", en PERALTA GUTIÉRREZ, A., y TORRES LÓPEZ, L.S., *El derecho y la inteligencia artificial*, Ed. Universidad de Granada, Granada, 2022, pág. 537.

En conclusión, el *sim swapping* es una modalidad de estafa informática, que requiere previamente para su perfeccionamiento, la obtención de datos personales del titular de la línea con el empleo de una gama de métodos (***phishing, smishing* o *vishing***).

Posteriormente en una **primera fase de ejecución** se emplean los datos personales, presuntamente secretos ('algo que solo yo sé', factor de conocimiento que integra usualmente el sistema de verificación en dos pasos), para suplantar la identidad del titular de la línea (bien de forma física, con empleo de documentación falsificada, lo que puede dar lugar al surgimiento de una falsedad documental en concurso medial con la estafa informática, bien de forma telemática) y obtener un duplicado de la tarjeta SIM, sin perder el número de teléfono pero no asociado al terminal en el que usualmente tenemos insertada la SIM.

Y después, en una **segunda fase de ejecución**, caracterizada por la rapidez de los actos defraudatorios (dado que el usuario de la línea se ha quedado sin servicio telefónico y puede percatarse rápidamente), quebrar el doble factor de autenticación ('algo que yo solo tengo' o factor físico, en este caso la SIM duplicada) y recibir uno de los famosos 'sms de verificación' que nos permiten re establecer los servicios bancarios online. A partir de ese momento, se consuma la estafa informática, bien **instalado app's** como bizum o hal cash, plataformas electrónicas que permiten el rápido envío del dinero proveniente de la cuenta corriente del perjudicado, bien solicitando **créditos rápidos preconcedidos** por la misma app del banco, bien ordenando **transferencias inmediatas** con origen en dicha cuenta corriente y destino a terceras personas (las denominadas 'mulas' o 'muleros').

Ello porque nos hallamos ante un **delito fruto de la ingeniería social** que suele contar con una **estructura piramidal** para su comisión, integrada por: los **líderes** de la organización –los sujetos cuya identidad es más difícil de desencriptar-, los **piratas informáticos** encargados de la obtención de datos sensibles –por medio del *phishing* o uso de otros medios, como la infección con *malware* de dispositivos de la víctima, si bien su figura puede ser sustituida por la compra de datos sensibles en la *deep web*-, los **captadores** –encargados de reclutar a los **ejecutores** de las dos fases de esta estafa, bajo la promesa de obtener un lucro y ofreciendo la mínima información que permita identificar a personas más relevantes de la estructura piramidal-, las personas encargadas de obtener el duplicado de la SIM, insertarla en su terminal teléfono u ordenar transferencias –todo ello a cambio de un porcentaje de la operación- y finalmente los **cibermuleros o muleros**, quienes reciben la transferencia patrimonial inconsentida en su cuenta corriente y que suelen ser, usualmente, los únicos procesados –bien como cooperadores necesarios en la estafa, bien como autores materiales de delito de blanqueo de capitales por imprudencia grave, según jurisprudencia menor-.

2. Respuestas al ciber fraude en el orden jurisdiccional civil

La irrupción de la cibercriminalidad ha tenido su reflejo no solo en la jurisdicción penal, como podría pensarse, sino también por aplicación del **Real Decreto-ley 19/2018, de 23 de noviembre** en la jurisdicción civil.

Debemos traer a colación, en primer término, la **SJPI nº 3, de Avilés, nº 33/2023, de 21 de febrero de 2023**, que estima la demanda formulada por un usuario de banca online contra su entidad bancaria, al apreciar, FJº2º *in fine* que "(…) la actuación de la entidad bancaria no fue todo lo diligente que debía, máxime si como se ha advertido, la actuación similar a la descrita en la demanda fue generalizada en su momento, con múltiples estafas a través de idéntico sistema, sin que la entidad hoy demandada haya procedido a una implementación de los mecanismos de

protección que eviten situaciones como la descrita y es objeto de *litis* (…)".

La Sentencia, tras una exégesis de los artículos 44 y 45 del Real Decreto-Ley 19/2018, con cita a la Sentencia de la Sección 3 de la Audiencia Provincial de Navarra de 25 de julio de 2019, si que aprecia el surgimiento de la responsabilidad de la entidad bancaria, a la que condena al abono de 2.000 euros, más intereses, no apreciando la concurrencia de los supuestos de exoneración del artículo 46. Y ello al estimar que "Debe tenerse en cuenta que estos mecanismos de pago, tanto por medio de tarjetas, como a través de la banca a distancia o digital, no solo los articula la entidad financiera a través de las correspondientes aplicaciones y software, sino que potencia su utilización por sus clientes y usuarios bancarios, por lo que tiene -y debe- implementar todas las medidas de seguridad necesaria para evitar fraudes, incluida la suplantación de identidad; y, si el fraude es externo, es decir, a través de estafas informáticas (o " phishing"), lo único que puede exigirse al usuario es que el dispositivo que utilice para la realización de este tipo de operaciones tenga un mantenimiento de seguridad que, en principio, pudiera evitarlo, exigencia que, en el supuesto que examinamos, ha verificado el demandante quien goza -no debe olvidarse- de la condición de "consumidor" y, en consecuencia, de una protección reforzada (…)".

En la **SJPI, n. º 15, de Zaragoza, n. º 266/2022, de 5 de septiembre**, la estimación de la demanda de juicio verbal en un supuesto de *sim swapping* que se ventila en ésta jurisdicción, conlleva la condena de la empresa telefónica a la cantidad de 2680 euros. En cuanto al *factum*, el titular de la línea telefónica fue objeto de un fraude en la cuenta bancaria de la que era titular, al haberse obtenido, previamente, por el defraudador -que no aparece identificado- un duplicado de su tarjeta SIM que no había sido solicitado por el titular de la línea, mediante el que consiguieron las claves bancarias para operar con la entidad de crédito e inclusive, llegaron a descargarse la aplicación Bizum, que nunca había tenido instalada.

El demandante formuló denuncia ante el orden penal -que sobre entendemos que fue archivada, por sobreseimiento provisional, por falta de autor conocido- y además, reclamación previa a la empresa telefónica, solicitando se le exhibiese el documento por el cual se autorizaba a la expedición del duplicado de la SIM, requerimiento que resultó infructuoso.

La operadora ponía de relieve que el demandante había reclamado previamente tanto a dos entidades bancarias, destacando que concurriría falta de legitimación pasiva, dado que "(…) resulta imprescindible para el perfeccionamiento del fraude la obtención previa de datos cuya diligente custodia corresponde bien al actor bien al proveedor de servicios de pago, y sin los cuales no habrían podido ordenarse las transferencias (...)".

La Sentencia efectúa un análisis de la normativa europea (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) así como del ya precitado Real Decreto-Ley 19/2018 y de la **SAP de Pontevedra, 539/2021, de 21 de diciembre** y del más genérico artículo 1101 del CC.

Sin embargo, reconoce el Juzgador que la cita legislativa y jurisprudencial, solo avalaría la condena de la entidad bancaria, pero no de la operadora telefónica. No obstante, aprecia una quiebra de las obligaciones del artículo 1101 del CC en relación con el artículo 7 del mismo cuerpo legal; especialmente del principio de confidencialidad de los datos regulado en el art. 5 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, debido a que la operadora gestionó la obtención de un duplicado de la SIM, no solicitado por su titular "(…) actuación que constituye uno de los eslabones de la "cadena

defraudadora" sin el cual no es posible completar la apropiación económica, por lo que, a juicio de este tribunal, nos encontraríamos ante un supuesto de responsabilidad solidaria de todas aquellas entidades que posibilitaron el daño sufrido por el demandante, sin perjuicio de las acciones que entre ellos se quieran ejercitar (...)", FJº2º.

Por su parte, la **SAP de Zaragoza, Sección 5ª, n. º 996/2022, de 17 de noviembre,** conoce en grado de apelación la **SJPI, n. º 7, de Zaragoza, n. º 292/2021, de 29 de octubre**, sentencia que confirma en dicho grado y por la que se condenó, en este supuesto, a la entidad bancaria a restituir al titular de la cuenta corriente, un total de 56.474,63 euros. Ello por apreciar que la actuación de la demandada en la gestión del fraude sufrido por el actor supone un incumplimiento de las obligaciones contractuales asumidas en el contrato de banca a distancia y contrato de cuenta corriente y/o depósito, actuación que habría producido daños y perjuicios que ahora se cifran y resarcen en la cuantía precitada.

La entidad bancaria, recurrente en apelación, alegó que la sentencia de instancia efectuaba una incorrecta presunción de que las operaciones bancarias no fueron autorizadas, cuando documentalmente a la entidad le constaba autorización y registro en sus sistemas informáticos, con las contraseñas facilitadas por la entidad al actor en la contratación de tales servicios, con independencia de que fuesen realizadas por el actor, o por otra persona.

La SAP controvierte dicho argumento con las reglas que, sobre la carga de la prueba, establece el artículo 44.1 del Real Decreto-Ley 19/2018; el actor negó haber efectuado tales operaciones y además, aportó prueba en contrario -aunque la carga de la prueba corresponde al proveedor de servicios de pago-. Para la Audiencia resulta probado, FJº2º *in fine* que "(…) las transferencias se realizaron por delincuentes que duplicaron la tarjeta SIM de la esposa del perjudicado accediendo a la información confidencial almacenada en ella. Se trata de una modalidad de estafa denominada "SIM swapping" que consiste en duplicar de forma fraudulenta la tarjeta SIM del teléfono móvil de una persona suplantando su identidad, y después, una vez que la víctima se queda sin servicio telefónico, accede a su información personal y toma el control de su banca digital utilizando los SMS de verificación que llegan al número de teléfono (...)".

Ello por lo que atañe al primer motivo de apelación, infracción de las normas de interpretación del artículo 36 del Real Decreto-Ley 19/2018. En lo concerniente al segundo motivo de apelación, infracción de las normas de interpretación de los artículos 44 y 45 del mismo cuerpo legal, nuevamente es desestimado. Recuerda la SAP que dicha normativa "(…) establece un sistema de responsabilidad cuasi objetiva de la entidad proveedora del servicio de pago (...)", sistema de responsabilidad civil que solo encuentra sus límites en lo preceptuado en el artículo 46, o sea actuación fraudulenta, incumplimiento deliberado o negligencia grave del ordenante.

Y en una más que acerva crítica, señala la SAP que "(…) esta conclusión responde a la lógica aplastante de que, si ha sido la banca la que principalmente se ha beneficiado de las nuevas tecnologías, abaratando costes con el sistema de convertir a los clientes en una especie de empleados suyos sin sueldo, lo que le permite cerrar sucursales y despedir empleados, justo será que se haga cargo de ese margen de riesgo que ha introducido el uso de las nuevas tecnologías y que antes, cuando las operaciones se hacían presencialmente, era inexistente (...)". La exención de responsabilidad bancaria, precisa de una actuación diligente, que no solo haya sus límites reglamentariamente fijados, sino también en los naturales límites del artículo 7 del CC, cobrando especial relevancia "(…) datos tales como, el perfil del cliente, los movimientos inusuales, los importes dispuestos, la hora en que se hace la operación (...)", FJº3º.

Por ello, el robo o sustracción de las claves bancarias no puede ser asimilable a negligencia del usuario, menos aún, grave. Sin que las advertencias genéricas de los bancos desplacen la imputación del riesgo al usuario bancario, no bastando "(…) con medidas genéricas de protección o avisos estereotipados de cuidado, pues tales avisos ostentarían la calificación de "formulas predispuestas", vacías de contenido. No son los clientes los que deben prevenir ni averiguar las modalidades de riesgos que el sistema conlleva, ni prevenir con su asesoramiento experto dichos riesgos (…), FJº3º y cita a la también SAP de Zaragoza, de 9 de julio de 2022. Las cláusulas de exoneración de riesgos, usualmente comprendidas en los contratos de cuenta, de tarjeta o de un servicio de banca on line, no pueden entenderse válidas, en tanto contrarias a un régimen normativo imperativo.

De forma similar a lo más arriba expuesto, localizamos la **SAP de Oviedo, Sección 5ª, n. º 170/2023, de 20 de abril**, que confirma en grado de apelación, la **SJPI, n. º 3, de Oviedo, de 13 de julio de 2022.** Se procede a la condena de la entidad bancaria, al reintegro de operaciones cargadas indebidamente por unas transferencias y operaciones bizum realizados de manera fraudulenta a través de la aplicación de la de dicha entidad. El mecanismo para obtener dicho fraude es idéntico al empleado en otros supuestos "(…) tercera persona autora de la sustracción utilizó el mecanismo denominado "SIM swapping", interesando fraudulentamente de la compañía telefónica un duplicado de la tarjeta SIM del teléfono móvil de la persona con la facultad de disposición y recabar de la entidad financiera las claves de acceso a banca online, que éste recibiría en aquel teléfono móvil y gracias las cuales puede realizar las operaciones fraudulentas (...)", FJº1º.

La entidad bancaria, recurrente en grado de apelación, argumentó con base en el artículo 44 del Real Decreto-Ley 19/2018, que el autor del fraude conocía los datos sensibles, bien a través del usuario, bien por no custodiarlos éste adecuadamente. La actuación negligente del cliente basada en la comunicación a terceros o cuidado de la clave de acceso no resulta acreditada, ni enervada por un certificado del responsable del departamento de banca digital. Tampoco se considera ni 'negligencia' ni 'grave' la demora en la comunicación de la incidencia a la entidad financiera, sobre la base de dos argumentos: "(…) la inoperatividad de una señal de telefónica puede deberse a multitud de causas, entre las que no se encuentra en sus primeros momentos, de acuerdo con criterios de normalidad, la sospecha de un fraude, que además no vendría referida al uso de aquella línea telefónica (...)" y "(…) por el contrario, en cuanto tiene conocimiento al día siguiente de la existencia de las transferencias fraudulentas se puso el cliente en inmediato contacto con la entidad bancaria, no sin superar las dificultades que al efecto suponían los mecanismos de comunicación establecidos por la entidad bancaria para los fines de semana y que no han sido tan siquiera negados por ésta (...)".

Sin embargo, desestimatoria de las pretensiones del actor – usuario de banca online, resulta la **SAP de Madrid, Sección 9ª, n. º 47/2023, de 26 de enero**, que confirma la también desestimatoria **SJPI, n. º 3, de Alcorcón, de 13 de mayo de 2022**. Por el actor se pretendía la devolución de operaciones efectuadas por medio de banca online, que sostenía que eran defraudadoras, de los años 2020 y 2021. La SAP aprecia negligencia grave en la custodia de su clave de acceso a la banca on line desde su teléfono móvil "(…) habiéndose puesto a disposición del defraudador o defraudadores los datos suficientes, este o estos clonaron o duplicaron la tarjeta SIM de la línea móvil titularidad del actor para, mediante la instalación de la aplicación Samsung Pay mediante tal SIM, ratificándose tal instalación mediante la confirmación ofrecida al contestar un SMS del banco (...)" ello en cuanto a las operaciones de 2020 y en cuanto a las de 2021, "(…) no se utilizó tal sistema de pago para las operaciones a efectuar sino que las mismas fueron confirmadas al contestar a SMS del banco remitido a la línea de móvil del demandante (…) y además el demandante ya conocía de las operaciones, que imputaba como fraudulentas, del año 2020.

En el caso de autos por el actor se habían efectuado alegaciones genéricas sobre operativas defraudatorias, lo que provocaba indefensión a la entidad bancaria demandada. "(…) las resoluciones de los tribunales sobre este tipo de defraudaciones examinan si el cliente de la entidad actuó con la diligencia debida, sin la negligencia grave a la que se refiere el precepto ya indicado, valorando la conducta del cliente en orden a la facilitación de sus claves de acceso a la banca *on line* y a su línea telefónica: Así, la SAP A Coruña de 19.10.2022 considera una negligencia grave de la cliente al facilitar la misma su número de tarjeta, pin de acceso a banca móvil y tecleo de 4 números de confirmación remitidos por SMA, ante una mera llamada al teléfono fijo de su domicilio. La SAP de Zaragoza de 1.7.2022, si bien condenó a la entidad bancaria a reintegrar el importe defraudado (por ausencia de autentificación reforzada en ese tipo de operaciones), valoró el acceso a los datos del cliente mediante la recepción de un correo electrónico con un link al que pinchó aquel facilitando el enrolamiento de la tarjeta al sistema de pago. La S AP Barcelona de 23.5.2022 apreció falta de diligencia en lo clientes al contestar a dos emails para descargar una aplicación en el móvil y contratando una tarjeta. La SAP de Madrid de 20.5.2022 condenó al banco al reintegro de cantidades defraudadas tras estudiar que la víctima fue víctima de un phissing al recibir un SMS al móvil asociado a la tarjeta y contrato de cuenta corriente, haciendo clic en un enlace clonado de la web del banco. La SAP de Pontevedra de 1.12.20202 desestimó la demanda frente al banco ya que la demanda hacía referencia únicamente al acceso fraudulento al ordenador del demandante, sin referencia alguna a la utilización indebida del móvil del actor, resultando de la pericial practicada la necesidad de disponer del dispositivo móvil para realizar la transferencia. La SAP Badajoz de 30.12.2021 aprecia negligencia grave de la demandante al responder a un correo irregular y no custodiar debidamente sus claves a fin de garantizar los pagos (...)".

3. El *sim swapping* y la protección de datos

Queremos hacer una breve mención, por su **relación entre el *sim swapping* y la protección de datos** a la **SAN, Sala de lo contencioso-administrativo, Sección 1ª, de 9 de febrero de 2023**, que desestima el recurso contencioso administrativo, interpuesto por una operadora de telefonía, frente a la Resolución de la Directora de la Agencia Estatal de Protección de Datos, que confirma en reposición la resolución por la que se le impone a la operadora, una sanción de 200.000 euros, por vulneración del art. 5.1 f) del Reglamento General de Protección de Datos[7].

El principio de confidencialidad de los datos se habría visto afectado, dado que la operadora, facilitó a terceros distintos del titular del teléfono móvil, duplicados de SIM, que constituyen el soporte mediante el cual se accede a datos de carácter personal del afectado. Acceso a datos personales del titular por un tercero que se produjo debido a que la operadora en liza, no contaba con medidas bastantes ni adecuadas en los términos del reseñado art. 5.1.f) del RGPD para comprobar que la persona que solicita el duplicado de la tarjeta SIM es el titular de la misma.

La Sentencia confirma en la jurisdicción, la sanción impuesta en el previo procedimiento administrativo sancionador, al cumplirse los principios de culpabilidad, responsabilidad

[7] La imposición de cuantiosas sanciones administrativas a las operadoras, en los supuestos de duplicado de tarjeta SIM ha generado importantes titulares, véase https://www.elespanol.com/invertia/empresas/tecnologia/20220203/proteccion-millones-operadoras-duplicados-fraudulentos-tarjetas-sim/647185524_0.html

personal, tipicidad, confianza legítima y buena fe, previstos en la Ley 40/2015, de 1 de octubre.

No obstante, ha habido pronunciamientos favorables a las operadoras, como la **SAN, Sala de lo contencioso-administrativo, Sección 1ª, de 22 de marzo de 2012**, cuando la operadora ha probado el cumplimiento de una diligencia razonable, así como ausencia del elemento subjetivo de culpabilidad necesario en la actuación de la operadora de telefonía.

Y es que la AEPD, dentro del marco de sus competencias, se ha pronunciado en dos ocasiones sobre el *sin swapping* y su relación con el tratamiento de datos por las operadoras telefónicas y por las FFCCSS en el ámbito de la investigación policial de estafas informáticas.

Así, en la **Consulta 48/2023**[8], sobre la adecuación al RGPD[9] y LOPDGDD[10] de determinados tratamientos de datos personales en la contratación y entrega de productos de operadores de telecomunicaciones, en relación a la solicitud de una fotocopia del DNI para obtener un duplicado de la SIM, "(…) siguiendo al apartado 76 del ciado Dictamen 1/2022, la información del documento de identidad que no sea necesaria para confirmar la identidad del interesado, en el contexto concreto, tal y como por ejemplo, el número del documento, la fotografía, o los datos que se pueden leer por máquina, nos lleva a concluir que la solicitud del DNI con la toma de una copia del mismo sería, en principio, un tratamiento excesivo, y que no puede instaurarse por sistema, sino que habrá que analizar, caso por caso, multitud de aspectos, que van desde la base jurídica que legitima dicho tratamiento, sobre todo si está previsto en la ley, hasta el riesgo de dicho tratamiento teniendo presente el principio de minimización y la proporcionalidad de dicha (…)".

Por su parte, la **Consulta 30/2021**[11], sobre adecuación al marco jurídico respecto del acceso por parte de las FFCCSS a la información de la que disponen las operadoras de telecomunicaciones, derivado de los servicios que prestan, trata con gran profundidad el fraude a través de *sim swapping* y las medidas que, tanto operadoras de telefonía, como entidades bancarias que proporcionan servicios de pago, han de adoptar en materia de tratamiento de datos personales, derivados de solicitud de duplicado de tarjeta SIM, ofreciendo las siguientes conclusiones:

- Las operadoras están **obligadas a proporcionar la información sobre vinculación IMEI e IMSI**, así como los **datos conexos al proceso de duplicado de la SIM**, siempre que no se encuentren vinculados a un proceso de comunicación –en ese caso se requiere autorización judicial- para la persecución del delito que hay detrás del *sim swapping*.

- Para dicho fraude es preciso que un tercero suplante la identidad del titular de los datos, para recibir el duplicado de la SIM, lo que supone un **tratamiento de datos por un tercero al margen del principio de licitud**, con vulneración de los principios de confidencialidad e integridad.

[8] https://www.aepd.es/documento/2023-0048.pdf

[9] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

[10] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

[11] https://www.aepd.es/documento/2021-0030.pdf

- Por dicha razón, este es un proceso en donde la diligencia **prestada por las operadoras** es fundamental para evitar este tipo de estafas y vulneraciones del RGPD. Diligencia que se traduce en el establecimiento de **medidas adecuadas** para garantizar que el tratamiento de datos es conforme al RGPD. Las operadoras como responsables del tratamiento, deben cumplir con los

  principios del artículo 5 RGPD[12] y aplicar las medidas técnicas y organizativas de los artículos 24.1[13], 25[14] y 32.1 b) y d)[15] del mismo cuerpo legal.

- Las operadoras deben de estar en disposición de establecer **mecanismos que impidan que se produzcan la duplicación fraudulenta de las tarjetas SIM**, medidas que respecten la integridad y confidencialidad de los datos y que

---

[12] 1. Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»); b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»); c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»); d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»); e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las
medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»); f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

[13] Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

[14] 1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados. 2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas. 3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

[15] Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

impidan que un tercero acceda a datos que no son de su titularidad, pues precisamente compete a la operadora tratar datos de carácter personal conforme al RGPD. **Responsabilidad proactiva** que deriva del artículo 5.2 RGPD[16].

- **No puede repercutirse en el usuario las carencias de un sistema de emisión de duplicados que abarque los supuestos al margen del procedimiento físico**, pues si la compañía ha establecido, entre otras, dicha posibilidad, debe en igual medida comprobar que el tratamiento de datos que sea necesario para tal fin (emisión del duplicado de la SIM) reviste de todas las garantías para cumplir con el RGPD.

- Y por lo que respecta a las **entidades bancarias**, que proporcionan servicios de pago, en cuyo ámbito se inicia este tipo de estafas, ya que el tercero tiene acceso a las credenciales del usuario afectado y se hace pasar por este, son responsables del tratamiento de los datos de sus clientes, les competen **idénticas obligaciones** que las señaladas hasta ahora para las operadoras referidas al cumplimiento del RGPD y la LOPDGDD, y además las derivadas del Real Decreto-ley 19/2018.

- La estafa requiere la **vulneración de al menos dos capas de seguridad**, la de la propia identificación y la de la operación en si misma considerada. Por ello las entidades financieras, deben establecer todas las medidas necesarias para que la identificación y la autenticación sea eficaces de modo que impidan o dificulten la comisión de este tipo de fraudes

4. Respuestas al ciber fraude en el orden jurisdiccional penal

En la jurisdicción penal hemos encontrado diversos ejemplos de *sim swapping* en los que se aprecia un **perfeccionamiento del *modus operandi*,** por ejemplo, mediante la solicitud de numerosas tarjetas de crédito asociadas a una misma cuenta por un único titular, para poder realizar, obtenido el ilícito desplazamiento, múltiples extracciones de efectivo, con la intención de dificultar su trazabilidad; el empleo de documentos falsificados o en ocasiones la receptación de bienes y servicios adquiridos mediante ilícitas transferencias que han, en expresión popular, 'vaciado' la cuenta corriente del perjudicado.

Nuestra primera mención es la **SAP de Soria, Sección 1ª, nº 70/2023, de 21 de julio**, en la que la condena es como **cooperador necesario de un delito de estafa informático continuado[17]**.

Suscita nuestro interés que el Ministerio fiscal en su escrito de calificación, solicitó la condena del encausado como autor –no como cooperador necesario- de un delito de estafa continuado agravado. La acusación particular, ejercitada por una entidad bancaria –dado que los perjudicados fueron resarcidos previamente en el importe total de la cuantía defraudada-

[16] El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

[17] Artículo 249.1 a) del Código Penal: 1. También se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años: a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

solicitaba la condena por un delito continuado de estafa informática, un delito continuado de blanqueo de capitales, un delito continuado de blanqueo de capitales por imprudencia grave, un delito continuado de receptación y un delito continuado de apropiación indebida.

Calificación que no compartimos, por ser algunos tipos penales, incompatibles con otros –como que un mismo encausado cometa primero el delito de blanqueo de forma dolosa y luego de forma imprudente- desde el punto de vista del elemento subjetivo; o por incorporarse los elementos de la estructura del tipo penal, en otro más especial –principio de especialidad- como acontece entre el delito de receptación y el delito de estafa informático.

Igualmente llama nuestra atención que, en el relato de hechos probados, se reconoce expresamente la intervención de terceras personas, desconocidas en su filiación y no enjuiciadas en dicho momento, con las que sin embargo existiría reparto de funciones y concierto de voluntades, tanto para la acción como para el resultado, elaborando para ello un plan con el común acuerdo de todos para obtener un beneficio patrimonial ilícito.

Los hechos probados, sucintamente, consisten en que el encausado aperturó personalmente una cuenta corriente, entregándosele una tarjeta; días después, por medio de la banca digital, solicitó hasta 20 tarjetas de crédito y de débito y las distribuyó entre terceras personas desconocidas, pero con las que estaba en connivencia y formaban parte del entramado defraudatorio. Se aprecia un arranque de la estructura de la estafa, más elaborado que en el ámbito civil. Posteriormente se pasaría a la primera fase del *sim swapping*, consistente en la obtención, por tercera persona desconocida, de un duplicado de la SIM. Nos resulta sorprendente que, si bien no se enjuicia a dicha persona, no se recoja de forma más clara, lo que puede suponer un delito de usurpación o un delito contra la intimidad, porque el duplicado se obtuvo empleando la fotocopia del DNI de la posteriormente, perjudicada, así como una falsa autorización para obtener el duplicado por tercera persona.

Obtenido el duplicado SIM, también por tercero desconocido pero en connivencia con el encausado se insertó en un teléfono móvil, accediendo a continuación al área de clientes online, donde se realizaron dos transferencias -por valor de 15.000 euros y de 14.900 euros-, no consentidas, de dinero, desde la cuenta corriente del perjudicado a la del encausado, si bien nuevamente esta segunda parte del andamiaje del *sim swapping*, lo que es propiamente la obtención del inconsentido desplazamiento patrimonial, fue efectuado por tercera persona, pero en connivencia con el encausado. Todo el dinero fue extraído el mismo día, en diversas localidades, por medio del uso de tarjetas asociadas a la cuenta del encausado. Además, descartando cualquier tipo de circunstancia exculpatoria, se recalca en los hechos probados que el encausado no denunció haber recibido indebidamente las importantes sumas en su cuenta corriente, ni haber sufrido una suplantación de su personalidad.

La AP aprecia que los hechos encajan en el delito de estafa, previsto y penado en el artículo 248.2 del Código Penal, denominado 'informática', con mención a las SSTS de 12 junio 2007, de 16 marzo del año 2009, 25 octubre del año 2012 y 28 de diciembre de 2022 y especialmente a la **SAP de Valladolid, nº 645/2023, de 24 de abril,** teniendo en cuenta una valoración conjunta de la prueba practicada en el plenario.

Y ello porque, si bien es cierto que a lo largo del perfeccionamiento del *sin swapping* intervienen, reiteradamente, terceras personas desconocidas, del acervo probatorio se desprenden diferentes datos de los cuales se infiere que el acusado formaba parte de una organización cuyo propósito es perpetrar estafas informáticas, como son, principalmente, la apertura de la cuenta corriente en la que recibir las transferencias ajenas, la solicitud de múltiples tarjetas de crédito y debido, la recepción de dos sustanciosas sumas de dinero, es

decir, que "(…) ha llevado a cabo un aporte esencial y consciente a la ejecución de un hecho ajeno (…)", FJº4º.

Asimismo, se consideran indicios relevantes de su cooperación en la trama defraudatoria, el escaso importe aportado a la cuenta corriente a pesar de haber manifestado querer ahorrar, la proximidad temporal entre todos los hechos, el número inusitado de tarjetas solicitadas por el encausado; "(…) resulta lógico pensar que el acusado, como titular de la cuenta bancaria, es quien ha tenido el control de la misma y de las tarjetas asociadas a la citada cuenta, que, por lo demás, como ya se ha indicado fueron entregadas en su domicilio (…)", FJº4º.

Por su parte, en la **SAP de Jaén, Sección 3ª, nº 133/2022, de 3 de mayo**, por el Ministerio Fiscal se evacuó escrito de calificación, solicitando la condena del acusados como autor de un **delito de blanqueo de capitales por imprudencia grave**[18]. La Sentencia se dicta en conformidad con el acusado, con aplicación de atenuante de reparación del daño causado y sin pronunciamiento sobre la responsabilidad civil, considerando probado que éste participó en una suerte de 'ingeniería social' que le permitió lucrarse, mediante la realización de un acto esencial que permitió encubrir el origen ilícito del dinero –suponemos que facilitar una cuenta corriente de su titularidad-.

En esa suposición en que nos hayamos, se considera probado que terceras personas desconocidas, por mor de la técnica del *sin swapping,* obtuvieron datos personales relevantes –dni, número de teléfono y número de cuenta corriente-, obtuvieron un duplicado de la tarjeta SIM y seguidamente al tener acceso al código de doble verificación, pudieron efectuar operaciones con banca on line, en una de las cuales se lucró el encausado.

Sinceramente, no entendemos el relato de hechos probados, ni tampoco la condena, dado que no se explican dichos extremos, a la luz de que también se declara probado que fue el encausado quien acudió a la comisaría a denunciar que se había quedado sin línea y había recibido una llamada de su operadora telefónica, manifestándole que le habían duplicado la SIM y que comprobase su cuenta corriente. En la denuncia se recogían diversas operaciones bancarias de fecha anterior y solamente consta una de fecha posterior a la denuncia, una transferencia a favor de la cuenta corriente del actor, por importe de 1000 euros, que satisfizo antes del plenario.

En ese sentido, consideramos, para acoger tal calificación, ha de quedar debidamente probada la omisión de las más elementales pautas de cuidado, que requiere la comisión del tipo de blanqueo por imprudencia grave –de ahí que aboguemos por la calificación de delito de estafa informática a título de cooperador necesario-.

Y es que como recuerda GONZÁLEZ URIEL[19] "(…) la forma culposa recae sobre el desconocimiento de la procedencia de los bienes. En este sentido, no requerimos un específico deber de conducta o vigilancia que venga establecido por la normativa administrativa, sino que

[18] Artículo 301.1 del Código Penal: El que adquiera, posea, utilice, convierta, o transmita bienes, sabiendo que éstos tienen su origen en una actividad delictiva, cometida por él o por cualquiera tercera persona, o realice cualquier otro acto para ocultar o encubrir su origen ilícito, o para ayudar a la persona que haya participado en la infracción o infracciones a eludir las consecuencias legales de sus actos, será castigado con la pena de prisión de seis meses a seis años y multa del tanto al triplo del valor de los bienes. En estos casos, los jueces o tribunales, atendiendo a la gravedad del hecho y a las circunstancias personales del delincuente, podrán imponer también a éste la pena de inhabilitación especial para el ejercicio de su profesión o industria por tiempo de uno a tres años, y acordar la medida de clausura temporal o definitiva del establecimiento o local. Si la clausura fuese temporal, su duración no podrá exceder de cinco años. 3. Si los hechos se realizasen por imprudencia grave, la pena será de prisión de seis meses a dos años y multa del tanto al triplo.

[19] GONZÁLEZ URIEL, D., *Aspectos básicos del delito de blanqueo de dinero*, Ed. Comares, Granada, 2021, págs. 314-315.

en cualquier transacción comercial o financiera, incluso entre sujetos que no se hallen especialmente obligados, han de cumplirse unos mínimos estándares de diligencia o de cautela. Por este motivo, dado que lo concebimos como un delito común, puede ser cometido tanto por particulares como por individuos especialmente obligados por las normas que disciplinen su profesión u oficio […] la diligencia que ha de desplegarse en la vida negocial lleva a que los participantes en el mercado no puedan obviar de forma grosera las más mínimas precauciones a la hora de transferir bienes, de constituir derechos reales o de crédito sobre ellos, de efectuar transmisiones o de llevar a cabo actos que puedan suponer su enmascaramiento. No se trata solo del interés particular o privado de la operación en cuestión, sino que el bien jurídico tutelado, la licitud de los bienes en el tráfico económico-financiero de curso legal, es de carácter general o global, y conlleva que todos los partícipes en el mercado deben observar unas mínimas medidas de precaución, de atención y de alerta. Asimismo, se tiene en cuenta que la imprudencia punible es la «grave», es decir, cuando se omitan las más elementales pautas de cuidado (…)".

Más acertada en su calificación, nos parece la **SAP de Valladolid, Sección 4ª, nº 83/2023, de 24 de abril**, que confirma la sentencia condenatoria en la instancia, por un delito de estafa informática mediante duplicación de tarjeta telefónica., en calidad de cooperador necesario. En la Sentencia se recoge el elaborado artificio informático empleado para la obtención de los fondos depositados en la cuenta corriente del perjudicado; aunque se reconoce que el encausado no participó en la manipulación informática, sí fue receptor de las transferencias no consentidas y conocedor de la procedencia ilícita del dinero percibido. Y es que con la prueba allegada, se considera probado más allá de toda duda razonable, que el encausado se valió de 'hombres de paja', a los que solicitaba recibir dinero en cuentas de su titularidad para luego entregárselo en mano, bajo la excusa de que su cuenta estaba bloqueada y embargada. Método que, además, dificulta la trazabilidad del origen ilícito del dinero.

5. Conclusiones

En la constante **búsqueda por la obtención de un desplazamiento patrimonial no consentido**, los delitos contra el patrimonio y singularmente, la **estafa informática**, han experimentado una notable evolución, con el surgimiento de la figura típica del *sim swapping* o estafa por intercambio de tarjetas SIM, siendo que la estafas de dicha clase comienzan a ser las mayoritarias dentro de los delitos contra el patrimonio[20].

Estafa informática que, combinando una **estructura piramidal** basada en **la ingeniera social**, el **uso fraudulento de la inteligencia artificial** y el **quebranto de los sistemas de verificación en dos pasos**, busca conseguir un resultado tan manido, como es una transferencia inmediata, un préstamo rápido o el uso de app's que permiten enviar y recibir dinero sin más complicaciones que un simple click.

El resultado obtenido, por tanto, no varía, tan solo la **sofisticación** en la ejecución de la estafa informática, caracterizada por un **estadio preliminar de búsqueda de datos sensibles**, con quiebra de la intimidad personal y empleo de torticeras técnicas, como el *phishing*; una primera fase de obtención del **duplicado** de la tarjeta SIM empleando una gama de medios para su consecución, físicos o telemáticos y una segunda fase de quiebra del sistema de verificación

[20] Véase https://www.europapress.es/la-rioja/noticia-fiscalia-senala-aumento-delitos-contra-libertad-sexual-estafas-informaticas-20230913143418.html o https://www.interior.gob.es/opencms/es/detalle/articulo/Las-fuerzas-y-cuerpos-de-seguridad-registraron-287.963-ciberdelitos-en-2020-un-32-por-ciento-mas-que-en-2019/

de dos pasos, con recepción de los manidos 'sms de confirmación' de las app's bancarias, accediendo a la banca online del perjudicado.

Sin duda, **sustituir uno de los dos factores de autenticación**, en concreto el factor 'algo que yo tengo' (factor físico, normalmente el código de verificación SMS que se suele recibir en la tarjeta SIM asociada a un número de teléfono móvil), como es el terminal telefónico, por el factor 'algo que yo soy' (factor inherente), es decir, la biometría, unido al factor más tradicional 'algo que yo sé' (factor de conocimiento), cortaría de raíz esta clase de estafas, al hacer el sistema de verificación en dos pasos, inaccesible a persona distinta al auténtico titular de la línea.

Y todo ello desde la perspectiva de que la autenticación de múltiples factores (**MFA o *multi factor authentication***) es otra posibilidad en liza, aunque quizás los usuarios podrían llegar a rechazarla, por su complejidad, dado que requiere de la presentación, por el usuario, de dos o más pruebas diferentes de que es quien dice ser.

El **ordenamiento jurídico español está preparado para dar respuesta a las nuevas formas de cibercriminalidad**, como el *sim swapping*, protegiendo los derechos de los perjudicados a través de la aplicación del clásico **delito de estafa informática del artículo 249.1 a) del Código Penal** o bien con la gama de medidas, preventivas y resarcitorias, del **Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera.**

A nuestro juicio, es nuestra **intimidad personal** y los datos especialmente sensibles que la integran, intimidad actualmente proyectada telemáticamente, la parcela que queda más desprotegida, siendo que muchas veces las **sanciones pecuniarias** en materia de protección de datos son más bien, el 'parche' que se pone tras la quiebra de la personalidad de nuestros datos, que han pasado de ser 'personales' a ser 'públicos' y mal utilizados.

Frente a la **pérdida de la privacidad de nuestros datos**, poco o nada podemos hacer cuando somos nosotros mismos los que hacemos dejación de ellos, 'regalando' nuestra intimidad a golpe de click y coste cero. Porque si hay algo que es sabido, es que **cuando algo es gratis, el precio eres tú y tus valiosos datos personales**. No podemos sino finalizar con una reflexión a modo preventivo: ¿si antes cuando andabas por la calle, no le dabas tus datos o la fotocopia de tu DNI a un desconocido, por qué ahora la entregas graciosamente a un desconocido telemático?

En Castellón, a 25 de Octubre de 2023.

Bibliografía

CABEZAS BERDIÓN, L., "El intercambio de tarjeta sim o sim swapping. Concepto y formas de ejecución", Centro de Estudios Jurídicos, Taller sobre la estafa 2FA mediante el intercambio de tarjeta SIM, Madrid, 2021.

FORADADA BERMEJO, J.A., "Medidas encaminadas a erradicar o a minimizar el impacto en la realidad socioeconómica del sin swapping", Centro de Estudios Jurídicos, Taller sobre la estafa 2FA mediante el intercambio de tarjeta SIM, Madrid, 2021.

GONZÁLEZ URIEL, D., *Aspectos básicos del delito de blanqueo de dinero*, Ed. Comares, Granada, 2021.

PERALTA GUTIÉRREZ, A., y TORRES LÓPEZ, L.S., *El derecho y la inteligencia artificial*, Ed. Universidad de Granada, Granada, 2022.

PILLADO QUINTAS, V., "Investigación Judicial de la modalidad delictiva de SIM Swapping. Calificación Jurídica y Cuestiones Prácticas cara el acto de Juicio Oral", Centro de Estudios Jurídicos, Taller sobre la estafa 2FA mediante el intercambio de tarjeta SIM, Madrid, 2021.

Índice jurisprudencial