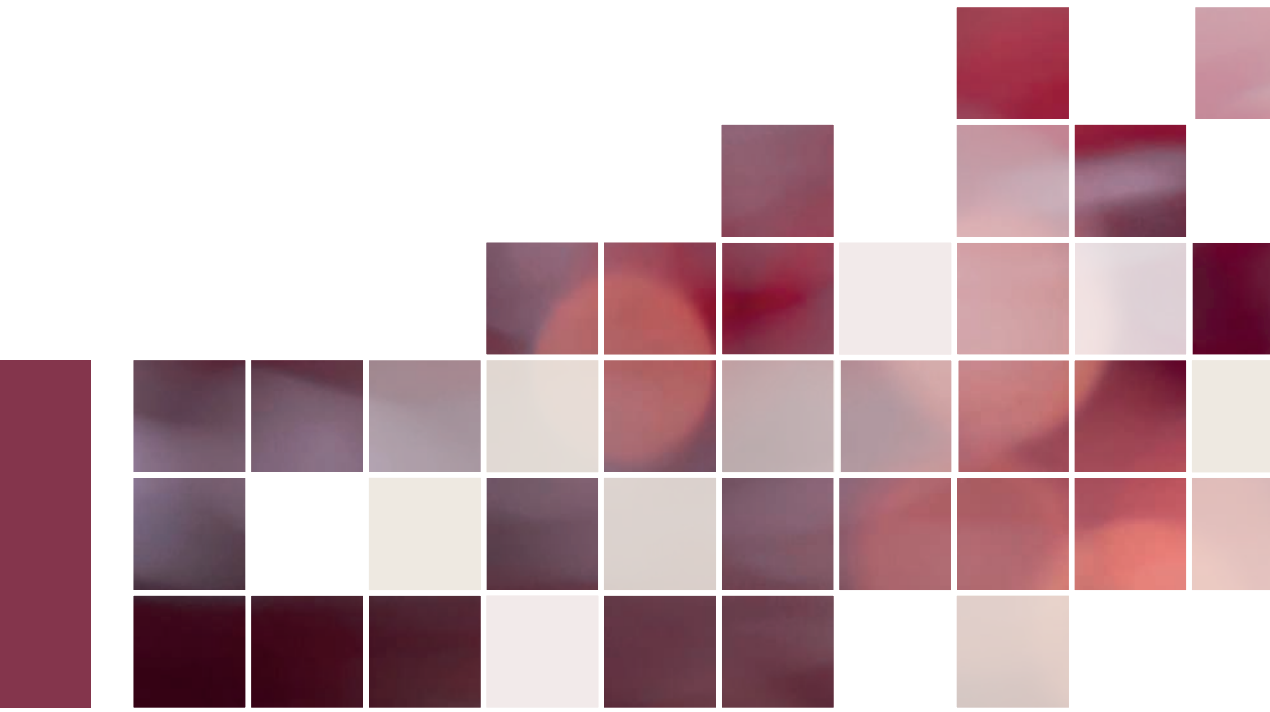
TEMAS

Fraude digital y contra medios de pago

Defraudaciones mediante phishing, bizum; criptoactivos, tokens y otros medios de pago

Eloy Velasco Núñez



LA LEY

© **Eloy Velasco Núñez**, 2024
© **LA LEY Soluciones Legales, S.A.U.**

LA LEY Soluciones Legales, S.A.U.
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 91 602 01 82
e-mail: clienteslaley@aranzadilaley.es
https://www.aranzadilaley.es

Primera edición: Noviembre 2024

Depósito Legal: M-24505-2024
ISBN versión impresa: 978-84-10292-27-7
ISBN versión electrónica: 978-84-10292-28-4

Diseño, Preimpresión e Impresión: LA LEY Soluciones Legales, S.A.U.
Printed in Spain

© LA LEY Soluciones Legales, S.A.U. Todos los derechos reservados. A los efectos del art. 32 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba la Ley de Propiedad Intelectual, LA LEY Soluciones Legales, S.A.U., se opone expresamente a cualquier utilización del contenido de esta publicación sin su expresa autorización, lo cual incluye especialmente cualquier reproducción, modificación, registro, copia, explotación, distribución, comunicación, transmisión, envío, reutilización, publicación, tratamiento o cualquier otra utilización total o parcial en cualquier modo, medio o formato de esta publicación.

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la Ley. Diríjase a **Cedro** (Centro Español de Derechos Reprográficos, **www.cedro.org**) si necesita fotocopiar o escanear algún fragmento de esta obra.

El editor y los autores no asumirán ningún tipo de responsabilidad que pueda derivarse frente a terceros como consecuencia de la utilización total o parcial de cualquier modo y en cualquier medio o formato de esta publicación (reproducción, modificación, registro, copia, explotación, distribución, comunicación pública, transformación, publicación, reutilización, etc.) que no haya sido expresa y previamente autorizada.

El editor y los autores no aceptarán responsabilidades por las posibles consecuencias ocasionadas a las personas naturales o jurídicas que actúen o dejen de actuar como resultado de alguna información contenida en esta publicación.

LA LEY SOLUCIONES LEGALES no será responsable de las opiniones vertidas por los autores de los contenidos, así como en foros, chats, u cualesquiera otras herramientas de participación. Igualmente, LA LEY SOLUCIONES LEGALES se exime de las posibles vulneraciones de derechos de propiedad intelectual y que sean imputables a dichos autores.

LA LEY SOLUCIONES LEGALES queda eximida de cualquier responsabilidad por los daños y perjuicios de toda naturaleza que puedan deberse a la falta de veracidad, exactitud, exhaustividad y/o actualidad de los contenidos transmitidos, difundidos, almacenados, puestos a disposición o recibidos, obtenidos o a los que se haya accedido a través de sus PRODUCTOS. Ni tampoco por los Contenidos prestados u ofertados por terceras personas o entidades.

LA LEY SOLUCIONES LEGALES se reserva el derecho de eliminación de aquellos contenidos que resulten inveraces, inexactos y contrarios a la ley, la moral, el orden público y las buenas costumbres.

Nota de la Editorial: El texto de las resoluciones judiciales contenido en las publicaciones y productos de **LA LEY Soluciones Legales, S.A.U.**, es suministrado por el Centro de Documentación Judicial del Consejo General del Poder Judicial (Cendoj), excepto aquellas que puntualmente nos han sido proporcionadas por parte de los gabinetes de comunicación de los órganos judiciales colegiados. El Cendoj es el único organismo legalmente facultado para la recopilación de dichas resoluciones. El tratamiento de los datos de carácter personal contenidos en dichas resoluciones es realizado directamente por el citado organismo, desde julio de 2003, con sus propios criterios en cumplimiento de la normativa vigente sobre el particular, siendo por tanto de su exclusiva responsabilidad cualquier error o incidencia en esta materia.

ÍNDICE SISTEMÁTICO

No es casualidad que la estafa esté regulada en la Sección 1ª del Capítulo VI de las **defraudaciones**, del Título XIII de los delitos **contra el Patrimonio y contra el orden socioeconómico** del Libro II de los delitos (y sus penas) del Código Penal.

Esa **ubicación sistemática** recalca que el delito que vamos a estudiar, con atacar el patrimonio y el orden socioeconómico —afectando, como veremos también, otros bienes sociales igualmente protegibles[1]—, pertenece —junto con la administración desleal, la apropiación indebida y las defraudaciones de fluido eléctrico y análogas— al **género** de las defraudaciones, o del fraude, por singularizarlo.

Fraude —económico[2]— que, se caracteriza por la transferencia/desplazamiento —apoderamiento—, a veces desconocido, siempre inconsentido, de activos patrimoniales de (el poder de disposición de) uno a otro sujeto, mediante diferentes modalidades o maneras comisivas —engaño, tergiversación, manipulación, artimaña, ocultación...—, que benefician ilícitamente a su autor o a un tercero por él, perjudicando el patrimonio origen del desplazamiento/transferencia.

Ínsitos al fraude aparecen siempre como **características**:

a) una actuación ilícita, deshonesta, clandestina, contraria al actuar debido y

b) la búsqueda de un lucro o provecho —en nuestro caso, económico—, y/o la generación de un perjuicio de esa naturaleza, a aquel a costa de cuyo patrimonio se consigue.

(1) Como la integridad de los datos o sistemas informáticos en la estafa informática o la protección de (la confianza en) los medios de pago alternativos a la moneda de curso legal, en la hecha con instrumentos de pago distintos del efectivo.

(2) Para diferenciarlo en el ámbito penal del fraude cometido por funcionario público, o fraude de concertación, previsto y penado en el art. 436 CP.

La Directiva (UE) 2019/713, del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo (en adelante **D 2019/713**), inspiración de la reforma del Código Penal operada en esta materia mediante L. O. 14/2022, de 22 de diciembre, en su Art. 6 describe el **fraude** como: «*la realización o causación de una transferencia de dinero, de valor monetario o de moneda virtual, con el ánimo de procurar un beneficio económico ilícito para el autor o un tercero ocasionando en consecuencia un perjuicio patrimonial ilícito a otra persona*».

Se diversifica el fraude económico, sin embargo, en varias **modalidades**, según nos fijemos en:

– **sobre quién/qué** se causa (persona física, máquina, dato o sistema informático, medio de pago, subvención pública, Hacienda...),

– cómo se causa (engañando, generando error, manipulando, suplantando, interfiriendo, abusando de la confianza o excediéndose de las facultades de administración recibidas...) o simplemente si se ocasiona ilícitamente beneficiándose económicamente de algo que sufraga otro sin saber o sin querer.

De ahí que la **estafa**, caracterizada por el modo comisivo activo de engañar o el pasivo de hacer sufrir un error que induzca a la víctima a realizar un acto perjudicial de disposición económica, sea una **modalidad del fraude**.

Estafa que, dentro de las diversas maneras de apoderarse del dinero o de los activos económicos ajenos, al llevarse a cabo mediante el uso del engaño y la generación de error, excluye otras vías más físicas y expeditivas de actuación (robo con fuerza, intimidación, violencia, hurto...)[3] menos civilizadas, más salvajes, erigiéndose en **la más intelectual manera de depredar el patrimonio ajeno**, razón por la que, según un país la use más o menos, se le suele identificar como una *«sociedad más o menos civilizada»*.

Sociedades avanzadas que, caracterizadas por haber desplegado una inusitada **transformación digital y tecnológica**, a la vez que evolucionado sus medios de pago y representación de valor, igualmente han ido variando el panorama criminal de la estafa misma.

Así, a la vez que se siguen produciendo estafas caracterizadas por el engaño, la irrupción de la Informática y sus aplicaciones en la **digitalización**

(3) Cicerón indicaba: «*Duobus modis fit iniuria: aut vi aut fraude*» *De officiis*, libro 1, capítulo XIII, n.º 41.

de nuestro mercado, y por ende, de nuestra sociedad, ha impulsado, como pocas, y sobre todo en el campo económico, las maneras en que este delito se manifiesta en la vida real, hasta convertirlo en el delito informático[4] más acaecido estadísticamente —de cada 100 delitos cibernéticos (375.506 en 2023 en España), el 90'4% son fraudes informáticos— de manera que, por un lado, conforme hemos ido ampliando su concepción clásica —para incluir modalidades más allá de las ocasionadas mediante engaño— con expresiones genéricas como la de «fraude», por otro, lo hemos ido troceando y parcelando hasta la **especialización**, de modo que, en puridad, hemos reservado el término «defraudación» para las subespecies del género donde, sin engaño, pero ilícitamente, alguien sufraga y sufre el coste económico, mientras otro correlativamente lo elude y se favorece con alguna prestación no debida (Art. 255 CP) —figura que tratamos en el Epígrafe 10 como defraudación tecnológica—.

En el presente estudio trataremos especialmente de analizar la delincuencia vinculada a lo que antes se conocía como estafa informática que, con el desarrollo de la digitalización, ahora extenderemos al **fraude informático/tecnológico/digital** —Art. 249 CP—; añadiremos un breve epígrafe para analizar también la **defraudación tecnológica** —Art. 255 CP—; y por su relación, especialmente en lo referente a los medios de pago, acabaremos tratando la **falsificación** de tarjetas de crédito y débito, cheques de viaje y demás instrumentos de pago distintos del efectivo (en adelante, IPDEs), —Art. 399 bis CP—, también denominados alternativos, a veces menos corpóreos, menos tangibles, más digitales, que, sobre la base de la tecnología de registro distribuido (blockchain) y otros aplicativos electrónicos —i. e.: bizum— están irrumpiendo con fuerza en las transacciones del llamado **mercado digital**, y por ende, están focalizando nuevas modalidades delictivas asociadas a ellos, que, en algunos casos, consisten en ataques a los mismos para hacerse con —apoderarse de— los valores económicos —**tokens**— que encierran, y en otros, en su mendaz alteración o creación, para defraudar después con ellos.

Igualmente, no podría ser de otro modo, pretendemos abarcar también la generación de esa transferencia patrimonial inconsentida (fraudulenta) cuando esta opera mediante el uso de la **Inteligencia Artificial** (en adelante IA), aprovechando para estudiar también la aplicación de esa nueva «constelación de tecnologías», en lo procesal, para combatir el fraude.

(4) Estudio sobre la cibercriminalidad en España. Ministerio del Interior de España 2022. Pág. 27. https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2022/Informe-Cibercriminalidad-2022

Panorama de cambios que, en parte, ha pretendido actualizar la **Directiva UE 2019/713** sobre lucha contra el fraude y falsificación de medios de pago distintos del efectivo (que sustituye la DM 2001/413/JAI), donde se **amplían las acciones y penas** con que afrontarlas, así como los **objetos de protección**, que giran en torno a los IPDEs —instrumentos de pago distintos del efectivo—, para incluir los medios de pago digitales/tecnológicos (pago a través de móvil, dinero electrónico, monedas virtuales...) que permiten transferir **valor monetario**, esto es, los denominados **E-money tokens**, excluyendo los tokens no monetarios (utility tokens, —valores de servicio— y los security tokens, —o valores de inversión—).

La D 2019/713, además, **no** admite la modalidad **imprudente**, aunque sí el dolo inferido por circunstancias objetivas, fácticas, y conforme a su Art. 8 sanciona la **inducción, la complicidad y la tentativa**, así como la cometida por **Persona Jurídica** en su beneficio, a la que anuda penas de multa e interdictivas y de otra naturaleza —en el caso español, recogidas en el Art. 33.7 CP—.

Junto con lo anterior, la D 2019/713, en esa ampliación de conductas y sanciones, a la vez que mantiene las **infracciones de resultado** —fraude relacionado con sistemas de información y uso fraudulento de IPDEs—, aumenta el número de **actos preparatorios** que penaliza, referidos a instrumentos de pago, ya sean materiales, ya inmateriales, y las herramientas que los posibilitan, sancionándolos con penas semejantes en función del **riesgo** de fraude que suponen y pretendiendo amparar no sólo los activos patrimoniales involucrados, sino también la confianza en ellos y el mercado que posibilitan.

6.1. DEFRAUDACIONES CON INTELIGENCIA ARTIFICIAL

La irrupción reciente de **aplicaciones que utilizan Inteligencia Artificial** (en adelante IA) mediante algoritmos programados y entrenados para engañar humanos o incluso para entrometerse en procesos de pago, adquisición o transacciones automatizadas, con el objetivo de transferir inconsentidamente dinero o activos a su autor, nos obliga, siquiera sea brevemente, a analizar penalmente esas posibilidades que llevan ya tiempo ocurriendo en el mercado digital.

En concreto, la digitalización y automatización posterior de procesos involucrando **reclamos** (cada vez menos llamativos para evitar su detección por programas informáticos antifraude), lleva tiempo usándose ayudando al delincuente no solo a multiplicar sus efectos dañinos al expandirlo entre más posibles víctimas, sino además, a evitar su identificación o las medidas de seguridad para detectar su mendacidad y a poner distancia física entre ellos de manera que hacen inefectiva la reacción de quienes los detecten, aumentando su impunidad.

La rentabilidad a la inversión que supone para el delincuente el gasto que le genera hacerse con el reclamo suplantador se obtiene de la difusión maquinal automatizada que permite multiplicar el número de posibles víctimas en el tiempo, y el hecho de que siempre hay un porcentaje rentable de estas que acaban «picando», aunque transaccionen cantidades pequeñas de dinero, de manera que, como explicábamos más arriba, el legislador no haya tenido más remedio que combatir estos fenómenos masivos delictivos mediante la tipificación penal de la confección/uso de herramientas diseñadas para ayudar a defraudar y descartar la discriminación penológica sobre cantidades inferiores a los 400 euros, adelantando la barrera punitiva incluso a la obtención de ilícitos beneficios y protegiendo como bien jurídico concurrente la seguridad de las transacciones y medios de pago usados en este nuevo mercado digital.

El riesgo mayor, envolviendo técnicas y aplicaciones con IA, deviene de la utilización de **manipulaciones de información**, falsedades que, desde una perspectiva penal, si operan y pretenden transacciones comerciales on line o económicas —entregas de dinero, bienes o servicios—, o permiten la realización de pagos o los derivan o desvían, podrán perseguirse como **concursos mediales** de delito de falsedad en documento electrónico mercantil (Art. 392 CP) con estafa, bien del Art. 248 CP si basculan sobre el engaño en el usuario y precisan del concurso de la actuación de la propia víctima, o del Art. 249 CP si, mediante un clic inicial, se pone en marcha la manipulación sobre el sistema o los datos de la víctima orientada a la obtención inconsentida y maquinal de sus activos económicos.

Principalmente los delincuentes programan o usan algoritmos confeccionados específicamente para defraudar (Art. 249.2.a CP) que adquieren por Internet, y que mediante lo que se han venido denominando **deep fakes** generadas por IA —falsas identidades, suplantaciones, añadidos de voz o imagen sintética— voice o face clonning —muy realistas...— infectan con reclamos —relatos falsos— páginas web, correos electrónicos, etc., o directamente se comunican mediante videollamadas suplantadas —que usan face renaisement y la técnica del hombre por detrás— con la intención de hacer que las víctimas crean estar transaccionando bienes, dinero o servicios electrónicamente, hasta conseguir transferir su contraprestación económica —normalmente exigida por adelantado— en favor de un delincuente no identificado que se apodera de ella.

Esas deep fakes van desde falsificar la imagen de una persona cualquiera para hacerla figurar como verídica, de modo que, a continuación, impunemente se expande el reclamo que suele engañar/triunfar en un porcentaje determinado de víctimas, hasta singularizar esa **suplantación** humana tecnologizada con la imagen o voz real (i. e.: en el vishing[94]) de alguien conocido, de manera que gana la confianza de la víctima más convincentemente para pedirle normalmente una cantidad de dinero que es de la que se apodera a distancia (Art. 248 CP).

Con la **IA generativa** (FraudGPT/WormGPT), los delincuentes pueden crear contenido falso (webs, anuncios en redes sociales, mensajes de correo electrónico) y lanzar campañas de fraude convincentes combinando texto,

(94) Los delincuentes llaman por teléfono a personas y usan IA que simula voces de familiares, amigos, allegados o compañeros de trabajo, solicitándoles datos personales, empresariales o incluso transferencias de dinero con cualquier pretexto, o lo hacen a través de transacciones comerciales camufladas. Las hemos abordado más arriba en el epígrafe 4.1.3: ESTAFA DEL FAMILIAR EN APUROS.

audio y video donde engañar a las víctimas para que compartan información económica personal o realizar transacciones no autorizadas.

Igualmente se está utilizando la IA para la captación torticera (**Phishing**) de información personal y económica, especialmente de datos bancarios y sobre criptoactivos ya sea mediante correos electrónicos —con mensajes cada vez más convincentes supuestamente emitidos por Bancos, portales de comercio electrónico...—, ya descargando programas espía mediante el clicado en enlaces (hipervínculos, links) maliciosos, o la descarga de archivos de procedencia desconocida.

Y aunque por **autoprotección/ciberseguridad** es recomendable revisar la procedencia —dirección de mail, cuenta de la red social...— de lo que nos llega electrónicamente o de las descargas que se nos solicitan, analizar antes de actuar cualquier señal de alerta —en la que la exigencia de prisas en el actuar suele ser bastante común— y comprobar personalmente por vía diferente que realmente proceden de quien dice remitirlas, muchas veces son prácticamente indetectables.

Igualmente los delincuentes están utilizando la IA en **manipulación documental** con ayuda de mejoras mediante la aplicación de técnicas de aprendizaje automático que alcanzan a la **verificación biométrica de identidad** (factores de autenticación) para posibilitar suplantaciones de identidad, sin necesidad del concurso de la víctima (Art. 249 CP).

Herramientas de IA que convierten texto en voz se usan para eludir los sistemas de autenticación de audio que son el preludio de suplantaciones muy realistas ante víctimas de quien conoce al titular de esa voz.

Esas suplantaciones de la persona titular del activo unidas al conocimiento y uso de las claves de acceso a los medios de pago a través de transacciones económicas operan mediante falsificaciones profundas con aplicaciones de intercambio de rostros —lip sync; face swapping— que ya últimamente no disminuyen ni siquiera los fines de semana como solían, detectándose de forma constante durante los siete días de la semana (porque las máquinas no necesitan descansar).

Con IA se está generando malware de forma rápida y automatizada (i. e.: Llama 2 de Meta con *software* de código abierto), que incluso evade las detecciones tradicionales; se están seleccionando objetivos específicos y evadiendo sistemas de seguridad, de manera que, i. e.: el ramsonware alcanza mayor efectividad; está ayudando a evadir sistemas de reconoci-

miento de imágenes y biometría de voz, de manera que cada vez más los delincuentes operan sin ser detectados o adaptan sus tácticas a las defensas que se vayan incorporando; se está usando para identificar puntos ciegos en las reglas de detección, de manera que los delincuentes manipulan datos para evadir sistemas de seguridad (bien jurídico que integradamente al patrimonio pretende proteger el Art. 249 CP); aprenden patrones de comportamiento para convencer de la legitimidad del reclamo facilitando la intromisión en las redes y la obtención de datos sensibles....

En definitiva, los fraudes con IA no suponen una nueva tipología de ciberataques, sino una **adaptación más sofisticada a los fraudes ya existentes** —con reclamos mejor redactados y fundamentados, simulaciones menos detectables por su alto realismo, clonaciones de voz e imagen irrastreables prácticamente, posibilidades de multiplicar su difusión, neutralizadoras de contramedidas de seguridad que impiden su descubrimiento...— vehiculizados ahora con nuevas y sofisticadas técnicas que, por novedosas, suelen estar menos asumidas a la hora de ser enfrentadas por sus hipotéticas víctimas.

No queremos acabar este epígrafe sin mencionar, cambiando de tercio, las **estafas mediante programación informática** que, consecuencia de la automatización de procesos productivos permitida por la IA y sin el consentimiento/conocimiento del cliente usuario, se integran en productos o servicios tecnológicos comerciales que tienen programado a la larga un uso deficiente invalidante —piénsese, i. e.: en las obsolescencias planificadas, como ocurrió con la batería de determinados teléfonos móviles/celulares que en poco tiempo los dejaban inoperativos—, que, desconocidos/inadvertidos por la víctima y de haberlos conocido, habrían evitado su compra/adquisición/uso, y que algunas empresas programan en ellos para que cada cierto tiempo se tengan que renovar, y que les hace responsables penales —engaño sustancial previo— por la vía del Art. 251 bis en relación con el 31 bis CP.

6.2. HERRAMIENTAS IA EN LA LUCHA CONTRA EL FRAUDE

De acuerdo con el dicho de que «*quien a hierro mata, a hierro muere*», entidades afectadas por el fraude tecnológico —bancarias y no— están combatiendo mecánicas comisivas que emplean IA, con IA misma, usando sofisticadas aplicaciones de esta constelación de tecnologías para detectar y prevenir, en tiempo real, ataques fraudulentos.

Gracias a la posibilidad que ofrecen las herramientas de IA de analizar simultáneamente enormes cantidades de datos —**big data**— que pueden

pautar, identificar y estudiar patrones transaccionales y el comportamiento —cómo se actúa— de gasto de clientes, usando el **aprendizaje automático, sus herramientas** detectan, señalan anomalías que permiten responder con inmediatez a los intentos sospechosos de fraude.

La IA ayuda a quienes combaten preventivamente la delincuencia económica mediante modelos de aprendizaje automático y su capacidad de adaptarse a la evolución de los métodos de fraude en línea, a detectar identificaciones falsas, datos repetidos en los intentos de fraude y comprobar signos de deep fakes en los sistemas de autenticación y acceso basados en parámetros biométricos de voz-audio e imagen-vídeo.

Por su parte, los chatbots se están utilizando para ayudar a los analistas a mejorar sus investigaciones sobre tipología y mecánicas de fraude.

Estas herramientas buscan proteger las operaciones transaccionales de dinero y reducir el riesgo de fraude, mediante *software* avanzado que obtiene y chequea mucha información y datos de sus usuarios con el objeto de identificar/detectar actividades sospechosas, interrumpiéndolas.

Por ejemplo, en materia de autenticación —como antídoto de la suplantación—, es posible sumar al control de la huella digital un segundo nivel de seguridad utilizando la dirección IP del usuario, su geolocalización o número de teléfono para verificar que se es quien se dice ser.

Para validar la identidad del usuario y asegurarse de que se trata de una operación legítima, en primer lugar, colecta información para conformar una **base de datos** que permita analizar las operaciones y establecer medidas de control.

A continuación, enriquece los datos produciendo información fehaciente a partir de un único punto de datos (dirección IP, ubicación...) para identificar operaciones sospechosas y verificar la identidad de los usuarios.

El **etiquetado de las operaciones sospechosas** y los intentos de fraude permite crear un registro y entrenar los módulos de machine learning.

Las **reglas de riesgo** permiten definir los parámetros de control y análisis más eficaces en función de la actividad sometida a análisis.

Las **alertas de riesgo** operan cuando las reglas de riesgo ya se encuentran definidas y automatizan el control.

Las sugerencias de IA y machine learning son especialmente útiles para detectar el fraude, pues utilizan algoritmos para aprender y mejorar con el entrenamiento.

Son además herramientas programables que crean reglas de riesgo personalizadas en función de la actividad o tipo de usuario que se es y que automatizan el funcionamiento y reducen el esfuerzo dedicado a la gestión de ciberseguridad, a la vez que reducen su coste económico mejorando su eficacia.

En definitiva, se trata de modelos de entrenamiento y detección de **actividades anómalas** de usuarios gobernadas por algoritmos de aprendizaje automático que cuando identifican **patrones sospechosos** en el uso de instrumentos de pago —cantidad, tipo de compra y comerciante—, adoptan **medidas preventivas como el bloqueo** de la operación económica que sólo se levanta si se verifica la real intervención del titular.

A veces la técnica puede ser tan inocua como que consiste en decisiones (normalmente el indicado bloqueo automático de la operación) adoptadas en función de la detección de anomalías descubiertas gracias a pautas detectadas derivadas del **registro de la actividad del usuario** en la web de comercio electrónico o bancaria —horas, ubicaciones, dispositivo iniciador de la transacción, duración de la sesión, velocidad de navegación, visita de producto, historial de interacciones, detalles del pedido, incluido su precio, cantidad y marcas de tiempo, dirección de facturación...—, los registros de **estado de control** —dirección de correo electrónico o número telefónico asociado, alertas de ubicaciones o dispositivos de inicio de sesión no usuales, duraciones prolongadas, frecuencia o patrón de vista de productos, realización simultanea de varios pedidos de alto valor, discrepancias entre la dirección de facturación y envío...— y los **datos históricos e incidentes** de fraude anteriores con el comportamiento del usuario y las probabilidades de que se omitan controles en casos de fraude histórico.

6.3. LÍMITES Y GARANTÍAS EN EL USO DE HERRAMIENTAS DE IA CONTRA EL FRAUDE

El considerando 22 de la EM de la D 2019/713, a efectos de homogeneizar la cooperación internacional en la lucha contra un fraude tan transnacional como es el tecnológico, indica que son necesarias «*herramientas especiales para investigar eficazmente el fraude y la falsificación de medios de pago distintos del efectivo*».

12.1. JURISDICCIÓN Y COMPETENCIA

La **jurisdicción**, es la (potestad) —atribución a un concreto Estado, pues es manifestación de su soberanía— de enjuiciar un determinado asunto a través de sus propios Tribunales.

Responde a la pregunta de qué país o países pueden conocer, con sus Tribunales, del enjuiciamiento de un determinado asunto (i. e: una estafa con víctimas en varios Estados)

La **competencia**, empero, es la (facultad) medida de la jurisdicción asignada a cada Juez o Tribunal, la atribución otorgada a las Autoridades judiciales para conocer de un asunto determinado.

Responde a la pregunta de a qué concreto Tribunal le corresponde el enjuiciamiento determinado de cada fase de conocimiento del asunto.

Entrando en la **jurisdicción** para el enjuiciamiento de las estafas y fraudes tecnológicos, como normalmente se desconoce quién y desde dónde se ejecutan, dónde y cómo ocurren, y a través de qué espacios físicos, al desplegarse su acción en el espacio virtual, nos preguntamos qué país concreto puede enjuiciar una trama transnacional de esa clase.

El considerando 20 de la EM D 2019/713, apelando a la eficacia, manifiesta que: «*en general, lo más adecuado es que se conozca de una infracción en el marco del sistema penal del país en el que se ha cometido. Por consiguiente, cada Estado miembro debe establecer su jurisdicción para conocer de las infracciones cometidas en su territorio y de las infracciones cometidas por sus nacionales. Los Estados miembros pueden también establecer su jurisdicción para conocer de las infracciones que provoquen daños en su territorio*».

De manera que, su Art. 12 expresa dos atribuciones jurisdiccionales principales —párrafo 1—:

– El país del territorio donde total o parcialmente se haya producido la estafa (que, según el párrafo 2, comprende el territorio donde físicamente estaba el autor al cometer la infracción, independientemente de dónde estuviera el sistema informático que haya utilizado para llevarla a cabo) o

– el de nacionalidad del autor;

y tres potestativas —párrafo 3— ante la más que real contingencia de ignorar quién es el autor y dónde atacó:

– el país del territorio donde reside habitualmente el presunto autor,

– el de establecimiento de la empresa que haya obtenido provecho del delito o

– el de sus víctimas siempre que al menos residan habitualmente[126] en él —de manera que este fuero alternativo basado en la **producción del daño**, por evidente, será el inicialmente más utilizado, al menos hasta que se descubra el presunto autor, en que operará el oportuno traslado de procedimiento—.

Y ello en consonancia con la teoría de que las **estafas se consuman** cuando, producto del ataque a una víctima concreta, se produce el **desplazamiento/transferencia económica** en su contra.

Como indica, por todas, la s TS 61/2012, de 8 de febrero: «*por regla general, el delito de estafa se perfecciona en el momento en que tiene lugar el acto por el cual el titular de un bien o un valor se desprende de él, sin que se requiera que el autor del delito pueda disfrutar de lo ilícitamente obtenido. La estafa se consuma cuando el engañado realiza la disposición patrimonial que provoca el daño en el patrimonio*».

Si se trata de una **defraudación tecnológica/maquinal**, el delito se entendería consumado donde operase la transferencia, pero al no ejecutarse una traslación física del activo depredado, sino tan solo informática, que, precisamente suele pretender una disponibilidad universal por el acceso al mismo, normalmente, desde cualquier punto geográfico donde se pueda conectar a Internet, debemos buscar fueros alternativos competenciales más físicos, normalmente, a falta de conocer donde radica el presunto defraudador, el de

(126) Quedando desamparados quienes no sean nacional o persona con residencia habitual en ese territorio. Los que sean atacados de paso por el país, en estancias temporales, vacaciones, escalas...

localización habitual/residencia de la víctima, lugar de manifestación del daño —la pérdida de la disponibilidad sobre el activo atacado—.

Caso de que hubiera varios países presuntamente competentes para enjuiciar la misma trama defraudatoria, el considerando 21 EM de la D 2019/713, apelando a las obligaciones establecidas en la Decisión Marco 2009/948/JAI[127] del Consejo y en la Decisión 2002/187/JAI[128] del Consejo, anima a las autoridades competentes a la posibilidad de establecer consultas directas con la ayuda de la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) para resolver ese conflicto jurisdiccional.

La atribución jurisdiccional en base al denominado **criterio mosaico/fragmentación de la jurisdicción**, esto es, el que lo establece en favor del **lugar de manifestación del daño** (extracontractual/delictivo), tiene la ventaja de que a su vez permite la atribución para aplicar las medidas restrictivas tecnológicas como podría ser el caso del bloqueo/impedimento del acceso desde un territorio al ataque en línea desde otros y alcanza a la persecución penal de las formas imperfectas de ejecución —tentativa, en los delitos de fraude con resultado— así como la de los delitos de riesgo por adelantamiento de la barrera punitiva.

Paradigmático, *mutatis mutandis*, es el caso resuelto por s TJUE (gran sala) de 21 de diciembre de 2021 en el caso Gtflix Tv, C-251/2020.

Mutatis mutandis, decimos, porque se trata de un asunto en que una entidad checa demanda en Francia contra un profesional húngaro, solicitando la rectificación/supresión de comentarios denigrantes publicados en varios sitios de Internet, a la vez que pide indemnización por perjuicios, situaciones derivadas de reclamaciones civiles que, sin embargo, deben empezar a procurarse también en la penal que, en el caso español, permite tanto la acumulación de medidas restrictivas tecnológicas como de reclamaciones civiles indemnizatorias.

En esa s TJUE (pero también en otras parecidas: s TJUE: 30/11/1976 (Bier, C-1976/166); 16/05/13 (Melzer C-228/11); 5/06/14 (Coty Germany C-360/12) se aboga por atribuir jurisdicción a cada Estado en cuyo territorio se hayan podido acceder a los comentarios denigrantes —en nuestro caso,

(127) Decisión Marco 2009/948/JAI del Consejo, de 30 de noviembre de 2009, sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales.

(128) Decisión 2002/187/JAI del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia.

i. e: donde se haya podido acceder al reclamo, link o web defraudatoria—para poder fijar la indemnización[129], y ello en razón a:

– La naturaleza ubicua de la información y contenidos publicados en línea en un sitio web —enlace o reclamo—,
– el alcance universal de su difusión y
– el intento de que la causa judicial sea única e indivisible.

En lo que hace a la **competencia** una vez ya dentro del Estado con jurisdicción, el problema, a falta de conocimiento de la concreta ubicación desde donde el presunto autor haya ejecutado el ataque defraudatorio, se repite.

Inicialmente (Art. 14.2 LECRim), será territorialmente competente para investigar la trama defraudatoria, el Juzgado de Instrucción del **lugar donde se hubiese cometido el delito**.

Pero comoquiera que la estafa cometida a través de Internet tiene la potencialidad de causar efectos en muy plurales territorios —de ahí las expresiones ciberespacio y mosaico—, la designación del concreto órgano judicial competente para instruir depende de que se aplique la:

– **Teoría de la acción** —siendo competente el Juzgado territorial del lugar desde donde se inició el ataque/reclamo—.
– **Teoría del resultado**/consumación —siendo competente el Juzgado de Instrucción donde se consume la estafa por su desplazamiento patrimonial, recepción de la transferencia, efectiva disposición de los fondos, apoderamiento del dinero, ubicación de la cuenta receptora....— o
– cualquiera de ellos —**teoría de la ubicuidad** (PNJ TS 3/02/2005), según la cual el delito se produce en todos los lugares en los que se hayan desarrollado las acciones del sujeto activo y pasivo: lugar del engaño, lugar de producción del perjuicio, lugar del desplazamiento patrimonial (A TS 31/01/2019; 9/12/2020; 8/06/2021)—,
– que es la solución inicial adoptada por el Tribunal Supremo al resolver las cuestiones de competencia planteadas entre diversos Tribunales afectados por una misma trama defraudatoria, hasta que últimamente se ha venido corrigiendo, en función de la masividad o no del fraude, mediante la denominada **teoría de la efectividad**.

(129) Aunque no sea competente para la demanda de rectificación/supresión (7.2 Reglamento –Bruselas I bis– 1215/2012, de 12/12/12, sobre competencia judicial, reconocimiento y ejecución de resoluciones judiciales civiles/mercantiles).

La presente monografía, a cargo del Magistrado y Doctor ELOY VELASCO NÚÑEZ, constituye una ambiciosa obra práctica procesal, penal y de responsabilidad civil derivada.

Además de explicar la relación actual entre la estafa (modalidad) y el FRAUDE (género) en el contexto de la evolución que la digitalización de la Economía y los nuevos medios de pago han supuesto para el Derecho europeo y español de nuestro días, la obra abarca fundamentalmente el análisis de los nuevos preceptos penales de la estafa o fraude maquinal/tecnológico (Art. 249.1.a CP), la utilización fraudulenta de instrumentos de pago distintos del efectivo (Art. 249.1.b CP), los actos preparatorios del fraude (Art. 249.2 y 3 CP), las conductas fraudulentas mixtas (estafas piramidales de inversión, SIM swaping, skimming, carding, phishing, pharming, smishing, vishing, spoofing, bizum,... ingeniería social, muleros...), la defraudación tecnológica (Art. 255 CP), la falsificación de medios de pago distintos del efectivo (Art. 399 bis y 400 CP), los delitos contra los criptoactivos, los fraudes cometidos por inteligencia Artificial y la responsabilidad civil vinculada al importe defraudado.

Del mismo modo se examinan también distintos aspectos relacionados con la investigación de estos actos: el papel de las empresas tecnológicas intermediarias, el de los CASP, el embargo de criptoactivos, herramientas de IA para combatir el fraude, búsqueda de claves privadas...

Y, adicionalmente se abordan también numerosas cuestiones procesales: jurisdicción, competencia, personación, análisis forense de dispositivos tecnológicos, medidas restrictivas tecnológicas, notificaciones con NFTs, actuación sobre la ID, decomiso...

ISBN: 978-84-10292-27-7

AENOR ER Empresa Registrada ISO 9001 ER-0280/2005
IQNet
AENOR Gestión Ambiental ISO 14001 GA-2005/0100

LA LEY