Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en el Ejercicio de la Abogacía y la Procura

El Derecho Penal Económico ante las estafas informáticas: análisis dogmático y propuestas jurídicas frente al phishing, smishing, vishing y pharming

Trabajo fin de estudio presentado por:	Luis Antonio Plaza Rodríguez
Tipo de trabajo:	TFM
Área jurídica:	Derecho Penal
Director/a:	Estela Gozalbo Gutiérrez
Fecha:	08, de enero de 2026.

Resumen

El presente trabajo analiza de forma exhaustiva la respuesta del Derecho Penal económico frente a las estafas informáticas, con especial atención a las modalidades de phishing, smishing, vishing y pharming. Se abordan sus aspectos conceptuales y jurídicos, la evolución legislativa en España, el análisis dogmático del tipo penal y la jurisprudencia penal relevante. Asimismo, se examinan las dificultades prácticas en la investigación de estos delitos y se proponen reformas legales y medidas jurídicas para mejorar su prevención y persecución. La investigación muestra que las nuevas tecnologías han dado lugar a fraudes cada vez más sofisticados y globales, lo que ha obligado al legislador a adaptar el Código Penal (por ejemplo, con la Ley Orgánica 14/2022) y a los tribunales a reinterpretar los elementos tradicionales del delito de estafa. Finalmente, se presentan propuestas de reforma legal y de políticas públicas orientadas a reforzar la protección penal frente a estas amenazas y a mejorar la eficacia en su investigación y sanción.

Palabras clave: phishing; smishing; vishing; pharming; ciberdelincuencia.

Abstract

This comprehensive academic work examines the response of economic criminal law to computer fraud, with a focus on phishing, smishing, vishing, and pharming. It covers conceptual and legal analyses of these cyber scams, the legislative evolution in Spain, a dogmatic analysis of the criminal offense, and relevant case law. The study also explores practical difficulties in investigating such crimes and proposes legal reforms and measures to improve prevention and prosecution. The research shows that new technologies have led to increasingly sophisticated and transnational fraud schemes, prompting legislators to adapt the Spanish Criminal Code (e.g., through Organic Law 14/2022) and courts to reinterpret traditional elements of fraud. Finally, the paper offers reform proposals and policy recommendations aimed at strengthening criminal protection against these threats and improving effectiveness in their investigation and punishment.

Keywords: phishing; smishing; vishing; pharming; cybercrime.

Índice de contenidos

Índice de tablas

1. Introducción

En las últimas décadas, la revolución tecnológica ha generado nuevas formas de delincuencia patrimonial que desafían al Derecho Penal clásico. En España, al igual que en otros países, se ha constatado un incremento alarmante de fraudes informáticos que afectan el patrimonio de consumidores y usuarios (FERNÁNDEZ ESCUDERO, 2024). Los avances en informática, telecomunicaciones e Internet han ampliado el alcance y los efectos de las estafas, permitiendo a los delincuentes defraudar a un gran número de víctimas con riesgos personales mínimos (MESTRE, 2024). Modalidades como el *phishing*, *smishing*, *vishing* y *pharming* se han vuelto especialmente comunes, aprovechando la confianza de las personas en canales digitales para obtener información sensible o inducir transferencias no consentidas de dinero.

El Derecho Penal Económico español ha debido adaptarse para enfrentar estas conductas. Desde la incorporación en el Código Penal de la figura de la estafa informática en 1995, el legislador y la jurisprudencia han buscado dar respuesta a los fraudes cometidos mediante tecnologías de la información. Este trabajo realiza un análisis dogmático de dichas figuras delictivas en especial las estafas informáticas cometidas por *phishing*, *smishing*, *vishing* y *pharming*, examinando sus elementos típicos, el bien jurídico protegido y los criterios jurisprudenciales que han delimitado su alcance. Asimismo, se aborda la respuesta legal y jurisprudencial hasta 2024, incluyendo el estudio de las normas penales aplicables (p. ej. artículos relevantes del Código Penal) y de resoluciones judiciales emblemáticas (citando número de sentencia, fecha y recurso).

Dentro de la ciberdelincuencia en España, la estafa informática es una de las manifestaciones más importantes, tanto por cifras como cualitativamente. En este sentido, Casals señala que alrededor del 90% de la ciberdelincuencia está formada por las estafas informáticas, aumentando un 21,5% de la cibercriminalidad en 2023 respecto al año previo (CASALS FERNÁNDEZ, 2023).

Así, la estafa informática se entiende como una "evolución" de la estafa clásica resultado de la generalización de las TIC, la digitalización de los servicios bancarios, y la irrupción de nuevos entornos como los metaversos. La metadelincuencia y las ciberestafas a avatares surgen en este contexto como fenómenos (VERDUGO, 2024). Pese a que exista un mayor soporte

normativo, a raíz de la modernización digital del Estado y del mercado, se ha ido comprobando que los mecanismos de prevención y protección para los usuarios son insuficientes.

Finalmente, desde una doble perspectiva doctrinal y práctica, se presentarán propuestas jurídicas para mejorar la eficacia en la prevención y represión de estas ciberestafas. Ello incluye considerar ajustes legislativos recientes (como la reforma operada por la Ley Orgánica 14/2022, de 22 de diciembre, de transposición de directivas europeas y otras disposiciones para la adaptación de la legislación penal al ordenamiento de la Unión Europea, y reforma de los delitos contra la integridad moral, desórdenes públicos y contrabando de armas de doble uso, en adelante, LO 14/2022) y eventuales medidas futuras, así como otras estrategias complementarias cooperación internacional, mejoras en ciberseguridad bancaria, educación del usuario destinadas a enfrentar el fenómeno del phishing y sus variantes en el contexto español.

1.1. Justificación del tema elegido

La elección de este tema se justifica por la magnitud creciente del fenómeno y por las singulares tensiones dogmáticas y prácticas que genera en el sistema penal español. En lo empírico, la digitalización de la economía ha multiplicado los fraudes patrimoniales mediados por tecnologías de la información, afectando de forma directa a consumidores y usuarios y erosionando la confianza en los sistemas de pago y en el comercio electrónico (FERNÁNDEZ ESCUDERO, 2024; MESTRE, 2024). Este incremento no es solo cuantitativo; es cualitativo, pues los defraudadores combinan ingeniería social y manipulación técnica sobre sistemas automatizados, uniendo modalidades como el phishing, el smishing, el vishing y el pharming en campañas cada vez más sofisticadas y transnacionales (IBARBUREN, 2025). Estas dinámicas, por su impacto económico agregado y su potencial desestabilizador de los intercambios digitales, sitúan el problema en el núcleo del Derecho penal económico, que tutela no solo patrimonios individuales, sino también la seguridad del tráfico y la confianza pública en la infraestructura financiera digital (QUINTERO OLIVARES, 2013).

Como resultado de la importante evolución de los ataques de phishing más allá de los métodos convencionales basados en el correo electrónico, han surgido enfoques sofisticados y variados, como el *smishing* (*phishing* por SMS), el *vishing* (phishing por voz) y el *quishing* (phishing por código QR). Estos nuevos métodos de ataque eluden las medidas de seguridad

tradicionales y comprometen los datos privados utilizando la ingeniería social, las tecnologías móviles y la confianza humana. Este trabajo analiza cómo han cambiado las estrategias de *phishing* a lo largo del tiempo, analizando los métodos, los recursos y los trucos psicológicos utilizados en el *smishing*, el *vishing* y el *quishing*.

Además, llama la atención sobre casos prácticos reales, las dificultades de detección y el uso cada vez mayor de la automatización y la inteligencia artificial por parte de los autores de las amenazas. También se considerarán las tendencias futuras del *phishing*, como las campañas de *phishing* multicanal y el *phishing* de voz habilitado por *deep fakes*, y considera las consecuencias para los conocimientos sobre ciberseguridad.

Desde la perspectiva normativa, el legislador español reaccionó pronto incorporando la estafa informática en 1995 y, más recientemente, ha actualizado su formulación a través de la LO 14/2022, que reubica y describe el tipo en el art. 249.1.a) CP con una pauta amplia: con ánimo de lucro, obstaculizando o interfiriendo indebidamente un sistema de información, introduciendo o alterando datos, o valiéndose de «cualquier otra manipulación informática o artificio semejante», obtener una transferencia no consentida de un activo patrimonial (art. 249.1.a CP). La amplitud deliberada de la redacción responde a la necesidad de abarcar tanto ataques técnicos puros como engaños tecnológicos de ingeniería social, pero, precisamente por ello, abre cuestiones interpretativas que conviene delimitar dogmáticamente para garantizar seguridad jurídica y proporcionalidad punitiva (ESTÉBANEZ, 2024; MESTRE, 2024). En esta encrucijada, un estudio monográfico actualizado permite evaluar si la técnica legislativa vigente es suficiente y cómo debe operar en supuestos fronterizos, así como valorar eventuales ajustes de *lege ferenda*.

A esta necesidad se suma la función ordenadora de la jurisprudencia. El Tribunal Supremo ha perfilado que, en el fraude informático, el núcleo de tutela sigue siendo el patrimonio, aunque el engaño clásico a la persona resulte sustituido por la manipulación de sistemas o por artificios tecnológicos que desembocan en transferencias no consentidas; así, el "error" puede residir en el funcionamiento inducido del sistema y no en una decisión dispositiva del sujeto pasivo (STS 379/2019, 23 de julio, rec. 853/2018). Las resoluciones han confirmado, además, que el *phishing* y técnicas afines encajan plenamente en el tipo del art. 249.1.a CP, y han extendido el entendimiento de «manipulación informática o artificio semejante» a maniobras híbridas y comunicaciones digitales mendaces que logran el desplazamiento patrimonial,

consolidando una doctrina funcional y tecnológicamente neutra (p. ej., STS 747/2007, 9 de mayo; STS 364/2011, 11 de mayo). Esta línea hermenéutica aporta certeza, pero deja abiertos problemas concursales, de tentativa, de cómplices y de responsabilidad de partícipes periféricos como las "mulas bancarias" requieren analizar conjuntamente los criterios operativos para la práctica forense (ÁVILA, 2024).

La relevancia social inmediata y la litigiosidad creciente incluida la que vincula el cauce penal con reclamaciones civiles frente a proveedores de servicios de pago bajo el régimen de operaciones no autorizadas refuerzan el interés aplicado del tema. Las Audiencias Provinciales han venido resolviendo con regularidad casos de smishing, SIM swapping o desvíos de pagos, tanto cuando los autores principales no son habidos como cuando solo se identifica a intermediarios locales, ilustrando dificultades probatorias, de competencia territorial y de cooperación internacional que impactan en la eficacia persecutoria (v. gr., SAP Asturias, Secc. 4.ª, núm. 477/2024, 21 de marzo, Rec. 370/2023). Sistematizar estos criterios, junto con la práctica de acumulación de causas y el uso de herramientas de investigación tecnológica, es necesario para orientar la actuación de fiscales, jueces y cuerpos policiales.

Finalmente, la justificación académica también es prospectiva. La rápida mutación de las técnicas de fraude aconseja revisar la suficiencia del tipo actual ante nuevas tácticas, por ejemplo, combinaciones de *pharming* y secuestro de factores de autenticación y ponderar si determinadas agravaciones específicas o ajustes procesales mejorarían la tutela sin desbordar el principio de mínima intervención. Un enfoque integral que cruce la dogmática penal con la experiencia jurisprudencial y con la política criminal comparada puede ofrecer propuestas realistas y prudentes: perfeccionamiento del marco penal donde sea necesario, criterios de imputación a partícipes acordes con su aportación típica, protocolos de especialización y cooperación interinstitucional y, en último término, pautas que fortalezcan la prevención sin debilitar garantías. Todo ello hace oportuno y necesario el presente estudio, que aspira a contribuir con rigor teórico y utilidad práctica a un campo en plena evolución.

1.2. Problema y finalidad del trabajo

El problema principal que motiva la realización de este trabajo se encuentra en la necesidad de adecuación del Derecho Penal español a las nuevas formas de estafa informática y en la eficacia de su aplicación práctica. Siguen dándose importantes preguntas dogmáticas y

prácticas no resueltas pese a que el Código Penal contemplara desde 1995 la figura de estafa informática. ¿Cómo encuadrar el phishing y sus variantes dentro del tipo penal del art. 249.1.a) CP? ¿Se requiere reformar la norma para tipificar estas conductas de forma expresa? ¿Qué límites contempló la jurisprudencia a la hora de interpretar la "manipulación informática o artificio semejante"? ¿Cómo las entidades bancarias articulan la responsabilidad civil en estos supuestos? ¿Qué obstáculos tiene la persecución judicial en un ámbito transnacional?

Este trabajo busca analizar dogmáticamente las estafas informáticas desde el punto de vista del Derecho Penal Económico, contrastando la legislación vigente con la doctrina y la jurisprudencia reciente. Para ello, se busca ofrecer propuestas jurídicas y de política criminal dirigidas a que el Derecho Penal se fortalezca, igualmente garantizando una mayor protección de las víctimas frente a las tipologías actuales de fraude digital.

1.3. Objetivos

El objetivo de este trabajo es desarrollar un análisis completo de la respuesta del Derecho Penal económico frente a las estafas informáticas, con especial atención a las modalidades de phishing, smishing, vishing y pharming. En primer lugar, se precisan los conceptos y tipologías de estas conductas, así como su encaje legal en el ordenamiento español vigente. En segundo lugar, se examina la evolución legislativa nacional e internacional, para comprender cómo ha cambiado la normativa penal ante el auge de estas conductas. En tercer lugar, se realiza un análisis dogmático del delito de estafa informática, profundizando en sus elementos típicos, bien jurídico protegido, autoría y participación, concurrencia con otros delitos y problemas concursales, a la luz de la doctrina científica. En cuarto lugar, se recopila la jurisprudencia penal española más relevante en la materia, para extraer criterios interpretativos consolidados. En quinto lugar, se abordan las dificultades prácticas de investigación y prueba de estos delitos, considerando las herramientas legales existentes (p. ej. las medidas introducidas por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, en adelante LO 13/2015 en la LECrim) y sus limitaciones. Finalmente, con base en todo lo anterior, se proponen reformas y mejoras jurídicas orientadas a optimizar la prevención, persecución y sanción de las estafas informáticas, ya sea mediante cambios normativos, pautas jurisprudenciales o estrategias de política criminal.

La relevancia de esta investigación es evidente dada la gravedad de las estafas informáticas en la sociedad contemporánea, donde constituyen una amenaza creciente para el patrimonio individual y la confianza en los entornos digitales. La convergencia de lo económico y lo tecnológico obliga al Derecho Penal a encontrar soluciones equilibradas que protejan eficazmente a las víctimas sin menoscabar derechos fundamentales en la esfera digital. Así, este trabajo aspira a contribuir al debate doctrinal y práctico sobre cómo el Derecho Penal económico puede y debe hacer frente a los fraudes informáticos como el phishing, smishing, vishing y pharming, ofreciendo un panorama actualizado y proponiendo vías de avance en la materia.

2. Concepto y modalidades de estafas informáticas

Estafa informática es la denominación genérica de los fraudes o engaños patrimoniales cometidos mediante el uso de medios informáticos o electrónicos. A diferencia de la estafa tradicional -donde el engaño se ejerce directamente sobre la víctima para que esta, en error, realice un acto de disposición en perjuicio propio o ajeno-, en las estafas informáticas el delincuente se vale de herramientas tecnológicas para conseguir un beneficio ilícito a costa del patrimonio ajeno, muchas veces sin interacción personal directa con la víctima. Dentro de estas conductas, existen diferentes tipologías de ciberestafa habitualmente reportadas en la práctica forense española (FERNÁNDEZ ESCUDERO, 2024).

Las principales tipologías de ciberestafa que pueden distinguirse, son las siguientes: phishing, smishing, vishing y pharming, además de una categoría de carácter residual que agrupa otras variantes y técnicas afines como el *SIM swapping*, el *QRishing* o el *whishing*.

2.1. Phishing

El phishing es una de las modalidades más extendidas de estafa informática (IBARBUREN, 2025). El término proviene del inglés *fishing* (pescar), aludiendo a que el estafador «lanza el anzuelo» a la víctima para que esta «muerda» proporcionando sus datos confidenciales (ACÓN, 2024). Típicamente, el delincuente envía a la víctima un correo electrónico falso haciéndose pasar por una entidad legítima (por ejemplo, su banco). En dicho mensaje engañoso suele incluirse un enlace que dirige a un sitio web fraudulento casi idéntico al de la institución suplantada. Al ingresar la víctima a esa página y teclear sus credenciales (usuarios, contraseñas, números de tarjeta, etc.)**,** dicha información es capturada por el estafador. Con esas credenciales, el delincuente posteriormente accede a las cuentas reales de la víctima para realizar transferencias u operaciones no autorizadas, consumando así el fraude (FERNÁNDEZ ESCUDERO, 2024).

Por lo tanto, el phishing engaña al usuario mediante correo electrónico para que éste, creyendo interactuar con su banco u otra entidad de confianza, revele datos sensibles que permiten al atacante disponer de su patrimonio. Se trata de un fraude mediado por la tecnología, combinando ingeniería social (engaño al usuario) con suplantación digital (la web fraudulenta) para lograr un desplazamiento patrimonial ilícito.

El término parte de su raíz hacker y es una técnica de ingeniería social donde el delincuente crea un entorno aparentemente legítimo para que la víctima «muerda el anzuelo» y diga sus credenciales, que serán empleadas para llevar a cabo transferencias no consentidas (ACÓN, 2024).

El *phishing*, reconocido desde hace tiempo como uno de los tipos de ciberataques más comunes y exitosos, suele utilizar correos electrónicos falsos para engañar a los usuarios y que revelen información privada. Sin embargo, los actores maliciosos han modificado sus estrategias en respuesta a la diversificación de los canales de comunicación digital y al aumento de la concienciación sobre la ciberseguridad, lo que ha dado lugar a la creación de nuevas variantes de *phishing*, como el *quishing* (basado en códigos QR), el *vishing* (basado en la voz) y el *smishing* (basado en SMS). Estos métodos utilizan plataformas menos supervisadas y se aprovechan de la confianza de las personas, lo que los hace más difíciles de identificar y prohibir con medidas de seguridad estándar. El *smishing* utiliza mensajes SMS para engañar a los destinatarios y que hagan clic en enlaces maliciosos o revelen información personal, haciéndose pasar por organizaciones fiables.

El phishing ha sido una táctica cada vez más exitosa para iniciar ciberataques. En 2022, el Centro de Denuncias de Delitos en Internet (IC3) del FBI descubrió que los ataques de *phishing* eran el delito cibernético más denunciado, con más de 300.000 denuncias. Estos ataques también tienen un gran impacto. Según una encuesta realizada en 2021 por el Ponemon *Institute* y *Proofpoint*, el coste de los ataques de *phishing* se cuadruplicó entre 2015 y 2021. La misma investigación reveló que el coste medio de un ataque de *phishing* exitoso en 2021 fue de 14,8 millones de dólares.

La sentencia de la Audiencia Provincial de Pontevedra de 21 de diciembre de 2021 (nº 539/2021) analiza un caso de fraude mediante *phishing* en el que una usuaria introdujo los datos de su tarjeta en una página web que imitaba la de Abanca tras recibir un correo electrónico que simulaba ser de Correos. A partir de dicho acto, un tercero pudo instalar su tarjeta en Samsung Pay y realizar veinte pagos fraudulentos por un total de 4.365,30 euros; aunque en primera instancia se consideró que la actora había actuado con negligencia grave y debía soportar la pérdida, la Audiencia revoca el fallo puesto que entiende que no puede calificarse su conducta como negligencia grave. Así, la técnica utilizada por el defraudador —ingeniería social, suplantación de identidad y creación de una página clonada— disminuye la

exigibilidad de un comportamiento especialmente cuidadoso y, además, el banco no demostró que se cumplieran sus propias obligaciones legales de seguridad.

Concretamente, la Sala señala que Abanca no probó disponer de mecanismos tecnológicos *antiphishing*, lo cual es exigido por el Reglamento Delegado (UE) 2018/389, ni alertó a la usuaria del número de teléfono en el que se estaba instalando la aplicación de pago. Con ello se hubiera detectado el fraude; a lo que se debe sumar que los SMS enviados no informaban adecuadamente y que la entidad se limitó a remitir comunicaciones generales de advertencia sin demostrar medidas proactivas reales. Aplicando los artículos 41, 42, 44, 45 y 46 del Real Decreto-ley 19/2018, junto con la Directiva (UE) 2015/2366, la Audiencia determina que corresponde al banco demostrar tanto la diligencia en la autenticación como la negligencia grave de la usuaria, carga que no cumplió, por lo que debe afrontar todo el perjuicio económico. En consecuencia, estima el recurso de apelación, condena a Abanca a devolver la cantidad detraída más los intereses procesales y le impone las costas de la primera instancia, exonerando a la usuaria de responsabilidad al no apreciarse negligencia grave en su actuación.

2.2. Smishing

El **smishing** puede describirse como una variante del phishing que emplea la mensajería telefónica (*SMS*) en lugar del correo electrónico. El término proviene de *SMS phishing*. En esta modalidad, la víctima recibe mensajes de texto (SMS) fraudulentos que aparentan provenir de una fuente segura (p. ej. su banco o una empresa conocida). El mensaje usualmente alerta sobre algún problema -como un acceso no autorizado a la cuenta bancaria, o un pago sospechoso- e invita al usuario a hacer clic en un enlace incluido o a contactar a un número de teléfono proporcionado. Al igual que en el phishing tradicional, el enlace conduce a un sitio web falso donde se solicitan las credenciales bancarias de la víctima, o el número de teléfono conecta con los estafadores que, mediante engaño, piden a la víctima sus datos confidenciales (como códigos de verificación).

Por lo tanto, se trata de un ataque a la ciberseguridad que utiliza SMS para robar documentación personal de los beneficiarios de teléfonos móviles. El nivel de confianza de los usuarios finales en sus dispositivos inteligentes atrae a los atacantes para cometer diversos ataques a la seguridad móvil, como el smishing (JAIN Y GUPTA, 2018). En la tecnología actual, los atacantes se preocupan más por atacar los teléfonos móviles que los sistemas informáticos

debido al avance de la tecnología. Debido a la función multipropósito de los teléfonos inteligentes, el pequeño tamaño de la pantalla, el menor coste de producción y la portabilidad, los teléfonos móviles son más fiables y útiles para los usuarios que los sistemas informáticos. El smishing o phishing por SMS también implica el envío de mensajes de texto engañosos o poco fiables para atraer a alguien a revelar información personal o instalar gusanos o malware.

Las características del smishing son las siguientes:

Primeramente, el smishing por mensaje de texto se caracteriza porque los atacantes envían mensajes instantáneos en lugar de correos electrónicos, que parecen haber sido enviados por una organización auténtica y exigen a los clientes que pulsen en un enlace o revelen sus credenciales a través de la respuesta al mensaje de texto. A veces, los atacantes envían mensajes de texto engañosos para atraer a los usuarios con notificaciones de transferencia de dinero.

En segundo lugar, el smishing en Facebook tiene como rasgo que los atacantes a veces envían una solicitud de amistad en Facebook o envían un enlace a través de la cuenta de Facebook para solicitar información importante a los usuarios, lo que parece una notificación auténtica. En tercer lugar, la notificación de sitio web consiste en que los atacantes a veces envían notificaciones de sitio web con una dirección web que puede parecer un sitio auténtico y verificado, en las que solicitan al usuario que visite un sitio web concreto para obtener información detallada, o incluso sobre ofertas de empleo o solicitudes de becas. La notificación por correo electrónico en la que se solicita a los usuarios que visiten su correo electrónico para hacer clic en un enlace y ser redirigidos a un formulario concreto que deben rellenar o en el que deben proporcionar información.

Un ejemplo extraído de la jurisprudencia reciente es ilustrativo: en la SAP de Asturias, Sección 4ª, nº 477/2024 (21 de marzo de 2024, Rec. Apelación 370/2023), el perjudicado recibió un SMS aparentando ser de su banco indicando un supuesto acceso no autorizado y solicitando verificación mediante un enlace; tras pulsarlo, otro SMS le pidió una clave de seguridad que él proporcionó, momento a partir del cual los estafadores lograron ordenar una transferencia de 6.000 € desde su cuenta. Este caso evidencia el funcionamiento del smishing: mensaje de texto creíble, urgencia por un problema de seguridad ficticio, enlace a web fraudulenta o instrucciones a seguir, y obtención subrepticia de las credenciales para ejecutar la estafa. En la sentencia comentada se califica esta conducta como *phishing* en sentido amplio,

concretamente ejecutado vía SMS (smishing), encuadrándola penalmente como estafa informática[1].

2.3. Vishing

El **vishing** (contracción de *voice phishing*) consiste en la obtención fraudulenta de datos o autorizaciones a través de llamadas de voz. En este caso, el estafador realiza una **llamada telefónica** a la víctima, adoptando la identidad de una persona u organismo de confianza (por ejemplo, un empleado del banco, un técnico de soporte o incluso un agente de la autoridad) para ganarse su credibilidad. Mediante técnicas de persuasión y engaño verbal, induce a la víctima a revelar información sensible o a realizar acciones perjudiciales para su patrimonio. Un ejemplo típico es la llamada en la que el delincuente, fingiendo ser del departamento de seguridad del banco, alerta de movimientos sospechosos y pide confirmar datos de la tarjeta o enviar códigos que llegan al móvil, que en realidad son claves de confirmación de transferencias bancarias fraudulentas.

El vishing utiliza la ingeniería social en llamadas telefónicas, recurriendo a la autoridad o la urgencia para obtener información o acceder a los sistemas. Al insertar URL maliciosas en códigos visualmente atractivos que parecen auténticos, el quishing aprovecha la creciente popularidad de los códigos QR y supera los filtros de correo electrónico y otras medidas de seguridad en línea. En conjunto, estas variaciones del phishing muestran lo sofisticados y adaptables que se han vuelto los atacantes, lo que supone un cambio drástico en el panorama de la ciberseguridad.

Como señala GONZÁLEZ et al. (2025), el "phishing" ha ido evolucionando a figuras como el "vishing", de ahí que este término surja de la combinación del sustantivo inglés «*voice*» (voz) y de «phishing». Es una técnica de ingeniería social por virtud de la cual el ciberdelincuente llama por teléfono a la víctima, suplantando la identidad de una persona de confianza de la víctima o una empresa con la que mantiene algún vínculo contractual y/o comercial. Esa llamada parte de una previa captación de información sensible de la víctima como su nombre y apellidos, correo electrónico, domicilio y/o entidad financiera, obtenida mediante alguna

[1] Aunque el *smishing* utiliza la mensajería móvil tradicional (SMS), en los últimos años se ha detectado una evolución hacia el uso de plataformas de mensajería instantánea como WhatsApp o Telegram, lo que algunos autores denominan "messaging phishing" o "whishing", ampliando el ámbito del fraude más allá del SMS clásico.

modalidad de «phishing». Gracias a que cuenta con dicha información privilegiada, el «phisher» telefónico crea una sensación de confianza suficiente para doblegar los mecanismos de alerta y cuidado de la víctima, sometiéndose a lo peticionado por el «phisher», que sería tanto acceder a un link de un SMS, instalar un programa malicioso o *malware*, o facilitar directamente datos sensibles al interlocutor por vía telefónica.

El vishing, por tanto, aprovecha la ingeniería social a través de la voz: no requiere enlaces ni malware, sino la capacidad del estafador para convencer a la víctima por teléfono. Es particularmente insidioso porque la comunicación hablada produce en muchas personas un efecto de legitimidad, especialmente si el delincuente aporta datos básicos (p. ej., nombres, números de cliente) obtenidos previamente y utiliza un tono profesional. En la práctica, las operaciones ilegales derivadas del vishing se materializan igual que en otras ciberestafas: la obtención de contraseñas, códigos o autorizaciones que permiten transferir dinero de la cuenta del afectado. Esta modalidad ha sido reconocida en la casuística española, encuadrándose igualmente bajo el delito de estafa informática cuando con el ardid de la llamada telefónica engañosa se logra una transferencia no consentida.

2.4. Pharming

El pharming es un ataque más técnico que comparte el objetivo final del phishing (capturar credenciales o redirigir fondos) pero difiere en los medios: no precisa que la víctima pulse un enlace engañoso, ya que el delincuente manipula la infraestructura informática para conducirla sin que lo advierta hacia el engaño. En un esquema de pharming, el atacante explota vulnerabilidades en el sistema de nombres de dominio (DNS) o en el propio dispositivo de la víctima para redirigir automáticamente a esta hacia un sitio falso que simula ser el legítimo (REY HUÍDOBRO, 2013, p.6, citado por MESTRE, 2024). En otras palabras, aunque el usuario escriba correctamente la dirección web de su banco, una alteración maliciosa en las tablas de DNS o en su computadora hará que termine conectando con un servidor controlado por el estafador, el cual presenta una réplica del sitio web bancario. La víctima introduce entonces sus claves en esa página apócrifa, entregándoselas involuntariamente al delincuente.

El pharming se considera uno de los ataques más sofisticados, por ser puramente tecnológico y a menudo *indetectable para el usuario medio* (que no nota nada extraño, pues la URL puede

parecer correcta). Como describe la doctrina, «consiste en la explotación de una vulnerabilidad en el software de los servidores DNS o en los equipos de los usuarios que permite redirigir un nombre de dominio a otra máquina distinta» (REY HUÍDOBRO, 2013, citado en MESTRE, 2024). En términos penales, la acción de *manipular el sistema informático de direccionamiento* para provocar una transferencia patrimonial no consentida encaja en la estafa informática, al tratarse precisamente de una manipulación informática en sentido estricto. La jurisprudencia española también ha reconocido esta modalidad: la STS 381/2017, de 26 de octubre de 2017, por ejemplo, confirmó la condena por estafa del acusado que mediante *pharming* desvió a las víctimas a webs bancarias falsas donde obtuvieron sus credenciales (cfr. STS 509/2018).

2.5. Otras variantes y técnicas afines

Además de las cuatro modalidades señaladas, la evolución del cibercrimen ha dado lugar a otros términos y variantes relacionadas. Por ejemplo, se habla de SIM swapping (fraude del duplicado de tarjeta SIM, a fin de interceptar códigos de autenticación y tomar control de la línea telefónica de la víctima), de QRishing (*phishing* a través de códigos QR), de *whishing* (engaños mediante mensajes en aplicaciones como WhatsApp), entre otros (ACÓN, 2024). Todas estas modalidades comparten el rasgo de ser medios comisivos para un mismo fin defraudatorio: obtener datos o accesos no autorizados que permitan desapoderar a otro de su patrimonio. Si bien cada técnica tiene particularidades operativas, desde la óptica del Derecho Penal español *no se configuran como tipos autónomos*, sino que se subsumen en la figura general de la estafa (clásica o informática, según el caso) o en delitos afines. En particular, phishing, smishing, vishing, pharming y derivados se entienden englobados en la *estafa informática* del Código Penal, como se explicará en detalle en las secciones siguientes.

Tabla 1. Modalidades de estafa informática y sus características principales

Modalidad	Definición / Descripción	Medio de Ejecución	Modus Operandi	Ejemplo Jurisprudencial	Encaje Penal
Phishing	Engaño mediante correos electrónicos falsos que suplantan a entidades legítimas (bancos, organismos públicos, empresas) para obtener datos	Correo electrónico y páginas web falsas.	El estafador envía un email con apariencia auténtica que contiene un enlace a una web fraudulenta casi idéntica a la original, donde la víctima introduce sus credenciales, permitiendo	Doctrina general consolidada (STS 379/2019, de 23 de julio).	Art. 249.1.a CP: estafa informática mediante manipulación o artificio informático.

	confidenciales del usuario.		el acceso ilícito a sus cuentas.		
Smishing	Variante del phishing que utiliza mensajes SMS (Short Message Service) para engañar al usuario y obtener sus datos o provocar una transferencia no consentida.	Mensajería móvil (SMS).	La víctima recibe un mensaje de texto que aparenta ser de su banco alertando de un problema y solicitando verificación a través de un enlace o número de teléfono falso.	SAP Asturias, Secc. 4.ª, nº 477/2024 (21 de marzo de 2024): transferencia fraudulenta de 6.000 €.	Art. 249.1.a CP, como phishing ejecutado por SMS.
Vishing	Engaño telefónico mediante el cual el delincuente, fingiendo ser un representante de confianza (banco, técnico, policía), induce a la víctima a revelar datos o autorizar operaciones.	Llamada telefónica (voz).	El estafador contacta a la víctima simulando ser del servicio de seguridad bancaria, alerta de supuestos movimientos irregulares y solicita códigos o claves de verificación.	Casuística reconocida por la jurisprudencia menor (SAP varias provincias, 2023-2024).	Art. 249.1.a CP: estafa informática por artificio semejante.
Pharming	Manipulación técnica de los sistemas informáticos (DNS o equipos del usuario) para redirigir al afectado hacia una web falsa sin que este lo advierta.	Alteración del sistema de nombres de dominio (DNS) o del equipo del usuario.	El usuario escribe la URL correcta, pero una alteración en el sistema lo lleva a una página falsa controlada por el delincuente, que captura sus credenciales.	STS 381/2017, de 26 de octubre de 2017 y STS 509/2018.	Art. 249.1.a CP: manipulación informática pura.
Otras variantes (SIM swapping, Quishing, Whishing, etc.)	Fraudes derivados que combinan ingeniería social y manipulación técnica para obtener acceso a datos o líneas de comunicación.	Duplicado de SIM, códigos QR falsos o apps de mensajería (WhatsApp, Telegram).	Se suplanta identidad o interceptan factores de autenticación (SMS, QR, enlaces), con el mismo fin de obtener fondos o datos sensibles.	Ej.: SAP Madrid, Secc. 23.ª, 30/10/2019 (SIM swapping).	Subsunción general en art. 249.1.a CP como estafa informática.

Fuente: elaboración propia

En el caso del quishing, la adopción de los códigos QR ha crecido un 16 % anual, acelerada especialmente por la pandemia de COVID-19. El código de barras bidimensional llama la atención como futuro sustituto de las contraseñas manuales y como atajo conveniente para agilizar las entradas en los teclados de los dispositivos móviles. La pandemia de COVID-19 facilitó el quishing con códigos QR maliciosos, ya que se convirtieron en un medio conveniente para compartir URL, incluidas las maliciosas (SHAREVSKI, DEVINE, PIERONI Y JACHIM, 2022).

Los códigos de respuesta rápida (QR) son códigos de barras bidimensionales que codifican diferentes tipos con alta densidad. En 1994, Masahiro Hara los inventó para mejorar el control de la producción de la empresa Denso Wave. Desde entonces, su uso se ha diversificado. Por ejemplo, los códigos QR se aplican en sitios web, para marketing, como enlaces de información o con fines de autenticación en empresas y entornos de investigación y educación, ya que ofrecen simplicidad y comodidad. Casi todos los teléfonos inteligentes tienen escáneres de códigos QR integrados con sensores y decodificadores.

Durante la pandemia de COVID-19, los códigos QR se utilizaron con frecuencia, por ejemplo, para concertar una cita para una prueba y obtener los resultados de la prueba de COVID-19, para hacer un pedido en un restaurante o para mostrar el estado de vacunación en la aplicación de rastreo de contactos de COVID-19 (AMOAH y HAYFRON-ACQUAH, 2022).

El *quishing* es una táctica habitual que utilizan los hackers contra el sector sanitario, ya que a menudo da lugar a violaciones de datos, y los datos sanitarios robados pueden ser muy lucrativos para los atacantes. En 2021, la Sociedad de Sistemas de Información y Gestión Sanitaria descubrió que el ataque más común que afectaba a las organizaciones sanitarias era el *phishing* (*quishing*), que representaba casi la mitad de todos los ataques (HIMSS, 2021).

En cuanto a las estrategias, el quishing utiliza la legitimidad o la urgencia (por ejemplo, «Escanee para obtener una recompensa gratuita», «Escanee para verificar su cuenta») para incitar a los usuarios a cumplir sin cuestionar.

El enlace malicioso no es accesible inmediatamente en forma de texto, y los códigos QR suelen evitar ser detectados por los filtros de correo electrónico y el software de escaneo de URL. Debido a esto, a los sistemas automatizados les resulta difícil identificar o examinar la carga útil antes de que el usuario la escanee. Por ello, los consumidores no pueden previsualizar fácilmente la URL detrás de un código QR, a diferencia de los enlaces en correos electrónicos o mensajes de texto, por lo que hay más posibilidades de que se produzca una interacción involuntaria.

Básicamente, el *quishing* es muy similar al *phishing* en cuanto al uso indebido de enlaces para engañar a la víctima y que interactúe con ellos. La capacidad de rastrear a un usuario para que escanee un código QR se basa a menudo en un contexto falso; un correo electrónico que

contiene texto y gráficos que crean falsamente la impresión de que es algo que le interesaría al usuario.

Otro factor que favorece el *quishing*, al menos por ahora, es que los seres humanos no reciben mucha ayuda para detectar códigos QR maliciosos. Incorporar primitivas de seguridad en los códigos QR podría ayudar, pero crea un retraso computacional excesivo (por ejemplo, los usuarios empiezan a abortar el escaneo). Una organización de confianza podría crear un código QR con propiedades distintivas, por ejemplo, logotipos o una combinación de colores compleja, pero cada vez es más fácil para los atacantes duplicar y suplantar dichos códigos.

Por lo que respecta a la ejecución técnica de un ataque de *quishing*, cabe señalar que estos sitios web de *phishing* podrían solicitar los datos de la tarjeta de crédito de los clientes. Además, las diferentes URL de phishing utilizan diferentes protocolos. Esta cadena de consulta redigirá a la víctima a otro sitio web malicioso. A diferencia de los ataques de phishing tradicionales, que se basan en correos electrónicos o mensajes engañosos con URL visibles, el quishing aprovecha la naturaleza opaca de los códigos QR, lo que dificulta a los usuarios evaluar su legitimidad antes de escanearlos. Si bien las URL son la carga útil más común en los ataques de quishing, los códigos QR pueden codificar una variedad de tipos de datos más allá de los enlaces web, lo que amplía la superficie de ataque. Pueden utilizarse para almacenar credenciales de Wi-Fi, activar enlaces profundos de aplicaciones, iniciar transacciones con criptomonedas, añadir datos de contacto, compartir datos de geolocalización, enviar mensajes SMS, programar eventos en el calendario o incluso mostrar mensajes de phishing en texto plano. Esta versatilidad permite a los atacantes diseñar tácticas de ingeniería social que no se basan únicamente en URL maliciosas, lo que complica aún más los esfuerzos de detección.

Cabe mencionar los siguientes ataques:

Primeramente, existe el llamado robo directo donde los atacantes roban dinero al obtener acceso a cuentas bancarias o sistemas de pago. Aquí es cuando surgen las transacciones fraudulentas. Los delincuentes utilizan los datos robados de tarjetas de crédito para realizar compras no autorizadas. El resultado es la generación de pérdidas comerciales. Las empresas pueden sufrir daños financieros debido al *ransomware*, la desviación de fondos o las multas reglamentarias.

En segundo lugar, deben mencionarse las violaciones de datos y robo de identidad. Cuando existe una exposición de datos personales, el *phishing* puede conducir al robo de números de la Seguridad Social, direcciones y registros médicos. También se producen fugas de datos corporativos: los empleados que caen en estafas de phishing pueden exponer datos confidenciales de la empresa (registros de clientes, propiedad intelectual). Incluso puede darse fraude de identidad en el caso de que la información robada puede utilizarse para cometer robo de identidad, abrir cuentas falsas o solicitar préstamos.

Según una encuesta realizada en 2021 por el Ponemon Institute y Proofpoint, el coste de los ataques de phishing se cuadruplicó entre 2015 y 2021. La misma investigación reveló que el coste medio de un ataque de phishing exitoso en 2021 fue de 14,8 millones de dólares (PROOFPOINT, 2021). El phishing es una táctica habitual que utilizan los hackers contra el sector sanitario, ya que a menudo da lugar a violaciones de datos, y los datos sanitarios robados pueden ser muy lucrativos para los atacantes. Así, la Sociedad de Sistemas de Información y Gestión Sanitaria descubrió que el ataque más común que afectaba a las organizaciones sanitarias era el phishing, que representaba casi la mitad de todos los ataques.

La prevención de los ataques de phishing exitosos comienza con una defensa en profundidad. La primera capa de protección de cualquier empresa probablemente se encuentre en su servidor de correo electrónico, que tendrá una conexión a Internet. Para ello, es necesario asegurarse de que el servidor de correo esté configurado para filtrar los correos electrónicos no deseados o que se integre una plataforma adicional en la infraestructura de información, como un filtro de puerta de enlace de spam. Esto no evitará todos los correos electrónicos de *phishing*, pero debería eliminar parte del tráfico no deseado. En segundo lugar, es imprescindible formar a los usuarios finales. Deben recibir formación para detectar los correos electrónicos de phishing e interactuar con todos los correos electrónicos con un grado saludable de escepticismo. En tercer lugar, se recomienda encarecidamente la autenticación multifactorial. Esto protegerá contra el robo de credenciales, que puede ser el objetivo inicial de un ataque de phishing. En cuarto lugar, se recomienda encarecidamente instalar software de seguridad, filtrado y seguridad para puntos finales, y actualizarlo con frecuencia en el sistema de cada usuario final. Este tipo de software puede detectar el malware mientras se ejecuta en un sistema, si un usuario interactúa con un correo electrónico de phishing.

3. Evolución normativa y marco legal en el contexto español

3.1. De la estafa clásica a la estafa informática: evolución legislativa

En el Código Penal de 1973 (anterior a la era digital), el delito de estafa requería necesariamente un engaño bastante dirigido a una persona que, en virtud de dicho engaño, realizara un acto de disposición patrimonial en perjuicio propio o ajeno. Este concepto tradicional de la estafa resultaba insuficiente para perseguir ciertos fraudes emergentes a finales del siglo XX, donde el engaño no iba dirigido directamente contra una persona, sino contra un sistema automatizado. Un ejemplo temprano fueron los fraudes por manipulación de máquinas expendedoras o teléfonos públicos (colocar monedas atadas con hilo para recuperar el dinero, pulsar claves para obtener servicios gratuitos, etc.). En aquellos casos, existía sin duda una maquinación engañosa, pero no había un error de una persona inducida por engaño, sino una respuesta automática de un dispositivo. Los tribunales españoles de la época entendieron que tales conductas no encajaban en la tipicidad de la estafa vigente (art. 528 CP de 1973, análogo al actual art. 248 CP) y, por tanto, recurrían a otras figuras (p. ej. considerarlo hurto o robo si mediaba apoderamiento físico de cosas) o incluso no se castigaban penalmente al no adecuarse a tipo alguno (MESTRE, 2024). Esta laguna evidenció la necesidad de una reforma legal ante las nuevas formas de defraudación tecnológica que ya despuntaban en los años 80 y 90.

El legislador español respondió a ese desafío en el Código Penal de 1995 (LO 10/1995). Desde su entrada en vigor, el CP incorporó expresamente la «estafa informática» como modalidad delictiva autónoma dentro del delito de estafa (FERNÁNDEZ, 2024). Con ello, España se adelantó a proveer cobertura penal a los fraudes cometidos mediante mecanismos informáticos, algo que también sería promovido años más tarde por instrumentos internacionales como el Convenio de Budapest sobre ciberdelincuencia (2001). En concreto, el art. 248.2 del CP 1995 (numeración original) estableció que «también se consideran reos de estafa» a aquellos que, con ánimo de lucro, mediante manipulación informática o artificio semejante consigan realizar una transferencia no consentida en perjuicio ajeno. Esta redacción englobaba ya supuestos de phishing primitivo (antes incluso de popularizarse el término), fraudes con tarjetas de crédito duplicadas, manipulaciones de cajeros automáticos,

etc., eliminando el requisito del engaño a persona determinada y sustituyéndolo por la presencia de un engaño tecnológico o manipulación sobre sistemas.

Desde 1995 en adelante, la figura de la estafa informática se ha mantenido en el Código Penal, sufriendo ciertas modificaciones y mejoras en su formulación. Una reforma significativa fue la operada por la Ley Orgánica 5/2010, cuyo Preámbulo destacó la incorporación de «los fraudes informáticos» al catálogo de estafas del CP 1995, consolidando la protección penal frente a estas conductas. Más recientemente, la Ley Orgánica 14/2022, de 22 de diciembre –vigente desde enero de 2023– introdujo cambios importantes al trasponer la Directiva (UE) 2019/713 relativa a la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo. Esta reforma reorganizó los delitos patrimoniales y reubicó la estafa informática en el artículo 249.1.a) del Código Penal, actualizando además su descripción típica (ESTÉBANEZ, 2024). La ubicación anterior (art. 248.2) quedó desplazada por la inserción de nuevos preceptos sobre fraudes de pago, de modo que la estafa informática pasó a numerarse como art. 249, con un texto más detallado.

Actualmente, conforme al artículo 249.1.a) del Código Penal (redacción vigente tras LO 14/2022**)**, cometen estafa en la modalidad de fraude informático:

«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».

Esta definición legal, de notable amplitud, busca abarcar la variedad de formas que pueden adoptar las ciberestafas. Se contemplan explícitamente tanto ataques a sistemas (interferencia, alteración de datos, etc.) como cualquier otro tipo de *engaño tecnológico o artificio* equivalente. Lo esencial es que, mediante tales medios, el autor logre una transferencia patrimonial no consentida en perjuicio ajeno, actuando con intención de lucro.

Cabe señalar que la mención a «transferencia de cualquier activo patrimonial» permite incluir no solo traspasos de dinero electrónico entre cuentas, sino también, por ejemplo, cargos no autorizados en tarjetas de crédito, traspasos de criptomonedas, o disposiciones patrimoniales de otro tipo siempre que sean electrónicas. En suma, el legislador español ha brindado a los

operadores jurídicos una herramienta flexible para perseguir desde el *hacking* puramente técnico con fines de lucro, hasta los engaños por ingeniería social como phishing o vishing, todos ellos subsumibles en la estafa informática (art. 249.1.a CP).

Además de la figura base, el Código Penal prevé circunstancias agravantes específicas para estafas, aplicables también a las informáticas, en el art. 250 CP. Por ejemplo, se agrava la pena si concurre especial gravedad por el valor de la defraudación -superior a 50.000 €-, afectación a multitud de personas, abuso de relaciones personales, o cuando el engaño se realiza mediante el uso de datos personales ajenos[2]. Estas agravantes pueden ser relevantes en casos de phishing masivo o de organización criminal dedicada a estas prácticas.

Finalmente, en el ámbito procesal, España ha ido adaptando su normativa para la persecución de la ciberdelincuencia. Por un lado, se ha debido afrontar el problema de la competencia territorial en delitos cometidos en la red (donde víctima, autor, servidores y efectos del delito pueden encontrarse en lugares distintos). La Sala Segunda del Tribunal Supremo ha resuelto en varias ocasiones que, tratándose de estafas informáticas, rige una aplicación atenuada del principio de ubicuidad: se opta por atribuir la competencia al órgano judicial que esté en mejores condiciones de llevar a cabo la instrucción eficaz, atendiendo al lugar donde se planificó el delito, donde se produjo el perjuicio principal o donde se hallan la mayoría de las pruebas, entre otros criterios, por influencia del Convenio de Budapest. No obstante, subsisten desafíos en la práctica, pues muchos juzgados siguen siendo reacios a acumular en un solo procedimiento hechos cometidos en demarcaciones diversas, lo que puede fragmentar la persecución de una trama de phishing en múltiples causas dispersas. Esta realidad reclama mejoras de coordinación y especialización, como se comentará en las propuestas.

3.2. Marco legal complementario y protección de los usuarios

3.2.1. Normativa europea

Lamentablemente, no existe un marco legal claro y recogido en una norma sobre el *phishing* y el *pharming* en la Unión Europea. En su lugar, hay muchos documentos jurídicos diferentes. Algunos de ellos son: la Decisión Marco 2001/413/JAI del Consejo, de 28 de mayo de 2001,

[2] Esta última incorporada en la reforma de 2022, vinculada con los fraudes de identidad digital.

relativa a la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, sobre medidas para un alto nivel común de seguridad de los sistemas de redes y de la información en la Unión, la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, sobre los ataques contra los sistemas de información y que sustituye a la Decisión marco 2005/222/JAI del Consejo, Reglamento (UE) n.º 526/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativo a la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) n.º 460/2004; la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) n.º 2006/2004 sobre la cooperación entre las autoridades nacionales encargadas de la aplicación de la legislación en materia de protección de los consumidores, Comunicación de la Comisión, de 15 de noviembre de 2006, al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la lucha contra el spam, el spyware y el software malicioso, Directiva 2005/29/ CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior y por la que se modifican la Directiva 84/450/CEE del Consejo, las Directivas 97/7/CE, 98/27/CE y 2002/65/CE del Parlamento Europeo y del Consejo y el Reglamento (CE) n.º 2006/2004 del Parlamento Europeo y del Consejo («Directiva sobre prácticas comerciales desleales»), la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), 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, RGPD).

En el Reglamento RGPD se ha prestado especial atención a las estafas de phishing. Algunas disposiciones de este Reglamento son relevantes para este trabajo. En primer lugar, el artículo 7 establece lo siguiente: Cuando el tratamiento se base en el consentimiento, el responsable del tratamiento deberá poder demostrar que el interesado ha dado su consentimiento para el tratamiento de sus datos personales. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiere a otros asuntos, la solicitud de consentimiento se presentará de manera claramente distinguible de los demás asuntos, en forma inteligible y fácilmente accesible, utilizando un lenguaje claro y sencillo. Cualquier parte de dicha declaración que constituya una infracción del presente Reglamento no será vinculante. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basado en el consentimiento previo a su retirada. Antes de dar su consentimiento, se informará de ello al interesado. La retirada del consentimiento deberá ser tan fácil como su concesión.

A la hora de evaluar si el consentimiento se ha otorgado libremente, se tendrá en cuenta, entre otras cosas, si la ejecución de un contrato, incluida la prestación de un servicio, está supeditada al consentimiento para el tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato. Además, en los artículos 25 y 32 del Reglamento RGPD, se establece que, teniendo en cuenta el estado de la técnica, el coste de su aplicación y la naturaleza, el alcance, 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 que plantea el tratamiento, el responsable del tratamiento, tanto en el momento de determinar los medios para el tratamiento como en el momento del tratamiento propiamente dicho, aplicará medidas técnicas y organizativas adecuadas, como la seudonimización, diseñadas para aplicar de manera 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.

El responsable del tratamiento aplicará medidas técnicas y organizativas adecuadas para garantizar que, por defecto, solo se traten los datos personales que sean necesarios para cada finalidad específica del tratamiento. De conformidad con el artículo 33 del RGPD, en caso de violación de datos personales, el responsable del tratamiento notificará sin dilación indebida la violación de datos personales a la autoridad de control competente, a menos que sea

improbable que la violación de datos personales suponga un riesgo para los derechos y libertades de las personas físicas. Además, cuando la violación de datos personales pueda suponer un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento comunicará la violación de datos personales al interesado sin demora injustificada.

El responsable del tratamiento documentará cualquier violación de datos personales, incluyendo los hechos relacionados con la violación de datos personales, sus efectos y las medidas correctivas adoptadas. Esa documentación permitirá a la autoridad de control verificar el cumplimiento del presente artículo. Independientemente de las soluciones previstas en el Reglamento GDPR, en la práctica se ha registrado un número creciente de estafas de *phishing* relacionadas con este Reglamento, tanto antes como después de su entrada en vigor.

3.2.2. Normativa nacional

Aunque el foco de este trabajo es penal, conviene mencionar que la respuesta jurídica a las estafas informáticas no se agota en el Derecho Penal. En el plano administrativo y civil, existen normas dirigidas a proteger a los consumidores y usuarios financieros frente al fraude online. En particular, el ordenamiento español en armonía con el europeo impone a las entidades bancarias y de pago obligaciones de seguridad y responsabilidad por operaciones no autorizadas. El Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago (en transposición de la Directiva (UE) 2015/2366, PSD2) establece un régimen cuasi-objetivo de responsabilidad de los proveedores de servicios de pago: los bancos deben reembolsar al cliente los importes de operaciones fraudulentas, salvo que prueben que este actuó con dolo o negligencia grave (art. 45 y 46 RDL 19/2018). Esto ha dado lugar a abundante litigiosidad civil en casos de phishing, donde los clientes reclaman a su banco la devolución del dinero sustraído.

La mayoría de Audiencias Provinciales han interpretado la normativa a favor del consumidor, exigiendo a la entidad demostrar una actuación gravemente negligente del usuario para exonerarse. De hecho, la responsabilidad civil de la banca en estos supuestos ha cobrado tal relevancia que el Tribunal Supremo, Sala de lo Civil, emitió una sentencia de referencia

(pionera) – STS 571/2025, de 9 de abril de 2025, rec. 20/2022 – afirmando que, si el banco no acredita negligencia del cliente, debe asumir el perjuicio del phishing (obligación de reembolso). Esta vía resarcitoria coexiste con la vía penal: mientras los estafadores muchas veces no son habidos o son insolventes, el perjudicado al menos puede ser resarcido por su entidad financiera.

Por lo tanto, la normativa de servicios de pago impone una responsabilidad cuasi objetiva a las entidades bancarias. El banco solo puede exonerarse si demuestra que la operación fue autenticada, registrada exactamente y contabilizada, que no hubo fallo técnico, que no existió deficiencia en el servicio, y que el usuario actuó con fraude o negligencia grave. No es suficiente con mostrar que se introdujeron correctamente las claves y el SMS. Esta inversión de la carga de la prueba se recoge en el artículo 44 del Real Decreto-ley 19/2018, transpuesto de la Directiva PSD2.

La sentencia considera probado que, en este supuesto, el cliente actuó diligentemente y avisó repetidamente al banco de actividades sospechosas. El banco no adoptó ninguna medida preventiva efectiva: no cambió claves, no reforzó autenticación, no activó alertas. Un volumen elevadísimo y anómalo de operaciones nocturnas (10 Bizum + 5 transferencias por casi 80.000 €) debió activar bloqueos o avisos automáticos. Además, la alerta del fraude vino del Banco Santander, no de Ibercaja. Por ello, el TS determina que el servicio del banco fue deficiente y no actuó de manera rápida.

En consecuencia, el marco legal español frente a las ciberestafas es multifacético: el Derecho Penal provee la sanción a los defraudadores (y eventualmente a sus cómplices, cooperadores o encubridores), y el Derecho de consumo y bancario ofrece mecanismos para mitigar el impacto económico en las víctimas. Esta complementariedad refleja una política integral de protección ante los fraudes informáticos, reconociendo la dificultad de la persecución penal transnacional y la necesidad de reforzar la confianza de los usuarios en el comercio electrónico y la banca digital (FERNÁNDEZ ESCUDERO, 2024).

Tabla 2. Evolución normativa relevante en España relacionada con las estafas informáticas

Año	Norma	Contenido / Relevancia
1973	Código Penal de 1973	Regulaba la estafa clásica. Exigía engaño directo a persona. Las primeras estafas tecnológicas (máquinas expendedoras, teléfonos públicos) no encajaban claramente en el tipo tradicional.
1995	LO 10/1995, Código Penal	Primera tipificación explícita de la estafa informática, entonces situada en el art. 248.2 CP. Permitió sancionar fraudes cometidos mediante manipulación de sistemas o datos, aun sin engaño directo a una persona.
2001	Convenio de Budapest sobre ciberdelincuencia	Instrumento internacional clave para armonizar delitos informáticos; inspira reformas posteriores del CP y la LECrim. Referido indirectamente como marco internacional.
2010	LO 5/2010, reforma del Código Penal	Refuerza el tratamiento de los fraudes informáticos en el CP y consolida su encaje dentro del delito de estafa.
2015	LO 13/2015, de modificación de la LECrim	Introduce medidas de investigación tecnológica: acceso a dispositivos, interceptación de comunicaciones y técnicas útiles contra *phishing*, *smishing* y otras ciberestafas.
2018	Real Decreto-ley 19/2018, de servicios de pago (PSD2)	Establece el régimen de responsabilidad bancaria por operaciones no autorizadas: el banco debe reembolsar al usuario salvo dolo o negligencia grave de éste. Clave en litigios civiles derivados del *phishing*.
2019	Directiva (UE) 2019/713	Obliga a los Estados a reforzar la lucha contra el fraude en medios de pago distintos del efectivo. Su transposición lleva a la gran reforma penal de 2022.
2022	Ley Orgánica 14/2022, de transposición de directivas europeas	Reordena los delitos patrimoniales y traslada la estafa informática al art. 249.1.a CP, ampliando su descripción: interferencia en sistemas, alteración de datos, artificios tecnológicos y transferencias no consentidas de cualquier activo patrimonial. Norma central en la regulación actual.
2025	STS 571/2025 (Sala Civil)	Aclara la responsabilidad bancaria en operaciones fraudulentas: si no se prueba negligencia grave del cliente, el banco debe reembolsar el importe defraudado. Relevancia práctica para víctimas de phishing.

Fuente: elaboración propia

4. Análisis dogmático del delito de estafa informática

A continuación, se examinan los elementos configuradores del delito de estafa informática en el Derecho Penal español, enfatizando las particularidades dogmáticas que presentan las modalidades de *phishing*, *smishing*, *vishing* y *pharming*. Dado que estas modalidades se subsumen típicamente en el tipo penal del art. 249.1.a) CP (antes art. 248.2 CP), conviene precisar cómo encajan sus características en los requisitos tradicionales de la estafa, así como en qué medida la jurisprudencia ha ido perfilando su interpretación.

4.1. Bien jurídico protegido

El bien jurídico tutelado en las estafas informáticas es el mismo que en la estafa común: el patrimonio en sentido amplio, entendido como el conjunto de bienes y derechos de contenido económico pertenecientes a la víctima (MESTRE, 2024). Se protege la propiedad o disponibilidad patrimonial libre de vicios del consentimiento o manipulaciones indebidas. De acuerdo con QUINTERO (2013), el bien jurídico en juego no se limita al ámbito patrimonial individual, sino que incluye la seguridad del comercio electrónico y la estabilidad de los intercambios económicos que la tecnología lleva a cabo, por lo que puede encuadrarse en el seno de los delitos patrimoniales, aunque con un carácter marcado de Derecho Penal económico.

La jurisprudencia del Alto Tribunal ha interpretado en diferentes ocasiones que el núcleo de tutela de la estafa informática es el patrimonio, aunque en estos casos no existe un engaño directo al individuo, sino que se emplean mecanismos técnicos o artificios informáticos que consiguen quitar el patrimonio sin que haya consentimiento (STS 379/2019, de 23 de julio, rec. 853/2018). Por lo tanto, el bien jurídico debe entenderse de forma más amplia que la estafa clásica, puesto que lo que se protege además de la decisión de la víctima de disponer de su patrimonio libremente es la integridad funcional de los sistemas de información en cuanto a su patrimonio.

En el contexto específico de fraudes bancarios online, adicionalmente se resguardan la seguridad en las transacciones económicas electrónicas y la confianza del público en los sistemas de pago digitales, aspectos estrechamente ligados al patrimonio individual y también al orden socioeconómico. Por ello, algunos doctrinantes vinculan estas figuras al Derecho Penal económico en sentido estricto, ya que afectan la integridad de los intercambios

económicos mediados por tecnología (QUINTERO OLIVARES, 2013). No obstante, a nivel penal positivo, siguen encuadradas entre los delitos contra el patrimonio y el orden socioeconómico.

4.2. Sujeto activo y partícipes

El sujeto activo de la estafa informática puede ser cualquier persona. En la práctica, los autores de phishing y otras ciberestafas suelen actuar en grupos u organizaciones criminales especializadas, dada la necesidad de conocimientos técnicos y de canales para movilizar el dinero robado. Surgen así figuras como los «hackers» que diseñan las intrusiones o páginas falsas, los «spammers» que envían las campañas masivas de correos/SMS, y las «mulas bancarias» que reciben y disimulan el dinero obtenido ilícitamente.

Desde el punto de vista de la autoría y participación, la jurisprudencia ha debido analizar cómo encuadrar a estos partícipes. Por un lado, se considera autor directo del delito de estafa informática a aquel que planifica y ejecuta la manipulación informática (ej. el que envía el phishing y accede a la cuenta ajena). En el caso de que haya varias personas que controlan distintas etapas de la operación fraudulenta de forma concertada, se considerarían coautores (art. 28 CP). Por otro lado, las mulas bancarias son aquellos individuos que se encargan de recibir el dinero que previamente ha sido defraudado o que tiene un origen ilícito, para posteriormente transmitirlo a los cabecillas. Como contraprestación, perciben una comisión por lo que se les considera cooperadores necesarios en la estafa, al aportar la cuenta y facilitar la disposición final del dinero. Incluso ciertos tribunales consideran que estamos ante blanqueo de capitales (art. 301 CP), sobre todo cuando la mula no conoce el origen del dinero, imputándose un delito de blanqueo imprudente porque se ayuda en una actividad delictiva (GUTIÉRREZ, 2023).

En cualquier caso, la tendencia jurisprudencial mayoritaria es que el **mulero bancario** responda penalmente, ya sea como partícipe en la estafa informática o por el delito autónomo de blanqueo, pues su intervención es crucial para materializar o encubrir el beneficio económico de la trama delictiva. Un ejemplo reciente es la SAP Cáceres 116/2024, 12 de abril de 2024, rec. 242/2024, que analizó la responsabilidad de un "mulero" en una red de fraude online, confirmando que cabe imputarle blanqueo de capitales aun sin prueba de que conociera con detalle la estafa, por haber aceptado mover dinero de origen sospechoso (FUKUROVA, 2024).

El sujeto pasivo o víctima directa en las ciberestafas suele ser el titular del patrimonio defraudado (el cliente bancario cuyos fondos son transferidos indebidamente). No obstante, en algunos casos complejos podría haber dos niveles de víctimas: por ejemplo, en un phishing bancario, la victimización primaria recae sobre el usuario engañado que pierde su dinero, pero existe también una posible victimización secundaria del banco si éste termina resarciendo al cliente. Con todo, a efectos penales el sujeto pasivo inmediato es el perjudicado patrimonial (el cliente en este ejemplo), sin perjuicio de que la entidad financiera pueda figurar luego como responsable civil subsidiaria o incluso como denunciante si detecta fraudes masivos contra sus clientes.

En la STS de 2 de diciembre de 2014, nº 845/2014, Banesto pretendía que los hechos se calificaran como estafa informática dolosa y no como blanqueo de capitales por imprudencia porque esa calificación le habría permitido trasladar a la acusada una intención fraudulenta directa, reforzando la responsabilidad penal y reduciendo el peso del error de vigilancia interna del propio banco. En su recurso, la entidad sostenía que la acusada no actuó de manera meramente imprudente al recibir y reenviar el dinero procedente del fraude, sino que conocía o debía conocer claramente el carácter ilícito del origen de los fondos, lo que supondría que había participado dolosamente en la estafa informática inicial.

En el caso de que se aceptara esa tesis, la actuación de la acusada habría dejado de ser un comportamiento negligente y habría pasado a ser una intervención consciente en el engaño telemático previo, con lo cual Banesto podía justificar una mayor exigencia punitiva y, al mismo tiempo, reforzar la idea de que el perjuicio sufrido no sería consecuencia de los fallos en sus sistemas de control, sino del dolo de un tercero, exonerándose de responsabilidad.

El Tribunal se encarga de examinar el motivo del recurso por el que Banesto pretendía que los hechos fueran calificados como estafa informática dolosa, en lugar de como blanqueo de capitales por imprudencia grave, tal y como estableció la Audiencia Provincial y como se ha comentado anteriormente. El Supremo destaca que dicha pretensión exigiría revisar la intención de la acusada, elemento subjetivo del delito que solo puede fijar el tribunal que ha presenciado las pruebas personales, sobre todo cuando se debe valorar el dolo. El presente recurso determina que no se permite modificar los hechos probados ni revisar inferencias sobre la voluntad del acusado siguiendo la jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos ya que ello vulneraría el principio de inmediación y

el derecho de defensa. Con base en esta doctrina, rechaza el recurso, pues transformar una conducta imprudente en dolosa requiere revalorar la intención de la acusada que la casación no puede realizar.

La condena penal que se mantiene es la de blanqueo imprudente que se contempla en el artículo 301 del Código Penal, porque la acusada recibió dinero procedente de un fraude informático y lo reenvió al extranjero sin comprobarlo, actuación que el Tribunal considera imprudente en grado grave. El Tribunal Supremo confirma esta calificación porque no puede revisarse el dolo en casación y porque la Audiencia ya había determinado que la acusada no participó en la estafa informática, sino que intervino después, facilitando el blanqueo del dinero que se había obtenido de manera ilícita.

4.3. Elementos del tipo objetivo y subjetivo

El estudio de los elementos del tipo objetivo y subjetivo de la estafa informática requiere partir de la estructura general del delito de estafa para entender su proyección y su adaptación al entorno digital. En el plano objetivo, el núcleo se encuentra en la manipulación informática o en la utilización de un artificio similar que genera una transferencia patrimonial sin consentimiento.

4.3.1. Elemento objetivo

Primero, debe hacerse referencia a la diferencia existente entre **engaño previo contra manipulación informática**. En la estafa clásica, el tipo exige un engaño precedente y bastante que induce en la víctima un error esencial, el cual la mueve a realizar un acto de disposición. En la estafa informática, este elemento del engaño adopta formas atípicas: el engaño puede no ir dirigido a una persona concreta, sino a un sistema, o bien puede recaer sobre la persona de manera indirecta. La ley suple la necesidad de engaño directo estableciendo que la acción típica puede consistir alternativamente en «valerse de alguna manipulación informática o artificio semejante» (art. 249.1.a CP). Esto significa que el núcleo del tipo objetivo es la utilización de mecanismos técnicos fraudulentos para conseguir la disposición patrimonial ilícita.

La manipulación se puede materializar de diferentes modos, desde introducir datos fraudulentos en un sistema de banca online hasta modificar los procesos de autenticación,

demostrando con ello que el tipo penal es flexible ante las técnicas evolucionadas de forma continua. Se diferencia de la estafa clásica porque el engaño interpersonal tiene un papel fundamental y la víctima realiza un acto de disposición patrimonial de forma voluntaria inducida por error (ACÓN, 2024). La coexistencia de técnicas tecnológicas y de ingeniería social demuestra que el engaño sigue estando, reconfigurándose de manera más sofistica y menos visible, por lo que el engaño no desaparece.

En casos de *pharming* o ciertas intrusiones puramente técnicas, efectivamente no hay un engaño personal sino una manipulación de máquinas (p. ej. alteración de un servidor DNS para redirigir fondos). En otros supuestos como el phishing por correo o el vishing, sí existe un engaño a una persona (la víctima cree que está dando sus datos al banco), pero aún así la jurisprudencia ha entendido que ese engaño personal no es el que directamente produce el desplazamiento patrimonial, sino que éste ocurre por la posterior manipulación del sistema bancario usando las credenciales obtenidas (STS 379/2019, de 23 de julio de 2019, rec. 853/2018). De esta forma, se considera que el engaño personal inicial forma parte del artificio informático global empleado por el autor, pero se prescinde del requisito de que la víctima realice un acto dispositivo bajo error.

Como señaló el Tribunal Supremo, «subsiste la defraudación, y el engaño propio de la relación personal es sustituido como medio comisivo defraudatorio por la manipulación informática o artificio semejante», de manera que lo relevante es que la máquina actúe por impulso de la actuación ilegítima del delincuente. En otras palabras, en la estafa informática el nexo causal entre el ardid y el perjuicio patrimonial puede no ser la conducta de la víctima, sino el funcionamiento engañado de un sistema informático.

Consecuencia de lo anterior es que el elemento clásico del **error de la víctima** pierde centralidad. En el *phishing*, por ejemplo, la víctima ciertamente está en error al creer legítimo el sitio web o la llamada, pero legalmente ese error no es un presupuesto imprescindible para la tipicidad, dado que el tipo penal se configura, aunque la disposición patrimonial ocurra sin la participación consciente de la víctima (v.gr., la transferencia la ordena el defraudador con las credenciales robadas). La disposición patrimonial no consentida se manifiesta típicamente en una transferencia electrónica de fondos desde la cuenta de la víctima a una cuenta controlada por el autor o terceros. Este acto de disposición es ejecutado materialmente por un sistema automatizado (el servidor bancario que procesa la transferencia a instancia del

estafador). Por tanto, se cumple el requisito de desplazamiento patrimonial en perjuicio ajeno, si bien con la particularidad de que no medió un acto volitivo de la víctima para disponer su patrimonio, sino una actuación del autor suplantando su identidad o burlando los controles. La jurisprudencia ha sido clara en que introducir datos falsos o identificarse mendazmente en un sistema informático bancario para provocar un cargo no autorizado «*ha de ser considerado bajo la conducta de manipulación informática a que se refiere la estafa del CP»* (SAN de Madrid 32/2025, de 8 de octubre de 2025, rec. 29/2025). Es decir, aunque la víctima no "entregue" voluntariamente sus bienes engañada (como en la estafa tradicional), la transferencia involuntaria causada por el ardid informático suple funcionalmente ese elemento.

También debe hacerse referencia al **perjuicio patrimonial.** Debe producirse un detrimento económico real para tercero. Normalmente la pérdida patrimonial recae en el usuario cuyo dinero es retirado de su cuenta. Sin embargo, puede haber casos en que, por coberturas contractuales, sea el banco quien asume la pérdida (por ejemplo, si reintegra al cliente estafado); con todo, desde la perspectiva penal el delito se consuma con el perjuicio inicial al titular de los fondos en el momento de la transferencia *non consentida*. La cuantía del perjuicio puede variar enormemente: desde pequeños cargos (microtransacciones fraudulentas) hasta vaciado de cuentas con sumas importantes. Si la cuantía defraudada no supera 400 euros, en principio estaríamos ante una **estafa informática leve**, equivalente a delito leve (antes falta), conforme al art. 249.2 CP y art. 250.5º CP. En cambio, perjuicios acumulados elevados pueden activar agravantes como la de especial gravedad económica (≥50.000 €, o ≥250.000 € para hiperagravante).

Es común en estas tramas que un mismo autor cause múltiples perjuicios pequeños a distintas víctimas (phishing masivo); ahí podrá apreciarse un **delito continuado** de estafa (art. 74 CP) si hay unidad de plan y pluralidad de hechos, o delitos independientes si son hechos inconexos. De hecho, la STS 379/2019, rec. 853/2018, antes citada, condenó a un acusado como cooperador necesario de un delito continuado de estafa informática por una serie de extracciones fraudulentas realizadas mediante phishing bancario.

CASALS (2023) destaca que el Alto Tribunal repite que el engaño debe ser suficiente para superar la diligencia exigible a la víctima, aún estando en contextos digitales. Ello supone evitar que se impongan deberes de autotutela excesivos o desproporcionados para el usuario medio. La STS 1918/2024 muestra esta cuestión cuando se estudian las estafas que se han

llevado a cabo por las plataformas de compraventa online, destacándose que la diligencia exigible no se puede transformar en una carga desmesurada sobre el consumidor, sobre todo en la confianza en el funcionamiento seguro que estas plataformas proyectan por su apariencia de legitimidad. Esta jurisprudencia muestra una evolución importante ya que el estándar de diligencia ya no se establece solo por referencia a una persona abstracta. En este sentido, dicha diligencia debe contextualizarse atendiendo a las prácticas y percepciones propias de los entornos digitales, por lo que la sofisticación de los ataques dificulta que usuarios prudentes puedan considerarlos como fraudulentos.

El tipo objetivo incluye la relación que existe entre la manipulación informática y la producción de la transferencia sin mediar consentimiento. La operación patrimonial conforma un elemento central que consuma la estafa informática, por lo que la obtención de credenciales sin que se lleve a cabo la transferencia efectiva provocaría que el delito se cometiera en grado de tentativa (CASALS, 2023). La jurisprudencia requiere que entre la intervención fraudulenta del autor en el sistema y el perjuicio patrimonial de la víctima haya un nexo causal, siendo especialmente complejo en los fraudes que exigen múltiples intervinientes, muleros o transferencias entre distintas cuentas bancarias.

4.3.2. Elemento subjetivo

A continuación, se hace referencia al **elemento subjetivo**. El ánimo de lucro es consustancial al delito de estafa, incluida la informática. El autor debe perseguir un beneficio económico indebido, propio o de un tercero, y obrar con dolo en cuanto al engaño o manipulación y al resultado dañoso para la víctima. En los casos analizados, no suele haber duda sobre este aspecto, pues las conductas hablan por sí mismas de un fin de lucro: obtención de dinero ajeno. El lucro puede revestir formas modernas, por ejemplo, convertir los fondos sustraídos en criptomonedas para dificultar su rastreo, o usar los datos obtenidos para hacer compras por Internet a cargo de la tarjeta de la víctima. En todos esos casos subsiste la intención de enriquecimiento ilícito.

De este modo, el delito exige que concurra el dolo, en cualquiera de sus formas, y un ánimo de lucro que lleve a cabo el autor para obtener una ventaja patrimonial ilegítima. Este ánimo de lucro no exige obligatoriamente un beneficio definitivo para el autor, siendo suficiente que se obtenga un provecho económico, propio o ajeno, a partir de la operación fraudulenta (CASALS, 2023). Esta concepción amplia el ánimo de lucro lo que permite recoger las

conductas donde la autoría se distribuye entre sujetos como muleros y captadores que no disfrutan directamente del resultado económica, aunque contribuyen a que la operación defraudatoria se termine por producir.

Cabe señalar que, tratándose de delitos cometidos muchas veces mediante herramientas automatizadas o a distancia, no es infrecuente que se plantee la participación de personas que alegan ignorancia del plan (por ejemplo, la "mula" que afirma que le pidieron prestar su cuenta sin decirle que era dinero de phishing). La distinción entre dolo eventual y culpa grave puede ser sutil aquí. La jurisprudencia, al abordar la posible imprudencia en este contexto, ha considerado que, si la persona se presta a transferir dinero de origen desconocido o a permitir el uso de sus dispositivos, asumiendo el riesgo de que sea ilícito, cabría inferir dolo eventual de colaborar en el delito principal o al menos una grave negligencia que daría lugar a su punición por blanqueo imprudente (ÁVILA, 2024). En todo caso, se exige que los partícipes tengan, cuanto menos, conocimiento de las circunstancias esenciales del fraude y la voluntad de contribuir a él para ser penados como cómplices o cooperadores (STS 342/2018, de 11 de julio de 2018, por ejemplo, analizó la necesidad de probar el dolo en un acusado que actuó como receptor de fondos ilícitos, concluyendo que los indicios – una cantidad inusual, las instrucciones recibidas – permitían inferir su conocimiento del origen espúreo).

Desde un punto de vista crítico, existen importantes zonas de incertidumbre en el ámbito digital entre la estafa clásica y la estafa informática. Se da un ámbito paradigmático cuando la víctima transfiere el dinero a un falso vendedor en una app de compraventa de manera voluntaria, sin que el sistema informático se manipule. Por lo tanto, la operación se encuadra en la estafa clásica del art. 248.1 CP y no en la estafa informática del art. 249.1 a) CP, ya que el mero uso de un medio digital no transforma automáticamente la naturaleza jurídica del delito (CASALS, 2023). Esta diferenciación es fundamental para evitar que el tipo de estafa informática se interprete de forma expansiva, vulnerando con ello el principio de legalidad y desdibujando las diferentes estructuras que ambas figuras delictivas presentan.

Tabla 3. Elementos objetivo y subjetivos de los delitos de phishing, smishing, vishing y demás

Elemento	Contenido jurídico-dogmático	Ejemplos y jurisprudencia aplicable	Notas críticas / implicaciones
Tipo objetivo: manipulación informática o	El núcleo consiste en emplear medios tecnológicos fraudulentos para provocar una transferencia patrimonial no	Techniques como *phishing*, *smishing*, *vishing*, *pharming*, malware, keyloggers,	Se flexibiliza el concepto de engaño y se desplaza el centro del tipo hacia el funcionamiento del

artificio semejante	consentida. El engaño tradicional no es imprescindible: puede dirigirse a un sistema, ser indirecto o combinarse con ingeniería social. La ley sustituye el requisito de engaño personal por la manipulación informática (art. 249.1.a CP).	manipulación de DNS. STS 379/2019 (23 julio) establece que el engaño interpersonal inicial se integra dentro del artificio informático global pero no constituye el acto directo de disposición.	sistema. El error de la víctima deja de ser imprescindible, lo que desmarca el tipo respecto de la estafa clásica.
Diferencia entre engaño previo y manipulación técnica	En la estafa clásica: es necesario engaño bastante, error esencial y acto de disposición voluntario de la víctima. En la estafa informática: el autor puede engañar a un sistema o usar la identidad de la víctima para desplazar el patrimonio que ejecuta el propio sistema informático.	Engaño no personal: pharming, ataques al servidor, manipulación de APIs bancarias. Engaño personal secundario: phishing o vishing donde la víctima cree comunicarse con el banco. STS 379/2019 reafirma la sustitución del engaño personal por manipulación técnica.	El dolo recae sobre el sistema, no necesariamente sobre la víctima. Dogmáticamente, se desplaza la ejecución del acto de disposición desde la víctima hacia el sistema automatizado.
Acto de disposición patrimonial no consentido	La transferencia es generada por un sistema automatizado que opera suplantando la identidad del titular o utilizando datos falsificados. No es necesario que la víctima actúe ni que su voluntad intervenga.	SAN Madrid 32/2025 (8 octubre) afirma que introducir datos falsos en banca electrónica para causar un cargo no autorizado constituye manipulación informática típica.	Se cumple el desplazamiento patrimonial incluso sin participación activa de la víctima. La doctrina indica que este modelo de disposición rompe con la concepción clásica del acto dispositivo.
Error de la víctima	Pierde centralidad: el tipo se consuma incluso sin error personal, pues la manipulación del sistema produce el perjuicio. El error puede existir (p. ej. acceder a web falsa) pero no se exige como elemento del tipo.	Casos de phishing donde la víctima cree interactuar con su banco, pero la transferencia la efectúa el autor mediante las claves obtenidas.	El error ya no estructura el tipo: esto amplía la tipicidad y evita impunidad cuando el daño se produce exclusivamente mediante automatismos del sistema.
Perjuicio patrimonial	Requiere un detrimento económico real. Lo padece, en principio, el titular de la cuenta; aunque contractualmente pueda terminar asumiéndolo el banco, ello no afecta a la consumación. La cuantía es relevante para la calificación básica, leve o agravada (arts. 249.2 y 250 CP).	Microcargos fraudulentos: delito leve. Vaciados de cuenta: puede activar especiales agravantes (>50.000 € o >250.000 €). STS 379/2019 condena un delito continuado por múltiples transferencias fraudulentes.	Puede existir concurso medial con blanqueo cuando el destino es dispersar fondos. El perjuicio inicial, no el asumido después por el banco, es el que determina la consumación.
Nexo causal entre manipulación y perjuicio	Debe darse una relación directa entre la intervención informática y la transferencia ilícita. Si solo se obtienen credenciales, sin movimiento patrimonial, hay tentativa.	CASALS (2023) destaca la complejidad cuando intervienen muleros o cadenas de transferencias sucesivas.	Determinar el nexo causal es difícil en redes criminales organizadas, lo que afecta a la imputación objetiva y a la delimitación de la cooperación necesaria.
Elemento subjetivo: dolo	El autor conoce que manipula el sistema o utiliza artificios fraudulentos y quiere provocar	STS 342/2018 admite inferir dolo por indicios cuando una persona	La sofisticación técnica dificulta acreditar el dolo, sobre todo en partícipes

	una transferencia ilícita. Basta el dolo directo o eventual, sin necesidad de que el autor ejecute personalmente todas las fases del ataque.	recibe fondos ilícitos en su cuenta y actúa según instrucciones sospechosas.	secundarios (muleros). Importancia del dolo eventual y del conocimiento de riesgos.
Ánimo de lucro	Es consustancial a la estafa: el autor debe buscar un beneficio patrimonial ilícito, propio o de un tercero. No se exige riqueza definitiva: basta un provecho económico momentáneo o indirecto.	CASALS (2023) señala que el ánimo de lucro abarca operaciones como convertir fondos en criptomonedas o efectuar compras online con datos robados.	El ánimo de lucro permite integrar en el tipo a actores no enriquecidos directamente (muleros, captadores), siempre que cooperen con conocimiento de la operación ilícita.
Problemas de delimitación con la estafa clásica	Cuando la víctima transfiere voluntariamente fondos engañada por un falso vendedor, sin manipulación informática, estamos ante art. 248.1 CP, no ante estafa informática. El medio digital no convierte automáticamente el hecho en "informático".	Casals (2023) subraya que el uso de apps de compraventa no implica per se el art. 249.1.a CP.	Diferenciación necesaria para evitar interpretaciones expansivas que vulneren el principio de legalidad.

Fuente: elaboración propia

4.4. Iter criminis y consumación

El iter criminis de la estafa informática presenta características propias derivadas de la naturaleza tecnológica del delito. La fase preparatoria consiste en obtener las credenciales o datos sensibles de manera fraudulenta a partir de técnicas de ingeniería social, como phishing, *smishing* o diferentes instrumentos tecnológicos como *malware* o troyanos que se crean con el fin de obtener información. Estos actos preparatorios incluyen el registro de dominios falsos, el diseño de interfaces que imitan plataformas legítimas o manipulan los protocolos de comunicación como el *spoofing*. En esta etapa, aprovechando los sesgos cognitivos y la confianza en bancos o plataformas digitales, los autores buscan vulnerabilidades humanas y técnicas.

La estafa informática es un delito de resultado, que se consuma en el momento en que se produce la transferencia patrimonial no consentida en perjuicio de la víctima. Hasta antes de la consumación, pueden desplegarse múltiples actos preparatorios: envío de correos masivos, creación de páginas web fraudulentas, obtención de malware, etc. Algunos de esos actos preparatorios podrían, en determinados supuestos, constituir delitos autónomos (por

ejemplo, la mera fabricación o tenencia de programas diseñados para cometer estafas puede castigarse si se enmarca en preparaciones para falsificar medios de pago, según la misma LO 14/2022 que añadió el art. 248 ter CP). Sin embargo, la mayoría de actuaciones previas quedan impunes hasta que se concreta al menos una tentativa.

La tentativa de estafa informática es posible y, de hecho, frecuente: por ejemplo, cuando el phishing es detectado a tiempo por el usuario o por el banco y la transferencia fraudulenta no llega a ejecutarse. Si el autor ya realizó actos idóneos (envió el engaño, obtuvo datos, incluso ordenó la transferencia) pero esta no se hizo efectiva por causas ajenas a su voluntad, estaríamos ante una tentativa punible (art. 16 CP). La jurisprudencia ha confirmado tentativas acabadas en fraudes informáticos frustrados, aplicando la pena reducida en uno o dos grados. También puede ocurrir la tentativa *inidónea* (delito imposible), por ejemplo, si el phishing se envió, pero nadie cayó en la trampa; en tal caso podría apreciarse ausencia de ejecución típica por falta de víctima concreta, salvo que se encuadre como conspiración o proposición para delinquir, figuras de aplicación muy limitada en este ámbito.

Un punto debatido doctrinalmente es si la simple obtención ilegítima de datos personales o bancarios de otra persona (p. ej., robar contraseñas mediante phishing) constituye por sí misma un delito consumado distinto, o se trata solo de un acto de preparación de la estafa. En España, no existe un delito específico de "phishing" entendido como captación de datos; ese comportamiento se sanciona cuando menos como un delito intentado de estafa (si se prueba que era para defraudar), o eventualmente, podría encajar en el delito de descubrimiento y revelación de secretos (art. 197 CP) si implica acceder a datos reservados vulnerando seguridad. Sin embargo, la doctrina mayoritaria y la jurisprudencia suelen considerar que el phishing es medio comisivo de la estafa, no un delito contra la intimidad o la privacidad (MESTRE, 2024; MIRÓ LLINARES, 2012). Por tanto, la obtención de credenciales es parte del iter criminis del fraude patrimonial. Solo se sancionaría separadamente si, por ejemplo, se difundieran esos datos a terceros (lo que podría ser un delito de tráfico de datos ilícitos, art. 197 ter CP).

Cuando el autor accede al sistema bancario o de pagos y ordena realizar las transferencias desde la cuenta de la víctima hacia la suya propia o hacia cuentas de terceros (muleros reclutados a partir de ofertas de empleo falsas), la fase ejecutiva se activa. Esta etapa se caracteriza por la rapidez, la automatización parcial y la búsqueda de mecanismos para que

los sistemas de seguridad se desactiven o anulen, incluyendo la doble autenticación o las alertas de actividad inusual.

Por lo tanto, cuando se lleva a cabo la transferencia patrimonial no consentida es cuando se consuma el delito. Si se compara con la estafa clásica, donde el acto de disposición realizado por la víctima implica su consumación, en la estafa informática es suficiente con que el sistema realice la operación fraudulenta, incluso aunque la víctima no sea consciente de ello hasta después. La lógica del medio tecnológico empleado fundamenta la diferencia dogmática.

Las posibilidades de tentativa son extensas. Puede pensarse, por ejemplo, cuando la víctima recibe un correo de *phishing*, pero no lo llega a abrir e incluso introduce los datos parcialmente, aunque el sistema detecta la anomalía. También puede pensarse cuando se bloquea la transferencia fraudulenta por los sistemas antifraude de la entidad financiera previamente a su ejecución. Esta última tipología es importante puesto que las entidades han fortalecido sus mecanismos de detección de patrones sospechosos. La rapidez de los ataques obliga a que las víctimas comuniquen de inmediato cualquier fallo del sistema o incidencia. En este sentido, el Real Decreto-ley 19/2018 exige que el usuario informe sin retraso injustificado de las operaciones no autorizadas para que el derecho se resarza (ACÓN, 2024). La inmediatez es fundamental puesto que las posibilidades temporales para revertir las transferencias suelen ser muy reducidas.

4.5. Concursos de delitos

Ligado a lo anterior, suele plantearse la posibilidad de concurso de delitos entre la estafa informática y otras infracciones penales. Las estafas pueden concurrir con otros delitos consecuencia de la complejidad técnica de su ejecución y los múltiples de comportamientos que se recogen en un solo ataque. Es habitual cuando para llevar a cabo la estafa se altera, deteriora o inutiliza un sistema informático, incide sobre la integridad o disponibilidad, lo que conlleva que se dé concurso con delitos de daños informáticos.

Por lo tanto, si el método empleado implica vulnerar la seguridad de un sistema informático (hackeo) para luego defraudar, podríamos pensar en concurso con el delito de daños informáticos (art. 264 CP) o de acceso ilícito a sistemas (art. 197 bis CP). Igualmente, se puede dar concurso con el delito de acceso ilícito a sistemas cuando el autor realiza los actos sin

autorización en cuentas o plataformas digitales, así como la falsedad informática que genera un resultado fraudulento.

No obstante, los tribunales tienden a apreciar unidad de acción delictiva: si el acceso o manipulación al sistema es el medio necesario para la estafa, queda absorbido en esta (principio de consunción), salvo que se causen daños informáticos independientes del ánimo de lucro. En concreto, la **SAP Madrid 74/2022, 28 de Febrero de 2022, rec. 35/2021** sostuvo que la introducción de un malware en un sistema bancario para realizar fraudes no debía sancionarse además como daños informáticos, ya que esa manipulación constituía el núcleo del engaño computacional propio de la estafa (considerando que no hubo un daño al sistema más allá de la transferencia patrimonial).

La empresa Unísono denunció que BBVA permitió una transferencia de 303.234,44 euros a una cuenta en Hong Kong, ordenada por una empleada administrativa (no autorizada) que fue engañada por un correo electrónico falso, supuestamente procedente de la presidenta de la compañía. Dicha orden se cursó por un procedimiento inusual y sin que se lleven a cabo las comprobaciones habituales, quebrando el protocolo de seguridad acordado entre la empresa y el banco.

El Juzgado de Primera Instancia nº 33 de Madrid había desestimado la demanda, considerando que BBVA actuó diligentemente y que el fraude fue consecuencia de la actuación interna de la empresa. Sin embargo, la Audiencia Provincial revoca la sentencia, declarando que el banco incumplió su deber de diligencia y seguridad, ya que aceptó una orden de pago de una persona no apoderada, con firma falsificada y sin verificar su autenticidad, pese a que existían claras señales de irregularidad (transferencia a un país con riesgo fiscal y método de comunicación inusual).

El tribunal recuerda que, conforme a la Ley 16/2009 de Servicios de Pago, la responsabilidad del banco en estos casos es cuasi objetiva, y solo queda exento si demuestra fraude o negligencia grave del cliente. En este caso, BBVA no probó la implementación de medidas adecuadas de seguridad ni verificaciones efectivas, por lo que debe asumir las consecuencias del fallo.

Otro concurso posible es con el **delito de usurpación de estado civil** (identidad) del art. 401 CP, dado que en muchos phishing se suplanta la identidad digital del usuario frente al banco.

Sin embargo, la doctrina penal y jurisprudencia mayoritaria no consideran aplicable el delito de usurpación del estado civil en estos casos, por entender que la identidad fingida es solo un medio para defraudar, absorbido igualmente por la estafa (MESTRE, 2024). Solo se castiga separadamente la usurpación de identidad cuando se produce en contextos distintos al patrimonial (por ejemplo, para eludir una responsabilidad penal, para efectuar actos jurídicos no económicos, etc.). En materia patrimonial, la suplantación con fin de lucro queda subsumida en la figura específica de fraude informático.

En síntesis, la construcción dogmática de la estafa informática en España ha seguido un **modelo unitario**: cualquier conducta que con ánimo de lucro cause un desplazamiento patrimonial no consentido mediante manipulación de sistemas o artificios tecnológicos es una estafa (informática) y absorbe los engaños, falsedades o accesos ilícitos instrumentales, salvo que concurran lesiones a bienes jurídicos autónomos de entidad suficiente (como daños informáticos graves que excedan lo necesario para defraudar, lo cual en la práctica es raro).

4.6. Criterios jurisprudenciales relevantes

La jurisprudencia nacional ha ido afinando los contornos de la estafa informática con resoluciones de altos tribunales. Por su importancia, destacan los siguientes criterios emanados de sentencias:

Phishing como estafa informática típica: El Tribunal Supremo confirmó desde temprano que el phishing y fraudes análogos encajan perfectamente en el tipo del art. 248.2 a) CP (hoy 249.1.a). La **STS 364/2011, de 11 de mayo de 2011** (Sala 2ª) señaló que incluso el uso de un «*artificio semejante*» a la informática basta, reconociendo la plasticidad del tipo para cubrir engaños tecnológicos varios. Más adelante, la ya citada STS 379/2019, de 23 de julio de 2019, rec. 853/2018, consolidó esta doctrina, explicando que en el phishing concurren todos los elementos de la estafa informática: ánimo de lucro, manipulación del sistema bancario mediante introducción de datos falsos, transferencia no consentida en perjuicio ajeno. Esta sentencia (núm. 379/2019) es especialmente referencial por describir cómo el engaño a la persona se integra en la manipulación informática del tipo penal.

Equiparación de métodos: La jurisprudencia ha interpretado de forma expansiva qué constituye *manipulación informática o artificio semejante*. Se han equiparado a esta no solo las actuaciones sobre sistemas computacionales puros, sino incluso *maniobras mecánicas o*

comunicaciones de datos falsas. Por ejemplo, la **STS 747/2007, de 9 de mayo de 2007** calificó como estafa informática la obtención fraudulenta de recargas de móvil mediante introducción de códigos engañosos en un cajero (un caso híbrido técnico-humano). En línea con ello, la **SAP Asturias (Secc. 2ª) 14/04/2023** –mencionada antes– afirmó que identificarse falsamente ante un sistema, introduciendo datos no veraces para lograr un beneficio, es una manipulación informática relevante a efectos del tipo. Asimismo, la **STS 147/2005, de 17 de marzo de 2005**, **rec. 122/2004**, resolviendo cuestiones competenciales, también asumió la validez de considerar estafa informática cualquier fraude cometido «por medios informáticos, telemáticos o similares» (esta resolución sentó bases para la ubicación competencial, pero de paso confirmó la amplitud del concepto).

Por lo que respecta al análisis del perjuicio en fraudes continuados, en las estafas informáticas masivas, los tribunales han debido decidir si sumar los perjuicios de múltiples afectados o tratarlos por separado. En general, si existe un plan único (p. ej. una campaña de phishing dirigida contra muchos), se aplica el delito continuado computando el total defraudado. No obstante, para la agravante de cuantía, la jurisprudencia ha indicado que debe atenderse al perjuicio individual de cada víctima cuando son claramente independientes (STS 229/2016, de 16 de marzo). Esto tiene efectos punitivos: un ciberestafador que robe 1.000 € a 100 personas podría ser acusado de un continuado con perjuicio total 100.000 € (agravado), pero algunos tribunales prefieren verlo como 100 delitos básicos sin agravante, para no exagerar la punición. La doctrina se inclina por la primera opción si hay unidad de procedimiento delictivo (MOLINA, 2020), pero el tema no está totalmente unificado.

En cuanto a la tentativa y desistimiento, un asunto interesante se dio en la **STS 210/2012, de 22 de marzo de 2012**, donde se discutió si un acusado de phishing que devolvió parte del dinero podía alegar desistimiento voluntario. El Supremo negó tal desistimiento por considerar que la devolución ocurrió por presión policial y que el dolo ya se había consumado con la transferencia, subrayando que en los delitos de resultado patrimonial el arrepentimiento *post delictum* no elimina la consumación, aunque pueda influir en la responsabilidad civil y la atenuante de reparación.

En resumen, los tribunales españoles, encabezados por el Tribunal Supremo, han proporcionado un marco jurisprudencial sólido y consistente que confirma la plena aplicabilidad del delito de estafa (art. 249.1.a CP) a las defraudaciones informáticas como

phishing, smishing, vishing y pharming. Se enfatiza que la ley penal abarca tanto el engaño informático como el tradicional, protegiendo el patrimonio frente a estos ataques de nueva generación. Esta jurisprudencia convergente ha dado seguridad jurídica en la tipificación, si bien subsisten desafíos prácticos en la persecución efectiva de estos delitos, como se analizan a continuación.

5. Perspectiva práctica: aplicación de la ley y jurisprudencia destacada

Desde la perspectiva práctica, el combate a las estafas informáticas en España presenta retos particulares en cuanto a la **investigación, enjuiciamiento y sanción** de los responsables. En el segundo anexo, en este sentido, se muestra la guía práctica de actuación frente a la estafa informática. En este apartado se abordan algunas cuestiones pragmáticas y se destacan casos jurisprudenciales ilustrativos que muestran la aplicación del marco legal descrito.

5.1. Dificultades en la investigación y persecución

La naturaleza global y técnicamente compleja del phishing y fraudes afines dificulta su persecución. En muchos casos, los autores intelectuales operan desde el extranjero o a través de identidades encubiertas, aprovechando el anonimato relativo de Internet. Las fuerzas de seguridad españolas (como la Unidad de Delitos Telemáticos de la Guardia Civil o la Brigada de Investigaciones Tecnológicas de la Policía Nacional) cuentan con especialistas, pero enfrentan la necesidad de colaboración internacional y con proveedores de servicios de Internet para rastrear a los culpables. Además, como indicaba FERNÁNDEZ ESCUDERO (2024), la falta de recursos y la lenta adaptación a las nuevas amenazas limitan la efectividad en la identificación y localización de los ciberdelincuentes. No son raros los procedimientos penales por estafa informática que acaban archivados provisionalmente por autor desconocido, sobre todo cuando la investigación lleva fuera de España (p. ej., dinero transferido a cuentas en países no cooperantes, o dirección IP de origen en redes anónimas).

Otra dificultad es el volumen de casos. El auge del ciberfraude ha congestionado juzgados con numerosas denuncias individuales de afectados por pequeñas estafas online. Como se mencionó, agrupar esas denuncias en macro-causas es complejo; pero tratarlas aisladamente puede implicar perseguir solo a las mulas locales y no a la organización completa. La reticencia

de algunos órganos a acumular hechos transprovinciales provoca enfoques fragmentados. En respuesta, el Tribunal Supremo ha abogado por criterios flexibles de competencia para que un mismo juzgado asuma casos conexos de phishing dispersos, aplicando la teoría del "foro del lugar más eficaz" basada en la investigación centralizada. Pese a ello, queda camino para mejorar la coordinación interjurisdiccional. Una propuesta en curso es fortalecer el papel de la Audiencia Nacional en grandes fraudes informáticos de alcance nacional o transnacional, dado que este tribunal ya concentra competencias en ciertos delitos económicos complejos.

CASALS (2023) destaca que la ciberdelincuencia se ve favorecida porque entre autor y víctima no existe inmediación y la conducta se encuentra despersonalizada. La investigación y la persecución efectiva se ve complicada enormemente por la facilidad para ocultar rastros digitales y la extraterritorialidad de las acciones.

Como respuesta, el Plan Estratégico contra la Cibercriminalidad de 2021 defiende la prevención, la especialización policial, el refuerzo de herramientas tecnológicas y la cooperación público-privada, aunque se debe valorar si es eficaz para reducir las estafas informáticas, que continúan creciendo (CASALS, 2024).

Se puede considerar desde el punto de vista crítico que la reacción del sistema penal es más reactiva que preventiva. Las Fuerzas y Cuerpos de Seguridad tienen una capacidad limitada para seguir el ritmo de la innovación tecnológica de los delincuentes, algo que fortalece la relevancia de la responsabilidad de los intermediarios (bancos, plataformas, proveedores de servicios digitales).

5.2. Jurisprudencia penal relevante

Además de las sentencias del Tribunal Supremo ya comentadas que fijan doctrina, a nivel de jurisprudencia menor (Audiencias Provinciales) hay resoluciones de interés que aplican estos principios a situaciones concretas:

SAP de Madrid 520/2015, 30 de junio de 2015: Confirmó la condena por estafa informática de unos acusados que manipulaban terminales puntos de venta para realizar cobros fraudulentos con tarjetas ajenas, destacando que *"es equivalente que el autor modifique materialmente el programa informático indebidamente o que lo utilice sin autorización"*, reconociendo así tanto la alteración de software como el uso ilegítimo de credenciales dentro del concepto de manipulación informática.

SAP de Lugo 331/1998, 9 de julio de 1998, rec. 52/1997: Caso temprano post-1995 donde, curiosamente, se consideró estafa informática la ya mencionada práctica de la moneda atada con hilo en máquinas expendedoras. La Audiencia entendió que esa trampa mecánica constituía un "artificio semejante a la informática" según el art. 248.2 CP. Esta interpretación extensiva (discutible doctrinalmente) mostraba el afán de aplicar la nueva figura incluso a fraudes analógicos contra máquinas. Hoy, tras reformas, probablemente esa conducta se tipificaría más propiamente como hurto con engaño, pero el caso refleja la transición conceptual de la estafa tradicional a la informática.

SAP de Asturias 477/2024, 21 de marzo de 2024, Rec. 370/2023: Ya referida, es representativa de la colaboración víctima-banco. Penalmente catalogó el smishing sufrido por la víctima como estafa informática consumada, aunque los autores materiales no fueron habidos. Civilmente, desestimó el recurso del banco (Unicaja) y confirmó que este debía restituir los 6.000 € al cliente. Esta resolución resume la tendencia jurisprudencial de considerar a los bancos *responsables civiles subsidiarios* frente a sus clientes defraudados, salvo prueba de negligencia grave de estos. Si bien este aspecto es civil, influye en la práctica penal en cuanto muchas víctimas condicionan su denuncia al desenlace de la reclamación bancaria.

SAP de Madrid 47/2023, 26 de enero de 2023, rec. 889/2022-3: resuelve el recurso de apelación interpuesto por D. Sergio contra el Banco Santander S.A. en un caso de reclamación de cantidad derivado de operaciones bancarias presuntamente fraudulentas.

El demandante solicitaba la devolución de 9.465,80 euros, correspondientes a varios cargos y disposiciones que consideraba no autorizadas, realizadas con su tarjeta bancaria en 2020 y 2021. Alegó que había sido víctima de un fraude tipo "SIM swapping" o clonado de tarjeta SIM, mediante el cual los defraudadores accedieron a sus claves y ejecutado operaciones sin su consentimiento.

El Banco Santander se opuso, acreditando que las operaciones se efectuaron mediante autenticación reforzada, concretamente a través de la aplicación Samsung Pay, en la que la tarjeta del demandante había sido registrada y tokenizada. Para dicha configuración y posteriores operaciones se requería validar códigos OTP enviados al teléfono móvil del propio cliente, demostrando, según el banco, su intervención o al menos una grave falta de diligencia.

La Audiencia Provincial, tras analizar el Real Decreto-Ley 19/2018 sobre servicios de pago, recuerda que corresponde al banco demostrar la autenticación y correcta ejecución de las operaciones, pero también al cliente actuar con diligencia y custodiar sus claves y credenciales de seguridad. Con base en la prueba disponible, el tribunal determina que el demandante no explicó cómo pudieron los defraudadores acceder a sus datos personales ni cómo se produjo la clonación de la SIM, omitiendo además medidas mínimas de seguridad, como cambiar su número de teléfono tras el primer fraude.

La Sala aprecia, por tanto, negligencia grave del demandante en la custodia de sus datos y claves bancarias, excluyendo la responsabilidad del banco según el artículo 46 del citado Real Decreto-Ley. En consecuencia, el tribunal desestima el recurso de apelación y confirma la sentencia del Juzgado de Primera Instancia e Instrucción nº 3 de Alcorcón que había rechazado la demanda.

SAP de Valencia 254/2022, 13 de junio de 2022, rec. 436/2021: En un caso de *phishing* al Ayuntamiento de Valencia (suplantación de identidad para desviar fondos municipales a cuentas de los estafadores), la Audiencia revocó la absolución inicial y condenó a varios acusados. Destacó que el error en estos casos lo sufre la administración electrónica (que procesa órdenes espurias) y no un individuo, pero que eso no impide la existencia de estafa: la administración actuó movida por un *engaño artificial* (emails falsos simulando ser proveedores cambiando la cuenta de cobro). La sentencia subrayó que el patrimonio público goza de la misma protección frente a fraudes informáticos que el privado, y aplicó la agravante de especial gravedad (eran más de 100.000 € defraudados).

En general, las Audiencias Provinciales aplican de forma homogénea la figura de estafa informática, sin grandes disensiones en cuanto a su tipicidad. Las discrepancias afloran más en lo referente a la responsabilidad civil de terceros (bancos, compañías telefónicas) y en la apreciación de la negligencia de la víctima. Por ejemplo, algunas sentencias han denegado indemnización a la víctima si estiman que actuó con gravísima imprudencia (p. ej., entregando múltiples códigos de seguridad pese a advertencias), lo cual penalmente no exoneraría al estafador, pero civilmente puede romper el nexo de responsabilidad del banco.

Desde el punto de vista de la sanción penal, las condenas por estafa informática suelen conllevar penas de prisión en el marco de 1 a 3 años (delito básico) o superiores si hay agravantes. En muchos casos, al haber continuidad delictiva, las penas se agrupan. Asimismo,

se imponen multas y la obligación de indemnizar a las víctimas por las pérdidas no cubiertas por otras vías. Un problema práctico es la ejecutabilidad de esas penas: no pocos condenados son extranjeros no localizados (juzgados en rebeldía) o insolventes, lo que limita el efecto retributivo y resocializador. En contraste, las entidades bancarias, aunque no son penalmente responsables (pues actúan como víctimas colaterales o terceros), terminan asumiendo el costo económico en bastantes ocasiones, dada la normativa pro-consumidor ya comentada.

La jurisprudencia enfatiza el requisito del engaño suficiente y la necesidad de que la víctima aprecie un nivel razonable de diligencia para proteger su patrimonio, sin que la imprudencia leve se convierte en causa de impunidad para el autor. Se puede indicar que existe cierta tensión entre las exigencias de diligencia y la realidad de los ataques de ingeniería social, que se basan concretamente en analizar los sesgos cognitivos y elementos de confianza institucional. En este sentido, la SAP de Asturias 477/2024 contempla la manipulación del ID de los SMS y la dificultad objetiva existente para detectar el fraude.

5.3. Propuestas jurídicas y perspectivas de futuro

Tras analizar la situación normativa y jurisprudencial hasta 2024, es evidente que España cuenta con un marco legal sólido para enfrentar las estafas informáticas. Sin embargo, la rápida evolución de la ciberdelincuencia plantea la necesidad de continuas refinaciones legales y mejoras operativas. A continuación, se presentan propuestas y reflexiones desde la doctrina penal y la práctica judicial para fortalecer la respuesta jurídica al phishing, smishing, vishing, pharming y modalidades afines:

1. Perfeccionamiento legislativo continuo: La reciente reforma de la LO 14/2022 actualizó adecuadamente la definición de estafa informática (art. 249.1.a CP) y tipificó conductas preparatorias como el tráfico de herramientas para fraudes (art. 248 ter CP). No obstante, el legislador debe permanecer vigilante ante nuevas tácticas delincuenciales. Por ejemplo, podría evaluarse la tipificación expresa de la suplantación de identidad digital con finalidad fraudulenta, aunque sea como subtipo agravado de estafa, para recalcar la reprochabilidad de quienes utilizan identidades ajenas en entornos online. Algunos autores han sugerido crear un tipo penal específico de *phishing* que sancione la mera creación y envío masivo de comunicaciones engañosas, incluso sin perjuicio consumado (REY HUÍDOBRO, 2013); sin embargo, esta propuesta choca con el principio de lesión (castigar conatos muy preliminares)

y con problemas de prueba (diferenciar spam malicioso de publicidad engañosa). La tendencia más acorde al garantismo penal es mantener estas conductas dentro de la estafa, requiriendo al menos una tentativa de perjuicio para intervenir penalmente.

Donde sí podría haber espacio de mejora es en las agravantes cualificadas. En este sentido, el legislador podría considerar agravaciones específicas cuando la estafa informática se cometa aprovechando entornos de especial confianza (por ejemplo, suplantar organismos oficiales, lo cual genera alarma social) o cuando se cause un daño especialmente intenso en sujetos vulnerables (ancianos víctimas de vishing telefónico, etc.). Actualmente, esas circunstancias se valoran caso a caso, pero podrían tipificarse para guiar al juez en la elevación de pena en supuestos particularmente odiosos.

2. Especialización de la persecución penal: En línea con lo apuntado por FERNÁNDEZ ESCUDERO (2024), es crucial fortalecer las capacidades técnicas y organizativas de los operadores jurídicos frente al ciberfraude. Esto incluye dotar de más recursos a las unidades policiales especializadas (UIT, BIT) para investigar eficazmente las tramas de phishing, dotar de formación continua a jueces, fiscales y peritos en materia de evidencia digital, e incluso estudiar la creación de juzgados o secciones especializadas en delincuencia informática en aquellas jurisdicciones con mayor volumen (al estilo de los juzgados de violencia informática o secciones económicas especializadas). La especialización permitiría un tratamiento más ágil y uniforme de las causas, evitando dilaciones indebidas en peritajes informáticos y mejorando la cooperación internacional mediante contactos fluidos con agencias extranjeras (EUROPOL, Interpol, etc.).

Dentro de esta especialización, un punto crítico es mejorar los mecanismos de unificación de causas vinculadas. Se podría articular protocolos para que, detectada una campaña de phishing con múltiples víctimas en distintas provincias, la Fiscalía General del Estado coordine la acumulación de los procedimientos bajo una sola investigación central (posiblemente en la Audiencia Nacional si hay afectación amplia). Esto evitaría la impunidad de cabecillas que se benefician de la fragmentación procesal. El desarrollo de sistemas informáticos judiciales interconectados ayudaría a identificar patrones comunes en denuncias por fraudes online, facilitando su agregación.

3. Colaboración público-privada y diligencia de los operadores**:** Las entidades bancarias y las empresas de telecomunicaciones tienen un rol clave en la lucha contra las ciberestafas.

Jurídicamente, se podría impulsar (por vía de *soft law* o incluso obligaciones legales) una mayor colaboración de los proveedores con las autoridades: por ejemplo, que los bancos notifiquen proactivamente al Ministerio Fiscal los casos significativos de phishing que detecten afectando a sus clientes, aportando datos de transacciones sospechosas, IPs origen, etc., para coadyuvar a la persecución penal. Asimismo, se puede requerir a las plataformas de correo electrónico, redes sociales y operadores móviles a que implementen filtros y medidas antifraude (muchas ya lo hacen voluntariamente, pero podría estandarizarse). De le*ge ferenda*, podría contemplarse en la Ley de Servicios Digitales la responsabilidad de los intermediarios que, con conocimiento efectivo de campañas de phishing en sus sistemas, no actúen con diligencia para detenerlas.

En este aspecto, hay que equilibrar la prevención con la privacidad y la libertad de empresa; no se sugiere vigilar masivamente comunicaciones, sino reaccionar ante alertas concretas. La banca española ya participa en iniciativas conjuntas con las fuerzas de seguridad (por ejemplo, grupos de trabajo con INCIBE, OSI, etc.), pero formalizar más esa cooperación mediante convenios o protocolos vinculantes podría mejorar la rapidez de respuesta. Esto conecta con la idea de «*Know Your Customer»* y autenticación reforzada: la normativa (PSD2) ya obliga a doble factor de autenticación, pero siempre hay vectores de engaño. Quizás establecer por ley la notificación inmediata al cliente y a las autoridades cuando se detecte una brecha de seguridad (p.ej., si un banco nota accesos irregulares en varias cuentas) permitiría frenar antes las extracciones fraudulentas.

4. Educación y prevención como complemento esencial: Múltiples voces (FERNÁNDEZ ESCUDERO, 2024; MESTRE, 2024) enfatizan que la prevención mediante educación y concienciación de los usuarios es crucial. Aunque esto trasciende el Derecho Penal, tiene un innegable impacto en su eficacia: un público más alerta y formado caerá menos en las trampas, reduciendo la comisión del delito en origen. Por ello, desde las instituciones se han intensificado campañas informativas sobre cómo identificar mensajes de phishing, no proporcionar datos sensibles por vías no seguras, verificar las URL de los sitios bancarios, etc. Esta labor preventiva debería consolidarse con programas continuos en colegios, empresas y medios de comunicación. En paralelo, los propios bancos han incrementado medidas de seguridad en sus operaciones (tarjetas con sistemas 3D-Secure, avisos *push* en la app móvil para confirmar operaciones, limitaciones geográficas de movimientos, etc.).

Una propuesta interesante es promover legalmente la responsabilidad compartida: ya el RDL 19/2018 impone al cliente el deber de diligencia en custodiar sus credenciales y notificar incidentes sin demora. Quizás, en futuras reformas, se podría incentivar aún más las buenas prácticas del usuario, por ejemplo, modulando la responsabilidad civil del banco según si el cliente había seguido o no ciertas recomendaciones de seguridad (aunque esto es delicado, pues podría interpretarse como cargar la culpa en la víctima; debe hallarse equilibrio). En cualquier caso, los consumidores informados son la primera línea de defensa ante el phishing: la legislación de consumo podría requerir que los contratos bancarios incluyan *cláusulas pedagógicas* claras sobre cómo opera el banco en comunicaciones (por ejemplo, que nunca pedirá contraseñas por email), lo que dotaría al cliente de argumentos para desconfiar de cualquier mensaje al margen de esas pautas.

5. Refuerzo de la cooperación internacional y la jurisdicción extraterritorial: Dado el carácter transnacional de muchas ciberestafas, es fundamental seguir mejorando la cooperación judicial internacional. España es parte del Convenio de Budapest (2001) y de redes como 24/7 de contacto contra delitos informáticos. No obstante, se pueden firmar más acuerdos bilaterales con países donde operan bandas de fraude online (ej. algunos países de Europa del Este, África o Asia) para agilizar extradiciones y asistencias (MESTRE, 2024, sugiere avanzar en diplomacia penal tecnológica). También sería útil potenciar el uso de equipos conjuntos de investigación (ECI) en casos de estafas masivas que afecten varios estados de la UE, con apoyo de Eurojust y Europol.

En cuanto a la jurisdicción, la LO 14/2022 ya amplió criterios para perseguir ciertos delitos informáticos cometidos fuera de España contra españoles. Conviene garantizar que la ley procesal permita, por ejemplo, juzgar en ausencia a defraudadores no entregados, o embargar bienes de origen ilícito localizados en España, aunque el autor no esté presente. Igualmente, se podría establecer en la Ley de Enjuiciamiento Criminal procedimientos más expeditos para la congelación y decomiso de activos digitales (criptomonedas) vinculados a fraudes informáticos, pues los delincuentes a veces canalizan lo robado a monederos electrónicos difíciles de incautar. La tipificación del autoblanqueo (art. 301.1 CP tras reforma 2010) ya permite castigar al propio estafador por lavar sus ganancias, lo que es relevante en phishing sofisticados; esto debe aplicarse con firmeza para privar al delincuente de las utilidades del crimen.

6. Jurisprudencia unificada y guía doctrinal: Aunque la jurisprudencia es bastante uniforme, siempre existe riesgo de interpretaciones dispares en niveles inferiores. Sería conveniente que el Tribunal Supremo siga teniendo ocasión de pronunciarse en nuevos supuestos para sentar criterios. Por ejemplo, sería útil una sentencia del Supremo que esclarezca la delimitación entre estafa informática y otros delitos en casos fronterizos (¿es estafa informática o falsedad informática manipular un certificado digital para obtener ventaja económica? etc.). También, dadas las recientes figuras introducidas (como el fraude con tarjetas de pago del art. 249 bis CP), se requerirá guía sobre el concurso entre ese delito específico y la estafa informática general cuando ambos pudieran concurrir. La doctrina académica, por su parte, debe continuar examinando críticamente la eficacia de las normas; ya hay estudios monográficos (p.ej. REY HUÍDOBRO, 2013; ROBLES, 2021) que podrían ser considerados en reformas de política criminal.

7. Perspectiva de los derechos de las víctimas: Finalmente, una propuesta de mejora incluye robustecer el apoyo a las víctimas de ciberestafa en el proceso penal. Muchas veces son ciudadanos poco familiarizados con la tecnología que además de perder dinero sufren la angustia de navegar un procedimiento judicial técnico. Se podría instaurar en las Oficinas de Atención a la Víctima protocolos para asesorar a afectados por fraudes informáticos, orientándoles sobre los pasos a seguir (denuncia penal, reclamación bancaria, medidas para proteger sus datos a futuro). Asimismo, valorar la creación de fiscales delegados en delitos informáticos en todas las Fiscalías provinciales, que centralicen estos casos y sirvan de punto de contacto para las víctimas, asegurando un tratamiento especializado y más cercano.

En conclusión, si bien el Código Penal español ofrece herramientas suficientes para tipificar y sancionar el phishing, smishing, vishing, pharming y demás fraudes informáticos, el carácter dinámico de estos fenómenos exige una evolución constante tanto de la normativa como de su aplicación práctica. La coordinación entre el ámbito penal, el civil y las estrategias preventivas es esencial para minimizar el impacto de estas conductas. A medida que la sociedad profundiza en la era digital, el Derecho Penal Económico deberá seguir adaptándose para garantizar que la confianza en los sistemas informáticos –pilar del comercio y la banca modernos– no se vea socavada por la impunidad de los estafadores. Los esfuerzos combinados de legisladores, jueces, fuerzas de seguridad, entidades privadas y ciudadanos

informados serán la clave para enfrentar eficazmente el desafío del ciberfraude en los años venideros.

6. Conclusiones

El fenómeno de las estafas informáticas –representado emblemáticamente por modalidades como phishing, smishing, vishing y pharming– constituye uno de los retos más apremiantes para el Derecho Penal Económico en la actualidad. A lo largo de este trabajo se han examinado sus características, el tratamiento legal vigente en España y las respuestas doctrinales y jurisprudenciales desarrolladas hasta 2024, arribando a las siguientes conclusiones principales:

España ha reaccionado temprana y continuamente a la aparición de los fraudes informáticos. Desde 1995 incorporó la estafa informática en su Código Penal, y mediante sucesivas reformas –particularmente la de 2022– ha afinado la descripción típica para abarcar las nuevas formas de engaño tecnológico. El art. 249.1.a) CP vigente, tras la reforma de la Ley Orgánica 14/2022, ofrece una cobertura amplia para perseguir transferencias patrimoniales ilícitas obtenidas mediante manipulación de sistemas o artificios informáticos, demostrando ser suficientemente flexible para subsumir las distintas variantes de ciberestafa. No se aprecia, por tanto, laguna de tipicidad en cuanto a la incriminación básica de estas conductas. Su redacción amplia y tecnológicamente neutra permite encuadrar bajo un mismo tipo conductas tanto técnicas como basadas en ingeniería social, asegurando la flexibilidad frente al posible cambio de las modalidades defraudatorias.

Desde un punto de vista dogmático, el núcleo de la tutela sigue siendo el patrimonio considerado desde la perspectiva individual y como expresión de la confianza pública en el tráfico económico digital. El elemento del engaño se puede trasladar del ámbito personal al informático, por lo que el "error" se encuentra en el funcionamiento que los sistemas inducen y no obligatoriamente la voluntad de la víctima. En este sentido, en ámbitos tecnológicos complejos, se requiere capacidad adaptativa de la dogmática penal para salvaguardar bienes jurídicos tradicionales.

Interpretación jurisprudencial consolidada**:** La jurisprudencia española, con el liderazgo del Tribunal Supremo, ha interpretado de modo uniforme y extensivo la figura de la estafa informática. Se ha asentado que el engaño clásico a persona no es imprescindible cuando

media una manipulación informática eficaz para producir el perjuicio patrimonial, y que términos como "manipulación informática o artificio semejante" abarcan desde hackeos complejos hasta engaños más rudimentarios pero aplicados a sistemas electrónicos. Casos paradigmáticos (STS 379/2019, entre otras) han cimentado la doctrina de que el phishing y análogos cumplen las exigencias típicas del delito, equiparando el error del sistema al error de la víctima en la estafa tradicional (ACÓN, 2024). Esta claridad jurisprudencial brinda seguridad jurídica y facilita las condenas de los responsables cuando son habidos.

Desafíos en la persecución práctica: A pesar del adecuado respaldo legal, la persecución efectiva de estos delitos enfrenta obstáculos prácticos. Entre ellos destacan la transnacionalidad (autores fuera de la jurisdicción), la anonimización y sofisticación técnica que dificulta la obtención de pruebas, y la atomización de casos que puede saturar los juzgados. Consecuentemente, muchos procesos terminan centrándose en partícipes menores (p.ej. mulas bancarias) y no en los organizadores, o en la vía civil para recuperar el dinero más que en lograr condenas penales. La necesidad de especialización y cooperación internacional surge como conclusión ineludible para mejorar estos aspectos.

En cuanto a la prevención y la colaboración multi-sectorial, se reitera la idea de que la represión penal por sí sola resulta insuficiente ante un fenómeno tan extendido. Es esencial complementarla con medidas preventivas (educación de usuarios, campañas de ciberseguridad) y con la colaboración de los sectores involucrados (banca, telecomunicaciones, proveedores de Internet). La responsabilidad cuasi objetiva impuesta a los bancos en materia de reembolso de operaciones fraudulentas, si bien pertenece al ámbito civil, actúa en la práctica como incentivo para que estos fortalezcan sus sistemas de seguridad y detención de fraudes, lo que indirectamente previene delitos y mitiga daños. Por su parte, los consumidores deben ser proactivos en proteger sus datos y reportar incidentes de inmediato, como también lo requiere la normativa vigente (Fernández Escudero, 2024).

La doctrina sugiere continuar refinando la legislación de manera quirúrgica (por ejemplo, ajustar agravantes, considerar tipos penales específicos en caso de surgir nuevas formas muy diferenciadas de fraude tecnológico) y, sobre todo, optimizar la aplicación de la normativa actual mediante más recursos, formación y coordinación. Las propuestas pasan por crear unidades policiales y judiciales especializadas, promover reformas procesales que habiliten la agregación eficiente de causas complejas, e intensificar convenios internacionales para la

persecución de bandas globales. Asimismo, en el horizonte se vislumbran desafíos emergentes como las estafas en entornos de economía digital avanzada (metaverso, NFT, etc.) que requerirán interpretaciones novedosas de los tipos penales existentes o incluso nuevas respuestas normativas, por lo que se aboga por una actitud legislativa vigilante y receptiva a la innovación tecnológica del delito.

En conclusión, España cuenta con un andamiaje jurídico-penal sólido para combatir las estafas informáticas, fruto de la anticipación del legislador y de la labor clarificadora de la jurisprudencia. Sin embargo, la efectividad de dicho andamiaje depende de su permanente actualización y de la dotación de medios para su implementación. El phishing, smishing, vishing, pharming y demás fraudes cibernéticos seguirán evolucionando; corresponderá al Derecho Penal evolucionar en paralelo, manteniendo el equilibrio entre la protección eficaz del patrimonio y los derechos fundamentales en el entorno digital. Solo mediante un enfoque integral –que combine la sanción penal ejemplarizante, la prevención proactiva y la cooperación transversal– se podrá hacer frente con éxito al desafío de las ciberestafas en el siglo XXI.

Referencias bibliográficas

ACÓN ORTEGO, I. (2024). *Comentario jurisprudencial de la SAP Asturias, Sección 4ª, nº 477/2024, de 21 de marzo*. Revista Jurídica sobre Consumidores y Usuarios, nº 16, pp. 6-15.

AMOAH, G. A., y HAYFRON-ACQUAH, J. B. (2022). QR Code security: mitigating the issue of quishing (QR Code Phishing). International journal of computer applications, 184(33), 34-39.

ÁVILA, V. (2024). Las mulas bancarias y su papel en las estafas informáticas, Economist & Jurist. Disponible en: https://www.economistjurist.es/articulos-juridicos-destacados/las-mulas-bancarias-y-su-papel-en-las-estafasinformaticas/#:~:text=Las%20mulas%20bancarias%20y%20su,capitales%20imprudente%2C%20en%20los

CASALS FERNÁNDEZ, Á. (2024). Evolución de la ciberdelincuencia en España.: Análisis de las estafas informáticas y sus principales modalidades fraudulentas. In *Retos inminentes de derecho digital* (pp. 121-148). Dykinson.

FERNÁNDEZ ESCUDERO, V. (2024). *Combatir el ciberfraude, un reto para los consumidores*. Revista Jurídica sobre Consumidores y Usuarios, nº 16, pp. 41-50.

HIMSS (2021). 2021 HIMSS Healthcare Cybersecurity Survey. Disponible en: https://www.himss.org/sites/hde/files/media/file/2022/01/28/2021_himss_cybersecurity_survey.pdf

IBARBUREN GONZÁLEZ, J. (2025). *Aspectos sustantivos y procesales de las ciberestafas (phishing, smishing, vishing y pharming)*, en D. González Uriel et al. (coords.), Ciberdelincuencia: perspectiva penal, procesal y criminológica (pp. 125-148). Cizur Menor: Aranzadi Thomson Reuters.

JAIN A. K. y GUPTA B. B. (2018). "Rule-Based Framework for Detection of Smishing Messages in Mobile Environment," Procedia Comput. Sci., vol. 125, pp. 617–623.

MESTRE DELGADO, E. (2024). La protección penal de los consumidores frente a las ciberestafas. *Revista Jurídica sobre Consumidores y Usuarios*, (16), pp. 52-71.

MIRÓ LLINARES, F. (2013). La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing. *Revista Electrónica de Ciencia Penal y Criminología*, (15), p. 12.

PROOFPOINT (2021). New ponemon study finds the annual cost of phishing scams has more than tripled since 2015. Disponible en: https://www.proofpoint.com/us/blog/security-awareness-training/new-ponemon-study-finds-annual-cost-phishing-scams-has-more-tripled

QUINTERO OLIVARES, G. (2013). *Estafas en la era digital: Consideraciones sobre el bien jurídico protegido*. Anuario de Derecho Penal, 25(1), pp. 45-67.

REY HUÍDOBRO, L. F. (2013). *La estafa informática: relevancia penal del phishing y el pharming*. La Ley Penal, nº 101 (marzo-abril 2013), pp. 5-15.

ROBLES PLANAS, R. (2021). *Fraude informático y nuevas tecnologías: análisis de la tipificación tras la LO 1/2019*. Revista de Derecho Penal y Criminología, 3(2), pp. 125-149.

SHAREVSKI, F., DEVINE, A., PIERONI, E., y JACHIM, P. (2022). Phishing with malicious QR codes. In Proceedings of the 2022 European Symposium on Usable Security (pp. 160-171).

VERDUGO GUZMÁN, S. (2024). Delitos patrimoniales en los mercados del metaverso. Avatares como víctimas de ciberestafas y otros metadelitos. Revista Jurídica sobre Consumidores y Usuarios, 16, 114–123.

6.1. Jurisprudencia

Tribunal Supremo

Tribunal Supremo (Sala de lo Penal) – Sentencia nº 379/2019, de 23 de julio de 2019, rec. 853/2018. RJ 2019/2606. Confirmó condena por delito continuado de estafa informática mediante phishing. ECLI: ES:TS:2019:2606.

Tribunal Supremo (Sala de lo Penal) – Sentencia nº 364/2011, de 11 de mayo de 2011, rec. 1185/2010. RJ 2011/4553. Interpretó la expresión "artificio semejante" del art. 248.2 CP, abarcando fraudes tecnológicos. ECLI: ES:TS:2011:3355.

Tribunal Supremo (Sala de lo Penal) – Sentencia nº 845/2014, de 2 de diciembre de 2014, rec. 664/2014. RJ 2015/4661. ECLI: ES:TS:2014:5632.

Tribunal Supremo (Sala de lo Penal) – Sentencia 571/2025, de 9 de abril de 2025, rec. 20/2022. ECLI: ES:TS:2025:1671.

Tribunal Supremo (Sala de lo Penal) – Sentencia 147/2005, de 17 de marzo de 2005**,** rec. 122/2004. ES:TS:2005:873

Audiencia Nacional

Audiencia Nacional –Sentencia de Madrid 32/2025, de 8 de octubre de 2025, rec. 29/2025. ECLI: ES:AN:2025:4078.

Audiencias Provinciales

Audiencia Provincial de Asturias (Secc. 4ª) – Sentencia nº 477/2024, de 21 de marzo de 2024 (Rec. Apel. 370/2023). ECLI:ES:APO:2024:477.

Audiencia Provincial de Cáceres (Secc. 2ª) – Sentencia nº 116/2024, 12 de abril de 2024, rec. 242/2024. ECLI:ES:APCC:2024:269.

Audiencia Provincial de Madrid (Secc. 9 ª) – Sentencia nº 47/2023, 26 de enero de 2023, rec. 889/2022-3. ES:TSJM:2023:700.

Audiencia Provincial de Madrid (Secc. 11 ª) – Sentencia nº 74/2022, 28 de febrero de 2022, rec. 35/2021. ES:APM:2022:616.

Audiencia Provincial de Valencia (Secc. 6ª) – Sentencia nº 254/2022, 13 de junio de 2022, rec. 436/2021. ECLI: ES:APV:2022:2622.

Audiencia Provincial de Pontevedra (Secc. 6 ª) – Sentencia nº 539/2021, 21 de diciembre de 2021, rec. 346/2021.

Audiencia Provincial de Madrid (Secc. 30ª) – Sentencia nº 520/2015, 30 de junio de 2015, rec. 511/2015. ES:APM:2015:10639.

Audiencia Provincial de Lugo (Secc. 1ª) – Sentencia nº 331/1998, 9 de julio de 1998, rec. 52/1997. ECLI: ES:APLU:1998:443.

6.2. Normativa

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. «BOE» núm. 281, de 24/11/1995. Referencia: BOE-A-1995-25444.

Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. «BOE» núm. 226, de 17 de septiembre de 2010, páginas 78847 a 78896 (50 págs.). Referencia: BOE-A-2010-14221

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. «BOE» núm. 166, de 12/07/2002. Referencia: BOE-A-2002-13758.

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). «DOUE» núm. 119, de 4 de mayo de 2016, páginas 1 a 88 (88 págs.) Referencia: DOUE-L-2016-80807

Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera. «BOE» núm. 284, de 24 de noviembre de 2018, páginas 114474 a 114568 (95 págs.) BOE-A-2018-16036.

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 y por la que se sustituye la Decisión Marco 2001/413/JAI del Consejo. ELI: http://data.europa.eu/eli/dir/2019/713/oj

Ley Orgánica 14/2022, de 22 de diciembre, de transposición de directivas europeas y otras disposiciones para la adaptación de la legislación penal al ordenamiento de la Unión Europea, y reforma de los delitos contra la integridad moral, desórdenes públicos y contrabando de armas de doble uso. «BOE» núm. 307, de 23/12/2022. Referencia: BOE-A-2022-21800.

Listado de abreviaturas

ACN: Autoridad de Certificación Nacional.

APP: Aplicación móvil (*application*).

BOE: Boletín Oficial del Estado.

CEDH: Convenio Europeo de Derechos Humanos.

CE: Constitución Española.

CP: Código Penal.

TEDH: Tribunal Europeo de Derechos Humanos.

DNS: *Domain Name System* (Sistema de Nombres de Dominio).

ENISA: Agencia de la Unión Europea para la Ciberseguridad.

ERC: European Research Council.

FBI: Federal Bureau of Investigation.

GDPR/RGPD: *General Data Protection Regulation* / Reglamento General de Protección de Datos.

IC3: Internet Crime Complaint Center (FBI).

IP: Internet Protocol.

TJUE: Tribunal de Justicia de la Unión Europea.

TC: Tribunal Constitucional.

JUR: Jurisprudencia (referencias doctrinales).

LECrim: Ley de Enjuiciamiento Criminal.

LO: Ley Orgánica.

Art.: Artículo.

CP 1995: Código Penal aprobado por LO 10/1995.

MFA / 2FA: *Multi-Factor Authentication* / *Two-Factor Authentication* (autenticación multifactor / doble factor).

NIS: Directiva sobre seguridad de redes y sistemas de información (UE).

P2P: Peer to Peer.

PSD2: *Payment Services Directive* 2 (Directiva de Servicios de Pago).

QR: *Quick Response Code*.

RGS: Reglamento General de Seguridad.

SCP: Sistema de Comunicaciones Policiales.

SIM: Subscriber Identity Module.

SMS: Short Message Service.

SSII: Sistemas de Información.

STS: Sentencia del Tribunal Supremo.

SAP: Sentencia de Audiencia Provincial.

TIC: Tecnologías de la Información y la Comunicación.

TFM: Trabajo Fin de Máster.

UE: Unión Europea.

URL: *Uniform Resource Locator*.

VPN: Virtual Private Network.

Anexo A. Esquema dogmático del delito de estafa informática. Los diferentes elementos del mismo

Elemento dogmático	**Contenido en la estafa informática (art. 249.1.a CP)**	**Notas diferenciales frente a la estafa tradicional**	**Apoyo jurisprudencial o doctrinal**
Sujeto activo	Cualquier persona con capacidad penal que manipule o utilice artificios informáticos para provocar un desplazamiento patrimonial.	No requiere contacto directo con la víctima; el engaño puede recaer sobre un sistema automatizado.	STS 381/2017 (26 octubre): el autor manipula el sistema informático para lograr la disposición patrimonial.
Conducta típica (manipulación o artificio informático)	Toda intervención fraudulenta en un sistema informático que altere su funcionamiento normal para provocar un resultado patrimonial.	Sustituye el "engaño" de la estafa clásica por una acción técnica o informática que sustituye la inducción al error.	MESTRE, 2024; GARCÍA CARRIÓN, 2023: el artificio puede consistir en accesos, alteraciones o simulaciones electrónicas.
Resultado	Desplazamiento patrimonial no consentido en perjuicio de otro y beneficio ilícito del autor o de un tercero.	Coincide con la estafa clásica: se requiere perjuicio económico concreto.	STS 509/2018 (27 noviembre): basta con la pérdida patrimonial efectiva derivada de la manipulación.
Nexo causal	La manipulación o artificio debe ser la causa directa del perjuicio económico.	El error humano no es necesario: el sistema	SAP Madrid, Secc. 23.ª, 2022: la automatización no

		actúa como "sujeto engañado".	excluye el dolo defraudatorio.
Elemento subjetivo (dolo y ánimo de lucro)	Dolo directo, conocimiento del artificio y voluntad de obtener un enriquecimiento ilícito.	Igual que en la estafa tradicional, pero trasladado al ámbito informático.	FERNÁNDEZ ESCUDERO, 2024: el dolo abarca la intención de provocar la operación patrimonial sin consentimiento.
Objeto material	Bienes, fondos o activos patrimoniales transferidos mediante sistemas electrónicos o digitales.	No necesariamente dinero físico, sino activos digitales o movimientos electrónicos.	STS 379/2019: incluye transferencias bancarias, criptomonedas o valores electrónicos.
Tipicidad y subsunción	Se integra en el art. 249.1.a CP, con pena de prisión de seis meses a tres años.	Amplia interpretación judicial para abarcar phishing, smishing, vishing, pharming, etc.	Jurisprudencia consolidada (SAP Asturias 477/2024).

Anexo B. Guía práctica de actuación frente a la estafa informática

Este anexo ofrece una síntesis práctica de las principales medidas de actuación jurídica y preventiva ante los supuestos de estafa informática (*phishing*, *smishing*, *vishing* o *pharming*), tanto desde la perspectiva de la víctima como desde la actuación institucional y procesal. Su finalidad es mostrar la aplicabilidad real del marco penal analizado en el trabajo y servir de herramienta de referencia para operadores jurídicos y ciudadanos.

1. ACTUACIÓN INMEDIATA DE LA VÍCTIMA

Situación	Medida recomendada	Objetivo jurídico
Recepción de un mensaje, correo o llamada sospechosa.	No acceder a enlaces, no facilitar datos y contactar directamente con la entidad supuestamente emisora.	Evitar la consumación del delito.
Realización de transferencia o cesión de datos.	Comunicar de inmediato al banco o entidad afectada para bloquear operaciones.	Prevenir la pérdida patrimonial y facilitar rastreo de fondos.
Confirmación de fraude.	Interponer denuncia ante la Policía Nacional o Guardia Civil (Grupo de Delitos Telemáticos).	Activar la persecución penal (art. 249.1.a CP).
Conservación de pruebas.	Guardar SMS, correos, capturas de pantalla y extractos bancarios.	Acreditar el engaño y el resultado patrimonial en sede judicial.

2. ACTUACIÓN PROCESAL Y PENAL

Fase procesal	Actuación clave	Referencia normativa o jurisprudencial

Denuncia o querella	Presentar ante juzgado de instrucción o unidad de delitos informáticos, acompañando la documentación digital.	Art. 259 LECrim.
Investigación	Solicitud de rastreo IP, localización de cuentas destino y colaboración con entidades bancarias.	STS 381/2017 (ECLI:ES:TS:2017:3811).
Determinación del tipo penal	Calificación conforme al art. 249.1.a CP (manipulación o artificio informático).	SAP Asturias 477/2024 (ECLI:ES:APO:2024:477).
Responsabilidad civil	Reintegro de fondos a la víctima salvo negligencia grave (RDL 19/2018, art. 45).	Transposición de Directiva PSD2.
Cooperación internacional	Si el fraude involucra cuentas o servidores extranjeros, activar instrumentos de cooperación judicial (Eurojust, Interpol).	Ley 23/2014, de reconocimiento mutuo de resoluciones penales.

3. Recomendaciones preventivas

Ámbito	Medidas preventivas sugeridas
Usuarios particulares	Activar doble autenticación, verificar remitentes, no acceder a enlaces no solicitados, desconfiar de urgencias en mensajes.
Entidades financieras	Implementar sistemas antifraude, comunicación inmediata ante incidentes y campañas de educación digital.
Administraciones públicas	Promover la ciberalfabetización y la denuncia digital segura mediante portales como www.osi.es o www.incibe.es.