TRABAJO FIN DE GRADO

GRADO EN DERECHO

CURSO ACADÉMICO 2020-2021

CONVOCATORIA JUNIO

TÍTULO:

"*PHISHING*: ASPECTOS TÉCNICOS Y PROCESALES DEL DELITO ESTRELLA EN TIEMPOS DE PANDEMIA"

DO NASCIMENTO FERNÁNDEZ, LUCÍA

76733461-X

GRADO EN DERECHO

DIRIGIDO POR: ALCÁCER GUIRAO, RAFAEL

Madrid, 10 de junio de 2021.

RESUMEN/*ABSTRACT*

La explosión de la era 2.0 ha causado un cambio de paradigma en nuestra manera de concebir la cotidianeidad, habiendo adaptado nuestra forma de vida a los mecanismos de los que nos ha proveído la tecnología. Esta variación ha afectado al sector del Derecho Penal, ya que los infractores de sus disposiciones han adquirido la formación necesaria para adaptar sus acciones a este instrumento, surgiendo, de este modo, nuevas formas de delinquir que varían con la misma celeridad que evolucionan los sistemas de la infomación. En este sentido, el pasado año se produjo un aumento exponencial de la comisión de delitos de *phishing* como consecuencia del incremento del uso de Internet derivado de los confinamientos por COVID-19. Considerando que esta nueva tipología de ilícitos presenta peculiaridades tanto en su estructura como en el tratamiento procesal que se les debe dispensar, se analizarán estos extremos desde el punto de vista legal y jurisprudencial.

The explosion of the 2.0 era has caused a paradigm change in our way of conceiving everyday life, having adapted our way of life to the mechanisms that technology has provided us with. This change has affected the Criminal Law sector, because people who infringe its provisions have acquired the necessary training to adapt their actions to this instrument, thus giving rise to new forms of crime that vary as quickly as information systems evolve. In this respect, last year saw an exponential increase in the commission of phishing crimes as a result of the increase in Internet use resulting from COVID-19 confinements. Considering that this new typology of offences presents peculiarities both in its structure and in the procedural treatment that should be given to them, these extremes will be analysed from a legal and jurisprudential point of view.

ABREVIATURAS

- **ART**.: Artículo
- **ATS**: Auto del Tribunal Supremo
- **BOE**: Boletín Oficial del Estado
- **C.P.**: Código Penal
- **DOUE:** Diario Oficial de la Unión Europea
- **Email**: *Electronic mail*
- **FJ**: Fundamento jurídico
- **INCIBE**: Instituto Nacional de Ciberseguridad
- **IP**: *Internet Protocol Address*
- **LECrim**: Ley de Enjuiciamiento Criminal
- **SAP**: Sentencia de la Audiencia Provincial
- **SMS**: *Short Message Service*
- **STS**: Sentencia del Tribunal Supremo
- **TS**: Tribunal Supremo
- **UE**: Unión Europea

PALABRAS CLAVE/*KEY WORDS*

Phishing; estafa informática; delito informático; *cracker*; ciberseguridad.

Phishing; computer fraud; cybercrime; cracker; cybersecurity.

ÍNDICE

1. INTRODUCCIÓN 4

2. CAPÍTULO PRIMERO: LA INFORMÁTICA COMO INSTRUMENTO PARA LA COMISIÓN DEL DELITO 6

2.1. Introducción 6

2.2. Los sistemas informáticos 7

2.2.1. Concepto y evolución 7

2.2.1.1. Evolución de los sistemas de la información 7

2.2.1.2. Concepto 9

2.3. Terminología básica en la normativa comunitaria y española 10

2.3.1. Software 11

2.3.2. Ingeniería social 11

2.3.3. *Malware* y *ransomware* 12

2.3.4. Phishing 14

2.4. La delincuencia informática 16

2.4.1. El delito informático 16

2.4.2. Ciberdelincuentes: concepto y perfil del *cracker* 17

***3.* CAPÍTULO SEGUNDO: EL DELITO DE ESTAFA DEL ARTÍCULO 248.2 DEL CÓDIGO PENAL, O *PHISHING* 20**

3.1. Introducción 20

3.2. Análisis jurídico-penal del tipo 21

3.2.1. Análisis del tipo objetivo 21

3.2.1.1. Bien jurídico protegido 21

3.2.1.2. Objeto material 23

3.2.1.3. Acción típica 25

3.2.1.4. Autoría y participación 29

3.2.1.5. Víctima: la obligación de autoprotección 33

3.2.2. Análisis del tipo subjetivo: el dolo como elemento diferenciador 34

3.3. Circunstancias modificativas de la responsabilidad criminal 36

3.4. Competencia judicial: la problemática del lugar de comisión de la infracción 40

3.5. Dificultad probatoria: la intangibilidad de la información y el anonimato inherente al medio empleado para cometer el delito 43

3.6. La responsabilidad de las entidades bancarias como depositarias del activo sustraído 46

4. CONCLUSIONES 48

5. BIBLIOGRAFÍA 52

6. ANEXO: JURISPRUDENCIA 57

1. INTRODUCCIÓN

En los últimos años se ha producido un cambio social ineludible y derivado de la explosión de la era tecnológica. La irrupción de un nuevo entorno, el virtual, en nuestra vida cotidiana, ha acelerado el proceso de digitalización de casi todas nuestras acciones: hábitos que hasta hace poco desarrollábamos en modalidad presencial, como las prestaciones laborales o la adquisición de productos de primera necesidad, son materializados en la actualidad vía *online* con la mayor naturalidad.

Esta modificación de nuestro *modus vivendi* ha ocasionado el traspaso de nuestros datos más sensibles (personales, bancarios, íntimos) a un ámbito revestido de una apariencia segura y atractiva, aunque hostil: Internet. Tal como ha publicado en noviembre del año 2020 el Instituto Nacional de Estadística (en lo sucesivo, "**INE**")[1], el 93% de la población que se encuentra en la franja de edad de 16-74 años es usuaria habitual de Internet, mientras que el 53,8% de esas personas ha comprado por esta vía en los últimos meses. Este incremento repentino del tráfico cibernético encuentra su origen en las restricciones de movilidad adoptadas durante crisis sanitaria ocasionada por la pandemia por COVID-19, que entre los meses de marzo y junio del pasado año enclaustró a la población española en sus domicilios abocándola a interaccionar con el exterior únicamente a través de la Red.

A pesar de la generalización del uso de esta herramienta, no es oro todo lo que reluce. Las encuestas y estudios realizados en los últimos tiempos muestran la insalubridad de los hábitos *online* de los usuarios españoles, ya que la mayoría de nosotros tiende a concebir Internet como una realidad paralela en la que reina la utopía de una seguridad que, por no ser manifiestas y tangibles las amenazas, es incontestable. Esta farsa nos hace proclives a acceder y utilizar las herramientas en línea sin adoptar previamente las medidas adecuadas para proteger nuestros datos de los ciberataques ideados en dicho medio.

En este sentido, desde el nacimiento de la Ciencia de la Computación en el siglo XIX habría de transcurrir un siglo para que la primera red de interconexión de ordenadores, llamada "ARPANET", permitiese coordinar proyectos de investigación a distancia entre cuatro universidades estadounidenses a través del simultaneado del desarrollo de documentos y la posibilidad de que los investigadores conversaran en línea. Asimismo, la comercialización de los primeros *Personal Computers* ("**PC**") con ocasión de la incorporación a las computadoras del primer microprocesador -lo que reducía los costes de su producción- causó que los hogares comenzasen a adquirir este nuevo producto para satisfacer las nuevas necesidades derivadas del traspaso de funciones laborales y escolares al ambiente digital.

Ambos hitos definirían el nacimiento de la conexión a Internet y su posterior incorporación a empresas, instituciones y, finalmente, a los domicilios en la década de los 90. A partir de entonces, los usuarios comenzaron a servirse de las prestaciones ofrecidas por la Red para efectuar las actividades referenciadas, si bien con el mismo desconocimiento del que hacemos gala en la actualidad. Este entorno (casi) libre de perímetros que salvaguarden nuestros datos ofrece un entorno atractivo para la delincuencia, circunstancia que ha derivado en la adquisición de formación específica por parte de los sujetos infractores y en la adaptación de modalidades comisivas tradicionales (especialmente de los delitos contra el patrimonio, contra la intimidad y

[1] **Instituto Nacional de Estadística**. "Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares. Año 2020", 16 de noviembre de 2020. Recuperado de: https://www.ine.es/prensa/tich_2020.pdf.

contra el honor) a dicho contexto; en definitiva, la incorrecta adaptación social a la nueva realidad digital ha originado el nacimiento de un nuevo tipo de delincuencia que, por su preparación y las características del medio en el que se emplea, es casi implacable.

En efecto, desde la creación del primer tipo de *malware* la actividad delictiva en Internet ha aumentado exponencialmente atendiendo a las circunstancias socio-económicas y/o políticas del momento. Teniéndolas en consideración, los ciberdelincuentes han acomodado sus métodos de agravio al desarrollo digital con el objetivo de revestir sus acciones de efectividad y del necesario anonimato dirigido a asegurar la consumación del delito. Además, muchos de ellos han llegado a especializarse en la perpetración de distintos tipos de ciberataques dirigidos contra determinados colectivos de víctimas (por ejemplo, el *ransomware* y el *smishing*) e ideados con diferentes motivaciones, que pueden abarcar desde el enriquecimiento injusto hasta el desafío político.

Dentro de esta categoría de ilícitos -que, como se analizará a lo largo de presente trabajo, han sido erróneamente catalogados como "delitos informáticos"- destaca por la frecuencia de su comisión el delito de estafa informática cometido a través de la técnica denominada *phishing*, consistente en el envío masivo de correos electrónicos (o, en menor medida, en la realización de llamadas fraudulentas) en los que el *cracker* suplanta la identidad de otra persona o entidad con el único objetivo de sustraer del haber de la víctima parte de su patrimonio. Al igual que lo acaecido con los restantes delitos informáticos, el analizado posee una serie de características propias que obligaron a modificar el Código Penal al legislador de 2010 para introducir una fórmula generalista en su artículo 248.2 que acogiese esta nueva modalidad delictiva, que, por la peculiaridad del medio en el que se desarrolla y los aspectos técnico-informáticos que intervienen en su correcta consecución, no era susceptible de ser subsumida en el delito básico de estafa.

Sin embargo, dada la rica casuística que presentan estas modalidades delictivas como consecuencia del continuo desarrollo de Internet y de los métodos empleados por los ciberdelincuentes, ha sido necesario un extenso desarrollo jurisprudencial que desgranase los elementos del tipo de estafa informática en comparación con los estructurales de la estafa básica, así como de la identificación y grado de participación de cada uno de los intervinientes en la trama defraudatoria atendiendo a su aportación al hecho principal. Asimismo, como consecuencia de la naturaleza de la realidad virtual donde se comete y de la volatilidad de los datos informáticos que documentan las conexiones efectuadas a través de él, el delito de estafa informática precisa, para su correcto enjuiciamiento, del aseguramiento inmediato de las evidencias de su perpetración, así como de la práctica de diligencias específicas de investigación dirigidas a determinar la identidad del *phisher*, los métodos empleados para lanzar el ataque, y el alcance de la citada intervención de los partícipes en la maquinación fraudulenta.

Por todo ello, este trabajo pretende ofrecer una visión global del citado injusto desde la perspectiva técnico-jurídica, que englobará el estudio del funcionamiento de los sistemas informáticos como soporte en el que se aloja el *malware* contenido en el mensaje para una mejor comprensión de su trascendencia jurídica, y un análisis pormenorizado de la normativa y jurisprudencia existentes sobre los aspectos jurídicos y procesales derivados de sus singulares características.

2. CAPÍTULO PRIMERO: LA INFORMÁTICA COMO INSTRUMENTO PARA LA COMISIÓN DEL DELITO

2.1. INTRODUCCIÓN

La Ciencia de la Computación, conocida también como "informática", encuentra su origen primigenio en el siglo XIX con el diseño de las primeras máquinas programables, que permitían automatizar procesos simples como el almacenamiento de información o el cálculo para fines meramente administrativos.

Los expertos apuntan a que su verdadero nacimiento se produjo en la segunda mitad del siglo XX con la fabricación y comercialización de máquinas denominadas "computadoras", que funcionaban a través de un sistema compuesto por válvulas de vacío y un lenguaje máquina, es decir, un código compuesto por instrucciones automatizadas. El máximo exponente de estos primeros ordenadores fue ENIAC (siglas de *Electronic Numerical Integrator And Computer*) ideado por los ingenieros estadounidenses J.P. Eckert y J.W. Mauchly y lanzado al mercado en 1946, que fue seguido en relevancia por UNIVAC I (siglas de *Universal Automatic Computer*), la primera computadora fabricada en serie.

Sin entrar en datos propios de un Grado en Ingeniería Informática, lo cierto es que esta Ciencia ha continuado desarrollándose a través del tiempo -en lo que se ha denominado las "cinco generaciones" de la evolución de la informática- alcanzando avances notables hasta la actualidad.

Sin perjuicio de lo anterior, la problemática analizada en el presente trabajo obliga al análisis y tratamiento del hilo conductor o medio que los "ciberdelincuentes" aprovechan para perpetrar el hecho jurídicamente reprochable: si la informática es a los (mal llamados) delitos informáticos el refugio de su modo de proceder, Internet (denominada también "Red" o "Ciberespacio") es el espacio o ámbito de cuyas características y fórmulas se sirven con el fin de atacar un bien jurídico, como pueden ser la libertad sexual y el patrimonio de la víctima.

Desde el establecimiento en 1969 de la primera red de interconexión de computadores, llamada ARPANET[2], se han desarrollado numerosos protocolos en la Red que responden a servicios tan dispares como la búsqueda de información (a través de la *World Wide Web* "WWW"), conversar con otras personas (mediante correo electrónico, chats en línea, *apps* que permiten la realización de videollamadas, entre otros) o el acceso a distancia a otros sistemas. Esta miscelánea de procedimientos dio lugar a la explotación de las singulares características de Internet por parte de los *crackers*, en especial, de las potenciales brechas de seguridad en los sistemas de los usuarios con diferentes objetivos, entre los que destacan el ánimo de lucro, los intereses políticos, la justicia social o el simple hecho de ganarse un renombre dentro del colectivo al que pertenecen.

[2] ARPANET fue una red informática descentralizada estadounidense fundada en 1969 a petición del Departamento de Defensa de EEUU, que conectaba cuatro equipos informáticos de universidades distintas (California, Santa Bárbara, Stanford y Utah), con el objetivo de coordinar proyectos de investigación.

Digital Guide IONOS. *Arpanet: los primeros pasos de Internet*. Recuperado de: https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/arpanet-los-inicios-de-internet/

Ese aprovechamiento dio lugar a la especialización de estos individuos, que, desde el nacimiento de Internet, han ideado innumerables tipos de *malware*[3] que actúan o infectan de forma distinta el *software* del sistema. A modo de ejemplo, y según una encuesta realizada por INTERPOL en el mes de agosto del pasado año 2020[4], durante la situación de alarma por COVID-19 se incrementaron los ciberataques en los Estados Miembros de la Unión Europea, concretamente, en un 59% el *phishing* y en un 36% el *ransomware*. Asimismo, es evidente la ampliación del radio del victimario elegido por parte de los atacantes, que, más allá de centrarse en las personas físicas, han lanzado amenazas cibernéticas a entidades como centros sanitarios (recordemos el sonado ciberataque que dejó al Hospital de Torrejón de Ardoz sin acceso a sus sistemas[5]), instituciones públicas (como el sufrido por el SEPE el pasado 9 de marzo[6]) o empresas proveedoras de servicios esenciales.

Para comprender la trascendencia jurídica de un ciberataque (objeto de estudio en el Capítulo Segundo), el presente Capítulo persigue analizar y esclarecer los conceptos clave implicados en él, realizando un recorrido que comienza por la complejidad de un sistema informático y su funcionamiento, continuando por los métodos de los que se sirven los ciberdelincuentes para que la víctima caiga en su trampa, pasando por algunos de los ataques más habituales en la actualidad, y desembocando en el perfil del atacante y su motivación para delinquir.

2.2. LOS SISTEMAS INFORMÁTICOS

2.2.1. CONCEPTO Y EVOLUCIÓN

2.2.1.1. EVOLUCIÓN DE LOS SISTEMAS DE LA INFORMACIÓN

Es un hecho indiscutible que, para que pueda producirse un ciberataque, éste debe ser emitido desde un sistema informático que utilice la Red para hacerlo llegar al sistema que se pretende infectar. Con el objeto de facilitar la comprensión del presente trabajo, resulta forzoso el abordaje de cuestiones propias de la informática tales como el origen y la evolución de los sistemas de la información, así como el concepto de "sistema informático" y su diferenciación del "sistema operativo", objeto de análisis en el siguiente epígrafe.

En primer lugar, debe tenerse en consideración que la evolución de los sistemas de la información es inseparable del surgimiento y desarrollo de la empresa en los

---

[3] *Creeper* fue el primer virus informático documentado de la historia de Internet. *Ab initio*, fue diseñado como un programa que debía autorreplicarse en discos duros diferentes; sin embargo, su creador descubrió que a medida que iba replicándose, el programa se auto eliminaba del disco duro anterior.

Kaspersky. *Una breve historia de los virus informáticos y lo que nos deparará el futuro*. Recuperado de: https://latam.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds.

[4] **INTERPOL**. *Ciberdelincuencia: efectos de la COVID-19*. Recuperado de: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19.

[5] **Sierra, Rosalía**. *Torrejón, primer hospital español "secuestrado" por un virus informático*. El Mundo, 22 de enero de 2020. Recuperado de: https://www.elmundo.es/ciencia-y-salud/salud/2020/01/21/5e274be1fdddffcf088b462d.html.

[6] **El País**. *El sistema informático del SEPE sufre un ciberataque*. 9 de marzo de 2021. Recuperado de: https://elpais.com/economia/2021-03-09/el-sistema-informatico-del-sepe-sufre-un-ciberataque.html.

países más desarrollados económica y socialmente, así como del poder de las instituciones públicas y de las universidades, habida cuenta que la razón de su invención fue agilizar el proceso de almacenamiento de cantidades ingentes de datos y automatizar operaciones.

Sin ánimo de incurrir en reiteraciones innecesarias, en este punto debe realizarse una remisión a la Introducción del presente Capítulo, en el que se efectúa una pequeña pincelada sobre los primeros modelos de ordenadores (ENIAC y UNIVAC I), surgidos en los últimos años de la década de los años 40. Como se ha apuntado, se trataba de modelos muy simples que poseían un sistema de procesamiento de transacciones, por lo que el usuario (en su mayoría, trabajadores) podía realizar operaciones de cálculo y crear registros de información.

El primer hito que significó una mejora palpable tuvo lugar en la década de 1960 con el nacimiento del Sistema de Información Gerencial ("SIG" o *Management Information System*, "MIS") [7]. Este novedoso sistema permitió por primera vez transformar los datos introducidos por el usuario en información a través de su comparación y recopilación en informes (por ejemplo, informes de control de inventario y de pedidos), por lo que, una vez más, simplificaba la labor de los trabajadores. Como se desprende de la definición ofrecida, para su implantación era necesario poseer previamente un sistema de procesamiento de transacciones en el que estuviesen alojados los datos.

Sin embargo, no es hasta los años 70-80 cuando se modificó la concepción original de estos efectos a través de dos invenciones y su incorporación a los sistemas preexistentes.

El primero de ellos fue el lanzamiento, el 15 de noviembre de 1971, de "Intel 4404", el primer microprocesador de la historia de la computación. Este procesador en formato *chip* revolucionó la fabricación de los ordenadores -que hasta ese momento portaban un procesador compuesto por placas de circuitos impresos-, redujo su tamaño y abarató los costes de producción. Como consecuencia de ello, surgieron los primeros ordenadores de uso personal o ***Personal Computers*** (en sus siglas, "PC"), de mayor potencia de procesamiento que sus antecesores, entre los que el modelo francés "Micral N"[8] fue el primero en utilizar el microprocesador.

Efecto del surgimiento de los ordenadores personales fue también la creación del Sistema de Soporte de Decisión[9] (en sus siglas "DSS"), desarrollado entre los años 80 y 90. Frente al de Información Gerencial, que únicamente tomaba los datos introducidos por el usuario para elaborar informes que le facilitasen ciertas tareas, el "DSS" es un tipo de *software* que toma en consideración datos internos (introducidos por el usuario) realizando un pronóstico a partir de la ejecución de análisis y ofreciendo una interfaz de sus resultados, ayudando al trabajador o directivo en la toma de decisiones. Este

[7] **Hernández Trasobares, Alejandro**. 2003. *Los sistemas de información: evolución y desarrollo*. Dialnet. Proyecto Social: Revista de relaciones laborales, núm. 10-11. Págs. 149-165. Recuperado de: https://dialnet.unirioja.es/descarga/articulo/793097.pdf.

[8] **Parcela Digital**. *Micral N, el primer ordenador comercial de la historia basado en microprocesador*. Recuperado de: https://parceladigital.com/2017/04/06/micral-n-el-primer-ordenador-comercial-de-la-historia-basado-en-microprocesador/.

[9] **Globalbit**. *¿Qué es un sistema de soporte a la decisión (DSS)?* Recuperado de: https://www.globalbit.co/2020/02/18/que-es-un-sistema-de-soporte-a-la-decision-dss/.

Sistema constituiría la base de muchos de los cambios introducidos en programación posteriormente, entre los que destaca el *software* de Sistema de Información Ejecutiva[10], que añade al análisis de datos internos, los externos (extraídos de Internet).

Entre los años 1990 y 2000 se produjo una auténtica explosión de la navegación por Internet que dio lugar a la difusión del conocimiento sin límites. En este marco fue creado el Sistema de Gestión del Conocimiento (*Knowledge Management System*, "KMS"), un *software* que tiene la capacidad de crear, guardar y difundir la información dentro de las organizaciones, lo que implica además la participación de los empleados en la actualización de esos datos. De este modo tienen acceso, por ejemplo, a información sobre procedimientos seguidos dentro de la empresa para cada gestión concreta, y a los datos de los clientes.

Finalmente, en la actualidad se están implementando los Sistemas de Información Estratégicos (SIS), a través de los que las empresas dan visibilidad a la táctica de posicionamiento en el mercado de sus respectivos servicios haciendo partícipe a su público potencial, reduciendo, de este modo, la ventaja de sus competidores. Una fantástica muestra de ello son las tiendas *online* y las páginas *web* de las compañías de telefonía, que, ofreciendo el mismo servicio, publicitan de forma periódica las diferentes tarifas u ofertas que han creado con la finalidad de captar nuevos clientes.

2.2.1.2. CONCEPTO

Cuando el usuario medio de un elemento informático se refiere al "sistema" en una conversación, es relativamente común que incurra en el error de identificar el "sistema informático" con el "sistema operativo". Sin embargo, ambos elementos poseen significados opuestos y se identifican con diferentes componentes de un equipo.

En este sentido, encontramos una primera aproximación al concepto de "sistema informático" en el Convenio del Consejo de Europa sobre Ciberdelincuencia de Budapest, de 23 de junio de 2001, en el que los Estados firmantes establecen que se entenderá por tal "todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa"[11]. De esta descripción podemos extraer que los sistemas informáticos están integrados por la pareja compuesta de *hardware* y *software* (conceptos objeto de estudio en el siguiente epígrafe).

No obstante, si retrocedemos a la primera parte de este apartado ("Evolución de los sistemas de la información") daremos cuenta de que este concepto, aunque cercano y de fácil comprensión, no abarca la amplitud de actividad que define a estos sistemas. Por ello, resulta necesario acudir a modelos conceptuales elaborados por instituciones especializadas en el sector de la informática.

La descripción que realiza el *T1.523-2001, Telecom Glossary 2000*[12], creado por el *American National Standards Institute* es la más completa hasta la fecha. Esta suerte

[10] **Circulante**. *Los sistemas de información ejecutiva, herramienta de seguimiento de indicadores de negocio claves en crisis*. Recuperado de: https://circulante.com/finanzas-corporativas/los-sistemas-informacion-ejecutiva-indicadores-crisis/.

[11] Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 y ratificado por España el 20 de mayo de 2010. Recuperado de: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

[12] El *T1.523-2001, Telecom Glossary 2000*, es un documento elaborado y publicado por la Alliance for Telecommunications Industry Solutions (ATIS), organización con sede en Washington acreditada por el

de diccionario toma como propia la concepción de "sistema informático" realizada por su predecesor, el *Federal Standard 1037C*[13], determinando que se trata de un "sistema o subsistema de telecomunicaciones o computacional interconectados que se utilicen para obtener, almacenar, manipular, administrar, mover, controlar, desplegar, intercambiar, trasmitir o recibir voz y/o datos, incluyéndose en el mismo tanto los programas (*software* y *firmware*) como el equipo (*hardware*)". De esta forma, tal significado es totalmente opuesto a la concepción de "sistema operativo", que únicamente hace referencia y consiste en el *software* principal al que se acomodan el resto de programas que son instalados en el sistema y que, en todo o en parte, son el objetivo primero de todo ciberataque.

De todo lo expuesto se extrae que un sistema informático está compuesto por el binomio *software-hardware*, conjunto que se encuentra englobado en la Sociedad de la Información[14] como consecuencia de su capacidad para almacenar e intercambiar datos, así como para intervenir en el tráfico de información y servicios propio de Internet.

2.3. TERMINOLOGÍA BÁSICA EN LA NORMATIVA COMUNITARIA Y ESPAÑOLA

Si bien es necesario atender a las políticas y normas promulgados en el continente americano por ser la cuna de la informática moderna (sin desmerecer los avances de otros países), para comprender la regulación elaborada en este campo en España es necesario estar a lo dispuesto en el acervo comunitario.

American National Standards Institute estadounidense. Su función consiste en desarrollar estándares y soluciones técnicas para las TIC. Entre sus miembros se encuentran empresas tecnológicas de reconocida solvencia como Apple, Dell Technologies, Cisco Systems o Google. El estándar puede ser consultado (salvo excepciones justificadas por derechos de propiedad intelectual) en la página *web* de la organización: https://glossary.atis.org/.

[13] El Federal Standard 1037C fue desarrollado y promulgado por la agencia estadounidense *General Services Administration* (GSA) en 1996, en el marco del *Federal Property and Administrative Services Act of 1949*. El objetivo perseguido con su creación fue dotar a la Administración de EEUU de un diccionario conceptual de términos utilizados en el sector de las telecomunicaciones. Aunque fue sustituido por el *T1.523-2001, Telecom Glossary*, en la actualidad se sigue acudiendo a sus acepciones. Puede ser consultado aquí: https://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm.

[14] El economista austro-estadounidense Fritz Machlup (1902-1983) fue pionero acuñando el término "Sociedad de la Información" en su obra *The Production and Distribution of Knowledge in the United States* (1962). Con él hacía referencia al movimiento protagonizado por la cantidad de población que hacía uso de las nuevas tecnologías, mayor en comparación con el porcentaje que efectuaba tareas que implicaban esfuerzo físico.

No obstante, el concepto elaborado más cercano a la actualidad fue el adoptado por la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, que transpuso la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio. La citada norma considera "Sociedad de la Información" en su Motivo II al conjunto "que engloba además de la contratación de bienes y servicios por vía electrónica, el suministro de información por dicho medio (como el que efectúan los periódicos o revistas que pueden encontrarse en la red), las actividades de intermediación relativas a la provisión de acceso a la red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, al alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio...), siempre que represente una actividad económica para el prestador. Estos servicios son ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades indicadas, incluido el comercio electrónico".

2.3.1. SOFTWARE

Este nombre, de terminología anglosajona y acuñado en el sector tecnológico por el estadístico estadounidense John W. Tukey en 1957, fue recogido en el Diccionario de la Real Academia Española en 2008 bajo la redacción "conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora". Al igual que lo sucedido con la definición de "sistema informático", el concepto resulta limitado para quien persigue el estudio y comprensión del funcionamiento de un sistema para determinar las consecuencias fácticas y jurídicas de una amenaza *online*. Por ello, se hace irreemplazable la consulta de la normativa emanada de las Instituciones de la Unión Europea, que, sorpresivamente, ha dedicado numerosas Directivas a la regulación de los comportamientos en Internet, la protección de los datos objeto de su tráfico y hasta de la protección de la titularidad de los programas informáticos, similar a la de las obras literarias.

Realizando una síntesis del contenido de dicha normativa, se considera *software* a todos los componentes de un equipo que son intangibles, es decir, a los programas, sus elementos y a los datos alojados en ellos. Asimismo, la lógica invita a considerar también como tal al sistema operativo del dispositivo e, incluso, al *malware*.

Ejemplo de esta concepción es la actual Directiva (UE) 2019/770 del Parlamento Europeo[15], que se refiere reiteradamente al *software* como "programa" o "programas". Esta norma fue incorporada al ordenamiento jurídico español a través de la Ley de Propiedad Intelectual[16], cuyo artículo 96 ofrece una definición muy completa del término analizado, disponiendo que "se entenderá por programa de ordenador toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuese su forma de expresión y fijación". De esta forma, la norma abandona la concepción unitaria de *software* previniendo que su ecosistema es el sistema informático, además de atender a las funciones que realiza dentro de él, independientemente de cuáles sean.

En conclusión, si un sistema informático está compuesto por el mencionado binomio *hardware*[17]*-software*, éste integra el sistema operativo del equipo (Windows 10, Linux, o iOS, entre otros) y el resto de programas o componentes instalados en él. Sirvan de ejemplo el Paquete Office, el Navegador que utilizamos para acceder a Internet, los antivirus y las amenazas cibernéticas.

2.3.2. INGENIERÍA SOCIAL

Como anticipaba en la Introducción de este Capítulo, los *crackers* han aprovechado en los últimos tiempos las brechas de seguridad de los sistemas de los

---

[15] Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales. Recuperada de: https://www.boe.es/doue/2019/136/L00001-00027.pdf.

[16] Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia. Recuperada de: https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930.

[17] En contraposición al *software*, el *hardware* o "elemento duro" hace referencia a los componentes físicos de un sistema. Son ejemplos de ello el monitor del equipo, el ratón o *mouse* y la impresora.

Softwarelab.org. *¿Qué es hardware y software? Definición y diferencias*. Recuperado de: https://softwarelab.org/es/que-es-hardware-y-software-definicion-y-diferencias/.

usuarios y perpetrado numerosos ciberataques a personas físicas, jurídicas y entidades públicas.

En este sentido, si un dispositivo resulta objeto de un ataque de esta clase y el ciberdelincuente consigue su fin último (por ejemplo, apropiarse de parte del patrimonio de la víctima o manipular datos que estén alojados en un sistema ajeno), su éxito derivará del engaño al que haya sometido al usuario para permitirle acceder al sistema o a su información más sensible sin que sea consciente de ello.

La estrategia a través de la que el *cracker* manipula al usuario para que le facilite esos datos o el acceso a los mismos se denomina "ingeniería social". Si bien el acervo comunitario no se ha ocupado de descifrar aún el contenido de este método de obtención de información, la normativa patria, a través de la Ley de Seguridad de las Redes y Sistemas de la Información, ha acertado en disponer que se trata de "técnicas que buscan la revelación de información sensible de un objetivo, generalmente mediante el uso de métodos persuasivos y con ausencia de voluntad o conocimiento de la víctima"[18], catalogándolo además como una clase de ciberincidente de riesgo "medio".

Parafraseando a Séneca, "largo es el camino de la enseñanza por medio de teorías; breve y eficaz por el camino de ejemplos", por lo que procede en este extremo exponer un caso real. El pasado mes de septiembre diversos medios de comunicación informaron[19] de que los Ministros de Justicia y de Asuntos Exteriores habían sido víctimas de *phishing*, que causó un bloqueo en los teléfonos que usan en el ejercicio de su cargo. Este ataque fue consumado a través de una técnica de ingeniería social consistente en el envío de un SMS en nombre de una Embajada a sus dispositivos móviles, mediante el que ésta les urgía a regularizar una situación administrativa haciendo *click* en un *link* adjunto. Ambos obedecieron, descargándose de este modo el *malware* programado por el ciberdelincuente e infectando sus teléfonos.

Según datos publicados por el Instituto Nacional de Ciberseguridad de España (INCIBE)[20], la ingeniería social se ha erigido como un medio especialmente idóneo para perpetrar un ciberataque por el alto grado de vulnerabilidad que presentan los individuos con falta de atención o que restan importancia a las cuestiones informáticas, con independencia de cuál sea su formación.

De este modo, el *cracker* se aprovecha del respeto infligido por instituciones como la Policía Nacional, la AEAT o Correos, así como de cebos de reconocida solvencia como la gratuidad en la obtención de un producto o servicio o el miedo a ser desprovistos de un servicio, para que el usuario no verifique la información del remitente y se fíe del mensaje.

2.3.3. *MALWARE* Y *RANSOMWARE*

[18] Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Anexo - Instrucción Nacional de notificación y gestión de ciberincidentes. 2. Clasificación/taxonomía de los ciberincidentes. BOE núm. 218, de 8 de septiembre de 2018, páginas 87675 a 87696. Recuperado de: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-12257.

[19] **Zofío Lleó, Lara**. *Los ministros y altos cargos del Gobierno fueron hackeados con técnicas de ingeniería social*. El Confidencial. 6 de septiembre de 2020. Recuperado de: https://www.elconfidencialdigital.com/articulo/seguridad/ministros-han-sido-hackeados-tecnicas-ingenieria-social/20200904170228159189.html.

[20] **INCIBE**. *Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse*. 5 de septiembre de 2019. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse.

Tradicionalmente, el usuario medio de cualquier producto informático teme que, por navegar por determinados sitios *web* o descargarse archivos de dudosa procedencia, su sistema pueda ser infectado por un "virus". Sin embargo, el uso universalizado del término no lo convierte en adecuado, al menos no en todo caso.

Grosso modo, la diferencia esencial entre el *malware* y un virus común radica en su comportamiento al infectar un sistema. En este sentido, el ordinal 7º del Anexo del Real Decreto-ley 12/2018, de 7 de septiembre, de Seguridad de las Redes y Sistemas de la Información, establece que será *malware* cualquier tipo de *software* que modifica los datos de un sistema o causa daños en él[21], conformando una categoría general de amenaza que acoge tantos subtipos como maneras de infectar un dispositivo existen.

De este modo, todo virus forma parte del concepto analizado, diferenciándose del mismo en que, una vez infectado el sistema o alguno de sus componentes *software*, se propaga o replica en otros equipos a través de Internet o *hardware* susceptible de ser incorporado, siquiera temporalmente, al sistema principal (por ejemplo, mediante la conexión de un puerto USB). Así lo aclara la citada norma al exponer que se trata del "tipo de *malware* cuyo principal objetivo es modificar o alterar el comportamiento de un sistema informático sin el permiso del usuario…Es reseñable que un virus requiere de la acción humana para su propagación a diferencia de otro *malware*"[22].

En lo que respecta al segundo término analizado, al igual que los virus, forman parte de la categoría *malware*, aunque vuelve a diferenciarse de éste en su manera de actuar. Mientras que el virus infecta y se replica para infectar otros sistemas, el *ransomware*[23] se caracteriza por estar programado para bloquear el acceso del usuario al

---

[21] Anexo del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de la información.

> "7. – *Malware* (código dañino): palabra que deriva de los términos "malicious" y "software". Cualquier pieza de software que lleve a cabo acciones como extracción de datos u otro tipo de alteración de un sistema puede categorizarse como *malware*. Así pues *malware* es un término que engloba varios tipos de programas dañinos".

Recuperado de: https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257.

[22] Anexo del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de la información.

> "7. – Virus: tipo de *malware* cuyo principal objetivo es modificar o alterar el comportamiento de un sistema informático sin el permiso o consentimiento del usuario. Se propaga mediante la ejecución en el sistema de un *software*, archivos o documentos con carga dañina, adquiriendo la capacidad de replicarse de un sistema a otro. Los métodos más comunes de infección se dan a través de dispositivos extraíbles, descargas de Internet y archivos adjuntos de correo electrónico. No obstante, también puede hacerlo a través de *scripts*, documentos y vulnerabilidades XSS presentes en la web".

Recuperado de: https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257.

[23] Anexo del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de la información.

> "7. - *Ransomware*: se engloba bajo este epígrafe a aquel *malware* que infecta una máquina, de modo que el usuario es incapaz de acceder a los datos almacenados en el sistema. Normalmente la víctima recibe posteriormente algún tipo de comunicación en la que se le coacciona para que se pague una recompensa que permita acceder al sistema y a los archivos bloqueados".

sistema o a alguno de sus componentes mientras no satisfaga las exigencias del *cracker*. Sirva como ejemplo el reciente ciberataque al Servicio Público de Empleo Estatal (SEPE)[24], en el que resultaron afectados sus servidores y página *web*, paralizando la actividad de dicho organismo durante semanas.

Para concluir este apartado, debe apuntarse que el hecho de que las analizadas constituyan categorías de amenazas diferentes no implica la imposibilidad de su convivencia. De este modo, en multitud de ocasiones nos encontraremos con que unas no pueden llevarse a cabo sin las otras en términos técnicos (pensemos en el anterior ejemplo, en el que los sistemas del SEPE fueron bloqueados[25]).

2.3.4. PHISHING

Una vez expuestos los términos más utilizados en el campo de la informática aplicada en el sector jurídico, procede abordar de manera sucinta, sin perjuicio de ulterior tratamiento en el Capítulo II, los aspectos técnicos de la temática protagonista del presente trabajo.

Probablemente, el ciberataque analizado sea el más acometido en los últimos tiempos. En efecto, la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT) advirtió en marzo de 2020 sobre el repunte de casos de *phishing*[26], hecho que se ha terminado constatando en el *Digital Report Defense 2020* emitido por Microsoft[27], una de las compañías más afectadas por la suplantación de identidad cometida a través de este método. Su éxito se debe fundamentalmente a dos factores: a) por un lado, a la escasa complejidad de su ejecución, sumada al abaratamiento de los costes de materiales necesarios para efectuarlo; b) por otro, a la alta probabilidad de éxito para lograr el fin perseguido.

Recuperado de: https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257.

[24] **Pastor, Javier**. *Así es Ryuk, el ransomware que ha dejado tumbado al SEPE (y que antes tumbó a muchos otros)*. Xataka. 10 de marzo de 2021. Recuperado de: https://www.xataka.com/seguridad/asi-ryuk-ransomware-que-ha-dejado-tumbado-al-sepe-que-antes-tumbo-a-otros-muchos.

[25] En el supuesto objeto de estudio concurren la infección del sistema por *ransomware* (bloqueo de los sistemas de la sociedad en cuestión) y por un troyano, que se introduce en el equipo y otorga su control al *cracker*, brindándole la oportunidad de disponer de toda la información alojada en el sistema. Lo más habitual, como en este caso, es que el primero haya sido introducido en el equipo a través del troyano, ya que éste se instala en el sistema como *software* de apariencia legítima aprovechando cualquier brecha de seguridad.

[26] **CCN-CERT**. *Alerta: repunte de campañas de phishing por COVID-19. 19 de marzo de 2020*. Recuperado de: https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/9716-ccn-cert-al-05-20-repunte-campanas-de-phishing-por-covid-19.html.

[27] En el Informe, Microsoft dictamina lo siguiente (traducción del inglés):

"En 2019 bloqueamos alrededor de 13 billones de emails maliciosos y sospechosos, de los que más de 1 billón fueron *phishing* basados en URL-malicioso (…). Hasta hace unos años, los ciberdelincuentes centraron sus esfuerzos sobre los ataques de *malware*, porque proporcionaban mayo retorno de la inversión realizada. Recientemente, han cambiado y se centran en los ataques de *phishing* (70%), con el objetivo de cosechar credenciales de usuarios".

Recuperado de: https://www.microsoft.com/en-us/download/details.aspx?id=101738.

El *phishing*[28] (del inglés, "fishing") es la amenaza cibernética que se perpetra a través del envío de correos electrónicos o SMS a los que se adjunta *malware* o acceso al mismo con el objetivo de aprehender datos sensibles del usuario, que termina dando al *cracker* acceso a éstos sin ser consciente de ello. En términos jurídicos, siempre que concurran los requisitos establecidos en el artículo 248.2.a) del Código Penal (en adelante, **"C.P."**) esta conducta será constitutiva de un delito de estafa especial, sin perjuicio de serlo también de un delito de daños informáticos tipificado en el artículo 264 del mismo cuerpo legal.

Concurren en la conducta del pirata informático dos elementos diferenciadores: además de engañar al usuario y desplegar un "cebo" para infligirle cierta premura en su actuación (urgencia o amenaza de desposeerle de un servicio, lo que constituye una técnica de ingeniería social), suplanta la identidad de empresas o entidades públicas al objeto de valerse de la de fiabilidad que éstas proyectan (por ejemplo, entidades bancarias o el servicio de Correos). En definitiva, aprovecha la falta de atención y la ausencia de comprobación de la procedencia de la comunicación por parte de la víctima para conseguir su objetivo final, que no es otro que obtener un beneficio económico a costa del patrimonio del usuario afectado.

El *phishing* presenta tantas modalidades como métodos de recepción de la comunicación sospechosa y perfiles de víctima existen. En este sentido, por nombrar las más comunes, concurren en el panorama ciberdelictivo amenazas recibidas por *email*, SMS (*smishing*), llamada telefónica (*vishing*), a través del escaneado de un código QR (*QRishing*), y cada una de ellas puede estar programada para ser enviada a diferentes perfiles de usuario.

De este modo, si el objetivo del *cracker* es acceder a los sistemas de un grupo de usuarios particulares y con un nivel básico de dominio de la informática, lo más probable es que aquél programe un *spear phishing*[29], mientras que si el objetivo es el CEO de una multinacional la modalidad más utilizada es la del *whaling*[30].

A continuación, adjunto una imagen donde se aprecia un modelo de tentativa de esta amenaza en su modalidad de *spear phishing*:

---

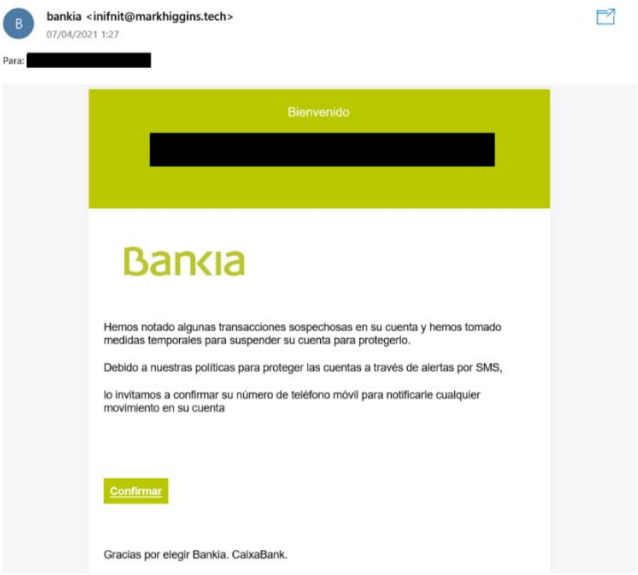
[28] **Malwarebytes**. *Suplantación de identidad (phishing)*. Recuperado de: https://es.malwarebytes.com/phishing/.

[29] El *spear phishing* se caracteriza por la creación de campañas de email engañosas cuyo contenido puede comportarse de tres maneras distintas: o contiene un *link* que redirige a un sitio *web* falso (aunque con apariencia fiable) en el que el usuario deberá dejar sus datos, o contiene un archivo que al ser descargado instala *malware* en el sistema que aprehende esa información, o bien presenta ambos elementos para lograr un más que probable éxito de la operación. En estos casos, los ciberdelincuentes acostumbran a suplantar la identidad de entidades bancarias o entidades con las que los ciudadanos suelen entablar relación por cuestiones mayoritariamente económicas, como el pago de impuestos o de sanciones.

Digital Guide IONOS. *Spear phishing: ciberataques personalizados*. 30 de abril de 2020. Recuperado de: https://www.ionos.es/digitalguide/correo-electronico/seguridad-correo-electronico/spear-phishing/.

[30] También conocido como "CEO fraud", el *whaling* (traducido del inglés, "caza de ballenas") está dirigido a un colectivo radicalmente distinto del *spear phishing*: los directivos de empresas de gran facturación. De esta forma, el pirata informático remite la comunicación sospechosa en nombre de altos cargos, instituciones importantes, o incluso de cargos superiores al receptor dentro de la misma empresa, por lo que el receptor siente la obligación de responder a lo que en ella se le pide.

Kaspersky. *¿Qué es un ataque de whaling?* Recuperado de: https://latam.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack.



En este ejemplo se aprecian varias evidencias del origen espurio del mensaje, entre las que destacan la dirección de *email* desde la que se remite la comunicación (no procede de una dirección asociada a un dominio oficial), la dirección de correo del destinatario como saludo (lo habitual es que la entidad bancaria donde el cliente tiene sus cuentas se refiera a él como "cliente" o por su nombre de pila), o el señuelo utilizado para engañar al usuario (suspensión del acceso a la cuenta bancaria por situación irregular y *link* donde presuntamente subsanará la misma).

Realizada una aproximación al término informático, tal como se ha anticipado, en el siguiente Capítulo (II) se abordará el *phishing* desde la perspectiva jurídico-penal.

2.4. LA DELINCUENCIA INFORMÁTICA

2.4.1. EL DELITO INFORMÁTICO

Como poníamos de manifiesto en los anteriores epígrafes, el nacimiento y expansión de las Tecnologías de la Información y la Comunicación (en lo sucesivo, "TIC"), en especial de Internet, han supuesto la adaptación y aprovechamiento de esta nueva vía para adaptar la consecución de ciertos comportamientos tipificados en el Código Penal.

Para determinar qué se entiende por "delito informático", la razón deduce que lo más adecuado es acudir al citado cuerpo legal. Sin embargo, las únicas referencias expresas a este tipo de ilícitos se encuentran en los artículos 127 bis (regulador de las consecuencias accesorias del delito), que señala como tales a los de los "apartados 2 y 3 del artículo 197 y artículo 264" (sancionadores del descubrimiento y revelación de secretos y daños informáticos, respectivamente); y en el artículo 573.2 (referente a los anteriores delitos cuando se cometan para facilitar el terrorismo).

La realidad socio-jurídica nos empuja a deducir que existen muchas más modalidades de delitos que son susceptibles de cometerse por vía informática, como, por ejemplo, la estafa, la falsedad documental y la pornografía infantil. En este sentido, el legislador ha optado por el tratamiento penal del medio empleado para cometer el delito dentro del articulado en el que se castigan ciertas conductas, en lugar de tipificar una acción u omisión cometida por medios informáticos como delito individual. En

definitiva, se reconoce a las TIC como medio idóneo para la acometida de delitos ya tipificados, acercando la regulación penal a la realidad social.

En lo que interesa al presente trabajo, el delito de estafa del artículo 248 C.P. constituye un ejemplo magnífico de lo expuesto, habida cuenta que, tras establecer el "tipo base", su ordinal 2º recoge como tipo especial el siguiente tenor literal:

> "2. También se consideran como reos de estafa:
>
> a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro".

En consecuencia, debemos concluir que los "delitos informáticos" no existen, porque para que ello sea posible deben estar tipificados como tales en el Código Penal. No obstante, se permite la alusión en estos términos respecto a conductas u omisiones efectuadas a través de las TIC.

La continuación del examen del concepto que da nombre a este apartado obliga a exponer las conclusiones que la razón alcanza cuando lo efectúa. Tomando como punto de partida el itinerario de un procedimiento penal a efectos de determinar las características del término, los delitos cometidos a través de Internet presentan ciertas dificultades en la incoación del procedimiento, en la fase de instrucción y en su enjuiciamiento.

Sin ánimo de incurrir en reiteraciones innecesarias, basta decir, como muestra de tales contingencias (serán objeto de análisis exhaustivo en el Capítulo II) que estas infracciones precisan de la readaptación del concepto "lugar de comisión del delito", ya que no es posible ubicar desde el punto de vista clásico la realización de la acción. Asimismo, la víctima debe contar con conocimientos mínimos y medios materiales suficientes para la recolección de pruebas que acrediten ciertos indicios de la presunta comisión de la acción gravosa, hecho por el que finalmente estos asuntos terminan en manos de la Brigada de Investigación Tecnológica de la Policía Nacional en fase de instrucción. Finalmente, es necesaria la formación de los Jueces y Magistrados en esta materia[31], ya que muchos de ellos carecen de conocimientos suficientes como para comprender lo que un perito informático pueda exponer en un informe y posterior comparecencia en juicio, y finalmente dictar una resolución conforme a Derecho que cumpla con las exigencias derivadas del derecho a la tutela judicial efectiva.

2.4.2. CIBERDELINCUENTES: CONCEPTO Y PERFIL DEL *CRACKER*

En los últimos tiempos, resultan bastante frecuentes las referencias a piratas informáticos con ocasión de los ciberataques perpetrados, que se han vuelto un plato recurrente en la prensa diaria. En este sentido, llama poderosamente la atención la referencia a éstos con el término *hacker*, error en el que también incurre la Real Academia de la Lengua Española.

Las figuras analizadas tienen su origen en el ámbito de la ingeniería informática, de tal manera que tanto *hackers* como *crackers* son expertos en acceder, monitorizar y llevar a cabo el mantenimiento de los sistemas informáticos. No obstante, a mediados de

[31] **Dans, Enrique**. *Sobre los jueces y la ignorancia*. Blog de Enrique Dans. 2 de julio de 2008. Recuperado de: https://www.enriquedans.com/2008/07/sobre-los-jueces-y-la-ignorancia.html.

la década de 1980 comenzaron a surgir individuos cuyo entretenimiento consistía en la violación de los mecanismos de seguridad de estos sistemas con objetivos dispares. Frente a ellos, los expertos en ciberseguridad que se encontraban dentro de la esfera legal de sus funciones acuñaron el término *cracker*[32] para referirse a los primeros, mientras que ellos patrimonializaron el concepto de *hacker*.

De esta forma, frente a los *hackers* (cuya función principal es solventar los problemas de seguridad de los sistemas), podemos definir a los *crackers*, también conocidos como "sombreros negros" o "piratas informáticos", como las personas que profanan la seguridad de un sistema informático sin consentimiento del usuario para obtener información que utilizarán con fines espurios y que redundarán en su propio beneficio.

En analogía con lo sucedido con los tipos de *phishing* (recordemos que se clasifican atendiendo a los métodos utilizados para infectar el sistema y a la clase de potenciales víctimas a los que van dirigidos), los *crackers* se catalogan dependiendo de la parte del sistema en la que estén especializados sus ataques y del lugar desde el que los perpetran[33]. Por ejemplo, existen individuos expertos en intervenir comunicaciones telefónicas (*phreakers*), en alterar la configuración de sitios *web* (*cyberpunks*) o parte de un *software* (*crackers* de sistemas), o que prestan sus servicios dentro de una empresa a la que atacan desde dentro de sus sistemas (*insiders*).

La motivación que empuja a este colectivo a violar los sistemas de seguridad de particulares y empresas es de carácter dispar y varía según los conocimientos que haya adquirido. En este sentido, un *cracker* novel estará capacitado para programar un ataque de *phishing* sencillo contra una persona o un colectivo determinado de ellas con el objetivo de que le faciliten sus datos bancarios y enriquecerse a costa del patrimonio de las víctimas mediante transferencias de cantidades pequeñas de dinero, pero no podrá violar los sistemas de seguridad del Gobierno de una nación sin ser detectado.

En muchas ocasiones, la motivación subyacente en la actuación de estos individuos no es tanto el enriquecimiento injusto, sino la reivindicación de una causa que creen justa[34], la simple diversión (aderezada por grandes cantidades de ego) o el desafío, mayoritariamente ejercitado a instancias de los Gobiernos contra otras organizaciones gubernamentales por motivos políticos o estratégicos. Resulta anecdótico que, pese a su ocupación, finalmente muchos de estos *crackers* (que

[32] El *T1.523-2001, Telecom Glossary 2000* define el término *cracker* como "alguien que rompe la seguridad de un sistema" y que "con intenciones maliciosas, obtiene o intenta obtener acceso ilegal a computadoras o programas de computadora" (traducción del inglés). El estándar puede ser consultado (salvo excepciones justificadas por derechos de propiedad intelectual) en la página *web* de la organización: https://glossary.atis.org/.

[33] **González, Yolanda**. *Cracker informático. ¿Es lo mismo que un hacker?* Grupo Atico34. 4 de septiembre de 2020. Recuperado de: https://protecciondatos-lopd.com/empresas/cracker-informatico/.

[34] Una muestra de este tipo de motivación es el caso WikiLeaks, sitio *web* fundado y dirigido por el programador australiano Julian Assange. Durante los años 2010 y siguientes, este *site* filtró y publicó documentos emitidos por el Gobierno de EEUU como "información clasificada". En la actualidad la web se encuentra inactiva, a la espera de que se resuelva el procedimiento incoado contra Assange, sobre el que se ha emitido una acusación por 17 delitos informáticos.

Scarpellini, Pablo. *Diez años de WikiLeaks: de poner en jaque a gobiernos, al silencio informativo*. El Mundo. 26 de julio de 2010. Recuperado de: https://www.elmundo.es/internacional/2020/07/26/5f1c6ffdfdddff71ba8b45db.html.

comienzan muy jóvenes en el "oficio") se reforman y son fichados por grandes empresas dedicadas a la seguridad en Internet[35].

[35] **Quevatre, Chris**. *Los hackers criminales rehabilitados que ahora se enfrentan contra delincuentes de Internet*. BBC News. 5 de abril de 2019. Recuperado de: https://www.bbc.com/mundo/noticias-47813809.

3. CAPÍTULO SEGUNDO: EL DELITO DE ESTAFA DEL ARTÍCULO 248.2 DEL CÓDIGO PENAL, O *PHISHING*

3.1. INTRODUCCIÓN

Tal como se ha expuesto en el Capítulo I del presente trabajo, resulta evidente que el matrimonio compuesto por los sistemas informáticos e Internet es idóneo para cometer determinados delitos, carácter del que se aprovechan los *crackers* para alcanzar su objetivo, que se identifica con el bien jurídico protegido de cada uno de los tipos susceptibles de comisión.

Ejemplificada esta gama de ilícitos en los epígrafes anteriores (véase "2.1. El delito informático"), la continuación del trabajo y redacción del presente Capítulo se encuentran inspiradas en nuestra realidad jurídico - social. En efecto, según el último Estudio sobre la Cibercriminalidad en España publicado por el Ministerio del Interior[36], los **fraudes informáticos** constituyen el **88,1% de los delitos cometidos a través de la Red**, por encima de los delitos sexuales cometidos por esta vía y de los daños informáticos derivados de la infección por *malware*.

Entre este tipo de ilícitos, existe un método para cometer el delito de estafa que en los últimos tiempos ha cobrado especial importancia, tanto por el aumento de ciberataques perpetrados a través de esta fórmula, como por su alta tasa de éxito: el *phishing*.

Evocando el contenido del Capítulo I ("1.2. Terminología básica en la normativa comunitaria y española; 1.2.4. *Phishing*"), los piratas informáticos utilizan en la construcción del ataque citado técnicas de ingeniería social con el fin de desorientar al usuario-objetivo, de manera que pase por alto su deber de comprobación de la veracidad del remitente del mensaje y facilite a través de su comportamiento datos sensibles que permitirán a los primeros acceder a su patrimonio y obtener beneficios a su costa.

Como se ha expuesto con anterioridad, estas técnicas son confeccionadas teniendo en cuenta el perfil de la víctima/s, de forma que, con independencia de su nivel de estudios, el ataque estará abocado al éxito. En este sentido, existe una evidente dicotomía entre el uso de los sistemas informáticos -muy universalizados como consecuencia del tránsito de la vida analógica a la digital- y la formación y concienciación en el ámbito de la ciberseguridad, que se encuentra apoyada en la apariencia garantista de unos medios a través de los que la amenaza no es física[37] ni, por tanto, palpable.

Como consecuencia de lo expuesto, la conducta descrita es reprochable desde el punto de vista social, pero, como se ha adelantado, también desde la perspectiva jurídica. Así

---

[36] Según los datos contenidos en el Estudio mencionado, el número de fraudes o estafas cometidas a través de medios informáticos documentados durante el año 2019 fue de 192.375, de los que más de 70.000 fueron registrados en Cataluña y la Comunidad de Madrid. Además, es interesante reseñar que el pódium de estos ilícitos se encuentra encabezado por las estafas bancarias.

Ministerio del Interior, Secretaría de Estado de Seguridad. *Estudio sobre la Cibercriminalidad en España*. Año 2019. Recuperado de: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Documents/2020/070620-cibercriminalidad.pdf

[37] **Meneses, Nacho**. *Cada vez más digitalizados, pero menos protegidos*. El País. 10 de junio de 2020. Recuperado de: https://elpais.com/economia/2020/06/10/actualidad/1591770763_800020.html

lo dispuso en su día la Decisión Marco del Consejo, de 28 de mayo de 2001[38], que ha sido sustituida por la Directiva (UE) 2019/713, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo[39].

Por todo ello, el objeto del presente Capítulo será realizar un estudio técnico-jurídico del *phishing*, que será abordado de manera artesanal partiendo de su subsunción en el artículo 248.2 C.P.

Siguiendo la clásica teoría del delito, se efectuará un análisis de los tipos objetivo y subjetivo del ilícito a través de la jurisprudencia, así como de las diferentes modalidades comisivas posibles desde el punto de vista informático. Para completar el estudio de la conducta de los sombreros negros, se observarán las eventuales circunstancias modificativas de la responsabilidad criminal que pueden incurrir en ella. Asimismo, sin perjuicio de las cuestiones de competencia judicial derivadas de las peculiaridades que el ilícito presenta en su comisión y de la eventual responsabilidad de las entidades bancarias que custodian el patrimonio sustraído, la parte final de este trabajo se centrará en las particularidades que presenta el delito mencionado en cuanto a su investigación y enjuiciamiento.

En definitiva, se pretende ofrecer un estudio global del delito de estafa informática cometida a través del método *phishing*, que abarcará su desglose desde el punto de vista jurídico-penal y procesal.

3.2. ANÁLISIS JURÍDICO-PENAL DEL TIPO

3.2.1. ANÁLISIS DEL TIPO OBJETIVO

3.2.1.1. BIEN JURÍDICO PROTEGIDO

Para comenzar con el estudio del ilícito mencionado es necesario efectuar una remisión al bien jurídico objeto de protección por parte del legislador a través de la tipificación de una conducta determinada y reprochable. Sin embargo, determinar cuál es en el caso concreto no es posible sin analizar previa y brevemente la acción (será objeto de análisis en el epígrafe "2.1.3. Acción típica").

En este sentido, y sin ánimo de incurrir en reiteraciones innecesarias, procede exponer el comportamiento que debe exhibir el sujeto activo (denominado *phisher*) para que aquél pueda ser subsumido en el ilícito penal objeto de estudio. Como se ha expuesto con anterioridad, el *phishing* consiste en el envío de *emails*, SMS o en la

---

[38] Decisión marco 2001/413/JAI del Consejo, de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo. Recuperado de: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32001F0413

"Artículo 3:

> Cada estado miembro adoptará las medidas necesarias para garantizar que las siguientes conductas sean delitos penales cuando se produzcan de forma deliberada: realización o provocación de una transferencia de dinero o de valor monetario (...) mediante: la introducción, alteración, borrado o supresión indebidas de datos informáticos especialmente datos de identidad, y la interferencia indebida en el funcionamiento de un programa o sistema informáticos".

[39] 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. Recuperado de: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A32019L0713

realización de llamadas que se envían suplantando la identidad de otras personas o entidades, con el objetivo de que el usuario ofrezca al *phisher* acceso a sus datos (generalmente bancarios); esta llave será utilizada por el pirata informático para realizar transferencias desde la cuenta bancaria de la víctima hasta otra, que habitualmente será propiedad de un tercero[40]. En definitiva, esta conducta implica un acto de disposición sobre el patrimonio ajeno (de la víctima), sin perjuicio de que el *malware* incluido en el mensaje enviado y descargado por el usuario pueda ocasionar daños en el sistema informático[41] invadido.

Como consecuencia de esa expoliación, el legislador ha optado por incluir la acción en el Capítulo VI "De las defraudaciones" de nuestro Código Penal, concretamente en la redacción del artículo 248, apartado 2º. Por tanto, situándose la citada conducta entre las tipificadas en el Capítulo que tiene por objeto sancionar aquellas acciones contra el **patrimonio**, debemos concluir que no es otro el bien jurídico protegido a través de la dicción del mencionado precepto.

Ejemplo de lo expuesto, entre otras, es la STS nº 421/2014, de 26 de mayo[42], que desestimó las peticiones de los recurrentes en casación, condenados por un delito continuado de estafa agravada por urdir un plan a través del que se hacían pasar por agentes inmobiliarios que convencían a terceros de solicitar préstamos para invertirlos en operaciones inmobiliarias de alta rentabilidad; posteriormente, los estafadores percibían para sí la cuantía de los préstamos y eran los estafados los que debían abonarlos a las entidades bancarias. El pronunciamiento dice lo siguiente (FJ Segundo):

> "Conviene tener presente que el bien jurídico protegido del delito de estafa no es la propiedad de lo defraudado. De razonar así estaríamos confundiendo el objeto material de la acción con el bien jurídico tutelado. Lo que se protege mediante la incriminación del delito de estafa no es otra cosa que el patrimonio, entendido éste como una universalidad, como un conjunto dinámico, funcionalmente dirigido a satisfacer las necesidades del titular."

Para concluir, es necesario mencionar que, en los últimos tiempos, ha surgido una corriente doctrinal que ha expresado la necesidad de la consagración de un bien

---

[40] En el argot policial, el tercero que recibe las transferencias a través de las que el *phisher* pone a buen recaudo las cantidades extraídas del patrimonio de la víctima se denomina "mulero", figura que será objeto de estudio en el epígrafe "2.1.4. Autoría y participación".

[41] Con frecuencia, el delito de estafa informática en su modalidad de *phishing* es imputable a su autor en conexión con un delito de daños informáticos, tipificado en el artículo 264 C.P. Pensemos en un *email* que el *cracker* remite a la víctima en nombre de una entidad bancaria, en el que se adjunta un archivo a través del que supuestamente se le pone al corriente de una situación irregular en su cuenta. Habitualmente, ese archivo es el asistente de ejecución del *malware* elegido por el *cracker* para extraer los datos del sistema atacado, por lo que, en cuanto la víctima lo descargue, estará auto infectando su propio sistema.

El delito de daños informáticos tendría acogida en esta acción si, por ejemplo, el *malware* descargado fuese del tipo *ransomware*, ya que la característica fundamental que presenta es el bloqueo del sistema a cambio de un rescate (de este modo, el *phisher* bloquea el sistema y aprovecha tal coyuntura para aprehender los datos bancarios del usuario). Esta conducta se podría encuadrar en lo preceptuado por dicho artículo cuando manifiesta que "el que por cualquier medio, sin autorización y de manera grave (…) hiciese inaccesible datos, programas informáticos o documentos electrónicos ajenos (…)".

[42] STS (Sala Segunda) nº 421/2014, de 26 de mayo. Recuperada de https://www.poderjudicial.es/search/AN/openDocument/5ed8cec8965eab4a/20140613.

jurídico común para todos los "delitos informáticos"[43]: la información y la seguridad de los sistemas informáticos. De esta manera, se añadiría al panorama jurídico-informático un nuevo valor susceptible de salvaguarda de carácter supraindividual, que, ante la comisión del delito, concurriría junto a los bienes objeto de especial protección que dotan de sentido a la existencia de los tipos penales en los que cada uno de los "delitos informáticos" se encuentran previstos (recordemos que no existen por sí mismos, habida cuenta que no están tipificados como tales en el Código Penal).

3.2.1.2. OBJETO MATERIAL

El estudio de los elementos que componen la estructura del citado delito es indivisible de la naturaleza del soporte que da cobertura a su comisión, y que ha sido expuesto en el Capítulo I del presente trabajo: los sistemas informáticos. Estos efectos están dotados de caracteres propios y especiales -intangibilidad de los datos y de los "lugares" en los que se registran, o el anonimato que protege a los ciberdelincuentes, entre otros- que los revisten de complejidad a la hora de desgranar su repercusión jurídico-penal.

Habiendo determinado que el *phishing* es una estafa especial que por sus particularidades se subsume en el consabido artículo 248.2 C.P., la lógica invita a comenzar el razonamiento que nos ocupa realizando una comparación entre los objetos materiales del denominado delito de estafa informática y el correspondiente a la estafa "básica".

Sin perjuicio de lo expuesto por el legislador en la dicción del artículo 248, la jurisprudencia se ha encargado de determinar en el caso concreto cuál es el elemento afectado por la acción típica en la estafa común cotejándolo con el objeto formal del ilícito, que no es otro que el bien jurídico lesionado. Muestra de ello son, entre otras, la SAP Alicante nº 408/2019, de 4 de noviembre[44]; la SAP Madrid nº 197/2020, de 20 de mayo[45]; SAP Vizcaya nº 26/2020, de 29 de abril[46]; o la SAP Barcelona nº 229/2020, de 30 de marzo[47].

La primera de las resoluciones citadas es especialmente gráfica en cuanto a dicha definición, ya que en su FJ Segundo el Tribunal dispone que el acto de disposición inconsentido y castigado en el consabido artículo 248.2 C.P. podrá afectar o desplegarse sobre cualquiera de los elementos que se encuentren integrados dentro del patrimonio de la víctima. Si acudimos al grueso de nuestra jurisprudencia y observamos la práctica habitual del sector del *cracking*, daremos con que el objeto de deseo de los ciberdelincuentes especialistas en la emisión de campañas de *phishing* es el patrimonio

---

[43] Entre otros: QUINTERO OLIVARES, G. *Internet y Derecho Penal. Imputación de los delitos y determinación de la competencia*. La Ley Penal: revista de derecho penal, procesal y penitenciario. Sección Estudios. Nº 37. 2007.

[44] SAP Alicante (Sección 2ª) nº 408/2019, de 4 de noviembre. Recuperada de https://www.poderjudicial.es/search/AN/openDocument/79d7b8a5db9c11b1/20201029.

[45] SAP Madrid (Sección 15ª) nº 197/2020, de 20 de mayo. Recuperada de https://www.poderjudicial.es/search/AN/openDocument/a34e5780f8cfde63/20201102.

[46] SAP Vizcaya (Sección 2ª) nº 26/2020, de 19 de abril. Recuperada de https://www.poderjudicial.es/search/AN/openDocument/b7f2b598b1a4e7c3/20210305.

[47] SAP Barcelona (Sección 2ª) nº 229/2020, de 30 de marzo. Recuperada de https://www.poderjudicial.es/search/AN/openDocument/33d326106d348fa8/20200706.

monetario ajeno, del que disponen sin miramientos a través de transferencias bancarias en beneficio propio y, naturalmente, sin consentimiento de la víctima.

En definitiva, "objeto material" será cualquiera de las cosas que se encuentran incluidas en el patrimonio propiedad del afectado y sobre las que el sujeto activo del delito haya desplegado la acción. Por ejemplo, en el supuesto de hecho descrito en el apartado anterior, no genera dudas que el objeto material del ilícito son las cantidades de dinero que los condenados sustrajeron de las víctimas bajo engaño en concepto de abono de unos presuntos préstamos. Si ahondamos en esta cuestión, observamos que el Código Penal no se limita a consagrar un tipo básico, sino que añade subtipos agravados que se diferencian de su matriz por el ente que sirve de diana a la conducta sancionada: por ejemplo, atendiendo a lo preceptuado en el artículo 250, destina penas distintas en caso de que los bienes afectados sean de primera necesidad, integren el patrimonio artístico[48] o estén valorados en más de 50.000 euros.

En cuanto al objeto material del *phishing*, no podemos si no concluir que posee la misma naturaleza que el de la figura que lo antecede en tratamiento en el presente trabajo. El apoderamiento ilícito de cantidades dinerarias es al delito de estafa (en todas sus modalidades comisivas) lo que los documentos o las cuentas anuales a los delitos de falsedad documental y societarios: su piedra angular.

Sobre la sustracción de estos efectos patrimoniales como pilar del reproche penal se pronuncia, entre otras[49], la SAP Barcelona nº 347/2017, de 24 de abril (FJ Séptimo)[50]:

> "Con relación al nuevo art. 248.2 hay que entender que dicho fraude informático no contempla la sustracción de dinero a través de la utilización no

[48] **Martínez, Santiago**. *Introducción sobre el delito de estafa mediante las obras de arte (II): análisis jurisprudencial*. Law&Trends. 22 de febrero de 2019. Recuperado de: https://www.lawandtrends.com/noticias/penal/introduccion-sobre-el-delito-de-estafa-mediante-las-obras-de-arte-ii-analisis-jurisprudencial-1.html

[49] Muestra de este "deber ser" es la jurisprudencia sobre la temática tratada emitida por la Sala Segunda del Alto Tribunal, que, lejos de efectuar un análisis pormenorizado de este elemento, ha erigido la materialización del ánimo de lucro del *phisher* como su razón de ser última para realizar la conducta típica. De este modo, excluye la manipulación informática o artificio semejante de la finalidad perseguida por el sujeto activo, erigiéndose éstos únicamente como los procedimientos a seguir para conseguir el citado fin. Esta forma de concebir los aludidos mecanismos converge con la atipicidad de los mal llamados "delitos informáticos", entre los que la estafa únicamente tiene de "informática" los medios a través de los que se comete.

Entre otras, podemos señalar la Sentencia de la Sala de lo Penal del Tribunal Supremo nº 2175/2001, de 20 de noviembre (FJ Primero):

> "La actual redacción del art. 248.2 del Código Penal permite incluir en la tipicidad de la estafa aquellos casos que mediante una manipulación informática o artificio semejante se efectúa una transferencia no consentida de activos en perjuicio de un tercero admitiendo diversas modalidades, bien mediante la creación de órdenes de pago o de transferencias, bien a través de manipulaciones de entrada o salida de datos, en virtud de los que la máquina actúa en su función mecánica propia".

La resolución ha sido recuperada de https://www.poderjudicial.es/search/AN/openDocument/1a6d6edff892eb94/20031203.

[50] SAP Barcelona (Sección 9ª) nº 347/2017, de 24 de abril. Recuperada de https://www.poderjudicial.es/search/AN/openDocument/f96884c89b48c8dc/20170621.

> autorizada de tarjetas magnéticas sobre los denominados "cajeros automáticos", porque la dinámica comisiva no aparece alejada de la clásica de apoderamiento, aunque presenta la peculiaridad de la exigencia del uso de la tarjeta magnética para poder acceder al objeto material del delito".

De esta manera, la manipulación informática o artificio semejante empleados por el sujeto activo para cometer el delito son meros cauces para alcanzar el objetivo final (serán objeto de tratamiento en el epígrafe "2.1.3. Acción típica"), que no es otro que incorporar a su patrimonio un activo monetario propiedad de la víctima, movimiento que, además, en la figura objeto de tratamiento se concreta en la realización de transferencias no consentidas vía *online*.

3.2.1.3. ACCIÓN TÍPICA

Como quiera que la teoría jurídica del delito exige que para que una conducta sea castigada por la jurisdicción penal debe ser típica, antijurídica y culpable, cabe, en primer término, comenzar el juicio de tipicidad descifrando la acción incluida en la parte positiva del tipo analizado. Al igual que lo sucedido con el estudio del bien jurídico protegido y el objeto material del delito, la disertación no puede sino realizarse desde el cotejo con el delito de estafa básico, toda vez que, como se deriva de la exposición realizada, el *phishing* es una defraudación perpetrada a través de la informática.

Tal como se ha referido en el Capítulo I, se trata de una técnica a través de la que el *cracker* (también denominado *phisher*) realiza un envío individual o masivo de *emails* o SMS a un usuario o grupo determinado de ellos haciéndose pasar por otra persona o entidad, a través del que utiliza el engaño para alentar a la víctima a facilitarle sus datos (generalmente bancarios) sin que ésta sea consciente de que las intenciones del remitente son arteras. No obstante, los Tribunales han incardinado también dentro de la estafa informática las defraudaciones cometidas a través de máquinas recreativas o "tragaperras" por el mero hecho de la naturaleza electrónica del instrumento a través del que se ejecuta la acción[51], así como la realización de llamadas telefónicas en las que el

[51] Esta modalidad comisiva del delito de estafa se desarrolla a rebufo con la implantación de las primeras máquinas de este tipo en nuestro país. Sin embargo, el ejercicio jurisprudencial sobre la incursión de esta conducta típica en el tipo regulado en el artículo 248 C.P. data de la década de los 2000. Esta actividad de los Tribunales, especialmente de las Audiencias Provinciales, experimentó un repunte entre los años 2010 y 2020, ínterin del que datan la mayoría de resoluciones dictadas sobre la materia y que coincide con la extensión del uso de Internet y de las nuevas tecnologías a un rango más amplio de población, independientemente de su edad y condición social.

El espectro de comportamientos que abarca la acción típica es variopinto. Desde la técnica del empujón que causa el bloqueo de la máquina, momento en el que el sujeto activo aprovecha que el encargado de su gestión intenta restablecerla para acceder al menú y obtener entregas de dinero sin juego previo (SAP Zaragoza nº 85/2014, de 19 de febrero. Recuperada de https://www.poderjudicial.es/search/AN/openDocument/1f9273cc74b7b71d/20140325); pasando por el vaciado de la máquina mediante la solicitud de devolución del crédito previamente introducido consistente en monedas y billetes sin tintar (SAP Castellón nº 313/2009, de 20 de julio. Recuperada de https://www.poderjudicial.es/search/AN/openDocument/72837c990d6a2dc1/20100415); por la introducción de una moneda atada a un hilo con el objetivo de que la máquina valide el crédito a la hora de jugar, técnica conocida como "moneda prisionera" (SAP Jaén nº 121/2019, de 28 de mayo. Recuperada de https://www.poderjudicial.es/search/AN/openDocument/8b3b124e7e72e573/20190701); hasta el *hackeo* del artilugio habilitado para acceder al menú de la misma (SAP Las Palmas nº 235/2019, de 29 de junio. Recuperada de https://www.poderjudicial.es/search/AN/openDocument/08a4ebcb3942162b/20190905); lo cierto es que

emisor de las mismas simula ser empleado de una empresa de confianza (*vishing*)[52] con el objetivo de engañar al receptor para que contrate un servicio o producto ficticio.

Del modo de proceder expuesto en primer término se pueden extraer dos planteamientos preliminares: a) El sujeto activo del delito suplanta la identidad de otra persona (ya sea pública o privada) en la comunicación maliciosa; y b) A través de su contenido induce a error a la víctima, que termina cayendo en la trampa y ofreciéndole acceso a su sistema, a sus datos, o a ambos[53]. El cómputo de ambos elementos resulta en un engaño que la jurisprudencia ha acertado en exigir y catalogar como "idóneo" o "bastante" para hacer referencia a la aptitud del embaucamiento ejecutado por el sujeto activo en relación con la inteligencia del ciudadano medio y de sus circunstancias específicas, que individualizan su capacidad de ser engañado (STS nº 465/2012, de 1 de junio[54]). En definitiva, la lógica invita a pensar que es necesario que las artimañas del sujeto activo causen finalmente error en el entendimiento de la víctima, que ofrecerá, en consecuencia, la llave de su patrimonio al *cracker*, el cual procederá a sustraer del mismo diversas cantidades monetarias en beneficio propio y sin consentimiento de su legítimo propietario.

Si desempolvamos el contenido del artículo 248.2 C.P., referenciado en el Capítulo I (2.1. El delito informático), deducimos que la acción descrita se encuadra en su contenido, por lo que procede iniciar el estudio pormenorizado de los elementos que la componen.

En primer término, para estar en presencia de un delito de estafa es absolutamente primordial que el autor engañe suficientemente al perjudicado con el fin de alcanzar un beneficio patrimonial no autorizado. Como ya se ha expuesto, en los supuestos de *phishing* el mecanismo a través del que se transmite el embuste se antoja más laborioso de producir (dependiendo de la modalidad utilizada, consistirá en elaborar una página *web*, campañas de *email*, etcétera); sin embargo, no es este extremo el que plantea incógnitas desde el punto de vista jurídico-penal, sino que es la entidad del sujeto engañado sobre la que han corrido ríos de tinta, tanto en el seno de la doctrina como de la jurisprudencia.

---

este compendio de procedimientos poseen en común constituir una manipulación de efectos electrónicos, hecho por el que los Tribunales incardinan estas acciones dentro del tipo analizado.

[52] En este sentido, se pronuncia, entre otras, la reciente SAP Madrid nº 412/2020, de 28 de septiembre (J Segundo). Recuperada de https://www.poderjudicial.es/search/AN/openDocument/2362dccd97a59bd8/20210107.

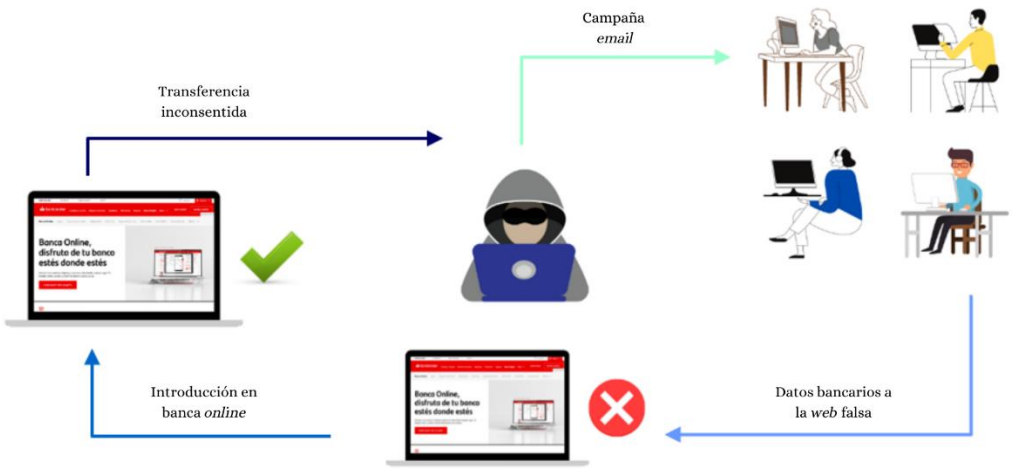
[53] El *phisher* tendrá acceso al sistema de la víctima o no dependiendo de si:

- El mensaje fraudulento va seguido de otro ciberataque consecuencia de la acción solicitada por el *cracker*. Pensemos en un *link* o documento adjuntos a la comunicación que han sido programados para activar la instalación de un troyano en el sistema cuando el usuario haga *click* en ellos, de manera que otorgará al ciberdelincuente el control remoto del mismo.
- Es la víctima la que facilita directamente los datos al pirata introduciendo sus datos en la *web* falsa creada en apariencia de fiabilidad por aquél (práctica denominada *web spoofing*). Por ejemplo, si en el mensaje se adjunta un enlace que lleva a una *web* igual a la del Banco Santander y el usuario escribe los datos de acceso a su cuenta en la banca *online* de dicho banco.

[54] STS (Sala Segunda) nº 465/2012, de 1 de junio. Recuperada de https://www.poderjudicial.es/search/AN/openDocument/bd0a5643f18570c6/20120615.

En este sentido, fue la promulgación del actual Código Penal la que marcó un antes y un después en la concepción del engaño llevado a cabo a través de medios informáticos, ya que hasta entonces no existía precepto alguno que regulase dicha modalidad comisiva. Antes de la entrada en vigor de la citada norma, las actuaciones subsumibles en el actual artículo 248.2 eran examinadas bajo la perspectiva ofrecida por el artículo 528 del Código Penal de 1973[55], que exigía que para determinar la comisión de un delito de estafa era necesario que el engaño fuese producto del ingenio de una persona y estuviese dirigido hacia otra, ficción mendaz que, como tendremos ocasión de analizar, en el *phishing* tiene un doble objetivo.

Para facilitar la comprensión de este extremo, se expondrá la problemática asistiéndola con la muestra de un ciberataque de la clase considerada: "A", aficionado a la informática, decide poner en práctica sus capacidades y, aprovechando el inicio de la campaña de recaudación del IRPF, elabora un modelo de *email* dirigido a varios contribuyentes españoles en los que se hace pasar por una entidad bancaria (utilizando sus signos distintivos) y apercibe a los destinatarios de que, debido a un error en los sistemas del banco, no se pueden ejecutar las domiciliaciones a través de las que se debería realizar el pago del impuesto, por lo que deben facilitar las claves de su banca *online* para que la entidad pueda ordenar la realización de esos pagos a través del acceso ofrecido en el enlace adjunto al mensaje. "B", que recibe en su bandeja de correo electrónico ese mensaje, hastiado por tener que resolver el trámite un año más, hace *click* en el enlace e introduce en la *web* a la que le ha dirigido sus datos bancarios. Días después, "B" accede a su banca *online* y advierte que se han efectuado varias transferencias a una cuenta desconocida, pero que él no las ha ordenado.



Formulado el supuesto de hecho, distinguimos en el comportamiento del autor, incardinado en el *iter criminis*, tres momentos bien diferenciados: a) Los actos preparatorios, integrados por la confección del *site*, de la campaña de *email* y su

[55] La dicción del mencionado artículo 528 recogido en el derogado Decreto 3096/1973, de 14 de septiembre, por el que se publicó el Código Penal, texto refundido conforme a la Ley 44/1971, de 15 de noviembre, clarifica la naturaleza de los sujetos que pueden intervenir en la acción, ya sea de manera activa como pasiva. De este modo, se preveía implícitamente que únicamente las personas físicas podían ser víctimas de un delito, dejando fuera del espectro penal los supuestos objeto de análisis en el presente trabajo. Recuperado de: https://www.boe.es/buscar/doc.php?id=BOE-A-1973-1715.

vinculación; b) La exteriorización de su voluntad defraudatoria, llevada a cabo a través del envío de la campaña portadora del engaño (tentativa); y c) La consumación, habida cuenta que a través de los datos bancarios facilitados por "B" ha efectuado transferencias inconsentidas de activos monetarios en perjuicio de la víctima. En definitiva, el dinero se obtiene de forma engañosa a través de una maquinación. Es evidente que el perjudicado es la persona que ve quebrantado su patrimonio, pero la identidad del sujeto engañado, como se ha adelantado, ha sido objeto de controversia.

Partiendo de la base de que lo innato a la estafa es que la distracción patrimonial perjudicial la efectúa el propio perjudicado[56], debemos tener presente que en los supuestos de *phishing* éste únicamente ofrece al pirata informático acceso a sus datos o a su sistema, siendo el ordenador o sistema central de la entidad bancaria donde éste tiene alojada su cuenta quien da curso a la orden emitida. Debe traerse a colación en este extremo lo manifestado sobre el fin bígamo de la insidia, ya que ésta debe pasar dos filtros para alcanzar el objetivo al que sirve: 1) El perjudicado, para que facilite sus claves sin ser consciente del fin para el que le son solicitadas, y 2) La entidad bancaria, frente a la que el *phisher* se hace pasar por el titular de la cuenta sobre cuyos activos dispone; a mayor abundamiento, el segundo embaucado ostenta la categoría de máquina y no es susceptible de ser engañado vía psicológica. En este sentido, la jurisprudencia ha sido vehemente al concepto del sujeto pasivo, declarando en numerosas ocasiones que únicamente puede serlo el titular del bien jurídico lesionado, esto es, el del patrimonio socavado.

Ahora bien, el citado enredo debe haberse ejecutado a través de lo que el C.P. ha denominado "manipulación informática o artificio semejante", elemento que la jurisprudencia ha tildado de excepcionalmente casuístico al existir infinitas modalidades para ejecutarlo, y que gira sobre un eje determinante: la aptitud del medio informático en cuestión para producir el daño patrimonial[57], que, además, se articula como nexo causal invisible entre el engaño y la producción del resultado gravoso[58]. De este modo, resultarán indiferentes las particularidades del itinerario delictivo elegido por el pirata informático siempre que en él se hayan adulterado los fines de la informática para tornarlos en beneficio de la consecución delictiva. En definitiva, serán manipulaciones informáticas ilícitas tanto las acciones del *phisher* a través de las que modifique un programa o sistema (por ejemplo, a través de la infección del sistema por *ransomware*), como las que consistan en su utilización sin el preceptivo permiso (acceso a la banca *online* del perjudicado, robo de la tarjeta de débito y su clave para retirada de efectivo en un cajero), siempre que lo haga buscando su propio enriquecimiento.

Teniendo en cuenta que esta adulteración de los efectos informáticos y el engaño deben coexistir, no puede sino concluirse que el engaño del perjudicado es esencial, mientras que el infligido a la máquina o sistema es instrumental para la consumación del delito. En este sentido, la actuación del autor sobre la máquina no puede ser comprendida como un engaño al uso, toda vez que los aparatos electrónicos no poseen capacidad ni voluntad para ser víctimas de manipulaciones de índole psicológica (de

[56] STS (Sala Segunda) nº 369/2007, de 9 de mayo, FJ Cuarto. Recuperada de https://www.poderjudicial.es/search/AN/openDocument/45bf2634bf3ee393/20070607

[57] STS (Sala Segunda) nº 509/2018, de 26 de octubre, FJ Segundo. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/c3f1f6a840993eef/20181109

[58] STS (Sala Segunda) nº 305/2019, de 11 de junio, FJ Tercero. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/b52cd60a75a07a54/20190621

afirmar tal cosa, se estaría asintiendo su participación activa -pero involuntaria- en la consumación del mismo). Por ello, la jurisprudencia ha acertado, en connivencia con el contenido del artículo reseñado, en acordar que en esta clase de ilícitos el engaño se subsume en la manipulación informática[59], ya que es la máquina la que efectúa el movimiento dinerario en favor del *phisher* o de un tercero[60] impulsada por un código de actividad automatizado, que se pondrá en marcha como consecuencia de la solicitud del ordenante que suplanta la identidad del propietario de la cuenta, o que ha alterado el funcionamiento del artilugio haciendo uso de técnicas ladinas.

3.2.1.4. AUTORÍA Y PARTICIPACIÓN

Tras lo expuesto en el anterior epígrafe y atendiendo al concepto restrictivo de "autor" fijado por el artículo 28 C.P., no puedo sino concluir que el *phisher* es el sujeto activo del delito, habida cuenta que es el individuo o el grupo criminal[61] que realiza la conducta típica (véase epígrafe "2.1.3. Acción típica"). Sin embargo, éste no suele ser objeto de control penal, ya que se beneficia de los mecanismos de ocultación propios de la Red -de los que es profundo conocedor- para dificultar o (en muchos casos) imposibilitar su identificación durante la fase de instrucción del proceso penal.

---

[59] *Idem*.

[60] La jurisprudencia ha tenido ocasión de desarrollar ampliamente el alcance y participación de esta figura en el phishing. Ejemplo de ello son las STS (Sala Segunda) nº 834/2012, de 25 de octubre (recuperada de https://www.poderjudicial.es/search/AN/openDocument/36942f02bd94a852/20121224); SAP Ciudad Real nº 159/2012, de 20 de septiembre (recuperada de https://www.poderjudicial.es/search/AN/openDocument/63ff53bad4b5197a/20121204); o la SAP Valencia nº 491/2016, de 5 de septiembre (recuperada de https://www.poderjudicial.es/search/AN/openDocument/7066c58318104256/20180307

[61] Como se ha expuesto en el Capítulo anterior (3.2. Ciberdelincuentes: concepto y perfil del *cracker*), el *phisher* no presenta un único perfil, sino que puede actuar motivado por una pluralidad de objetivos que pueden determinar tanto su conceptualización como delincuentes como su organización interna. De esta forma, es posible que nos encontremos ante el ciberdelincuente persona física o ante una organización o grupo criminal asentados en España o en el extranjero. En el caso de la organización criminal, la jurisprudencia ha tenido ocasión de pronunciarse sobre la concurrencia de los presupuestos regulados en el art. 570 bis C.P., determinando que son: a) conjunto formado por más de dos personas, b) de carácter estable y por tiempo indefinido, c) con concierto y coordinación, o al menos aceptación y sumisión, que alcance la distribución de tareas encaminadas a la comisión del delito. Ejemplo de esta doctrina son la STS (Sala Segunda, Sección 1ª) nº 65/2018, de 6 de febrero (recuperada de: https://www.poderjudicial.es/search/AN/openDocument/23a87414f7531a51/20180412), y la STS (Sala Segunda, Sección 1ª) nº 51/2020, de 17 de febrero (recuperada de: https://www.poderjudicial.es/search/AN/openDocument/54a1aff4683d8f63/20200707). Por su parte, el grupo criminal se define como la agrupación de más de dos personas que no reúnan alguno de los elementos definitorios de la organización criminal y tengan como fin delinquir (SAP Zaragoza nº 195/2014, de 23 de junio. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/d466da5373041376/20140730). El contenido de ambos delitos arroja una diferenciación de índole cuantitativa y cualitativa, toda vez que, aunque comparten estructura, la organización criminal implica un mayor riesgo para la seguridad del tráfico jurídico que es castigada con más severidad por el C.P.

La calificación de estas uniones cambia en el caso de que la organización esté compuesta únicamente por dos sujetos, en cuyo caso nos hallaremos ante un supuesto de codelincuencia, que también englobará aquellas integradas por más de dos personas pero que hayan sido constituidas de manera fortuita. Sobre este extremo se pronuncia, entre otras, la STS (Sala Segunda, Sección 1ª) nº 350/2019, de 5 de julio (recuperada de: https://www.poderjudicial.es/search/AN/openDocument/b0ec9ff4080fcd7d/20190715).

Son muchos los supuestos enjuiciados en los que se hace patente la concurrencia habitual de más sujetos en el curso de los hechos, por lo que es necesario analizar el alcance de su intervención y la consecuente calificación jurídico-penal de la misma.

En los supuestos de *phishing* suele ser habitual la colaboración de terceros impulsados por un claro ánimo de lucro que, como se ha expuesto, redundará en perjuicio de la víctima. Su participación acostumbra a consistir en constituirse en una suerte de depositarios del activo monetario aprehendido ilegítimamente, para, posteriormente, desprenderse de él a través de servicios como Western Union o MoneyGram[62] en favor de cuentas bancarias domiciliadas en Estados con los que España no cuenta con mecanismos de cooperación judicial (por ejemplo, Rusia o Tailandia): en el argot policial, reciben el nombre de "mulas" o "muleros bancarios"[63].

El modo en que estas personas son "contratadas" aporta al estudio de su participación en el delito la piedra angular sobre la que los órganos jurisdiccionales pivotan para determinar hasta qué punto conocen el origen ilícito de las cantidades que custodian en sus cuentas bancarias. En este sentido, la oferta de "trabajo" más frecuente es emitida a través de llamada telefónica o *email* y promete la obtención de dinero fácil a través de un sistema de "teletrabajo", en el que el receptor únicamente debe acoger cantidades de dinero en una o varias cuentas bancarias de su propiedad (creadas *ad hoc* o preexistentes) de las que se quedará un porcentaje en concepto de remuneración. Obsérvese que nos encontramos ante la única figura participante en la operativa defraudatoria cuya identidad se encuentra al descubierto desde el inicio de la trama, al recibir el dinero en cuentas bancarias cuya titularidad ostenta.

Podemos encontrarnos desde supuestos en los que una persona sin estudios, con dificultades económicas y que no se imagina siquiera que el dinero que va a guardar ha sido receptado sin permiso de su propietario acepta esta oferta, hasta casos en los que un ex empleado de una entidad bancaria la acepta sospechando el origen de dichas cantidades. En definitiva, la formación académica del "mulero" y el conocimiento de la fuente de los activos que custodia se erigen como aspectos fundamentales a la hora de calificar su conciencia como dolosa o imprudente.

Lo cierto es que la doctrina y la jurisprudencia no han logrado alcanzar un acuerdo sobre el tipo de responsabilidad penal que ostentan estos sujetos, concurriendo hasta la fecha tres opiniones correspondientes a tres tipos diferentes que los muleros pueden cometer a través de la conducta reseñada: estafa informática, receptación y blanqueo de capitales.

En lo que respecta al delito analizado en el presente trabajo, el Tribunal Supremo ha declarado en numerosas ocasiones, en sintonía con la corriente doctrinal mayoritaria, que la actuación del mulero contribuye de manera esencial al alcance del

---

[62] El uso de estos servicios no es casual, ya que todos ellos coinciden en permitir realizar envíos de dinero sin identificar al ordenante. Al efecto, la empresa facilita al ordenante un número de identificación, de manera que, para recoger el dinero, el receptor únicamente debe facilitar esa clave y el nombre de la persona que realizó el envío.

Panda Security. *¿Western Union ligado al cibercrimen?* 20 de mayo de 2010. Recuperado de: https://www.pandasecurity.com/es/mediacenter/seguridad/western-union-ligado-al-cibercrimen/.

[63] **Rodríguez Caro, María Victoria**. *Estafa informática. El denominado phishing y la conducta del "mulero bancario": categorización y doctrina de la Sala Segunda del Tribunal Supremo*. Noticias Jurídicas. 30 de octubre de 2015. Recuperado de: https://noticias.juridicas.com/conocimiento/articulos-doctrinales/10617-estafa-informatica-el-denominado-phishing-y-la-conducta-del-ldquo;mulero/.

fin del hecho ajeno porque su aportación es *conditio sine qua non* para que el dinero aprehendido sea entregado al *phisher* con éxito[64]; por tanto, será atendiendo al caso concreto cuando se podrá determinar si con su conducta aporta un bien escaso a la consecución del delito o, por el contrario, se trata de una asistencia superflua que, aunque útil, no determina el éxito de la ejecución del hecho principal (en cuyo caso responderá en calidad de "cómplice"). Además, el Alto Tribunal penaliza lo que ha venido a denominar "ignorancia deliberada", determinando que no es posible que la figura tratada desconozca o no sospeche siquiera el probable origen ilícito de los fondos que le son transferidos[65] cuando ignora la identidad de la persona que se los transfiere y de la/s que se los va a transferir, todo ello sin mencionar que de esos fondos extraerá la remuneración correspondiente a la operación. En definitiva, al subsumirse este comportamiento en la dicción del art. 248.2 C.P. ("…consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro"), el Tribunal ha determinado que la actuación del mulero encaja en la figura de la cooperación necesaria regulada en el art. 28 C.P., por lo que será castigado como partícipe a título de cooperador necesario en el delito de estafa informática cometido por el autor y se le impondrá la misma pena que a éste.

Un segundo criterio doctrinal es aquel que considera que la participación del mulero se subsume en el tipo de receptación del art. 298 C.P. Para los adeptos a esta opinión, el mulero desarrolla su aportación en la fase de agotamiento del delito, lo que implica que ya ha sido consumado y que el fin último del mismo ha sido alcanzado (en estos supuestos, será el enriquecimiento de sí mismo o de terceros). Esta fórmula excluye el conocimiento del ilícito previo, pero, por el contrario, requiere de conciencia por parte del mulero de que los efectos de los que dispone en favor de otras personas y de sí mismo son de procedencia ilegal, concretamente, derivados de la consumación de un delito contra el patrimonio, excluyéndose jurisprudencialmente los supuestos en los que concurra mera culpa o sospecha. Este parecer minoritario obliga a discernir cuál es el momento en que se consuma esta estafa, porque si porfiamos por la participación postdelictiva del mulero negaremos que su acción ha contribuido a la obtención del fin perseguido a través de la realización de la acción típica previa, de cuyos efectos pretende aprovecharse[66]. Este pensamiento podría tener una base lógica si llegasen al citado interviniente los efectos económicos sustraídos sin haber ostentado más participación que la de cavilar cómo sacar el máximo partido de ellos, pero, teniendo en cuenta que existe un acuerdo previo en base al que ha facilitado una o varias cuentas bancarias a personas que desconoce para recibir dinero cuyo origen ignora, esta idea hace aguas. Así lo ha entendido el Tribunal Supremo, que, habiendo sentado jurisprudencia en la que fija como consumativo del delito el momento en que se produce el desplazamiento patrimonial[67], se ha decantado por subsumir el

[64] STS (Sala Segunda) nº 834/2012, de 25 de octubre. FJ Segundo. Cit. p. 24.

[65] STS (Sala Segunda) nº 533/2007, de 12 de junio. FJ Primero. Recuperada de: https://www.poderjudicial.es/search/TS/openDocument/8ca791eb038076d3/20070712

[66] **Congil Díez, Almudena**. *Phishing. Problemática relativa a la calificación jurídica de la participación de los denominados "muleros bancarios". Estado actual de nuestra doctrina y jurisprudencia*. El Derecho, Lefebvre. 15 de marzo de 2013. Recuperado de: https://elderecho.com/phising-problematica-relativa-a-la-calificacion-juridica-de-la-participacion-de-los-denominados-muleros-bancarios-estado-actual-de-nuestra-doctrina-y-jurisprudencia-2

[67] Ejemplo de este parecer jurisprudencial es el ATS de 12 de noviembre de 2009, en el que la Sala Segunda del Alto Tribunal resolvió una cuestión de competencia suscitada entre dos Juzgados de

comportamiento del *phisher-mule* dentro de la opción del delito de estafa informática o del blanqueo de capitales, siempre atendiendo a las concretas circunstancias del supuesto de hecho sometido a su conocimiento.

No obstante lo anterior, y realizando una sucinta referencia a lo expuesto al inicio del presente epígrafe, existen resoluciones de carácter anecdótico -debido a su escasez- en las que los órganos jurisdiccionales han calificado como "atípica" la actuación del mulero por hallarse ésta afectada por un error invencible[68], toda vez que los acusados en los procedimientos de los que dimanan carecían de cualificación suficiente para comprender o siquiera suponer que sus acciones podían lesionar el patrimonio de un tercero (entre otras, STS de 3 de diciembre de 2012[69]). Además, para terminar de catalogar al acusado como víctima y no como verdugo, dicha circunstancia aparece acompañada de la ausencia de conocimiento del origen ilícito del dinero.

En último lugar, resta el tratamiento de los supuestos en que los Tribunales han calificado como delito de blanqueo de capitales la contribución del citado partícipe. Para ello, se tomará como ejemplo la resolución antecedente a la referida STS nº 834/2012, esto es, la SAP Audiencia Provincial de Palencia nº 14/2011, de 3 de noviembre[70]. Al igual que lo expuesto en las restantes corrientes doctrinales, la calificación de los hechos como un delito de blanqueo se apoya en la intencionalidad del sujeto a la hora de actuar y su grado de participación en la mecánica defraudatoria. Los adeptos de esta teoría consideran que el mulero no colabora en la acción típica de la estafa informática porque no interviene en la creación y emisión de la manipulación informática necesaria para que la víctima facilite el acceso a su cuenta bancaria, sino que aparece con posterioridad a la consumación del delito de estafa y facilita imprudentemente la ocultación de sus efectos transfiriéndolos a lugares de donde no pueden ser recuperados y devueltos a su legítimo titular.

Como se puede extraer de lo expuesto, para efectuar este juicio de tipicidad de nuevo juega un papel definitivo el conocimiento del origen del dinero y el discernimiento de la trama en la que se encuentra inmerso, de manera que, si se considera probado que el partícipe actuó mediando dolo en su ánimo no procedería una condena a título de autor de un delito de blanqueo de capitales, sino que el título de imputación se mantendría incólume respecto al delito de estafa referido. En definitiva, la jurisprudencia ha declarado que, si atendiendo a su formación y a sus circunstancias personales el mulero pudo suponer que el dinero procedía de un engaño orquestado para obtener un lucro ilícito pero decidió no indagar en este hecho (inobservancia del deber

---

Instrucción situados en localidades diferentes, en el marco de la investigación de dos delitos de estafa informática, uno consumado y otro en grado de tentativa. Para solucionar la cuestión, y dado el momento procesal en el que se planteó la misma, el Tribunal debió determinar anticipadamente el momento en que se consumó el delito acabado para proceder a la aplicación del art. 18.1 LECrim, estimando que dicho instante se concreta con la anotación de la entrada de la transferencia en la cuenta bancaria del mulero, aunque éste no haya dispuesto del dinero con posterioridad.

Recuperado de: https://www.poderjudicial.es/search/AN/openDocument/71668b92ae3eddf9/20091203

[68] La citada problemática será analizada en el epígrafe "2.2. Análisis del tipo subjetivo: el dolo como elemento diferenciador".

[69] STS (Sala Segunda) nº 987/2012, de 3 de diciembre. FJ Cuarto. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/13dd9710e948cd2c/20121228

[70] SAP Audiencia Provincial de Palencia nº 14/2011, de 3 de noviembre. FJ Tercero. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/413db0378f4a7887/20111124

de diligencia exigible, equivalente a una imprudencia grave), no será admisible que blanda en su defensa la citada ignorancia deliberada para evitar ser condenado como reo de un delito de blanqueo de capitales.

3.2.1.5. VÍCTIMA: LA OBLIGACIÓN DE AUTOPROTECCIÓN

Sin ánimo de incurrir en reiteraciones innecesarias, y a pesar de que se ha hecho referencia en los epígrafes precedentes a la posición que ocupa la víctima del delito dentro de la mecánica defraudatoria, es preciso rememorar sucintamente cuál es la repercusión de su actuación y determinar qué grado de observancia le es exigible a efectos de protegerse frente a este tipo de amenazas informáticas.

Como se ha manifestado anteriormente (véase el epígrafe "2.1.3. Acción típica"), el engaño producido a través de la conducta típica se encuentra incardinado en la manipulación informática a través de la que se pretenden conseguir los datos bancarios de la víctima; no obstante, a través de dicha adulteración el *phisher* le envía un mecanismo de acceso a ellos que se encuentra camuflado por un aura de confiabilidad, y a través de cuya activación aquélla dará la clave de acceso a sus datos. Cabe recordar que el sujeto de los inmersos en la trama que recibe el título de "víctima" es el que sufre el detrimento patrimonial consecuencia de la maquinación fraudulenta.

Lo analizado previamente respecto al elemento subjetivo de los delitos de estafa informática, blanqueo de capitales y receptación cometidos por el mulero bancario ofrece al analista un punto de partida sólido para estudiar el alcance de la conducta de la víctima desde el punto de vista del deber de cuidado propio frente a los ciberataques. En efecto, si atendemos a lo que sucede en el *ring* que suponen los procedimientos por estafa informática, un argumento recurrente por parte de las defensas de los investigados es el consagrado "deber de autoprotección", a través del que se pretende atribuir cierto grado de responsabilidad en los hechos a la víctima con fundamento en la imprudencia que ha mostrado al recibir el *email* o SMS sospechoso y fiarse de su contenido.

Lo cierto es que este razonamiento se encuentra justificado en los procedimientos donde resulta probado que el engaño contenido en la manipulación se puede calificar de "burdo" o "estúpido" -y, por tanto, inidóneo para lograr el fin perseguido- atendiendo a múltiples factores o elementos que lo componen y que cualquier persona con un mínimo raciocinio puede apreciar. De esta manera, la credulidad de la víctima en estos supuestos puede ocasionar la atipicidad de la conducta. Pensemos en un *email* presuntamente remitido por una entidad pública española repleto de faltas de ortografía, en un castellano deficiente, encabezado por un signo distintivo de una institución de otro país y dirigido a una persona diferente de la receptora.

En este mismo sentido se ha pronunciado, por ejemplo, la STS nº 845/2014, de 2 de diciembre[71], que hace referencia a la doctrina asentada y emitida por la misma Sala Segunda en un procedimiento por estafa informática. En palabras del propio Tribunal (FJ Duodécimo), "una cosa es la exclusión del delito de estafa en supuestos de engaño *burdo*…y otra que se pretenda desplazar sobre la víctima de estos delitos la responsabilidad del engaño y se le exija un modelo de autoprotección que no está definido en el tipo". Por tanto, de tan gráficas palabras se puede extraer que los

[71] STS (Sala Segunda) nº 845/2014, de 2 de diciembre. FJ Duodécimo. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/32aa4ceb2bf7a528/20150206

supuestos de engaño zafio constituyen la única excepción a la inexigibilidad de autotutela a la víctima.

Dejando de lado esta singularidad, y teniendo en cuenta que el autor del delito de estafa informática actúa mediando dolo en su fuero interno y con el objetivo de que el engaño realizado produzca error en la víctima, la jurisprudencia ha declarado en numerosas ocasiones que el principio de confianza y de buena fe procesal no admite la realización de excepciones que desequilibren la posición de las partes, por lo que en ningún caso podrá cargarse a la víctima con una culpa que no ostenta[72]. Por ello, la comprobación en el caso concreto de la idoneidad del fraude *ex ante* resultará fundamental para determinar si, de haber recurrido la víctima a una mínima comprobación de la fiabilidad del mensaje (sin recurrir a profesionales de la informática o a mecanismos únicamente al alcance de los mismos), podría haberse evitado la consumación del engaño.

3.2.2. ANÁLISIS DEL TIPO SUBJETIVO: EL DOLO COMO ELEMENTO DIFERENCIADOR

Expuesto todo lo anterior, no cabe duda alguna de que la citada manipulación informática no se reduce a la materialización de un mero engaño, sino que su instrumentalización exige un diseño concreto para cuya ejecución se precisan conocimientos informáticos que no son patrimonio del usuario medio. Por ello, no es posible analizar el comportamiento del *phisher* desde la perspectiva de un delito de estafa común, en el que cualquier persona puede ser castigada en concepto de "autor", sino que, como se ha adelantado en los epígrafes precedentes, nos encontramos ante un autor especialmente cualificado cuya preparación exige necesariamente que medie dolo en su conducta para poder ser calificado como tal.

Como de la lógica cabe deducir, la necesidad de la presencia del ánimo deliberado de delinquir no se extrae únicamente de la cualificación especial que se requiere para elevar a físico dicha manipulación, sino más bien de la deducción consistente en que, de no ser deseo del *cracker* el de remitir el producto de su trabajo a terceros con el objetivo de lucrarse a través del acceso que éstos le briden a sus datos bancarios como consecuencia de la apariencia de fiabilidad que aquél presenta, no efectuaría las labores de diseño del método del que se pretende servir para ello. De igual modo, si el sujeto no posee los conocimientos necesarios, aunque desee lucrarse a través de este método todo parece indicar que tendrá ciertas dificultades técnico-cognitivas[73]

---

[72] Ejemplo de ello son las STS (Sala Segunda) nº 229/2007, de 22 de marzo (recuperada de: https://www.poderjudicial.es/search/AN/openDocument/feb3c0fb350b0960/20070419), o la STS (Sala Segunda) nº 482/2008, de 28 de junio (recuperada de: https://www.poderjudicial.es/search/AN/openDocument/32aa4ceb2bf7a528/20150206).

[73] No obstante lo expuesto, en los últimos tiempos abundan en los buscadores accesos a páginas *web* en los que expertos en la materia explican al usuario medio cómo crear y distribuir una campaña de *phishing*, que, lejos de la acepción tratada en el presente trabajo, se trata de un método utilizado también para evaluar, por ejemplo, la aceptación y riesgos de un determinado producto que se pretende lanzar al mercado. Una muestra de este tipo de *sites* es *Hackplayers* o *Redhacking*.

La razón de que los interesados en delinquir a través de esta vía se aprovechen de los conocimientos que los expertos en ingeniería informática se animan a difundir, radica en la *vis atractiva* que constituye el dinero fácil y en las escasas probabilidades de ser acusado y condenado por un delito de estafa informática, toda vez que, como se ha manifestado, el *phisher* se alza como un delincuente anónimo a la sombra de sus colaboradores.

para ejecutar su anhelo. Este parece ser el pensamiento del legislador de 1995, ya que compuso el tipo subjetivo del delito analizado como originalmente doloso y excluyó del mismo la imprudencia al no estar contemplada en el art. 248.2.

El elemento estudiado requiere, además, que el autor actúe o emita dicha manipulación o engaño con el fin de obtener un beneficio económico en perjuicio de tercero; esto se deduce de la propia dicción del precepto mencionado, en el que se exige la obtención del provecho codiciado para apreciar la consumación del delito ("los que, con ánimo de lucro…consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro"). De esta forma, este ánimo se alza como presupuesto específico de concurrencia del tipo, por lo que, de no ser apreciado examinados unos hechos concretos, la conducta del autor podrá ser incardinada en otro tipo (por ejemplo, descubrimiento y revelación de secretos), pero no en el de estafa informática.

Al igual que en la posición del autor del hecho principal (*intraneus*), el dolo juega un papel determinante en la calificación de la actividad del mulero bancario (*extraneus*), que, como se ha expuesto en el anterior epígrafe, podrá ser castigado como partícipe a título de cooperador necesario en el delito de estafa informática principal, como autor de un delito de blanqueo de capitales, o ser absuelto del primero con todos los pronunciamientos favorables.

La primera de las opciones mencionadas implica que el mulero, al recibir la oferta de trabajo y conocer las condiciones del mismo, **se ha representado como probable** que el dinero que debe custodiar y transferir a ciertos desconocidos tiene origen en un hecho ilícito que puede perjudicar a un tercero, pero ha decidido no indagar en la génesis de la trama que puede sostener dicha operación por si se pudiese ver privado de la remuneración que lleva acarreada su participación, además de para alegar desconocimiento en el supuesto de que los hechos lleguen a ser enjuiciados. Nos encontramos, pues, ante la formulación clásica del dolo eventual, sobre la que el Alto Tribunal se ha pronunciado en numerosos momentos con ocasión del examen en sede casacional de supuestos de esta estafa especial[74]; más aún, ese concepto se exige en la modalidad que jurisprudencialmente ha venido en denominarse "doble dolo", por cuanto el *extraneus* deduce: a) Que el dinero procede de la comisión de un delito, y b) Que su acción consistirá en poner a salvo de su legítimo propietario el patrimonio aprehendido, y c) Asume dichas consecuencias como ciertas y propias. En definitiva, y sin ánimo de reiteración (véase el epígrafe "2.1.4. Autoría y participación"), el TS ha declarado que, atendiendo a las circunstancias del hecho concreto, habrá de dilucidarse si el partícipe pudo llegar a presentarse mentalmente cuáles serían las consecuencias de sus actos y si comprendió el riesgo en el que ponía el patrimonio del perjudicado al transferirlo a cuentas desconocidas (y probablemente domiciliadas en el extranjero). En definitiva, si el elemento volitivo expuesto va acompañado de la aportación esencial constituida por el proceder habitual de los muleros bancarios, lo más probable es que resulte condenado como partícipe a título de cooperador necesario del hecho principal.

En segundo lugar, puede suceder que el *phisher-mule* **sospeche que el dinero posee un origen turbio** por las circunstancias en las que ha llegado a sus manos, pero no se represente o desconozca cuál es ese origen concretamente y decida no investigarlo por no considerarlo plausible. Se trata de supuestos en los que el interviniente ni siquiera se representa como probables las consecuencias de la trama en la que se halla

[74] STS (Sala Segunda) nº 997/2013, de 19 de diciembre. FJ Tercero. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/c8b9510931739b07/20140217

inmerso -por lo que no se puede apreciar dolo eventual-, sino que su conciencia se detiene en un estadio anterior: la posibilidad de que ese dinero tenga un origen extraño por el halo de misterio que lo envuelve. En estos casos, la doctrina considera que el mulero interviene desde que el delito de estafa ha sido consumado con el objetivo de ocultar sus efectos, si bien al desconocer el fin real con el que realiza las transferencias a cuentas de terceros desconocidos lo hará afectando su conocimiento la imprudencia grave (art. 301.3 C.P.).

En este sentido, el TS ha declarado que en estos supuestos no podrá operar la ignorancia deliberada como catalizador de su responsabilidad, toda vez que la sospecha nacida le exige que proceda a investigar el círculo en el que se mueve el dinero, de qué fuente procede y con qué fin transita[75]. En conclusión, al concurrir los elementos constitutivos del delito de blanqueo de capitales el mulero podrá ser condenado como reo del mismo en su modalidad imprudente, sin que, como se ha manifestado, pueda alegar la citada ignorancia para evitar ser condenado como reo del delito referenciado. Además, si de la investigación de los hechos se desprende que el mulero actuó conociendo el alcance de su actividad y buscando el resultado inherente a ella (dolo) no será posible su condena a través del blanqueo, sino que las tornas girarán a favor de su cooperación necesaria al delito de estafa informática.

Finalmente, si el mulero **desconoce** que el dinero que recibe y que debe transferir procede del patrimonio de sujetos que han sido estafados, y no sospecha en absoluto de la legitimidad de las operaciones que se le ordena realizar (por ejemplo, porque haya sido engañada sobre el destino real de ese dinero, o porque sea de nacionalidad extranjera y desconozca o no domine el idioma local), el elemento volitivo del mulero no se encontrará viciado por elemento alguno que desvirtúe su libre absolución del delito de estafa informática; cuestión distinta será si de la instrucción de los hechos se desprende que actuó sometido a error vencible o invencible, y, en este sentido, que su conducta puede ser subsumida en el tipo de blanqueo de capitales o de receptación.

3.3. CIRCUNSTANCIAS MODIFICATIVAS DE LA RESPONSABILIDAD CRIMINAL

Tal como se ha manifestado a lo largo del presente trabajo, nos hallamos ante un delito especial debido al peculiar instrumento a través del que se comete, a las circunstancias en las que se gesta, y a la identidad y cualificación de su autor. En consonancia con esta significación, además de las circunstancias modificativas de la

[75] La "ignorancia deliberada" (en la terminología anglosajona, *willfull blindness*) es un término de origen jurisprudencial utilizado para conceptualizar los supuestos en los que un sujeto opta por mantenerse en la ignorancia respecto a una determinada situación cuyas circunstancias puede y debe conocer por existir razones de peso (como la sospecha de ilegalidad de una operación) que le incumban como para efectuar una investigación al respecto. Se trata de una fórmula incardinada en el tipo subjetivo del delito de difícil prueba, por lo que la acusación deberá enfangarse en demostrar ante el órgano jurisdiccional que el acusado se ha situado en la ignorancia deliberada de manera voluntaria, esto es, que conoció y se representó

Ejemplo de resoluciones sobre la materia son la STS (Sala Segunda) nº 970/2016, de 21 de diciembre (recuperada de https://www.poderjudicial.es/search/AN/openDocument/ea0775e0131d1c9e/20170110); y la STS (Sala Segunda) nº 70/2017, de 8 de febrero (recuperada de: https://www.poderjudicial.es/search/AN/openDocument/28eeb389ca4a7e0e/20170222).

responsabilidad criminal comunes[76] reguladas en los artículos 20, 21 y 22 C.P., los preceptos que siguen al 248.2 consagran determinadas circunstancias que agravan el rango penológico de carácter general establecido en el artículo 249 del mismo cuerpo legal.

Cabe, en primer término, realizar una breve mención al artículo referido en último lugar, habida cuenta que se trata del regulador de la pena a imponer a los reos de estafa. El legislador establece en él dos rangos, uno para delitos menos graves (si la cuantía de lo defraudado no excede de 400 € se impondrá al autor una multa de 1 a 3 meses) y otro "base" para los supuestos que, por exceder la cuantía fijada en el anterior, deban ser castigados en proporción a la gravedad del hecho (prisión de 6 meses a 3 años). En lo que respecta a esta armonía entre el hecho y la pena, el precepto señala al juzgador los condicionantes a los que debe prestar atención para individualizar la pena correspondiente al sujeto, entre los que se encuentran el detrimento patrimonial causado al perjudicado, la relación entre el autor y la víctima (si existe), o los medios empleados por aquél para llevar a éxito la conducta típica.

Establecidas las penas susceptibles de castigar las estafas en general, es necesario hacer referencia a algunas de las circunstancias agravantes específicas más relevantes y concurrentes en la práctica de las establecidas por el citado art. 250 C.P y aplicables a las estafas informáticas, que determinarán que la pena se halle dentro del lapso temporal consistente en prisión de 1 a 6 años y multa de 6 a 12 meses. *A priori*, podemos afirmar que pueden afectar a la acción del *phisher* los subtipos agravados obrantes en los ordinales 2º (abuso de firma de otro), 4º (especial gravedad debido a la

[76] Como se tratará en el epígrafe "5. Dificultad probatoria: la intangibilidad de la información y el anonimato inherente al medio empleado para cometer el delito", en los supuestos de estafa informática la prueba de la comisión del delito reviste una especial dificultad en su obtención, toda vez que el autor/s hacen uso de todas sus capacidades y mecanismos de los que les dota Internet para ocultar el testimonio de su actuar. De este modo, la acusación deberá valerse de un peritaje informático elaborado por expertos en la materia, así como de la información contenida en los informes que la Brigada de Investigación Tecnológica (B.C.I.T.) emitirá a petición del instructor.

En este sentido, como atenuante destaca, por la frecuencia de su concurrencia, la de "dilaciones indebidas", regulada en el art. 21.6 C.P. Sobre ella existe abundante jurisprudencia, resultando especialmente gráfica la reciente SAP Madrid (Sección 7ª) nº 121/2020, de 6 de marzo, que resolvió un supuesto de *smishing* (modalidad de *phishing* consistente en la realización de llamadas fraudulentas) realizadas por un agente externo desde diferentes instalaciones de Telefónica a líneas de clientes que previamente había manipulado y que, además, coincidían con los terminales de facturación de la compañía. Desde la interposición de la denuncia hasta la emisión de la sentencia transcurrieron 6 años, sin que los mismos fuesen imputables al autor o a la complejidad de la causa.

La resolución declaró lo siguiente:

> "El derecho a proceso sin dilaciones viene configurado como la exigencia de que la duración de las actuaciones no exceda de lo prudencial, siempre que no existan razones que lo justifiquen. O que esas propias dilaciones no se produzcan a causa de verdaderas "paralizaciones" del procedimiento que que se debieran al mismo acusado que la sufre, supuestos de rebeldía, por ejemplo, o a su conducta procesal.
>
> …Lo cierto es que, en este caso, la sala estimó con razón que las dilaciones de que se trata fueron de una entidad que justifica la especial cualificación de la atenuante. Pues carece de toda justificación que una causa por hechos tan simples como los de ésta haya precisado el transcurso de más de ocho años para ser enjuiciada".

Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/b9777598e8de484e/20200709

situación precaria en la que el autor abandona a la víctima), 5º (valor de la defraudación superior a 500.000 € o que ésta afecte a un número elevado de personas), y 6º (abuso de relaciones personales o de la credibilidad empresarial o profesional). De este modo, procede el tratamiento de cada una de ellas desde el punto de vista jurisprudencial.

En lo que concierne al abuso de firma, la jurisprudencia ha determinado que la utilización de las claves alfanuméricas -obtenidas a través de la mecánica defraudatoria- empleadas para acceder a la banca electrónica del perjudicado por parte del ciberdelincuente no tiene cabida en este subtipo agravado, toda vez que con el término "firma" la norma pretende referirse únicamente a la rúbrica realizada manualmente por parte del perjudicado[77]. A pesar de ello, los supuestos en los que el autor o partícipe hacen uso de la firma física de otro/s para lograr su propósito vía Internet sí se encuentran incluidos dentro del ámbito de aplicación de esta agravante. Ejemplo inmejorable de ello es la STS nº 860/2008, de 17 de diciembre[78], en la que el Alto Tribunal resolvió un litigio donde la trabajadora de una sociedad ordenaba vía fax al banco con el que solían trabajar, sirviéndose de la firma física de uno de los administradores de la sociedad, la realización de transferencias a una cuenta corriente de su propiedad por operaciones reales y con siglas falsas. Este mismo artículo incluye los casos de sustracción, ocultación o inutilización de proceso, expediente, protocolo o documento público u oficial; todas estas acepciones pueden encontrarse en modalidad física y electrónica, siendo lo más común en la tipología analizada la modificación e instrumentalización de efectos informáticos como las bases de datos, la "nube" o las facturas elaboradas en programas de este tipo para lograr las transferencias inconsentidas. Piénsese, por ejemplo, en la introducción de un troyano en el sistema de un trabajador encargado de la facturación de una empresa, a través del que el *phisher* modifica el número de cuenta del beneficiario de una factura; posteriormente, el trabajador envía esa factura al cliente, que termina abonando el importe en la cuenta falseada.

Respecto a las agravantes cualificadas de los ordinales 4º y 5º, procede su estudio conjunto como consecuencia de su entidad monetaria compartida. La primera de ellas deberá ser apreciada en función de las circunstancias personales y económicas del perjudicado[79] y del importe de lo sustraído, de modo que la gravedad imputable a la acción y la vulnerabilidad que ésta cause a la víctima -que, en palabras del TS, no tiene por qué equivaler a penuria o indigencia[80]- no será la misma si se sustraen 3.000 € de la cuenta corriente de una persona que gana mensualmente el SMI que a un integrante de la lista Forbes. En definitiva, se trata de una circunstancia modificativa de la responsabilidad criminal que admite una riquísima casuística y que no es posible apreciar prescindiendo del análisis de los hechos objeto de la *litis*.

---

[77] Ejemplo de ello son la STS (Sala Segunda, Sección 1ª) nº 256/2015, de 7 de mayo, FJ Tercero (recuperada de https://www.poderjudicial.es/search/AN/openDocument/bf8940ea34eecfb9/20150522), o la SAP Pontevedra (Sección 5ª) nº 47/2009, de 15 de julio, FJ Tercero. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/2dba7c47414cbe8a/20090806

[78] STS (Sala Segunda, Sección 1ª) nº 860/2008, de 17 de diciembre, FJ Cuarto. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/692d2557812d3947/20090122

[79] SAP Murcia (Sección 2ª) nº 70/2019, de 27 de febrero, FJ Segundo. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/f4f15e1c665382a0/20190402

[80] STS (Sala Segunda, Sección 1ª) nº 1169/2006, de 30 de noviembre, FJ Primero. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/5a04b820e5a9949f/20061221

Por otro lado, el ordinal 5º establece dos criterios de carácter objetivo y excluyente (pueden concurrir juntos o por separado): que el valor de lo defraudado supere la cifra de 50.000 €[81] (será necesario aportar prueba de cargo que desvirtúe la inexactitud inicial del objeto de la trama defraudatoria) o que afecte a un elevado número de personas. Es frecuente que el contenido de los ordinales 4º y 5º sean valorados de manera conjunta por parte de los Tribunales; este hecho no carece de lógica, ya que si con la tipificación de delitos contra el patrimonio es su perjuicio el que se persigue evitar y toda sustracción del mismo comporta un perjuicio para él, nada obsta para que la cuantía señalada sea tenida en cuenta como punto de partida al objeto de determinar finalmente cuál ha sido la entidad del quebranto patrimonial ocasionado. En lo que se refiere al "número elevado de personas" como concepto jurídico indeterminado, el artículo analizado evoca el conocido término "estafa piramidal" o "en cascada" acuñado por el Alto Tribunal para hacer referencia a entramados defraudatorios únicos diseñados para dañar a un número indeterminado de personas que terminan por constituir lo que ha venido en denominarse "sujeto pasivo masa". De este modo, el Tribunal ha declarado que se debe estar al caso concreto para dilucidar si nos encontramos ante ese número de personas o, por el contrario, ante una generalidad de ellas[82] (en cuyo caso, si concurriese junto con la notoria gravedad de los hechos, nos encontraríamos ante un "delito masa").

Por último, el C.P. ha querido dotar de un plus de antijuridicidad al comportamiento afectado por lo que considera un engaño diferente del genérico por el plus de vileza que presenta, y que subyace bajo el engaño del hecho principal: se trata de aquella defraudación perpetuada a través del aprovechamiento de la confianza existente entre el autor y la víctima por existir entre ellos relaciones familiares[83], de

[81] En el texto original del C.P., en vigor desde el 25 de mayo de 1996, el actual ordinal 5º ostentaba el sexto lugar dentro del art 250, que no establecía un criterio cuantitativo a partir del cual entender aplicable la agravante analizada. De este modo, el Tribunal Supremo terminó por resolver esta cuestión sentando jurisprudencia en la que determinó que este subtipo agravado sería aplicable si el valor de lo defraudado superaba la cantidad de 36.060,73 €. Ejemplo de esta doctrina son la STS (Sala Segunda, Sección 1ª) nº 482/2000, de 21 de marzo, FJ Cuarto (recuperada de: https://www.poderjudicial.es/search/AN/openDocument/6033c0352d823f82/20030830); o la SAP La Rioja (Sección 1ª) nº 138/2013, de 3 de diciembre, FJ Quinto (recuperada de: https://www.poderjudicial.es/search/AN/openDocument/6ae94f4cc030d9f4/20140129).

Respecto a los delitos continuados de estafa, la jurisprudencia del TS ha determinado, en cumplimiento del Acuerdo de Pleno no Jurisdiccional de 30 de octubre de 2007 (recuperado de: https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunal-Supremo/Jurisprudencia-/Acuerdos-de-Sala/Acuerdo-de-30-de-octubre-de-2007-sobre-delito-continuado-de-estafa-y-apropiacion-indebida), que cuando las cantidades defraudadas no superen individualmente la cifra de 50.000 €, serán consideradas en conjunto todas las disposiciones patrimoniales inconsentidas llevadas a cabo durante el lapso de tiempo enjuiciado para la aplicación del subtipo cualificado referenciado. En este sentido se pronuncia, entre otras, la STS (Sala Segunda, Sección 1ª) nº 143/2019, de 14 de marzo, FJ Tercero (recuperada de: https://www.poderjudicial.es/search/AN/openDocument/8939261909812050/20190329).

[82] STS (Sala Segunda, Sección 1ª) nº 94/2018, de 23 de febrero, FJ Noveno. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/1414e539d40f90c9/20180320.

[83] Los supuestos de *phishing* no son habituales entre familiares; sin embargo, sí son frecuentes las denominadas estafas informáticas en la modalidad de *skimming*, es decir, el robo o utilización sin consentimiento de una tarjeta de crédito o débito al objeto de retirar efectivo en un cajero. Una muestra de ello es la STS (Sala Segunda, Sección 1ª) nº 1476/2004, de 21 de diciembre, FJ Primero. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/2b15875e60f6439f/20050126.

amistad[84], de pareja[85], o de trabajo[86]. Esta burla aparece en el relato de los hechos como el instrumento que saca rédito criminal de la confianza labrada en esa afinidad y que actúa como refuerzo del engaño inmediatamente anterior a la realización de la conducta castigada, por lo que a juicio del legislador ha merecido un tratamiento penológico más gravoso que le diferencie de un supuesto de estafa común (en el que el engaño ya forma parte de su tipo objetivo).

3.4. COMPETENCIA JUDICIAL: LA PROBLEMÁTICA DEL LUGAR DE COMISIÓN DE LA INFRACCIÓN

Una vez analizados los aspectos sustantivos del delito de estafa informática en su modalidad de *phishing*, procede abordar las consecuencias de carácter procesal que lo acompañan. En efecto, si atendemos a los elementos constitutivos del tipo estudiado y a las características propias del medio utilizado para cometerlo (Internet permite realizar una multiplicidad de tareas *online* sin necesidad de asentamiento un lugar determinado) repararemos, en primer lugar, en que la concepción clásica del lugar de comisión del delito (*forum commissi delicti*) consagrada en el art. 14 LECrim presenta problemas de aplicación.

Pensemos en el siguiente supuesto de hecho: la organización clandestina "HackingXmoneY", con el objetivo de enriquecerse ilegítimamente, creó una campaña de *phishing* dirigida a los ciudadanos españoles consistente en el envío masivo de correos electrónicos a una cantidad indeterminada de personas, comunicaciones que iban acompañadas de todos los signos distintivos de Correos y de un mensaje de premura a través del que se avisaba a los receptores de que tenían pendiente la recogida de un paquete en las oficinas más próximas a sus domicilios, por lo que debían pedir cita para su recogida y abonar un recargo por la retención del paquete en la oficina haciendo *click* en el enlace adjunto al mensaje, que redirigía al usuario a una página *web* idéntica a la de la institución. A su vez, para no ser descubiertos, contactaron vía *email* con un grupo de personas en situación de desempleo ofreciéndoles trabajo consistente en aperturar una cuenta bancaria a su propio nombre para recibir y realizar transferencias, de cuyo movimiento extraería el 15% en calidad de remuneración por sus servicios. Esta oferta fue aceptada por "Y", residente en Madrid, que procedió a abrir al efecto una cuenta en la entidad "Banco Santander".

El día 1 de junio de 2020 "X", residente en Valencia, recibió en su bandeja de entrada una comunicación aparentemente remitida por Correos, y, como estaba esperando recibir un paquete por productos adquiridos a través de una compra *online*, accedió a la web enlazada al *email* para realizar el pago del recargo y pedir cita en la oficina donde guardaban el paquete. El día 29 del mismo mes accedió a la banca *online* y reparó en que se habían realizado anotaciones en su cuenta por transferencias realizadas a "Y" los días 3, 10, 12, 17 y 22 de junio por un valor total de 23.676 €. Al no haberlas realizado él ni haber dado su consentimiento a otra persona para que las efectuase, decidió personarse en la Comisaría de Policía más cercana para denunciar a "Y" por los hechos acaecidos.

[84] SAP Huelva (Sección 3ª) nº 231/2018, de 7 de noviembre, FJ Primero. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/7e7e5e0ea5bef73a/20190129.

[85] SAP Guipúzcoa (Sección 1ª) nº 147/2018, de 28 de junio, FJ Cuarto. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/f311ebae6853b317/20181016.

[86] SAP Barcelona (Sección 3ª) nº 8/2013, de 8 de enero, FJ Segundo. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/2a3c12f771a0d14d/20130301.

Con ocasión del estudio de la problemática anunciada, se ofrecerá solución a este ejemplo.

Con la llegada de la realidad virtual y el auge de los delitos cometidos a través de la Red, la Sala Segunda del Tribunal Supremo se reunió en Pleno no Jurisdiccional de 3 de febrero de 2005[87] con el objetivo de deliberar sobre el criterio aplicable a la hora de determinar la competencia territorial de los Juzgados y Tribunales españoles con respecto a la investigación y enjuiciamiento de los delitos informáticos. En este sentido, la Sala fijó como criterio jurisprudencial de aplicación el **principio de ubicuidad**, según el cual los delitos informáticos se cometen en todos los lugares en los que se haya realizado algún elemento del tipo (la manipulación informática o artificio semejante, y el acto de disposición patrimonial)[88]; de esta forma, todos los órganos jurisdiccionales cuya competencia objetiva se circunscriba a la instrucción de infracciones penales y que se encuentren en dichos lugares son competentes para investigar los hechos presuntamente constitutivos de un delito de estafa informática.

El citado acuerdo determina, además, que entre ellos será competente para conocer del asunto, en principio, el que haya iniciado primero la investigación de las actuaciones, debiendo inhibirse en su favor aquél que haya incoado el procedimiento con posterioridad[89]. Sin embargo, esta regla podrá verse desvirtuada en caso de que el **principio de eficacia en la instrucción** otorgue competencia al órgano situado en el lugar donde la instrucción pueda tener más éxito (es decir, donde arroje datos más ilustrativos para el esclarecimiento de los hechos); habitualmente, éste radica donde se encuentra la residencia o el centro de operaciones del mulero, así como en el lugar donde se encuentra domiciliada la cuenta bancaria con la que ha actuado[90], ya que es ahí donde ha tomado contacto con el *phisher* u organización criminal, ha recibido las transferencias procedentes del patrimonio del perjudicado, y donde radican el ordenador y las comunicaciones de las que se ha servido para participar en la mecánica analizada.

El supuesto de hecho que ejemplifica este epígrafe aporta dos lugares en los que existe constancia de la realización de los elementos del tipo: a) Valencia, donde se produce el acto de desplazamiento patrimonial (al ser el lugar donde se encuentra domiciliada la cuenta del perjudicado, y b) Madrid, donde el mulero recepciona las

[87] Acuerdo de Pleno no Jurisdiccional del Tribunal Supremo, de fecha 3 de febrero de 2005. Recuperado de: https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunal-Supremo/Jurisprudencia-/Acuerdos-de-Sala/Acuerdos-de-3-de-febrero-de-2005-sobre--1--Principio-de-ubicuidad---2--Clausulas-de-reserva-de-dominio-y-prohibicion-de-enajenar---3--Principio-de-minimos-psicoactivos-en-relacion-al-art--368-CP.

[88] Existen numerosas resoluciones sobre cuestiones de competencia emitidas por la Sala Segunda del Alto Tribunal. Entre otras, el ATS (Sala Segunda, Sección 1ª) de 1 de abril de 2004 (recuperado de: https://www.poderjudicial.es/search/AN/openDocument/9459eacd588d0bd3/20040506), el ATS (Sala Segunda, Sección 1ª) de 24 de enero de 2007 (recuperado de: https://www.poderjudicial.es/search/AN/openDocument/260000bf5d1ba7ea/20070301), y el ATS (Sala Segunda, Sección 1ª) de 21 de septiembre de 2011 (recuperado de: https://www.poderjudicial.es/search/AN/openDocument/de4b1d1882501106/20111013).

[89] ATS (Sala Segunda, Sección 1ª) de 26 de octubre de 2011. Recuperado de: https://www.poderjudicial.es/search/AN/openDocument/3896535ad1704006/20111114.

[90] Entre otros, se pronuncian en este sentido los ATS (Sala Segunda, Sección 1ª) de 26 de septiembre de 2012 (recuperado de: https://www.poderjudicial.es/search/AN/openDocument/4c34d1315b1f93f1/20121106), y el ATS (Sala Segunda, Sección 1ª) de 29 de enero de 2015 (recuperado de: https://www.poderjudicial.es/search/AN/openDocument/8c918323f91192f7/20150206).

cantidades sustraídas al primero. Según la teoría de la ubicuidad, serían competentes para instruir los hechos los Juzgados de Instrucción de ambas ciudades.

Si en lugar de existir un tercer intermediario hubiese actuado el *phisher* directamente y el lugar desde el que opera fuese conocido por el denunciante o revelado a lo largo de la instrucción, también sería susceptible de ser incluido en este listado.

Hasta este momento se ha analizado la presente cuestión tomando como punto de partida la posibilidad de se tenga constancia del lugar donde se ha efectuado algún elemento del tipo, o que éstos datos hayan sido descubiertos durante la investigación. No obstante, esta visión se encuentra disconexa de la realidad socio-jurídica, toda vez que lo más frecuente es que el perjudicado ignore la identidad de su atacante y conozca únicamente el lugar donde se ha producido el daño -por encontrarse él mismo incluido de forma involuntaria en la fase de comisión del delito-, así como la identidad del mulero (recordemos que se encuentra identificado en todo momento, al ser el titular de la cuenta corriente a la que se realiza la transferencia de activos inconsentida). En estos supuestos, en lugar de acudir a la aplicación del principio de ubicuidad entrará en juego directamente el de eficacia en la instrucción[91] en la significación expuesta (lugar de actuación y residencia del mulero); en definitiva, no se tendrán en cuenta el lugar desde el que se han emitido los *emails* falsarios ni el de residencia de los perjudicados o el de sus cuentas corrientes.

Si atendemos al principio de eficacia reseñado y fijado por la jurisprudencia del TS, únicamente será útil una instrucción realizada en Madrid al ser el lugar donde reside el intermediario y desde donde ha llegado a cabo su intervención en los hechos delictivos.

Por último, puede suceder que al inicio de las actuaciones se desconozca la identidad del tercero intermediario, por lo que sólo se cuente con el conocimiento del lugar en el que se ha producido el perjuicio patrimonial. En estos supuestos se acudirá al principio de ubicuidad expuesto, que habilitará al denunciante para interponer la denuncia en el lugar donde se ha llevado a cabo el desapoderamiento perjudicial, esto es, el lugar donde esté domiciliada su cuenta bancaria.

En este sentido, si "X" desconociese la identidad del titular de la cuenta que se ha beneficiado del activo que le ha sustraído (por ejemplo, porque "Y" ha abierto la cuenta sirviéndose de una identidad falsa) podrá interponer la denuncia ante las autoridades valencianas, que, previo examen de los hechos relatados en la misma, procederán a dar traslado a los Juzgados de Instrucción de Valencia. El adjudicatario por reparto incoará un procedimiento de diligencias previas a través del que podrá oficiar a la Policía Nacional para que averigüe la entidad financiera donde se ha abierto la cuenta beneficiaria y, posteriormente, oficiar a dicho banco para que facilite todos los datos relativos a la misma.

En definitiva, la jurisprudencia diferencia tres escenarios divergentes y dependientes del grado de conocimiento sobre la identidad de los intervinientes en la trama defraudatoria, su posible participación y los lugares desde los que desarrollan sus respectivas funciones, estableciendo que se aplicará un principio u otro atendiendo al potencial éxito de la instrucción y, por ende, al restablecimiento del patrimonio de la víctima.

[91] ATS (Sala Segunda, Sección 1ª) de 22 de febrero de 2018. Recuperado de: https://www.poderjudicial.es/search/AN/openDocument/41044a6eb410bc67/20180305.

3.5. DIFICULTAD PROBATORIA: LA INTANGIBILIDAD DE LA INFORMACIÓN Y EL ANONIMATO INHERENTE AL MEDIO EMPLEADO PARA COMETER EL DELITO

Como se ha manifestado a lo largo del estudio objeto del trabajo, a pesar de que la naturaleza de los delitos mal llamados "informáticos" no presente novedades respecto a su concepción original, la vía empleada para su comisión posee características propias que dotan también de singularidad a su investigación con respecto a los tipos restantes. Así, es innegable que desde que los seres humanos realizamos un uso universalizado de Internet hemos desarrollado la capacidad de requerir inmediatez a las tareas más sencillas como consecuencia de las prestaciones que este medio nos ofrece, tales como comunicarnos, desarrollar prestaciones laborales o recibir la compra en casa en menos de 24 h. Esta celeridad no es desconocida por los *crackers*, que, como sujetos especialmente cualificados y conocedores de las posibilidades de la Red, sacan rendimiento de ellas utilizándolas para dificultar el descubrimiento de su identidad y la consecuente imputación del hecho delictivo que han perpetrado a través de dicho mecanismo.

Con el fin de facilitar la comprensión de los inconvenientes experimentados en la investigación de estos delitos, su estudio se dividirá en tres puntos: a) Divergencia espacio-temporal en la comisión del delito; b) Objeto material de la indagación; y c) Tareas de investigación en el proceso penal.

a) **Divergencia espacio-temporal en la comisión del delito**: el paralelismo espacio-temporal que concurre en los delitos consumados a través de la presencialidad resulta, en muchas ocasiones, inútil para efectuar el juicio de imputabilidad en el proceso penal por delitos informáticos. En efecto, Internet ha posibilitado que, por ejemplo, una persona pueda acceder a los archivos almacenados en su ordenador a través de un dispositivo diferente y desde un rincón lejano del Mundo. Esto es posible como consecuencia de la invención de programas, aplicaciones y opciones integradas en las funcionalidades de los equipos informáticos (muchos de ellos disponibles para su descarga gratuita) que resultan tremendamente útiles en entornos de trabajo competitivos. Sin embargo, estas herramientas encuentran su antítesis en el *malware*, que, configurado en algunas de sus modalidades, también ofrece acceso a un sistema y a sus archivos con fines radicalmente distintos a los anteriores[92]. La tecnología también presenta la posibilidad de programar tareas en nuestro equipo que serán ejecutadas por el sistema en la fecha y hora que planifiquemos, lo que, en el proceder de un ciberdelincuente, puede constituir un medio impeditivo del descubrimiento de su identidad y de la técnica que ha utilizado para apropiarse de los datos o patrimonio de la víctima, ya que cuando los hechos acometidos por él comiencen a ser investigados en el seno de un procedimiento penal es muy probable que haya desplegado una multiplicidad de acciones para evitar que eso suceda.

[92] En las décadas de los 90 y los 2000, los cibercafés se convirtieron en todo un fenómeno para jóvenes que no disponían de Internet en sus casas. Además, constituyeron verdaderos refugios para los *crackers*, ya que les dotaban de conexión pública, anonimato y sistemas informáticos con los que efectuar los ataques que ideaban. Uno de los más comunes fue el ciberataque a través de *bots*, consistente en la infección de un sistema (para lo que recurrían a los ordenadores dispuestos en el café) que, a su vez, infectaría por auto propagación a todos aquellos que se encontraran conectados a la misma Red. En definitiva, se aseguraban de que cualquier dispositivo que se conectase a la Red del cibercafé donde se encontrara el *bot* resultase infectado y pudiese propagar el *malware*.

Cinco días, El País. *¿Estoy protegido frente a un espía industrial?* 31 de agosto de 2013. Recuperado de: https://cincodias.elpais.com/cincodias/2013/08/30/sentidos/1377874039_831624.html

Por tanto, la Red excluye de plano la concepción física de los parámetros "tiempo" y "espacio"[93] en los delitos que nos ocupan, creando en su lugar una dimensión codificada a través de conexiones invisibles (coloquialmente conocida como "ciberespacio") mediante la que los sistemas que la componen interaccionan por orden de los usuarios, y en la que los *phishers* podrán atacar a otros usuarios desde espacios físicos diferentes (mención especial a la transnacionalidad) e incluso en tiempos dispares. Asimismo, éstos disponen de técnicas de las que se sirven para ocultar las pruebas de su proceder y procurar el mantenimiento de su anonimato, en su mayoría orquestadas mediante la manipulación del *software* empleado para efectuar el ataque.

b) **Objeto material de la indagación**: lo expuesto respecto a la dicotomía espacio-temporal del ciberespacio es asumible también para el objeto de su tráfico, aunque con los matices inherentes a su naturaleza. Obsérvese que los datos objeto de tratamiento en las operaciones informáticas no son tangibles[94], sino que el soporte físico ha sido sustituido por el magnético con las contingencias que ello conlleva en las tareas de investigación: sirva como ejemplo la dificultad de comprobar la validez y veracidad de los documentos electrónicos. Como se ha expuesto en el anterior punto, de esta inmaterialidad deriva la volatilidad propia de estos datos y la que el *phisher* desee otorgarles a través de la acción dirigida a auto encubrirse.

En definitiva, resulta primordial para el perjudicado asegurar que el testimonio del delito por el que se ha visto afectado perdure en el tiempo a través de la recopilación de pruebas para hacer valer su derecho en un procedimiento penal posterior. En este sentido, será fundamental que se sirva de un documento gráfico en el que conste el contenido del *email* completo a través del que el *phisher* ha orquestado su manipulación psicológica y el resultado de la carga del enlace adjunto (en caso de redirigir a una *web* falsa), así como los documentos (bancarios, de identidad) que demuestren que los datos utilizados por el ciberdelincuente para realizar el desapoderamiento patrimonial le pertenecen. También es recomendable recurrir al encargo de una pericial informática lo antes posible tras el ciberataque (para evitar la potencial eliminación de pruebas), que será efectuada por un equipo de titulados expertos que autenticarán su efectiva consecución, determinarán los medios que el *phisher* ha empleado, y que podrá ser aportada como prueba preconstituida en el proceso penal.

c) **Tareas de investigación en el proceso penal**: tras la denuncia del perjudicado, que apertura el correspondiente atestado, se inicia la fase de investigación policial en la que varios agentes designados al efecto llevarán a cabo la recopilación de evidencias probatorias al objeto de remitirlas al Juzgado de Instrucción a quien por reparto corresponda conocer del asunto. Uno de los cometidos de mayor relevancia de la investigación policial es apreciar, tras el examen previo de los datos aportados o

---

[93] **Miró Llinares, F**. *La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen*. Revista Electrónica de Ciencia Penal y Criminología. Núm. 13-07. 2011. Recuperado de: https://www.unedpamplona.es/docs/file/documentacion%20fernando%20miro.pdf

[94] Como consecuencia del surgimiento de este nuevo tipo de información, y dado que la Ley penal anterior a mediados del siglo XX no contemplaba la posibilidad de que los bienes jurídicos ya consagrados pudiesen ser lesionados a través de la utilización de sistemas informáticos, el legislador se vio abocado a la reforma del Código Penal a través de la LO 5/2010, de 22 de junio, en los términos expuestos en el Capítulo I.

Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Recuperada de: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-9953

extraídos de la misma, la necesidad de oficiar un mandamiento al proveedor de servicios de Internet del que el presunto *cracker* se ha servido para efectuar el ataque al objeto de que facilite la dirección "IP" (siglas de *Internet Protocol Address*)[95] desde la que éste ha tenido lugar. La solicitud de realización del mandamiento debe remitirse al Juez o Magistrado encargado de la instrucción del procedimiento, que decidirá sobre la idoneidad de la práctica de la prueba. En este punto es necesario recordar la volatilidad de los datos informáticos, si bien los proveedores de servicios tienen la posibilidad de conservar unos ficheros históricos o *log*[96] en los que se almacenan de manera automática y secuencial los de todas las conexiones realizadas a través del servicio que ofrecen; la existencia de estos registros posibilita la identificación de las "IPs" intervinientes en el tráfico y su geolocalización, referencia que será de suma utilidad en el proceso. No obstante, existen voces discordantes respecto al valimiento de este medio de prueba para identificar al *phisher*, siendo más partidarias de sustituirlo por un mandamiento judicial a través del que se requiera al proveedor de servicios para que conserve esos ficheros en tanto el procedimiento penal se encuentre abierto[97]. Para seguir el curso de una instrucción menos engorrosa, lo cierto es que ambos mandamientos son compatibles e, incluso, experimentan una relación de necesidad mutua, en tanto existe un riesgo de borrado de la información que haría inviable la determinación de la IP interviniente.

Una vez determinada la IP desde la que ha operado el sujeto activo del delito, el instructor podrá decidir mediante Auto motivado, en razón del principio de idoneidad, librar un mandamiento a la compañía telefónica -habitualmente a petición de la Policía Judicial- para que haga constar los datos del abonado, es decir, el domicilio donde se encuentra instalada, los datos del titular de la conexión a Internet y de la línea telefónica utilizada, así como los datos técnicos asociados a dicha conexión.

Sin embargo, es posible que nos encontremos ante uno de los supuestos en los que el ciberdelincuente ha procedido desde una red pública, en cuyo caso el mandamiento será devuelto por la compañía significando que la dirección es una "IP NAT"; en estos casos, para identificar cuál es la conexión con más probabilidades de corresponder al *phisher* deberá atenderse al puerto de acceso o salida de la red o a las horas coincidentes con los hechos denunciados.

En definitiva, todas estas diligencias de investigación podrán ser apoyadas, dependiendo de la complejidad del procedimiento y de la necesidad de su práctica, con

---

[95] La dirección "IP" es una composición alfanumérica única asignada a cada dispositivo, integrada por cuatro grupos de número naturales separados entre sí por puntos; en términos coloquiales, la matrícula del mismo. Existen dos tipos en función de su operatividad: las privadas, que están asignadas a dispositivos que funcionan dentro de una red local (por ejemplo, las de todos los dispositivos conectados a una red wifi familiar); y las públicas, correspondientes a dominios de Internet y al *router* visto desde el exterior.

Avast Academy. *¿Qué es una dirección IP?* 19 de mayo de 2021. Recuperado de: https://www.avast.com/es-es/c-what-is-an-ip-address

[96] **Digital Guide IONOS**. *Ficheros log: toda la información de registro en un archivo*. 30 de junio de 2016. Recuperado de: https://www.ionos.es/digitalguide/online-marketing/analisis-web/el-log-el-archivo-de-registro-de-procesos-informaticos/

[97] **López, A**. *La investigación policial en Internet: estructuras de cooperación internacional*. Monográfico "III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas". Revista de Internet, Derecho y Política. Universitat Oberta de Catalunya. 2007. Recuperado de: file:///C:/Users/missm/Downloads/Dialnet-LaInvestigacionPolicialEnInternetEstructurasDeCoop-2372614.pdf

la adopción de medidas tales como la entrada y registro (art. 545 y siguientes LECrim) en el domicilio del *cracker* identificado para el precinto de dispositivos -junto con los documentos físicos que apoyan su funcionamiento- y volcado de los datos contenidos en ellos, las intervenciones telefónicas, las labores de vigilancia policial ordinaria[98] y la localización y destino final de los fondos sustraídos (tarea complicada en los asuntos de componente internacional, habida cuenta que, en estos casos, el *phisher* acostumbra a afincarse en Estados que carecen de instrumentos de cooperación judicial internacional con España).

A pesar de la exigencia de conocimientos que implica la instrucción de un procedimiento incoado por la presunta comisión de un delito cometido a través de las TIC, lo cierto es que las estadísticas arrojan datos que evidencian que la mayoría de Jueces y Magistrados acusan una gran ignorancia en estas lides, que les aboca a la dependencia informativa de las manifestaciones vertidas en los informes emitidos por las unidades especiales de investigación tecnológica de las FFCCSS a petición propia, o a los realizados por el representante del Ministerio Fiscal [99] en el curso del procedimiento. Como todo dato dependiente de la *res* socio-cultural, tiene razón en las circunstancias en las que dichos profesionales ejecutan su trabajo: nos referimos a un colectivo que desarrolla sus funciones en un entorno en el que concurren una gran cantidad de trabajo y poco tiempo para desarrollarlo, a lo que debemos sumar que el 71% de la carrera judicial ha declarado poseer ordenador con Internet en su domicilio y utilizarlo para fines corrientes y dictar resoluciones[100], lo que, en plena era cibernética hace necesaria la instauración e implementación de una formación tecnológica de calidad y gratuita a cargo del CGPJ que exceda de las labores propias del cargo (como, por ejemplo, del uso del sistema de gestión procesal). Solo de esta manera se podrán complementar los conocimientos jurídico-técnicos de Jueces y Magistrados con el fin de facilitarles la comprensión de la comisión de los delitos informáticos y guiar su proceder en la investigación de los mismos.

Asimismo, es de destacar la redacción de la LECrim como una de las principales culpables de la desadaptación de la Justicia para la instrucción y enjuiciamiento de estos delitos, toda vez que presenta una evidente desconexión de la realidad social actual, y, por ende, no ofrece los instrumentos adecuados y adaptados a las peculiaridades antes manifestadas para que el procedimiento llegue a buen puerto.

3.6. LA RESPONSABILIDAD DE LAS ENTIDADES BANCARIAS COMO DEPOSITARIAS DEL ACTIVO SUSTRAÍDO

[98] **Rayón Ballesteros, M.C. y Gómez Hernández, J.A**. *Cibercrimen: particularidades en su investigación y enjuiciamiento*. Anuario Jurídico y Económico Escurialense, XLVII. Pp. 209 a 234. 2014. Recuperado de: file:///C:/Users/missm/Downloads/Dialnet-Cibercrimen-4639646.pdf

[99] En el año 2011 se creó el Área Especializada de la Fiscalía para la Criminalidad Informática, a través de la que se buscaba la preparación de sus integrantes para ejercitar la acción pública en delitos cometidos a través de la informática.

Instrucción 2/2011, de 11 de octubre, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías. Recuperada de: https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-I-2011-00002.pdf

[100] **Revista E-Justicia**. *Tecnologías de la Información y las Comunicaciones*. Núm. 3. Mayo de 2007. Recuperada de: file:///C:/Users/missm/Downloads/EJusticia3_1.0.0.pdf

Analizados los aspectos jurídico-técnicos del delito de *phishing*, es necesario realizar una referencia, aunque sucinta, a su consecuencia más inmediata: la restitución del activo sustraído y la determinación del sujeto que ha de hacer frente a la misma.

Si prestamos atención a las fases que componen el *iter criminis* o camino del delito, observamos que, además del sujeto activo y del perjudicado, en la fase de ejecución de la acción típica interviene un tercer individuo cuya participación ha sido analizada en el presente Capítulo (2.1.3. Acción típica): la entidad bancaria en la que el perjudicado ostenta una cuenta corriente, donde deposita su patrimonio o parte de él. Así, es el banco el que autoriza vía *online* las transferencias de los fondos del perjudicado a la cuenta del *phisher* o del mulero, por lo que es necesario determinar qué tipo de responsabilidad le es exigible por parte de la víctima del delito.

En este sentido, la Ley de Servicios de Pago[101] determina cuáles son las obligaciones del prestador de los servicios de crédito y condiciones en las que debe ofrecerlos a través de la banca en línea. Para garantizar que tales prestaciones se ofrezcan íntegramente y de la forma más segura posible, el art. 36 de la citada norma, inspirado en la realidad delictiva actual, exige el consentimiento del cliente para la efectiva realización de operaciones de pago tales como las transferencias, por lo que será la entidad la obligada a establecer mecanismos que dificulten al tercero de ánimo espurio disponer de fondos ajenos a través de este método; un ejemplo de ellos es la doble autenticación, a través de la que el sistema del banco conmina al cliente a facilitarle un código que le envía a su teléfono móvil y a introducir, además, su firma electrónica. En caso de falta de asunción de este deber, y, por tanto, por no haber implantado instrumentos que limiten el acceso a la banca electrónica y a la movilidad del dinero a terceros no autorizados, el banco no podrá descargar la responsabilidad sobre el cliente.

No obstante, puede suceder que, a pesar de haber establecido dichos instrumentos de control, el sujeto activo del delito consiga traspasar su seguridad y realizar la disposición inconsentida de activos. Incluso para este trance la jurisprudencia ilustra los deberes de la entidad bancaria, que se extienden hasta momentos posteriores a la salida del dinero de su ámbito de actuación. De este modo, el banco debe pugnar por la devolución de los importes sustraídos a su legítimo titular para evitar la consumación del delito, encontrándose este actuar dentro de la diligencia exigible para evitar responder en concepto de responsabilidad civil ante su cliente[102], obligación que se prolonga incluso entre entidades bancarias diferentes como consecuencia de la normativa en vigor sobre prevención del blanqueo de capitales.

Por otro lado, la norma también atribuye al contratante de las prestaciones bancarias la obligación de custodia de su clave de acceso a la banca *online* (art. 41); así, en caso de pérdida o sustracción de la misma procederá poniéndolo en conocimiento de la entidad bancaria al objeto de la modificación inmediata de esta llave. Sin embargo, en el supuesto de que un tercero no autorizado acceda a la banca electrónica y disponga de los activos del cliente como consecuencia de la actuación negligente o deliberada de éste (sirvan como muestra de ello los supuestos en los que el ordenante facilita su clave de acceso a una persona que apenas conoce, o aquellos en los que repara en los

[101] Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera. Recuperada de: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16036

[102] SAP Málaga (Sección 3ª, Penal) nº 606/2013, de 23 de octubre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/5b0ffdb8a0a589d6/20131219

movimientos fraudulentos en su cuenta pero tarda en comunicárselo al banco), la Ley dispone que será él y no el prestador de servicios el que soportará la pérdida de su patrimonio.

De la exposición realizada deriva la **responsabilidad cuasi-objetiva** de la entidad de crédito, de manera que cuando proceda autorizando un traspaso de activos entre cuentas sin la debida comprobación de su legitimidad (esto es, sin disponer de los citados mecanismos de verificación de la identidad del ordenante y generándole un riesgo innecesario de fraude), y salvo los casos de negligencia grave del cliente, deberá restituirle íntegramente los importes de los que se ha visto desposeído por causa de su imprudencia. En este sentido se pronuncia asentada jurisprudencia, entre las que destacan la SAP Asturias nº 351/2012[103], la SAP Valencia nº 37/2017[104], o la SAP Alicante nº 107/2018[105].

Como de todo ello se deduce, el cliente debe comunicar al banco en el plazo máximo de 3 meses desde la fecha del adeudo la realización de las transferencias realizadas en su nombre y sin su consentimiento (art. 43) con el objetivo de que le sean restituidos los importes sustraídos. No obstante, al alegar el usuario del servicio de pago la falta de autorización del movimiento fraudulento, esta negativa se verá amparada por una presunción de veracidad que corresponderá al banco desvirtuar; este cometido encuentra su máxima expresión en la inversión de la carga de la prueba durante el ejercicio de la acción civil, a través de cuyo ejercicio deberá demostrar que "la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado"[106].

En fin, cabe recordar al respecto que, tal como establece el art. 111 LECrim, el perjudicado podrá ejercitar la acción civil contra la entidad bancaria para reclamar la responsabilidad *ex delicto* en el seno proceso penal, o ante la jurisdicción civil (previa reserva de acciones), si bien podrá requerir la reparación del daño al *phisher* o al banco, pero nunca a ambos. Lo más habitual será que el perjudicado reclame el resarcimiento a la entidad de crédito, ya que en muchas ocasiones la identificación del cibercriminal resulta muy compleja y muchos de los procedimientos en los que se enjuician delitos de estafa informática terminan por dirigirse únicamente contra el mulero.

4. CONCLUSIONES

Como se ha expuesto a lo largo de este trabajo, la ciberdelincuencia avanza siguiendo el ritmo del imparable progreso tecnológico y exprimiendo las circunstancias derivadas de las crisis socio-económicas sufridas en las sociedades. De este modo, debido a la generalización del uso del Ciberespacio -en el que se gestan las conductas constituyentes de delitos informáticos- y al aumento alarmante de las amenazas consumadas en los últimos años, este fenómeno delictivo se ha convertido en un nuevo problema de índole social que precisa de un tratamiento normativo y sintomatológico novedoso y acorde a las características que le son propias.

[103] SAP Asturias (Sección 1ª, Civil) nº 351/2012, de 18 de septiembre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/b39fd042a2fce878/20121127

[104] SAP Valencia (Sección 2ª, Penal) nº 37/2017, de 25 de enero. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/ac8ac51d541d47ef/20170614

[105] SAP Alicante (Sección 8ª, Civil) nº 107/2018, de 12 de marzo. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/9718501a458ca5d7/20180613

[106] Dicción literal recogida en el artículo 44.1 de la Ley de Servicios de Pago.

En lo que respecta su consideración normativa, no se puede obviar el ejercicio legislativo desarrollado por organizaciones supranacionales como la Organización de las Naciones Unidas (ONU) o la Unión Europea, que han tratado de ofrecer a sus Estados miembros un marco normativo lo más actualizado posible a las exigencias derivadas del tratamiento defensivo frente a los ciberataques y al aseguramiento de los datos de los usuarios de la Red. Un ejemplo significativo de esta actividad es el tantas veces mencionado Convenio de la Ciberdelincuencia de Budapest, instrumento innovador en cuanto a la precisión técnico-jurídica de muchos conceptos informáticos clave para comprender la confección de un ciberataque y la trascendencia jurídica de la actuación del ciberdelincuente.

En este sentido, la legislación patria en materia de delincuencia informática debe su existencia a la exigencia contenida en el citado cuerpo legal, obligación consistente en la adaptación de las normativas nacionales al marco ofrecido en materia de contingencias que pueden surgir en el marco de las manipulaciones de los sistemas de la información. En lo que se refiere al objeto de este proyecto, es el Artículo 8 del Convenio el que exige a los Estados firmantes la adopción de medidas legislativas para tipificar las conductas tendentes a causar un detrimento patrimonial a los usuarios a través de los medios informáticos, así como las consistentes en causar cualquier tipo de interferencia o daño en sus sistemas. A pesar de que el citado instrumento data del año 2003, no fue hasta 2010 cuando el legislador español decidió formar parte de sus firmantes e incorporarlo a nuestro ordenamiento jurídico a través del correspondiente instrumento de ratificación, año en el que modificó el Código Penal para hacer frente a las demandas en él contenidas. Así, observamos que en una realidad cada vez más virtual, el legislador español ha optado por depender del impulso normativo de otras organizaciones, sin prestar atención hasta fechas cercanas a la actual a los problemas derivado del uso de las redes.

La manifestación más cercana al objeto de análisis de este trabajo es la dicción literal del artículo 248.2 C.P., que, como se ha indicado, contiene una fórmula de carácter genérico que pretende abarcar los supuestos de estafa que, por estar afectadas de ciertos elementos específicos (la utilización de Internet como medio para la comisión del delito o el engaño efectuado a través de la manipulación informática) no son subsumibles en el delito de estafa común. Como consecuencia de la ausencia de revisión de este precepto, los Jueces y Magistrados españoles han debido adaptar la realidad social a la práctica jurídica a través de la reinterpretación de lo legislado, de tal modo que, acudiendo a la jurisprudencia por ellos elaborada, observamos que hechos tan dispares como las defraudaciones efectuadas a través del método *phishing* y el denominado "timo de las tragaperras" pueden ser constitutivos de un delito de estafa informática, a pesar de que en el último de estos casos el uso de la citada máquina no implica la incursión en los hechos de un sistema de la información. Esta inadaptación de la normativa de contenido material ha ocasionado la temida (y, por desgracia, habitual) desconexión entre legislación y realidad social, dejando en el aire una multiplicidad de situaciones que derivan del continuo desarrollo de los sistemas informáticos y de las redes de la información.

La mencionada problemática es imputable también a los instrumentos provistos por nuestra decimonónica LECrim para la investigación y enjuiciamiento de los delitos informáticos. Lo cierto es que, tras la reforma llevada a cabo en el año 2015, el legislador procuró surtir de instrumentos de investigación adecuados a los encargados de instruir esta clase de ilícitos, incorporando a la fase de investigación métodos de averiguación y aseguramiento de pruebas tales como la intervención *online* de un

miembro de los grupos especiales de actuación ante medios informáticos pertenecientes a las distintas FFCCSS al efecto de enviar al presunto *cracker* ficheros "señuelo", o la intervención de las comunicaciones telemáticas del tercero interviniente en los supuestos en los que se tenga constancia de que el pirata informático se está valiendo de él para emitir órdenes o mensajes dentro de la trama defraudatoria. Sin embargo, los preceptos a través de los que se intentó adaptar la norma a esta problemática se encuentran plagados de incoherencias técnico-informáticas que dificultan su comprensión y la labor de los jueces instructores, además de la del resto de operadores jurídicos intervinientes en el procedimiento judicial concreto.

A la ambigüedad e insuficiencia de las disposiciones legales aplicables a la citada problemática, se debe añadir el desconocimiento generalizado de la mayor parte de los operadores jurídicos del funcionamiento de un sistema informático. Esta ignorancia se hace más palpable a medida que ascendemos en la pirámide jurídica y atendemos al escaso conocimiento que poseen los Jueces y Magistrados españoles en estas lides, que, como se ha expuesto, trae causa de las circunstancias derivadas de la edad de la mayoría de los miembros de la Judicatura, con escasas excepciones. Esta falta de abordaje de su desconocimiento, constituida en una suerte de descargo de importancia del problema, incide de manera determinante en cómo perciben la peligrosidad de las conductas analizadas y en su representación de los delitos informáticos, en los que deben analizar los hechos para separar los aspectos técnicos que han incidido en su perpetración (método utilizado y su complejidad, que indicarán el grado de conocimiento que posee el *cracker;* conocimiento de la trascendencia de la determinación de la "IP" para identificarlo) de los jurídicos derivados de los hechos materiales acaecidos. En definitiva, la inconsciencia sobre los aspectos más básicos del ciberataque priva al instructor del entendimiento sobre la proyección jurídica de la amenaza materializada, despojándole del discernimiento sobre las diligencias de investigación adecuadas a adoptar para asegurar las pruebas de la comisión del delito y abocándole, posiblemente, al dictado de una resolución que no satisfará las exigencias derivadas del derecho a la tutela judicial efectiva del justiciable.

Parafraseando al dramaturgo William Shakespeare, "no hay tinieblas sino en la ignorancia", por lo que para afrontar esta falta de conocimientos no hay mejor instrumento que la formación. En este sentido, el CGPJ ha tomado cartas en el asunto incluyendo en los últimos tiempos los delitos informáticos y su tratamiento técnico-informático en el Plan Docente de Formación de la Carrera Judicial, con el objetivo de que los nuevos miembros de la Judicatura posean las nociones suficientes para encabezar las labores de investigación del delito con adecuación a las características que presente el caso concreto; en este orden de cosas, el Consejo también organiza -aunque no con la asiduidad que sería deseable- en diferentes sedes judiciales cursos de formación sobre los ilícitos analizados. Sin embargo, continúa al alza el número de instructores que desconocen los aspectos básicos de la informática incidentes en la investigación de estos delitos, por lo que resulta primordial la creación e instauración de un programa de formación tecnológica de calidad por parte del CGPJ que supla estas deficiencias y permita a los jueces adquirir estas competencias de manera gratuita y con adaptación a las particularidades del cargo que ostentan y a sus circunstancias personales (horarios, conciliación familiar, etcétera).

Por último, y no menos importante, debemos poner el acento sobre los hábitos *online* de los usuarios. La realidad siempre ilustra la teoría, y en el campo de la ciberseguridad resulta evidente que no sólo los *crackers* se especializan cada vez más en orden a dotar de eficacia a sus métodos para lograr un cometido artero, sino que los

beneficiarios de las prestaciones de la Red ostentan un nivel de desconocimiento sobre la *res* informática que facilita en grado sumo la actividad de los primeros. Esto se debe a que, a pesar de que en la actualidad se ha universalizado el uso de las nuevas tecnologías para las actividades más cotidianas, sigue siendo frecuente que esa utilización se lleve a cabo sin adoptar las mínimas medidas de seguridad que imposibiliten o dificulten el acceso de los piratas informáticos a nuestros datos, fenómeno que responde a la apariencia de seguridad que la intangibilidad de las amenazas vierte sobre el medio empleado.

Al igual que lo sucedido con la formación de los Jueces y Magistrados, es fundamental dispensar información a la población que conciencie a los ciudadanos de la invisibilidad de las amenazas gestadas en la Red y de la posibilidad de ser víctima de ellas, todo ello en orden a ofrecerles mecanismos de seguridad de fácil adaptación según las capacidades de cada usuario. En este sentido, en los últimos tiempos se ha comenzado a introducir el aprendizaje de las TIC en las etapas educativas más tempranas, implementándose paulatinamente a medida que éstas avanzan en dificultad y edad. Si prestamos atención a las entidades de educación superior, observamos que muchas de ellas han incluido en sus guías docentes programas específicos de formación en ciberseguridad, protección de datos de carácter personal y prevención de la delincuencia informática. En lo que al público general se refiere, entidades como INCIBE o el Cuerpo Nacional de Policía son habituales en las redes sociales realizando alertas sobre ciberataques al alza en diferentes momentos o divulgando contenido informativo para prevenir al usuario sobre los peligros que le acechan en Internet y ofrecerle herramientas identificadoras de los mismos.

En definitiva, a pesar de la excepcional labor jurisprudencial de nuestros Tribunales con ocasión de adaptar el preceptuado del C.P. a la ciber-realidad existente, resulta necesaria la concienciación del legislador sobre la importancia del abordaje normativo de las nuevas metodologías delictivas originadas en el terreno de la informática, reformulando la tipificación de tales conductas y dotando a los operadores jurídicos de mecanismos adecuados para el aseguramiento de evidencias de la comisión del delito y de diligencias de investigación tendentes a la averiguación del método empleado y de la identidad del pirata informático, todo ello con el objetivo de depurar las responsabilidades pertinentes. Esta dotación de importancia no debe circunscribirse únicamente al terreno legislativo, sino que es necesario continuar desarrollando políticas educativas que no sólo incluyan en los planes de formación la tecnología, sino que también provean de mecanismos útiles a los ciudadanos para hacer frente a los ciberataques más comunes y, de este modo, equilibrar la desigualdad cognoscitiva entre autor y potencial víctima.

5. BIBLIOGRAFÍA

MANUALES, REVISTAS Y *BLOGS*

- **Congil Díez, Almudena**. *Phishing. Problemática relativa a la calificación jurídica de la participación de los denominados "muleros bancarios". Estado actual de nuestra doctrina y jurisprudencia*. El Derecho, Lefebvre. 15 de marzo de 2013. Recuperado de: https://elderecho.com/phising-problematica-relativa-a-la-calificacion-juridica-de-la-participacion-de-los-denominados-muleros-bancarios-estado-actual-de-nuestra-doctrina-y-jurisprudencia-2
- **Dans, Enrique**. *Sobre los jueces y la ignorancia*. Blog de Enrique Dans. 2 de julio de 2008. Recuperado de: https://www.enriquedans.com/2008/07/sobre-los-jueces-y-la-ignorancia.html
- **Davara Fernández, E. y Davara Fernández, L**. *Delitos informáticos*. Davara Rodríguez, M.A. (Coord.). Pamplona, Ed. Aranzadi. 2017.
- **Hernández Trasobares**, **Alejandro**. *Los sistemas de información: evolución y desarrollo*. Dialnet. Proyecto Social: Revista de relaciones laborales, núm. 10-11. Págs. 149-165. 2003.
- **López, A.** *La investigación policial en Internet: estructuras de cooperación internacional*. Monográfico "III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas". Revista de Internet, Derecho y Política. Universitat Oberta de Catalunya. 2007. Recuperado de: file:///C:/Users/missm/Downloads/Dialnet-LaInvestigacionPolicialEnInternetEstructurasDeCoop-2372614.pdf
- **López-Muñoz, J**. *Cibercriminalidad e investigación tecnológica*. Madrid, Ed. Dykinson. 2020.
- **Martínez, Santiago**. *Introducción sobre el delito de estafa mediante las obras de arte (II): análisis jurisprudencial*. Law&Trends. 22 de febrero de 2019. Recuperado de: https://www.lawandtrends.com/noticias/penal/introduccion-sobre-el-delito-de-estafa-mediante-las-obras-de-arte-ii-analisis-jurisprudencial-1.html
- **Miró Llinares, F.** *La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen*. Revista Electrónica de Ciencia Penal y Criminología. Núm. 13-07. 2011. Recuperado de: https://www.unedpamplona.es/docs/file/documentacion%20fernando%20miro.pdf
- **Quintero Olivares, G**. *Internet y Derecho Penal. Imputación de los delitos y determinación de la competencia*. La Ley Penal: revista de derecho penal, procesal y penitenciario. Sección Estudios. Nº 37. 2007.
- **Rayón Ballesteros, M.C. y Gómez Hernández, J.A**. *Cibercrimen: particularidades en su investigación y enjuiciamiento*. Anuario Jurídico y Económico Escurialense, XLVII. Pp. 209 a 234. 2014. Recuperado de: file:///C:/Users/missm/Downloads/Dialnet-Cibercrimen-4639646.pdf
- **Revista E-Justicia**. Tecnologías de la Información y las Comunicaciones. Núm. 3. Mayo de 2007. Recuperada de: file:///C:/Users/missm/Downloads/EJusticia3_1.0.0.pdf
- **Rodríguez Caro, María Victoria**. *Estafa informática. El denominado phishing y la conducta del "mulero bancario": categorización y doctrina de la Sala Segunda del Tribunal Supremo*. Noticias Jurídicas. 30 de octubre de 2015.

Recuperado de: https://noticias.juridicas.com/conocimiento/articulos-doctrinales/10617-estafa-informatica-el-denominado-phishing-y-la-conducta-del-ldquo;mulero/

- **Velasco Núñez, E**. *Delitos tecnológicos: cuestiones penales y procesales*. La Ley. 2021.
- **Velasco Núñez, E. y Sanchís Crespo, C**. *Delincuencia informática. Tipos delictivos e investigación*. Ed. Tirant lo Blanch. 2019.

PÁGINAS *WEB*

- **Avast Academy**. *¿Qué es una dirección IP?* 19 de mayo de 2021. Recuperado de: https://www.avast.com/es-es/c-what-is-an-ip-address
- **CCN-CERT**. *Alerta: repunte de campañas de phishing por COVID-19.* 19 de marzo de 2020. Recuperado de: https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/9716-ccn-cert-al-05-20-repunte-campanas-de-phishing-por-covid-19.html
- **Circulante**. *Los sistemas de información ejecutiva, herramienta de seguimiento de indicadores de negocio claves en crisis*. 22 de julio de 2020. Recuperado de: https://circulante.com/finanzas-corporativas/los-sistemas-informacion-ejecutiva-indicadores-crisis/
- **Digital Guide IONOS**. *Ficheros log: toda la información de registro en un archivo*. 30 de junio de 2016. Recuperado de: https://www.ionos.es/digitalguide/online-marketing/analisis-web/el-log-el-archivo-de-registro-de-procesos-informaticos/
- **Digital Guide IONOS**. *Arpanet: los primeros pasos de Internet*. 19 de marzo de 2018. Recuperado de: https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/arpanet-los-inicios-de-internet/
- **Digital Guide IONOS**. *Spear phishing: ciberataques personalizados*. 30 de abril de 2020. Recuperado de: https://www.ionos.es/digitalguide/correo-electronico/seguridad-correo-electronico/spear-phishing/
- **Globalbit**. *¿Qué es un sistema de soporte a la decisión (DSS)?* 18 de febrero de 2020. Recuperado de: https://www.globalbit.co/2020/02/18/que-es-un-sistema-de-soporte-a-la-decision-dss/
- **González, Yolanda**. *Cracker informático. ¿Es lo mismo que un hacker?* Grupo Atico34. 4 de septiembre de 2020. Recuperado de: https://protecciondatos-lopd.com/empresas/cracker-informatico/
- **Hackplayers.** *Cómo hacer una campaña de phishing paso a paso con Phishing Frenzy*. 31 de julio de 2015. Recuperado de: https://www.hackplayers.com/2015/07/campana-de-phishing-paso-a-paso-phishing-frenzy.html
- **INCIBE**. *Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse*. 5 de septiembre de 2019. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse
- **INTERPOL**. *Ciberdelincuencia: efectos de la COVID-19*. 4 de agosto de 2020. Recuperado de: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

- **Kaspersky**. *Una breve historia de los virus informáticos y lo que nos deparará el futuro*. Consultado el 2 de abril de 2021. Recuperado de: https://latam.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds
- **Kaspersky**. *¿Qué es un ataque de whaling?* Consultado el 22 de marzo de 2021. Recuperado de: https://latam.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack
- **Malwarebytes**. *Suplantación de identidad (phishing)*. Consultado el 20 de febrero de 2021. Recuperado de: https://es.malwarebytes.com/phishing/
- **Panda Security**. *¿Western Union ligado al cibercrimen?* 20 de mayo de 2010. Recuperado de: https://www.pandasecurity.com/es/mediacenter/seguridad/western-union-ligado-al-cibercrimen/
- **Parcela Digital**. *Micral N, el primer ordenador comercial de la historia basado en microprocesador*. 6 de abril de 2017. Recuperado de: https://parceladigital.com/2017/04/06/micral-n-el-primer-ordenador-comercial-de-la-historia-basado-en-microprocesador/
- **Red-hacking.** *Campaña de Phishing Controlada (CPC)*. 2015. Recuperado de: https://www.redhacking.com/campana-de-phishing-controlada/
- **Softwarelab.org**. *¿Qué es hardware y software? Definición y diferencias*. Consultado el 3 de marzo de 2021. Recuperado de: https://softwarelab.org/es/que-es-hardware-y-software-definicion-y-diferencias/

ARTÍCULOS PERIODÍSTICOS

- **Cinco días**. *¿Estoy protegido ante un espía industrial?* 31 de agosto de 2013. Recuperado de: https://cincodias.elpais.com/cincodias/2013/08/30/sentidos/1377874039_831624.html
- **El País**. *El sistema informático del SEPE sufre un ciberataque*. 9 de marzo de 2021. Recuperado de: https://elpais.com/economia/2021-03-09/el-sistema-informatico-del-sepe-sufre-un-ciberataque.html
- **Meneses, Nacho**. *Cada vez más digitalizados, pero menos protegidos*. El País. 10 de junio de 2020. Recuperado de: https://elpais.com/economia/2020/06/10/actualidad/1591770763_800020.html
- **Scarpellini, Pablo**. *Diez años de WikiLeaks: de poner en jaque a gobiernos, al silencio informativo*. El Mundo. 26 de julio de 2010. Recuperado de: https://www.elmundo.es/internacional/2020/07/26/5f1c6ffdfdddff71ba8b45db.html
- **Sierra, Rosalía**. *Torrejón, primer hospital español "secuestrado" por un virus informático*. El Mundo, 22 de enero de 2020. Recuperado de: https://www.elmundo.es/ciencia-y-salud/salud/2020/01/21/5e274be1fdddffcf088b462d.html
- **Zofío Lleó, Lara**. *Los ministros y altos cargos del Gobierno fueron hackeados con técnicas de ingeniería social*. El Confidencial. 6 de septiembre de 2020. Recuperado de:

https://www.elconfidencialdigital.com/articulo/seguridad/ministros-han-sido-hackeados-tecnicas-ingenieria-social/20200904170228159189.html

INFORMES

- **Microsoft Corporation**. *Digital Defense Report, September 2020*. Consultado el 9 de abril de 2021. Recuperado de: https://www.microsoft.com/en-us/download/details.aspx?id=101738
- **Ministerio del Interior, Secretaría de Estado de Seguridad**. *Estudio sobre la Cibercriminalidad en España*. Año 2019. Recuperado de: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Documents/2020/070620-cibercriminalidad.pdf

NORMATIVA

- **Consejo de Europa**. Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Boletín Oficial del Estado, núm. 226, de 17 de septiembre de 2010, pp. 78847 a 78896. Recuperado de: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

- **España**. Real Decreto de 14 de noviembre de 1882, por el que se aprueba la Ley de Enjuiciamiento Criminal. Boletín Oficial del Estado, núm. 260, de 17 de septiembre de 1882, pp. 803 a 806. Recuperado de: https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036
- España. Decreto 3096/1973, de 14 de septiembre, por el que se publica el Código Penal, texto refundido conforme a la Ley 44/1971, de 15 de noviembre (derogado). Boletín Oficial del Estado, núm. 297, de 12 de diciembre de 1973, pp. 24004 a 24018. Recuperado de: https://www.boe.es/buscar/doc.php?id=BOE-A-1973-1715
- España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Boletín Oficial del Estado, núm. 281, de 24 de noviembre de 1995, pp. 33987 a 34058. Recuperada de: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444
- España. Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia. Boletín Oficial del Estado, núm. 97, de 22 de abril de 1996, pp. 14369 a 14396. Recuperado de: https://www.boe.es/diario_boe/txt.php?id=BOE-A-1996-8930
- España. Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico. Boletín Oficial del Estado, núm. 166, de 12 de julio de 2002, pp. 25388 a 25403. Recuperado de: https://www.boe.es/buscar/doc.php?id=BOE-A-2002-13758
- España. Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. BOE núm. 152, de 23 de junio, pp. 54811 a 54883. Recuperado de: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-9953
- España. Instrucción 2/2011, de 11 de octubre, sobre el Fiscal de Sala para la Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías. Recuperada de: https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-I-2011-00002.pdf

- España. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Anexo - Instrucción Nacional de notificación y gestión de ciberincidentes. "2. Clasificación/taxonomía de los ciberincidentes". BOE núm. 218, de 8 de septiembre de 2018, pp. 87675 a 87696. Recuperado de: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257
- España. Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera. Boletín Oficial del Estado, núm. 284, de 24 de noviembre de 2018, pp. 114474 a 114568. Recuperado de: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16036

- **Unión Europea**. Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior. Diario Oficial de las Comunidades Europeas, núm. 178, de 17 de julio de 2000, pp. 1 a 16. Recuperada de: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:L:2000:178:TOC
- Unión Europea. Decisión Marco del Consejo, de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo. Diario Oficial de la Unión Europea, núm. 149, de 2 de junio de 2001, pp. 1 a 4. Recuperada de: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32001F0413
- Unión Europea. 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. Diario Oficial de la Unión Europea, núm. 123, de 10 de mayo de 2019, pp. 18 a 29. Recuperada de: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32019L0713
- Unión Europea. Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales. Diario Oficial de la Unión Europea, núm. 136, de 22 de mayo de 2019, pp. 1 a 27. Recuperada de: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32019L0770

ACUERDOS DE LA SALA SEGUNDA DEL TRIBUNAL SUPREMO

- Acuerdo de Pleno no Jurisdiccional de 3 de febrero de 2005. Recuperado de: https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunal-Supremo/Jurisprudencia-/Acuerdos-de-Sala/Acuerdos-de-3-de-febrero-de-2005-sobre--1--Principio-de-ubicuidad---2--Clausulas-de-reserva-de-dominio-y-prohibicion-de-enajenar---3--Principio-de-minimos-psicoactivos-en-relacion-al-art--368-CP
- Acuerdo de Pleno no Jurisdiccional de 30 de octubre de 2007. Recuperado de: https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunal-Supremo/Jurisprudencia-/Acuerdos-de-Sala/Acuerdo-de-30-de-octubre-de-2007-sobre-delito-continuado-de-estafa-y-apropiacion-indebida

6. ANEXO: JURISPRUDENCIA

TRIBUNAL SUPREMO

- **AUTOS**

– Auto (Sala Segunda, Sección 1ª) de 1 de abril de 2004. Recuperado de: https://www.poderjudicial.es/search/AN/openDocument/9459eacd588d0bd3/20040506

– Auto (Sala Segunda, Sección 1ª) de 24 de enero de 2007. Recuperado de: https://www.poderjudicial.es/search/AN/openDocument/260000bf5d1ba7ea/20070301

– Auto (Sala Segunda, Sección 1ª) de 12 de noviembre de 2009. Recuperado de: https://www.poderjudicial.es/search/AN/openDocument/71668b92ae3eddf9/20091203

– Auto (Sala Segunda, Sección 1ª) de 21 de septiembre de 2011. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/de4b1d1882501106/20111013

– Auto (Sala Segunda, Sección 1ª) de 26 de octubre de 2011. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/3896535ad1704006/20111114

– Auto (Sala Segunda, Sección 1ª) de 26 de septiembre de 2012. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/4c34d1315b1f93f1/20121106

– Auto (Sala Segunda, Sección 1ª) de 29 de enero de 2015. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/8c918323f91192f7/20150206

– Auto (Sala Segunda, Sección 1ª) de 22 de febrero de 2018. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/41044a6eb410bc67/20180305

- **SENTENCIAS**

– Sentencia (Sala Segunda, Sección 1ª) nº 482/2000, de 21 de marzo. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/6033c0352d823f82/20030830

– Sentencia (Sala Segunda, Sección 1ª) nº 2175/2001, de 20 de noviembre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/1a6d6edff892eb94/20031203

– Sentencia (Sala Segunda, Sección 1ª) nº 1476/2004, de 21 de diciembre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/2b15875e60f6439f/20050126

– Sentencia (Sala Segunda, Sección 1ª) nº 1169/2006, de 30 de noviembre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/5a04b820e5a9949f/20061221

– Sentencia (Sala Segunda, Sección 1ª) nº 229/2007, de 22 de marzo. Recuperada de:

https://www.poderjudicial.es/search/AN/openDocument/feb3c0fb350b0960/20070419

- Sentencia (Sala Segunda, Sección 1ª) nº 369/2007, de 9 de mayo. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/45bf2634bf3ee393/20070607
- Sentencia (Sala Segunda, Sección 1ª) nº 533/2007, de 12 de junio. Recuperada de: https://www.poderjudicial.es/search/TS/openDocument/8ca791eb038076d3/20070712
- Sentencia (Sala Segunda, Sección 1ª) nº 482/2008, de 28 de junio. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/32aa4ceb2bf7a528/20150206
- Sentencia (Sala Segunda, Sección 1ª) nº 860/2008, de 17 de diciembre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/692d2557812d3947/20090122
- Sentencia (Sala Segunda, Sección 1ª) nº 465/2012, de 1 de junio. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/bd0a5643f18570c6/20120615
- Sentencia (Sala Segunda, Sección 1ª) nº 834/2012, de 25 de octubre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/36942f02bd94a852/20121224
- Sentencia (Sala Segunda, Sección 1ª) nº 987/2012, de 3 de diciembre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/13dd9710e948cd2c/20121228
- Sentencia (Sala Segunda, Sección 1ª) nº 997/2013, de 19 de diciembre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/c8b9510931739b07/20140217
- Sentencia (Sala Segunda, Sección 1ª) nº 421/2014, de 26 de mayo. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/5ed8cec8965eab4a/20140613
- Sentencia (Sala Segunda, Sección 1ª) nº 845/2014, de 2 de diciembre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/32aa4ceb2bf7a528/20150206
- Sentencia (Sala Segunda, Sección 1ª) nº 256/2015, de 7 de mayo. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/bf8940ea34eecfb9/20150522
- Sentencia (Sala Segunda, Sección 1ª) nº 970/2016, de 21 de diciembre. Recuperada de:

https://www.poderjudicial.es/search/AN/openDocument/ea0775e0131d1c9e/20170110
- Sentencia (Sala Segunda, Sección 1ª) nº 70/2017, de 8 de febrero. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/28eeb389ca4a7e0e/20170222
- Sentencia (Sala Segunda, Sección 1ª) nº 94/2018, de 23 de febrero. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/1414e539d40f90c9/20180320
- Sentencia (Sala Segunda, Sección 1ª) nº 509/2018, de 26 de octubre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/c3f1f6a840993eef/20181109
- Sentencia (Sala Segunda, Sección 1ª) nº 143/2019, de 14 de marzo. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/8939261909812050/20190329

AUDIENCIAS PROVINCIALES

- **SENTENCIAS**

- Sentencia de la Audiencia Provincial de Pontevedra (Sección 5ª) nº 47/2009, de 15 de julio. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/2dba7c47414cbe8a/20090806
- Sentencia de la Audiencia Provincial de Castellón (Sección 1ª) nº 313/2009, de 20 de julio. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/72837c990d6a2dc1/20100415
- Sentencia de la Audiencia Provincial de Palencia (Sección 1ª) nº 14/2011, de 3 de noviembre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/413db0378f4a7887/20111124
- Sentencia de la Audiencia Provincial de Asturias (Sección 1ª) nº 351/2012, de 18 de septiembre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/b39fd042a2fce878/20121127
- Sentencia de la Audiencia Provincial de Ciudad Real (Sección 1ª) nº 159/2012, de 20 de septiembre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/63ff53bad4b5197a/20121204
- Sentencia de la Audiencia Provincial de Barcelona (Sección 3ª) nº 8/2013, de 8 de enero. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/2a3c12f771a0d14d/20130301
- Sentencia de la Audiencia Provincial de Málaga (Sección 3ª) nº 606/2013, de 23 de octubre. Recuperada de:

https://www.poderjudicial.es/search/AN/openDocument/5b0ffdb8a0a589d6/20131219

- Sentencia de la Audiencia Provincial de La Rioja (Sección 1ª) nº 138/2013, de 3 de diciembre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/6ae94f4cc030d9f4/20140129
- Sentencia de la Audiencia Provincial de Zaragoza (Sección 1ª) nº 85/2014, de 19 de febrero. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/1f9273cc74b7b71d/20140325
- Sentencia de la Audiencia Provincial de Valencia (Sección 5ª) nº 491/2016, de 5 de septiembre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/7066c58318104256/20180307
- Sentencia de la Audiencia Provincial de Valencia (Sección 2ª) nº 37/2017, de 25 de enero. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/ac8ac51d541d47ef/20170614
- Sentencia de la Audiencia Provincial de Barcelona (Sección 9ª) nº 347/2017, de 24 de abril. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/f96884c89b48c8dc/20170621
- Sentencia de la Audiencia Provincial de Alicante (Sección 8ª) nº 107/2018, de 12 de marzo. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/9718501a458ca5d7/20180613
- Sentencia de la Audiencia Provincial de Guipúzcoa (Sección 1ª) nº 147/2018, de 28 de junio. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/f311ebae6853b317/20181016
- Sentencia de la Audiencia Provincial de Huelva (Sección 3ª) nº 231/2018, de 7 de noviembre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/7e7e5e0ea5bef73a/20190129
- Sentencia de la Audiencia Provincial de Murcia (Sección 2ª) nº 70/2019, de 27 de febrero. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/f4f15e1c665382a0/20190402
- Sentencia de la Audiencia Provincial de Jaén (Sección 2ª) nº 121/2019, de 28 de mayo. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/8b3b124e7e72e573/20190701
- Sentencia de la Audiencia Provincial de Las Palmas de Gran Canaria (Sección 1ª) nº 235/2019, de 29 de junio. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/08a4ebcb3942162b/20190905
- Sentencia de la Audiencia Provincial de Alicante (Sección 2ª), nº 408/2019, de 4 de noviembre. Recuperada de:

https://www.poderjudicial.es/search/AN/openDocument/79d7b8a5db9c11b1/20201029

- Sentencia de la Audiencia Provincial de Madrid (Sección 7ª) nº 121/2020, de 6 de marzo. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/b9777598e8de484e/20200709
- Sentencia de la Audiencia Provincial de Barcelona (Sección 2ª) nº 229/2020, de 30 de marzo. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/33d326106d348fa8/20200706
- Sentencia de la Audiencia Provincial de Vizcaya (Sección 2ª) nº 26/2020, de 19 de abril. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/b7f2b598b1a4e7c3/20210305
- Sentencia de la Audiencia Provincial de Madrid (Sección 15ª), nº 197/2020, de 20 de mayo. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/a34e5780f8cfde63/20201102
- Sentencia de la Audiencia Provincial de Madrid (Sección 23ª) nº 412/2020, de 28 de septiembre. Recuperada de: https://www.poderjudicial.es/search/AN/openDocument/2362dccd97a59bd8/20210107