Universitat Autònoma de Barcelona

TÍTULO: Los delitos económicos en internet

AUTORA: Irene Rodríguez Rodríguez

GRADO: Grado en Administración y Dirección de empresas y Grado en Derecho

TUTOR: Luís Salgado Rodríguez

FECHA: 4 de junio de 2019

RESUMEN

Cuando hablamos de delitos económicos en internet, nos situamos en un plano donde se une algo tradicional (los delitos) con algo sumamente novedoso históricamente hablando (internet). Es esta conjunción la que hace que aparezcan sendas dificultades que actualmente aún no gozan de respuesta práctica ni teórica a la que poder acogernos para solventar todas las contingencias presentes y futuras que se presentan y/o podrán presentarse en un futuro próximo.

No obstante, esta triple unión de delitos, economía y tecnología no resulta tan ampliamente conocida e identificada como puede ocurrir con otra tipología distinta de delitos. Es por ello que, en el presente trabajo, trataremos de abordar las cinco preguntas esenciales a la hora de configurar el marco teórico de cualquier cuestión: qué, cuándo, dónde, cómo y quién. Así mismo, se tratará de plasmar de forma sucinta aquellas problemáticas presentes y futuras más relevantes que existen alrededor de esta cuestión.

Por tanto, la finalidad del presente estudio versará sobre la identificación y descripción de esta tipología de delitos menos conocida pero que está ganando cada vez más terreno a los delitos tradicionales o físicos.

Contenido

INTRODUCCIÓN

La cita que encabeza este trabajo puede resultar curiosa, atrevida e incluso graciosa, en algunos casos. No obstante, esta frase representa mucho mejor la realidad de lo que en realidad podamos llegar a imaginar.

En primer lugar, los delitos informáticos en sí mismos ya representan "los grandes desconocidos" dentro de todo el elenco de tipos delictivos existentes en el Código Penal. En segundo lugar, cuando estos además de ser informáticos reciben la etiqueta de "económicos", la cuestión acaba revirtiéndose de una doble complejidad nada difícil de abordar y dilucidar.

A pesar de este desconocimiento general que existe acerca de los mismos, esto no quiere decir, ni de lejos, que sean tipos delictivos inusuales o "residuales" dentro de la vida cuotidiana actual. De hecho, podría decirse que son los tipos delictivos que más importancia tienen en una sociedad donde la tecnología, las redes sociales y el mundo virtual es un elemento esencial para toda persona que se precie.

Es por ello que, en el presente trabajo, se intentará dar respuesta a las principales preguntas que pueden surgir ante cualquier elemento novedoso y desconocido como son los delitos económicos en internet: ¿Qué? ¿Cuándo? ¿Dónde? ¿Cómo? ¿Quién?

Además de ello, y como parte final del estudio, se pondrán de relieve numerosos problemas presentes y futuros relacionados con los delitos informáticos en internet (todo ello sin ánimo exhaustivo, puesto que a medida que la tecnología avanza, los problemas también avanzan inevitablemente con ellos).

Con ello, espero poder arrojar un rayo de luz a esta cuestión y conseguir que, después de navegar entre estas líneas, el lector sea capaz de tener una noción general de los principales elementos y problemáticas que rodean los delitos económicos informáticos tan presentes en la sociedad. Un primer contacto con un mundo que, posiblemente, a la luz de los recientes acontecimientos, no tardará en convertirse el único mundo que conoceremos.

1. ENCAJE DE LA REALIDAD VIRTUAL EN UNA SOCIEDAD CARACTERIZADA POR LA REALIDAD FÍSICA

Cuando entra en escena el término "**informática**" en cualquiera de los contextos de la realidad, todo parece volverse menos claro y más difuso para la gran mayoría de personas. Cuando hablamos de la realidad virtual, aunque estemos tratando de algo tan simple como una compra por internet, por mucho que pueda parecerse a una compra física de las que se han llevado a cabo hasta ahora, todo parece cambiar y convertirse en algo completamente diferente. Lo mismo ocurre con los delitos por internet.

Nos encontramos en un entorno en el que el Big Data juega un gran papel fundamental, tanto en la vida cuotidiana que transcurre en los hogares de las personas de a pie como en los más altos despachos donde se firman los contratos más exclusivos a nivel mundial. Hoy en día, el 87% de los hogares tienen acceso a la electricidad y un 43% de la población mundial tiene acceso a internet. Ahí es donde entra en escena el Big Data, aunque aún no seamos plenamente conscientes de ello o de su magnitud.

En este sentido no debemos olvidar que, cuando hablamos de Big Data, y según el concepto dado por el Instituto de Ingeniería del Conocimiento, nos estamos refiriendo al "*gran volumen de datos que debe ser capaz de tratar, la velocidad con la que puede procesar esos datos, la variedad de formas que pueden tomar los mismos y el valor que se obtiene por la información extraída de los datos*" y, todos ellos obtenidos a través de fuentes tecnológicas. Es por ello que éste tiene un gran impacto cuando hablamos de los delitos a través de internet, ya que muchos de ellos se configuran a raíz de los datos que fraudulentamente se han obtenido a través de cualquier dispositivo tecnológico, por ejemplo ordenadores, móviles y, cada vez más, electrodomésticos[1].

Así las cosas, aunque la dinámica actual esté caracterizada por ser un entorno mayoritariamente físico, esta no parece ser la tendencia mundial verso a la cual avanzamos a pasos agigantados, en gran parte propiciado por el aumento del uso de

[1] Estos últimos conectados a internet, configurándose así el fenómeno conocido como *"internet of the things"*, el internet de las cosas. El origen de este término data de 1999, cuando fue por primera vez utilizado en el título de una conferencia por Kevin Ashton, cofundador del Instituto de Tecnología de Massachusetts. ASHTON, Kevin. (3 de julio de 2010). The "Internet of the Things" thing. *RFID Journal*. Recuperado de: http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf

dispositivos tecnológicos y, en particular, el aumento de la población mundial con acceso a los dispositivos móviles. Una gran muestra de ello es la aparición de las **criptomonedas**, unas divisas encriptadas de carácter puramente virtual y sin ningún soporte físico que han sido objeto de un gran fenómeno especulativo en los últimos años.

La sociedad actual está pasando por un período de transición de la realidad física a la **realidad virtual**, escenario que también se está produciendo en el campo de los de los delitos cometidos por internet. En este sentido, DE EUSEBIO. L., director adjunto de la Europol y miembro del Cuerpo Nacional de Policía, indica que, "*mientras que el crimen tradicional está registrando un descenso de entre el 3 y el 4%, en España el cibercrimen aumenta en torno al 12%, en la misma proporción que en otros países europeos de nuestro entorno"*[2].

Cada vez más la realidad virtual va ganando terreno en muchos aspectos de la vida cuotidiana y, como parte de ella, tal como nos indicaba DE EUSEBIO, L., también está ganando terreno la comisión de delitos a través de internet, aunque no siempre se sepa identificarlos como tal[3]. En la línea de no poder vislumbrar la totalidad de este fenómeno, y para ilustrar más gráficamente esto, en este campo se habla del término "**iceberg**", que significaría que realmente lo que somos capaces de ver y conocer es la punta de este iceberg, pero que debajo de él hay un entramado mucho más grande y que representa cerca del 96% de todo el conjunto[4].

Es por ello que, a las cifras de los delitos cometidos por internet -también llamado cibercrimen-, se les conoce popularmente como "**cifras negras**"[5], dado que es prácticamente imposible poder llegar a saber con certeza el impacto económico real que éstos pueden llegar a tener. A este entramado subyacente y al que no se puede acceder con facilidad se le conoce como "**deep web**". Se trata de una "red sumergida" en la cual

[2] *El 80 % de los delitos en internet son estafas y el 10 % pornografía infantil*. (7 de mayo de 2015). La Vanguardia. Recuperado de: https://www.lavanguardia.com/tecnologia/20150506/54431079001/el-80-de-los-delitos-en-internet-son-estafas-y-el-10-pornografia-infantil.html

[3] MARTÍNEZ, María José. (28 de febrero de 2017). El 5% de los delitos se cometen por internet y redes sociales. Córdoba: *Cadena Ser*. Recuperado de: https://cadenaser.com/emisora/2017/02/28/radio_cordoba/1488277241_095891.html

[4] Unión Europea. (2017) Informe SOCTA (Serious and Organised Crime Threat Assessment): Crimen en la era de la tecnología.

[5] Facultad de Informática - Universidad Complutense de Madrid. (21 de enero de 2015). *Delitos en internet*. [Archivo de vídeo]. Minuto 12:29. Recuperado de: https://www.youtube.com/watch?v=o7u0T7cpyJQ

la mayoría de los usuarios llevan a cabo actividades ilícitas o subrepticias utilizando una serie de cifrados o encriptaciones que favorece el anonimato de los mismos y propicia, en cierto modo, la impunidad de los delitos allí cometidos.

Dentro de los delitos cometidos a través de internet existen muchas clases o subgrupos, pero los que han sido analizados y categorizados como los que provocan un mayor impacto económico han sido los **delitos económicos**. Estos, a su vez, son los que han experimentado un mayor aumento en los últimos años, llegándose incluso a quintuplicar[6], especialmente los delitos de estafa[7]. Es por todo ello, que en este trabajo trataremos de desgranar los elementos esenciales que afectan a los delitos cometidos por internet y, especialmente, a los delitos económicos.

[6] GARCÍA, Isabel. Cibercrimen: "En España solo se resuelve el 3% de los ciberdelitos denunciados". (24 de abril de 2018). *Nueva tribuna*. Recuperado de: https://www.nuevatribuna.es/articulo/sociedad/cibercrimen-ciberseguridad-ciberdelincuente-ciberatracador-mujeres-hackers-ransanwed-wenacraid-pentesting/20180424183449151198.html

[7] *Injurias o calumnias en Internet y Phishing, los delitos informáticos más comunes. Robo de identidad y estafa, los que más han aumentado*. (20 de octubre de 2014). Noticias Jurídicas. Recuperado de: http://noticias.juridicas.com/actualidad/noticias/4135-injurias-o-calumnias-en-internet-y-phishing-los-delitos-informaticos-mas-comunes-robo-de-identidad-y-estafa-los-que-mas-han-aumentado/

2. ¿QUÉ SON LOS DELITOS INFORMÁTICOS?

2.1. Concepto de delito informático

Como punto de partida, cabría efectuar una conceptualización de lo que se entiende por "**delito informático**". A causa de la reciente implantación jurídicamente hablando de los mismos y de su también reciente aparición en la vida cuotidiana como algo usual, no gozamos por el momento de conceptos oficiales amplios y precisos por parte de ninguno de los organismos estatales, europeos o internacionales que se ocupan diariamente del estudio y del control de los mismos. En este sentido encontraríamos la definición efectuada por parte de la Comisión Europea en una de sus comunicaciones afirmando que se entiende por delito informático "*cualquier delito que de alguna manera implique el uso de tecnología de la información*"[8].

Así las cosas, a la espera de que finalice la transición para la incorporación de los mismos al ordenamiento jurídico, la doctrina ha querido ir elaborando una serie de conceptos más extensos sobre ello, uno de los cuales es que "*constituye un delito informático aquellas operaciones ilícitas realizadas por medio de internet*" y "*cualquier conducta criminal que para su realización haga uso de la tecnología informática, ya sea como método, medio o fin, siendo su objetivo principal destruir y dañar ordenadores, medios electrónicos y redes de internet*"[9].

Tal como hemos podido observar, cuando se habla de delito informático, podemos estar refiriéndonos a dos posibles casuísticas: a) Cualquier actividad ilícita que se lleve a cabo a través de internet, tenga como objetivo un dispositivo informático o no –**concepto amplio del término-**; y b) La conducta que engloba única y exclusivamente aquellas actividades ilícitas que tienen como objetivo la afectación de un dispositivo informático –**concepto estricto del término-**.

[8] Unión Europea. (26 de enero de 2001). *Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos*. Bruselas. p.12.
[9] POVEDA CRIADO, Miguel Ángel. *Delitos en la red*. Editorial Fragua. Madrid. 2015. p.3.

2.2. Características comunes a los delitos informáticos

A pesar de la poca unanimidad acerca del concepto mismo de delito informático, donde sí que ha habido una estandarización en la doctrina ha sido en referencia a las características que los estudiosos y figuras emblemáticas en la materia (policías, fiscales, entre otros) han observado en relación a la comisión de esta modalidad delictiva de reciente implantación. Estas características comúnmente aceptadas, ayudarán a entender un poco mejor qué es a lo que nos referimos cuando se está hablando de un delito informático.

Como punto de partida tendríamos el **desconocimiento de internet**. Conforme se apuntaba con anterioridad, si bien es cierto que gran parte de la población tiene acceso a las nuevas tecnologías y en particular a internet, también lo es que ello no siempre va aparejado con el conocimiento y el buen manejo de los mismos. Este extremo puede desencadenar que muchos ciberdelincuentes se sientan atraídos por la falta de seguridad en línea del usuario y vean en ellos una oportunidad de negocio sin correr excesivos riesgos.

En segundo lugar, y muy ligado con el desconocimiento de internet que apuntábamos supra, podríamos hablar de la **ingenuidad del ciudadano** en sí misma. Con ello se apunta que, a pesar de que los usuarios puedan tener un mayor o menor grado de conocimiento de las herramientas informáticas, puede darse la situación en la cual un usuario sea excesivamente confiado mientras navega por internet no siendo consciente de a todos los peligros a los que se expone mientras navega.

Ello no quiere decir que los ciberdelincuentes únicamente tengan acceso a estos ciudadanos más confiados o menos conocedores de los elementos informáticos, ya que en realidad **cualquiera está expuesto**. Esta tercera característica podría matizarse en tanto en cuanto existen ciertos elementos que podrían aumentar la seguridad en línea de cualquier persona que utilice dispositivos informáticos y disminuirían el riesgo de sufrir un ciberataque. No obstante, esto no garantiza una total inmunidad, ya que existen ciberdelincuentes con unos niveles muy altos de conocimiento informático que podrían llegar a truncar esa seguridad (aunque con mayor dificultad que si el ciudadano no dispusiera de ningún nivel de seguridad).

La cuarta característica la integraría la **facilidad de comisión del tipo delictivo informático**. Todo lo que se ha podido observar en las características anteriores (desconocimiento de internet, ingenuidad del ciudadano y la posibilidad de que todo el mundo esté expuesto) configuran los elementos básicos de la facilidad de los ciberdelincuentes para cometer estos delitos, en tanto en cuanto los esfuerzos que tienen que emplear para poder llevar a cabo un ciberataque son mucho menores que si la comisión del tipo va dirigida contra un usuario consciente de todos los riesgos y peligros de internet. Además de ellos, la facilidad también vendría dada por la sencillez implícita en la utilización de las nuevas tecnologías, según afirmaba el inspector de la Policía Nacional y jefe del Grupo de Delitos Informáticos de Burgos Antonio Salguero[10].

La facilidad alegada va unida, indudablemente, con la quinta característica de los delitos informáticos, la **comisión a distancia**. Los delitos tradicionales en su mayoría exigían la perpetración de los mismos mediante la concurrencia física en espacio y lugar entre la víctima y su agresor, reflejando así la poca relevancia de la que gozaba la tecnología en la vida cuotidiana de la sociedad.

No obstante, los avances tecnológicos e informáticos se han ido abriendo paso, obligando así a la sociedad a adaptarse en todas sus facetas, incluyendo la jurídica. De este modo, a medida que fueron apareciendo los delitos informáticos, se fue produciendo un cambio de paradigma en tanto en cuanto se empezó a concebir la posibilidad de que un delito se pudiera cometer sin exigir la concurrencia de espacio y tiempo entre la víctima y el autor del hecho delictivo.

La sexta característica sería la configuración de los delitos informáticos como **delitos en masa**. Al tratarse de delitos de fácil comisión y perpetrables a distancia, esto provoca que la cantidad de potenciales víctimas aumente de manera exponencial, dado que es posible efectuar un ataque informático simultáneamente a varios usuarios sin que esto exija una complejidad añadida para el autor. Este hecho, además de aumentar las probabilidades de

[10] *Los delitos con internet y las redes sociales suben un 52%*. (11 de septiembre de 2018). Diario de Burgos. Recuperado de: https://www.diariodeburgos.es/noticia/ZB62F8BE4-F63F-D2CA-C76B2012B3B6133E/Los-delitos-con-internet-y-las-redes-sociales-suben-un-52

efectividad del ataque, aumentan considerablemente los potenciales beneficios que se pueden extraer del mismo, dado que las ganancias se multiplican.

Ligado a ello, encontraríamos la séptima característica consistente en la **comisión instantánea** de los delitos informáticos. Lo que esta representa es la brevedad existente respecto al lapso de tiempo entre que el autor del delito inicia los actos necesarios para la realización delictiva y la consumación del mismo.

La característica expuesta quizá configure una de las más aparentemente nimias de todas las examinadas hasta el momento, pero lo cierto es que guarda estrecha relación con una de las características esenciales dentro de los delitos informáticos y, en general, del ámbito de las nuevas tecnologías, la **rapidez**. En este sentido, para los autores de estos tipos delictivos, la posibilidad de realizar las conductas típicas de forma rápida y eficaz proporciona un doble beneficio: 1) Aumenta la posibilidad de efectividad del ataque evitando la capacidad de reacción de las futuras víctimas; 2) Disminuye el peligro para la persona del autor acortando en el tiempo la perpetración del mismo en tanto en cuanto se reducen las posibilidades de que el ataque se frustre.

Todas estas características materiales se completan con las características personales en la comisión de los delitos informático. Por parte del autor del tipo delictivo, el **anonimato** facilita y propicia en gran medida que estos delitos existan y sean tan frecuentes en la sociedad. En este sentido, a pesar del anonimato más obvio como sería el de que estos actos no se cometan mediante la concurrencia física en tiempo y espacio entre la víctima y el autor, también encontraríamos otras medidas de anonimización de lo que llamaríamos la "identidad informática", esto es, la identidad de cada persona en el mundo tecnológico representado a través de medios como la IP.

Como última característica encontraríamos el **desconocimiento de las víctimas** contra las cuales los autores de los delitos informáticos dirigen sus ataques. La relevancia de esta característica recae en el hecho de que, en los delitos tradicionales en lo cuales no intervienen medios tecnológicos, la concurrencia de espacio y tiempo entre la víctima y el agresor lleve al hecho de que el autor sea consciente en todo momento de contra quien está dirigiendo sus actos, quién es la víctima. No obstante, cuando hablamos de un delito informático, este panorama en ocasiones puede verse alterado ya que, si bien en algunos

casos los autores pueden tener identificadas a las víctimas contra las cuales quieren actuar, en la mayoría de ocasiones lo desconocen.

2.3. Los delitos informáticos en el Código Penal

Al ver que existen dos conceptos diferentes acerca de lo que considera delito informático, cabe hacer una enumeración de los diferentes grupos de delitos existentes en el actual Código Penal (de ahora en adelante, CP) al respecto, con tal de poder delimitar el ámbito de estudio al que nos estamos circunscribiendo.

De nuevo nos encontramos que, al ser una materia de tan reciente incorporación, existe discrepancia acerca de cuáles son exactamente los artículos que quedarían englobados aquí. De este modo, lo que ofreceremos a continuación será la pormenorización más detallada al respecto, dado que así lograremos no dejar fuera artículos que parte de la doctrina especializada en la materia considera de especial importancia para entender este fenómeno legislativo.

Grosso modo, los delitos informáticos podrían ser agrupados en tres grandes categorías:

2.3.1. Delitos exclusivamente informáticos[11]

Aquí se integrarían aquellos preceptos del Código Penal que prevén en la conducta típica el elemento informático para incurrir necesariamente en el tipo, es decir que, en el caso de no darse este elemento, quizá estaríamos incurriendo en un delito de todas formas, pero no en unos de los listados a continuación. En este sentido, nos encontraríamos con los siguientes delitos:

a) Delito de **allanamiento informático** del artículo 197 bis.1 CP; donde se tipifica el acceso a un sistema de información o la facilitación de dicho acceso a terceros.

[11] Relativos a los artículos 197 bis.1, 197 bis.2 y 197 ter del Capítulo II del Título II, Libro II; 248.2.a) y 248.2.b) de la Sección 1ª del Capítulo VI del Título XIII, Libro II; 264, 264 bis y 264 ter del Capítulo IX del Título XIII, Libro II; y 573.2 de la Sección 2ª del Capítulo VIII del Título XXII, Libro II; todos ellos pertenecientes a la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

b) Delito de **interceptación de transmisiones no públicas de datos informáticos** del artículo 197 bis.2 CP; cuya conducta típica consiste en el apoderamiento de datos informáticos privados producidos "*desde, hacia o dentro de un sistema de información*".

c) Delito de **facilitación en la comisión del delito de espionaje informático o interceptación de datos informáticos** del artículo 197 ter CP; la conducta típica del cual consiste en la "*producción, adquisición o facilitación*" de programas informáticos o códigos de acceso a terceros para favorecer la comisión de los delitos de espionaje informático o interceptación de datos informáticos.

d) Delito de **estafa informática** del artículo 248.2.a) CP; en el que se castiga la obtención de una "*transferencia de activo no consentida*" por el titular, causándole un perjuicio económico al mismo y haciendo uso de algún tipo de "*manipulación informática*".

e) Delito de **facilitación de la comisión del delito de estafa informática** del artículo 248.2.b); en donde se penaliza el hecho de "*fabricar, introducir, poseer o facilitar programas informáticos específicamente destinados a cometer el delito de estafa*" informática.

f) Delito de **sabotaje informático** del artículo 264 CP; constituyendo como como conducta típica del mismo cualquier daño grave producido a "*datos informáticos, programas informáticos o documentos electrónicos*".

g) Delito de **obstaculización o interrupción informática** del artículo 264 bis CP; en el que se tipifica la afectación mediante "*obstaculización o interrupción del funcionamiento de un sistema informático*" transfiriendo los datos que en él se encuentran o causando daños a los mismos.

h) Delito de **facilitación de la comisión del delito de sabotaje informático o de obstaculización o interrupción informática** del artículo 264 ter CP; la conducta típica del cual es "*facilitar*" la obtención de medios informáticos para cometer los delitos de sabotaje y obstaculización o interrupción informáticos.

i) Delito de **terrorismo informático** del artículo 573.2 CP; en el que el hecho típico constituye la comisión de alguno de los delitos informáticos previstos en los artículos 197 bis, 197 ter o 264 a 264 quater del CP con las "*finalidades*" previstas para el delito de terrorismo del apartado primero del mismo artículo 573 CP.

La mayoría de estos delitos fueron introducidos a raíz de la última reforma operada al texto penal mediante la Ley Orgánica 5/2010, ya que existía una cierta presión desde múltiples organismos europeos e internacionales para regular y tipificar este tipo de conductas por el reproche penal de las mismas y el crecimiento de este tipo de delitos en la sociedad actual.

Además de ello, no únicamente se han tipificado las conductas en sí mismas, sino que también se han querido plasmar en el texto penal todas aquellas conductas destinadas a facilitar la comisión de las mismas, dado que se castiga del mismo modo los llamados actos preparativos punibles.

2.3.2. Delitos parcialmente informáticos[12]

Formarían parte de este grupo aquellos delitos en cuyo articulado aparece reflejada la intervención de algún elemento informático para la comisión del tipo (de forma expresa o mediante conceptos dentro de los cuales se podrían incluir) pero que no representan el único modo de incurrir en el tipo, dado que se posibilita la intervención de medios alternativos que darían lugar, del mismo modo, a la realización típica.

a) Delito de **descubrimiento y revelación de secretos** del artículo 197 CP; cuya conducta típica consiste en el "*apoderamiento*" de comunicaciones privadas, una de las cuales la constituyen los correos electrónicos.

[12] Relativos a los artículos 197 del Capítulo I del Título X, Libro II; 211 del Capítulo III del Título XI, Libro II; 255 y 256 de la Sección 3ª del Capítulo VI del Título XIII, Libro II; 270 de la Sección 1ª del Capítulo XI del Título XIII, Libro II; 273 de la sección 2ª del Capítulo XI del Título XIII, Libro II; 278 y 286 de la Sección 3ª del Capítulo XI del Título XIII, Libro II; y 390 de la Sección 1ª del Capítulo II del Título XVIII, Libro II; todos ellos pertenecientes a la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

b) Delito de **publicidad de calumnias e injurias a través de medios de difusión** del artículo 211 CP; cuya conducta típica la integra la "*propagación*" de las calumnias e injurias a través de medios tales como "*la imprenta, la radiodifusión o cualquier otro*" que repute una eficacia similar. Por mucho que este delito pueda parecer exactamente igual al delito de calumnias e injurias a través de internet considerados individualmente, cabe decir que lo que realmente se está castigando aquí no es la mera realización de dichas conductas típicas a través de medios informáticos, sino su difusión a un número de personas considerable, lo que podría cumplirse en el caso de que dichas calumnias o injurias se propagaran a través de internet, ya sea mediante portales o mediante redes sociales.

c) Delito de **defraudación fluidos** del artículo 255 CP; donde se tipificaría la utilización de "*fluidos o telecomunicaciones ajenos*" entre los cuales se incluiría la utilización de telecomunicaciones informáticas ajenas, como por ejemplo internet.

d) Delito de **utilización fraudulenta de equipos de telecomunicación** del artículo 256 CP; donde la conducta típica sería utilizar "*sin el consentimiento del titular y con perjuicio económico*" para el mismo de "*cualquier equipo terminal de telecomunicación*", entre los cuales se incluirían los terminales informáticos.

e) Delito contra la **propiedad intelectual** del artículo 270 CP; por el que se castiga la "*explotación económica*", con fines lucrativos, "*de obras literarias, artísticas o científicas en cualquier soporte*", dentro del cual podrían incluirse con facilidad aquellas fijadas en soportes informáticos (como la difusión de dichas obras a través de un portal de internet, tal como se explicita en el apartado tercero del mismo precepto).

f) Delito contra la **propiedad industrial** del artículo 273 CP; penalizándose la "*fabricación, importación, posesión, utilización, ofrenda o introducción*" "*con fines industriales o comerciales*" "*objetos amparados*" por un derecho de patente o modelo de utilidad. En este sentido, la relación con los elementos informáticos vendría dada por el hecho de que, dentro de la comercialización de dichos productos, podría incluirse la comercialización a través de internet tan extendida actualmente.

g) Delito de **descubrimiento de secreto de empresa** del artículo 278 CP; la conducta típica del cual es el "*apoderamiento*" de "*datos o documentos en cualquier soporte*", incluidos expresamente los informáticos, con la finalidad de "*descubrir un secreto de empresa*".

h) Delito de **facilitación de acceso a medios de comunicación** del artículo 286 CP; la comisión del cual se daría en el momento en el que, "*sin consentimiento del que presta servicios y con un fin comercial*", un individuo "*facilite el acceso*" a dichos servicios, dentro de los cuales se incluirían, de manera expresa según el propio precepto, "*los servicios interactivos prestados a distancia por vía electrónica*".

i) Delito de **falsedad documental** del artículo 390 CP; la conducta típica del cual la integraría la "*alteración*", "*simulación*", "*falta a la verdad*" o "*suposición de intervención de personas en actos que no la han tenido*" en relación con un documento.

   A pesar de que el propio precepto no nos otorgue una definición expresa de documento, el propio texto penal sí lo hace, concretamente en el artículo 26 CP, donde se establece que *"se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica"*. Es en este extremo donde podemos justificar su vinculación con los elementos informáticos, ya que resulta palmario afirmar que también recibe la consideración de documento aquellos soportes exclusivamente informáticos.

2.3.3. Delitos informáticos sin previsión expresa[13]

En este último grupo se integrarían todos aquellos delitos que, a pesar de no haberse previsto expresamente la utilización de elementos informáticos para su realización

[13] Relativos a los artículos 187, 188 y 189 del Capítulo V del Título VIII, Libro II; 205 del Capítulo I del Título XI, Libro II; 208 del Capítulo II del Título XI, Libro II; 238.5 del Capítulo II del Título XIII, Libro II; 243 del Capítulo III del Título XIII, Libro II; 282 de la Sección 3ª del Capítulo XI del Título XIII, Libro II; 301 del Capítulo XIV del Título XIII, Libro II; y 399 bis.1 y 399 bis.3 de la Sección 4ª del Capítulo II del Título XVIII, Libro II; todos ellos pertenecientes a la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

(primer grupo) y no hacerse referencia a un concepto dentro del cual cabría entender incluidos los medios informáticos (segundo grupo), la doctrina mayoritaria ha considerado que, por su probabilidad o habitualidad de comisión haciendo uso de los mismos, deberían ser considerados, del mismo modo, delitos informáticos. Los delitos integrados en el último eslabón de la clasificación, sin pretensión de constituir un numerus clausus, serían los siguientes:

a) Delito de **proxenetismo** del artículo 187 CP. De este modo, la inclusión de este delito como un delito informático vendría dado por la ingente cantidad de prostitución virtual llevada a cabo en la actualidad, cosa que nos puede llevar a pensar que, igual que su ejercicio, la determinación a ejercer también puede darse por medios exclusivamente informáticos.

b) Delito de **prostitución de menores o discapacitados** del artículo 188 CP. En el mismo sentido que en el delito de proxenetismo analizado *supra* en relación con la prostitución adulta, en la prostitución de menores o discapacitados también podemos observar como en múltiples ocasiones se han hecho uso de medios exclusivamente informáticos para poder llevar a cabo este tipo de conductas.

c) Delito de **captación o uso de material pornográfico de menores o discapacitados** del artículo 189 CP. Siguiendo la línea de los anteriores dos delitos, a medida que la sociedad se ha ido informatizando, también lo están haciendo ciertos servicios/negocios, como puede ser el caso de la distribución de material pornográfico a través de portales de internet.

d) Delito de **calumnias** del artículo 205 CP. En relación con ello, el elemento informático aquí lo podríamos encontrar en el hecho de que, cada vez con más asiduidad, la sociedad está haciendo un uso mayor de los medios informáticos para poder difundir sus ideas, pensamientos y creencias produciéndose, en algunos casos, una extralimitación del derecho a la libertad de expresión favorecido por el anonimato, elemento que puede llevar al individuo a cometer un ilícito penal a través de internet.

e) Delito de **injurias** del artículo 208 CP. El elemento informático aquí se puede explicar del mismo modo que ocurría con el delito de calumnias a través de internet, dado que una extralimitación del derecho a la libertad de expresión del artículo 20 de la Constitución Española (de ahora en adelante, CE) utilizando elementos informáticos, podría llevar a un individuo a estar cometiendo un acto ilícito tipificado en el texto penal.

f) Delito de **robo con fuerza** del artículo 238.5 CP. Al respecto, según nos muestra VELASCO, E., dentro de este tipo delictivo podrían aparecer los elementos informáticos en tanto en cuanto se puede utilizar, para cometer el robo, la inutilización de lo que el autor llama "*sistemas de guardia criptográfica*"[14], que sería un sistema de seguridad haciendo uso de encriptaciones informáticas.

g) Delito de **extorsión** del artículo 243 CP. Como hemos podido observar que ocurre en muchos de los delitos analizados supra dentro de este mismo grupo, el elemento informático aquí recaería sobre la posibilidad cada vez mayor de que se produzcan este tipo de conductas delictivas a través de medios virtuales aprovechando la facilidad de comisión, el anonimato o el menor riesgo personal, entre otros factores que más adelante se examinarán.

h) Delito de **publicidad engañosa** del artículo 282 CP. En este aspecto, el elemento informático podría formar parte del ilícito penal toda vez que esa publicidad incierta se hiciera a través de medios informáticos, un supuesto muy habitual y extendido en el sector comercial.

i) Delito de **blanqueo de capitales** del artículo 301 CP. Dada la configuración tan amplia del tipo delictivo y, concretamente, de las conductas típicas que lo integran, se ha podido observar en la doctrina jurisprudencial más reciente del Tribunal Supremo que han existido múltiples casos sobre delitos informáticos en los cuales se ha acusado también al autor de dichos delitos (e incluso en alguno de ellos, condenado) de la comisión del delito de blanqueo de capitales.

[14] VELASCO NÚÑEZ, Eloy. *Delitos cometidos a través de internet*: *Cuestiones procesales*. Editorial La Ley. Madrid. 2010. p. 42.

j) Delito de **falsificación de tarjetas de crédito o débito y cheques de viaje** del artículo 399 bis.1 CP. El elemento informático aquí juega un papel fundamental ya que, al menos en el caso de las tarjetas, no puede concebirse la realización del tipo (es decir, su falsificación) sin que intervenga alguno de los elementos informáticos mencionados con anterioridad para poder falsificar la banda electromagnética.

k) Delito de **utilización de tarjetas de crédito o débito y cheques de viaje falsos** del artículo 399 bis.3 CP. En cuanto a ello, el factor relacional con los elementos informáticos recaería en la posibilidad de la utilización de los mismos a través de internet.

2.3.4. Otros delitos informáticos conexos

A pesar de que se haya intentado delimitar por la doctrina cuáles son aquellos delitos que pueden englobarse dentro del concepto de "delitos informáticos", esto no se ha logrado completamente. En este sentido, lo que se ha podido observar al respecto es que, si bien es cierto que muchos de ellos tienen una vinculación mayor con el fenómeno virtual que muchos otros tipos delictivos, también lo es que otros muchos delitos aquí no incluidos también pueden llegar a ser cometidos a través de medios informáticos.

Aunque pueda llegar a sorprender en cierto sentido, podemos decir que en la actualidad prácticamente todos los delitos previstos en el Código Penal pueden llegar a cometerse a través de internet. Resulta difícil poder afirmar que esto es posible en todos los casos, ya que en ciertos tipos delictivos sí que necesitamos un elemento físico para que se cometa dicho ilícito, pero lo que no puede negarse es que cada vez más la sociedad está avanzando hacia un mundo más tecnológico del que los delitos económicos y los delitos en general son parte.

3. ¿CUÁNDO UN DELITO INFORMÁTICO ES UN DELITO ECONÓMICO INFORMÁTICO?

3.1. Concepto de delito económico informático

Dentro de estos grupos de delitos informáticos, se puede observar que algunos de ellos poseen un carácter económico, es decir, que la finalidad delictiva del mismo es la de obtener un lucro económico para el sujeto activo que lo comete, convirtiéndolos así en derechos económicos.

La doctrina ha considerado que se tratan de **delitos económicos** aquellos incluidos dentro del Título XIII del CP de los artículos 234 a 304 CP, que tiene por nombre "*Delitos contra el patrimonio y contra el orden socioeconómico*". Esto sería el **concepto estricto** del término, ya que quedarían incluidos aquí aquellos preceptos donde la ganancia económica es el único fin de la realización típica de los mismos, es decir, el enriquecimiento del sujeto activo a costa de un tercero.

Por otro lado, igual que ocurría con los delitos informáticos, tendríamos el **concepto amplio** del término delito económico, donde se plasmarían todos aquellos tipos delictivos donde existe dicha finalidad de obtener un lucro por parte del sujeto infractor, pero que no representa la única finalidad del mismo, sino que puede haber otros objetos u objetivos por el cual se está incurriendo en el tipo.

3.2. Los delitos económicos informáticos en el Código Penal

De este modo, se ha querido hacer una clasificación de los **delitos económicos informáticos**:

3.2.1. Delitos económicos informáticos puros[15]

Dentro de este grupo, quedarían incluidos aquellos tipos delictivos que responderían al concepto de delito económico en sentido estricto (es decir, incluidos dentro del Título de los delitos socioeconómicos del CP) cometidos haciendo uso de elementos informáticos.

Así las cosas, los delitos englobados aquí serían los siguientes: robo con fuerza mediante la inutilización de sistemas de guardia criptográfica (238.5 CP); extorsión informática (243 CP); estafa informática (248.2.a CP); actos preparatorios de la estafa informática (248.2.b CP); defraudación de telecomunicaciones (255 CP); uso fraudulento de terminales informáticos (256 CP); sabotaje informático (264 CP); obstaculización o interrupción informática (264 bis CP); facilitación del sabotaje o de la obstaculización o interrupción informática (264 ter CP); contra la propiedad intelectual a través de medios informáticos (270 CP); contra la propiedad industrial a través de medios informáticos (273 CP); apropiación de secretos de empresa a través de medios informáticos (278 CP); publicidad engañosa a través de medios informáticos (282 CP); acceso a servicios interactivos prestados a distancia por vía electrónica (286 CP) y blanqueamiento de capitales a través de medios informáticos (301 CP). Todos ellos objeto de análisis con anterioridad.

3.2.2. Delitos económicos informáticos mixtos[16]

Dentro de este grupo, quedarían incluidos aquellos tipos delictivos que responderían a un concepto más amplio de delito económico, ya que a pesar de que la finalidad lucrativa pueda estar presente en los mismos, usualmente viene acompañada de otras finalidades añadidas que gozan de igual protagonismo que la económica.

---

[15] Relativos a los artículos 238.5 del Capítulo II del Título XIII, Libro II; 243 del Capítulo III del Título XIII, Libro II; 248.2.a) y 248.2.b) de la Sección 1ª del Capítulo VI del Título XIII, Libro II; 255 y 256 de la Sección 3ª del Capítulo VI del Título XIII, Libro II; 264, 264 bis y 264 ter del Capítulo IX del Título XIII, Libro II; 270 de la Sección 1ª del Capítulo XI del Título XIII, Libro II; 273 de la Sección 2ª del Capítulo XI del Título XIII, Libro II; 278 de la Sección 3ª del Capítulo XI del Título XIII, Libro II; 282 y 286 de la Sección 3ª del Capítulo XI del Título III, Libro II; y 301 del Capítulo XIV del Título XIII, Libro II; todos ellos pertenecientes a la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

[16] Relativos a los artículos 187, 188 y 189 del Capítulo V del Título VIII, Libro II; 197, 197 bis.1 197 bis.2 y 197 ter del Capítulo I del Título X, Libro II; 390 de la Sección 1ª del Capítulo II del Título XVIII, Libro II; y 399 bis.1 y 399 bis. 3 de la Sección 4ª del Capítulo II del Título XVIII, Libro II; todos ellos pertenecientes a la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Así las cosas, los delitos englobados aquí serían los siguientes: proxenetismo virtual (187 CP); prostitución virtual de menores o discapacitados (188 CP); difusión de materiales pornográficos de menores o discapacitados a través de medios informáticos (189 CP); descubrimiento y revelación de secretos (197 CP); allanamiento informático (197 bis.1 CP); interceptación de transmisiones no públicas de datos informáticos (197 bis.2 CP); facilitación en la comisión del delito de espionaje informático o interceptación de datos informáticos (197 ter CP); falsedad documental a través de medios informáticos (390 CP); falsificación de tarjetas de crédito o débito y cheques de viaje (399 bis.1 CP) y utilización de tarjetas de crédito o débito y cheques de viaje falsos (399 bis.3 CP) . De nuevo, todos ellos han sido objeto de análisis con anterioridad.

3.3. El gran desconocimiento de los tipos delictivos económicos

La doctrina, los tribunales e incluso los ciudadanos de a pie con ciertos conocimientos jurídicos conocen el contenido de las conductas castigadas en el Código Penal, pero lo cierto es que estos solo representan una pequeña parte de la sociedad. Cuando hablamos de delitos ajenos a los delitos económicos existe una cierta conciencia social de cuáles son realmente las conductas que están prohibidas en sociedad, debiéndose en su mayoría a la educación que estos individuos han ido recibiendo a lo largo de su vida sobre las conductas "buenas" y las conductas "malas".

No obstante, cuando el tipo de delitos a los cuales se hace referencia son de carácter económico, el desconocimiento de qué conductas están tipificadas en el texto penal aumenta de manera significativa. No podemos negar que existen ciertos delitos económicos que la población en su mayoría detecta fácilmente como un delito como tal, como por ejemplo en el caso del delito de robo. No obstante, si hablamos de otros como por ejemplo la extorsión o el blanqueo de capitales, el panorama cambia de manera sustancial. Con ello no se quiere hacer referencia a que exista un desconocimiento total de los mismos o que sea una minoría de la población la que es consciente de que existen, simplemente se pretende poner de relieve que estos no han sido tan interiorizados como otros presentes en el texto penal.

Si existe cierto desconocimiento en relación con algunos delitos no económicos y bastante desconocimiento de los delitos económicos… ¿Qué ocurre con los delitos económicos

informáticos? En relación a ellos, se han dado varios fenómenos: (i) Su reciente introducción; (ii) Su distorsión por los medios de comunicación o medios tecnológicos; y (iii) Su configuración como delitos virtuales.

3.3.1. La reciente introducción

Esto ha propiciado que de la gran mayoría de ellos no se conozca ni tan siquiera su existencia como ilícitos penales propiamente. A pesar de que el texto penal y sus modificaciones se hacen públicos a través del Boletín Oficial del Estado, son muy pocos los ciudadanos que acuden al mismo para poder comprobar qué nuevas conductas han quedado tipificadas, qué otras se han suprimido y cuáles han sufrido algún tipo de modificación.

3.3.2. La distorsión por los medios de comunicación o medios tecnológicos

En este sentido estarían las redes sociales, el internet, la prensa o la televisión. Este hecho configura una práctica común en la sociedad actual. A parte del desconocimiento general verso a estos tipos delictivos, cuando se da el hecho de que algunos de estos delitos sí son conocidos en multitud de ocasiones este conocimiento no es del todo cierto. Es en este extremo donde entra el papel de las nuevas tecnologías toda vez que, aunque favorecen el conocimiento globalizado de la implantación de nuevas conductas punibles en el código penal, también propician a que la literalidad de las mismas se difumine. Esto puede provocar que no siempre se acabe teniendo una imagen fiel del tipo delictivo en cuestión, sino que únicamente se acabe por configurar una imagen mental simplificada del mismo y, en ocasiones, errónea.

3.3.3. La configuración como delitos virtuales

Esto ha provocado que aquellos delitos que anteriormente a dicha introducción ya existían en nuestro Código Penal como delitos tradicionales hayan gozado, en algunos casos, de cierta "invisibilidad". Este hecho sucede en la medida en que, cuando un individuo tiene interiorizado que una cierta conducta delictiva debe ser necesariamente física, es ciertamente complicado poder desconfigurar esa idea para introducir, en su lugar, un concepto mucho más amplio y mucho menos intuitivo. Esto puede ocurrir en el caso de

una estafa, por ejemplo. En este tipo delictivo, pese a que su configuración penal es mucho más amplia, un individuo medio consideraría que se está incurriendo en este delito toda vez que alguien engaña a otro para conseguir una transmisión patrimonial en perjuicio del mismo. Dentro de este concepto tan llano, el ciudadano de a pie puede visualizar la situación en la cual unos vendedores ambulantes (con un ánimo de engaño previo) convencen al individuo de adquirir un producto muy novedoso a un precio muy razonable por tratarse de una oferta irrepetible, haciéndole abonar en el mismo momento una cantidad en concepto de paga y señal para luego enviarle el producto a su domicilio, cosa que nunca llega a suceder. Pero ¿Cuántos de ellos se imaginarían el hacer una compra por internet de una cuantía no muy elevada a un proveedor inexistente sin saberlo y que el producto nunca llegue a su domicilio? Muchos menos que en el primer supuesto.

3.4. El aumento cuantitativo de los delitos económicos informáticos

A pesar de que todo lo expuesto convierta a los delitos económicos en internet en uno de los grupos delictivos más desconocidos entre la sociedad, esto no quiere decir que sean menos comunes o que se cometan con menos asiduidad. Prácticamente se produce el fenómeno contrario.

Atendiendo a los últimos datos sobre criminalidad aportados por el Ministerio del Interior en su balance del tercer trimestre de 2018, los delitos económicos representan alrededor del 48,34%[17] de la totalidad de delitos que se producen a nivel nacional. Pese a que no exista una división entre los delitos económicos físicos y los delitos económicos cometidos a través de medios informáticos en el mismo, debemos recordar que EUSEBIO, el director adjunto de la Europol y miembro del Cuerpo Nacional de Policía, ha constatado que los delitos informáticos vienen experimentando un crecimiento anual de entorno a un 12% mientras que los delitos físicos experimentan un descenso de un 3 o un 4%, aproximadamente.

[17] Ministerio del Interior. (2018). *Infracciones penales registradas en Comunidades Autónomas, provincias, islas, capitales y localidades con población superior a 30.000 habitantes.* Recuperado de: http://www.interior.gob.es/documents/10180/8736571/informe+balance+2018+3%C2%BA%20trimestre.pdf/4169ea84-3a74-48f1-913a-86869a8525be

Unido a este hecho, tal como apunta el magistrado y juez español VELASCO NÚÑEZ[18], se estima que alrededor de un 70% de los delitos informáticos que se denuncian son delitos económicos. De este modo, se puede observar que este porcentaje es mayor en los delitos informáticos que en los delitos tradicionales, donde recordemos se trataba de aproximadamente de alrededor de un 50%. Este dato nos indica que la aparición de estos delitos informáticos se ha debido, en su gran mayoría, a un afán de obtener ganancias de manera totalmente fraudulenta.

3.5. Circunstancias favorecedoras de los delitos económicos informáticos

Una vez delimitado en el plano teórico cuándo podríamos decir que nos encontramos ante un delito económico informático, ahora cabe señalar sucintamente aquellos elementos o factores más representativos que hacen que en el plano práctico se lleven a cabo este tipo de delitos con preponderancia a cualquier otro tipo de delito informático o tradicional.

En este sentido, BARRERA, Inspectora de la Policía Nacional especializada en cibercrimen, durante todos sus años de experiencia ha podido detectar que uno de los factores que tienen en cuenta los delincuentes para llevar a cabo estos tipos delictivos es en aquellos supuestos donde hay un **riesgo personal menor**. De este modo, la Inspectora indica que la posibilidad de perpetración de los mismos desde otros países elimina el riesgo personal de los autores al mínimo, dado que la investigación que ello acarrea puede significar alrededor de 2 o 3 años de investigación para poder actuar a nivel policial, siempre y cuando logren identificar al responsable de dichos hechos delictivos[19].

Además de ello, tanto BARRERA como DE EUSEBIO coinciden en que otro factor que es tenido muy en cuenta por los delincuentes a la hora de determinarse a cometer el ilícito penal es el **beneficio** que el mismo reporte. Según la Inspectora, los delitos económicos informáticos mueven actualmente más dinero que el narcotráfico pero, a pesar de ello, la preocupación o concierto sobre ellos no llega al mismo nivel que en estos últimos. EUSEBIO indica que el cibercrimen representa alrededor de 500.000 euros al año, ocupando así uno de los tres tipos delictivos más lucrativos, del que forman parte tanto el

[18] VELASCO NÚÑEZ, Eloy. *Delitos cometidos a través de internet.* Op., cit., p. 42.
[19] Andalucía es digital. (10 de mayo de 2017). *Claves para estar preparados frente a los delitos en Internet*. [Archivo de vídeo]. Minutos 19:25 y 19:35. Recuperado de: https://www.youtube.com/watch?v=kYoYYwiilm4

narcotráfico, mencionado con anterioridad, como la prostitución. Además, desde la Unión Europea, se ha cuantificado este problema indicándose que el impacto económico de los mismos es cinco veces mayor que cuatro años atrás.

No obstante, los elevados beneficios no son tenidos en cuenta de manera absoluta por parte de los delincuentes económicos en internet, sino que lo que llevan a cabo es una relativización de los mismos, comparándolos con el riesgo que supone alcanzarlos. De este modo, se toma en consideración una **ratio beneficio/riesgo** y únicamente actúan en aquellos supuestos donde la misma es considerablemente alta.

En último lugar, una de las situaciones que más propician que estos delitos aumenten exponencialmente y que se sigan perpetrando con la misma intensidad es la **baja ratio entre denuncias esclarecidas y denuncias planteadas**. En este sentido, BARRERA indicaba que la Fiscalía General del Estado en su memoria del año indicaba que, del total de denuncias planteadas en dependencias policiales acerca de delitos informáticos, únicamente se esclarecían un 3%, una cifra extremadamente baja y que otorga cierta impunidad a estos tipos delictivos, constituyendo un factor atractivo a posibles futuros ciberdelincuentes.

4. ¿DÓNDE SE ENTIENDE COMETIDO UN DELITO ECONÓMICO INFORMÁTICO?

4.1. El principio de territorialidad en los delitos económicos informáticos

Cuando se habla del **principio de territorialidad** se hace referencia a "*la aplicación de la normativa nacional a todos los hechos o situaciones que se lleven a cabo en el territorio del Estado incluyendo su mar territorial de 12 millas y su espacio aéreo*", según la definición dada por el Poder Judicial. Aplicando esta definición a los delitos económicos informáticos, la cuestión radicaría en dilucidar cuándo podemos entender que un delito cometido a través de medios tecnológicos se ha cometido en territorio español y, consecuentemente, que le sea aplicable el Derecho Penal Español.

Al hablar de un delito tradicional, donde en la mayoría existe concurrencia espacial y temporal entre la víctima del delito y el autor del mismo, la territorialidad no presenta excesivos problemas prácticos ni jurídicos, dado que cuando se ha presentado una casuística especial, el Tribunal Supremo las ha ido resolviendo sin gran complejidad. No obstante, en los delitos económicos informáticos, según apunta MORÓN LERMA[20], hay una gran indeterminación del ámbito geográfico, dado que inexistencia de coincidencia física entre autor y víctima hace que existan, mínimo, dos localizaciones espaciales distintas donde puede entenderse cometido el ilícito penal (pueden existir muchas más si las víctimas o los autores de estos tipos delictivos se desplazan por múltiples territorios durante la comisión del mismo, tal como refleja BARRERA[21]).

En este sentido, la Inspectora también indica que lo usual es que se trate de bandas organizadas que deciden llevar a cabo sus actividades delictivas desde países ajenos al territorio español[22], dado que así aprovechan las disfuncionalidades existentes entre los diferentes países, como por ejemplo la falta de cooperación policial y judicial transfronteriza para poder investigar y enjuiciar los posibles actos ilícitos.

---

[20] Facultad de Informática - Universidad Complutense de Madrid. (21 de enero de 2015). *Delitos en internet*. [Archivo de vídeo] Minuto 25:16. Recuperado de: https://www.youtube.com/watch?v=o7u0T7cpyJQ

[21] Pido la palabra. (15 de mayo de 2013). *Francisco Hernández (Delitos por internet) - Pido la Palabra - 9 de mayo 2013* [Archivo de vídeo]. Recuperado de: https://www.youtube.com/watch?v=6AbL98Sc7rs

[22] Andalucía es digital. (10 de mayo de 2017). *Claves para estar preparados frente a los delitos en Internet*. [Archivo de vídeo]. Minuto 17:06. Recuperado de: https://www.youtube.com/watch?v=kYoYYwiilm4

No obstante, como indican conjuntamente la Inspectora y JARAUTA, profesor de la Escuela Técnica Superior de Ingeniería (ICAI), puede darse el caso de que el ataque no se esté produciendo efectivamente desde un tercer país, sino que se esté cometiendo dentro del territorio español cambiando la IP o utilizando servidores que no estén sitos en España para impedir que las actuaciones ilícitas sean rastreadas por los miembros de los cuerpos de seguridad del Estado[23].

A pesar de ello, sí que existe una cierta conciencia de dónde se están cometiendo todos estos tipos delictivos económico-informáticos, ya que desde los miembros de seguridad del estado se utilizan ciertas herramientas de rastreo especializadas para poder ubicar geográficamente a los mismos y saber cómo actuar frente a ellos. En este sentido, BARRERA indicaba que mayoritariamente este tipo de ataques informáticos provienen de los países del Este y una de las razones para ello es que, en la legislación rusa, los ataques informáticos no están tipificados en todos los casos, únicamente cuando estos se lancen contra el propio país, no si los dirigen fuera del mismo[24]. Del mismo modo, JARAUTA indica que, a nivel del territorio español, España ocupa la cuarta posición dentro de los países que más sufren ciberataques[25].

4.2. Respuesta jurisprudencial al problema de la territorialidad

Vista la indeterminación geográfica que presentan los delitos informáticos y el silencio de la ley ante dicha problemática, el Tribunal Supremo se ha visto en la tesitura de interpretar jurisprudencialmente dónde se entienden cometidos los mismos a fin de determinar la ley penal aplicable, dado que uno de los extremos del principio de territorialidad recae en el hecho de que el Derecho Penal Español únicamente podrá alcanzar a aquellos actos delictivos que efectivamente se cometan dentro de España.

---

[23] *La legislación española debería modificarse para luchar mejor contra los ciberdelitos.* Comillas Universidad Pontificia. Recuperado de: https://www.comillas.edu/es/noticias-comillas/3723-la-legislacion-espanola-deberia-modificarse-para-luchar-mejor-contra-los-ciberdelitos

[24] Andalucía es digital. (10 de mayo de 2017). *Claves para estar preparados frente a los delitos en Internet*. [Archivo de vídeo]. Minuto 17:06. Recuperado de: https://www.youtube.com/watch?v=kYoYYwiilm4

[25] La legislación española debería modificarse para luchar mejor contra los ciberdelitos. Comillas Universidad Pontificia. Recuperado de: https://www.comillas.edu/es/noticias-comillas/3723-la-legislacion-espanola-deberia-modificarse-para-luchar-mejor-contra-los-ciberdelitos

En cuanto a los delitos informáticos en general, tal como apunta ORTIZ PRADILLO[26], existe una gran inseguridad jurídica al respecto dado que el Tribunal Supremo no ha sido consistente en su jurisprudencia y ha ido alternando entre la teoría de la actividad (entender cometido el hecho allí donde se lleven a cabo las acciones u omisiones necesarias para realizar la conducta típica), la del resultado (entender cometido el hecho donde se exteriorice el resultado de la conducta típica llevada a cabo por el autor) y la de la ubicuidad (poder entenderse cometido el hecho tanto donde se han llevado a cabo las acciones que integran el comportamiento típico como donde se produce el resultado). En estos casos, como norma general, lo que hace el alto tribunal es examinar las circunstancias concretas del caso y, a raíz de ello, decidir cuál de las tres teorías podrán llevar a un mejor enjuiciamiento de los hechos.

No obstante, como también nos indica ORTIZ PRADILLO, el Tribunal Supremo sí que ha sido consistente en relación con los delitos económicos informáticos, en especial en relación con el delito de estafa, dado que en estos casos ha considerado que la teoría adecuada para el enjuiciamiento de los mismos es la de la ubicuidad[27], ampliando así las posibilidades de enjuiciamiento incluso en el caso de que el autor del delito se encuentre fuera del territorio español.

En este sentido el Tribunal Supremo en el Auto de 22 de febrero de 2018[28], indica que "*el delito de estafa comete en todos los lugares en los que se han desarrollado las acciones del sujeto activo (engaño) o del sujeto pasivo (teoría de la ubicuidad)" criterio que viene corroborado por el Pleno no jurisdiccional de esta Sala de fecha 3 de febrero de 2005, en el que se acordó: "el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo, en consecuencia, el Juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para la instrucción de la causa".*

[26] ORTIZ PRADILLO, Juan Carlos. (23 de mayo de 2016). *Determinación de la jurisdicción y competencia para la investigación y enjuiciamiento de los daños informáticos*. Madrid. Recuperado de: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/ponencia%20Ortiz%20Pradillo%20Juan%20Carlos.pdf?idFile=cd54640d-efbe-4839-bb98-27f9b0c17d67

[27] En el mismo sentido, PÉREZ MACHÍO, ANA ISABEL. Delincuencia Informática. Tiempos de Cautela y Amparo. Thomson Reuters Aranzadi. Navarra. 2012. p.276

[28] España. Tribunal Supremo (Sala de lo Penal, Sección 1ª). Auto de 22 de febrero de 2018 (Rec. 21048/2017).

De este modo, vemos que el tribunal sigue pronunciándose de este modo desde la Sentencia del Pleno del mismo de 3 de febrero de 2005, lo que indica que la jurisprudencia al respecto está consolidada, lo que muestra que, a pesar de que el principio de territorialidad presente conflicto en relación con otros delitos, respecto los delitos económicos el alto tribunal no tiene dudas.

4.3. Necesidad de colaboración y cooperación policial y judicial

A pesar de que el Tribunal Supremo haya resuelto el problema en relación con el principio de territorialidad en los delitos económicos informáticos, ello no hace que las dificultades relacionadas con el lugar de comisión delictiva se solucionen en absoluto, ya que existen otros factores que siguen obstaculizando el enjuiciamiento de los mismos.

De este modo, cuando se hace frente a estos delitos de carácter trasfronterizo, es absolutamente necesario que se lleve a cabo una intensa colaboración y cooperación a nivel policial y judicial entre los diferentes países (tanto a nivel europeo como internacional) para evitar que ciertos obstáculos formales dificulten en exceso la identificación y enjuiciamiento de los autores de los mismos, favoreciendo así el atractivo de este tipo de actuaciones ilícitas por dichas disfunciones.

Este extremo ya ha sido objeto de preocupación por parte de los organismos europeos tal como anunciaba ANSIP, vicepresidente responsable del Mercado único Digital, al referirse a que "*ningún país puede hacer frente, por sí solo, a los retos de ciberseguridad. Nuestras iniciativas refuerzan la cooperación de forma que los Estados miembros de la UE puedan acometer juntos estos desafíos*"[29].

No obstante, esta cooperación y colaboración tanto a nivel policial y judicial no es fácil de llevar a cabo, dado que la multiplicidad de legislaciones y modos de proceder existentes dificulta enormemente esta tarea a consecuencia de que los procedimientos que cada uno debe llevar a cabo para proceder con las mismas en ocasiones pueden llegar a ser muy distintos, con todos los problemas añadidos que esto presenta.

[29] ALONSO LECUIT, Javier. (5 de diciembre de 2017). *Relanzamiento del Plan de Ciberseguridad de la UE*. Real Instituto Elcano. Recuperado de: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciberseguridad/ari97-2017-relanzamiento-plan-ciberseguridad-ue-union-europea

Este hecho lo que provoca es que se "*requiera un nivel de inteligencia y coordinación no solamente nacional entre fuerzas de seguridad y justicia, sino entre esos mismos organismos de otros países*"[30], puesto que se requiere que existan acuerdos y pactos previos entre los diferentes Estados que prevean de una manera suficientemente extensa como para poder desplegar un auténtico operativo policial y/o judicial en el momento que se produzca un delito informático que afecte a ambos y, además, que el resultado sea satisfactorio.

[30] Pido la palabra. (15 de mayo de 2013). Francisco Hernández (Delitos por internet) - Pido la Palabra - 9 de mayo 2013 [Archivo de vídeo]. Recuperado de: https://www.youtube.com/watch?v=6AbL98Sc7rs

5. ¿CÓMO SE LLEVA A CABO UN DELITO ECONÓMICO INFORMÁTICO?

En la labor de conceptualización y localización de los delitos económicos informáticos se ha podido comprobar que, si bien no se trata aún de algo exacto y bien delimitado por la reciente introducción de estos tipos delictivos en el texto penal, si que se pueden acotar para llegar a hacerse una idea de los mismos, a diferencia de lo que ocurre con las modalidades de comisión de estos delitos.

Según indica la Inspectora BARRERA[31], existen una infinidad de modus operandi que los delincuentes utilizan para perpetrar estos actos ilícitos y, cada vez más, están surgiendo nuevas modalidades que los ciberdelincuentes están utilizando para engañar a las víctimas y lograr la consumación del delito, dado que si utilizaran únicamente unas modalidades determinadas éstas se acabarían conociendo, con la consecuente reducción de potenciales víctimas y la influencia que ello tendría en los también potenciales beneficios.

Dentro del ámbito de delitos económicos informáticos el delito que más modus operandi presenta son las **estafas informáticas**, dado que el engaño de la potencial víctima tradicionalmente ha representado uno de los elementos clave y definitorios para que la transferencia patrimonial perjudicial se llegue a producir, definiéndose así su éxito. No obstante, la jurisprudencia del Tribunal Supremo[32] ha venido matizando este precepto para aclarar que, actualmente, ya no se exige que exista engaño para entender cometido este delito, desvinculándose así del elemento fundamental de las estafas tradicionales.

Uno de los métodos más utilizados y que más ha aumentado en los últimos años para cometer el delito de estafa informática es el llamado ***phishing***, técnica admitida doctrinal y jurisprudencialmente como tipo de estafa informática[33]. Se estima que el aumento del mismo en el tercer trimestre de 2018 ha sido del 27,5%, situando al territorio español en el tercer país del mundo en sufrir este tipo de ataques, según un estudio de Europapress[34].

---

[31] Andalucía es digital. (10 de mayo de 2017). *Claves para estar preparados frente a los delitos en Internet*. [Archivo de vídeo]. Minuto 26:37. Recuperado de: https://www.youtube.com/watch?v=kYoYYwiilm4

[32] España. Tribunal Supremo (Sala de lo Penal, Sección 1ª). Sentencia núm. 533/2007 de 12 de junio.

[33] QUINTERO OLIVARES, Gonzalo (Director). *Monografías. La reforma penal de 2010: análisis y comentarios.* Editorial Thomson. 2010. y España. Tribunal Supremo (Sala Penal, Sección 1ª). Sentencia núm. 506/2015, de 27 de julio y 3537/2007, de 12 de junio.

[34] *España, tercer país del mundo más afectado por 'phishing' en el tercer trimestre de 2018.* (30 de noviembre de 2018). Portaltic. Madrid. Recuperado en:

Dos de los motivos que pueden explicar este gran aumento sería, por un lado, el perfeccionamiento que han llevado a cabo los criminales en sus modus operandi que podría venir representado por la creación de nuevos y desconocidos métodos delictivos y, por otro lado, la utilización de los terminales móviles para la comisión de los mismos[35].

La conceptualización de lo que se entiende como *phishing* ha sido bastante pacífica, dado que tanto la doctrina como la jurisprudencia entienden que se trata de "*un concepto informático que denomina el uso de un tipo de fraude caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria)*"[36]. Con ello, tal como apuntaba el fiscal delegado de Criminalidad Informática y Cooperación Internacional de la Fiscalía Provincial de Granada HERNÁNDEZ[37], hay que tener presente que el *phishing* solo representa una técnica usada para cometer un intrusismo informático, ya sea para perpetrar un delito de estafa o cualquier otro tipo de delito informático, no siendo exclusivamente defraudatorio.

Pero, como ya se avanzaba, el *phishing* no es la única técnica utilizada por los ciberdelincuentes para la comisión del delito de estafa informática, existiendo una variedad ingente de modalidades delictivas que van en aumento con el paso del tiempo. En este sentido, a modo puramente ejemplificativo, existen las siguientes técnicas[38]:

El más conocido de todos lo constituiría el **fraude nigeriano**. En sí mismo, este tiene muchas vertientes y modalidades comisivas, ya que su nombre viene dado por el hecho de que el delincuente siempre utiliza la explicación de que reside en algún país africano. Este tipo de estafa tiene su origen en 1920, hecho que indica que este no surgió con la

https://www.europapress.es/portaltic/ciberseguridad/noticia-espana-tercer-pais-mundo-mas-afectado-phishing-tercer-trimestre-2018-20181130165759.html

[35] *Injurias o calumnias en Internet y Phishing, los delitos informáticos más comunes. Robo de identidad y estafa, los que más han aumentado*. (20 de octubre de 2014). Noticias Jurídicas. Recuperado de: http://noticias.juridicas.com/actualidad/noticias/4135-injurias-o-calumnias-en-internet-y-phishing-los-delitos-informaticos-mas-comunes-robo-de-identidad-y-estafa-los-que-mas-han-aumentado/

[36] España. Audiencia Provincial de Logroño (Sala Penal, Sección 1ª). Sentencia núm. 233/2014, de 16 de abril.

[37] Pido la palabra. (15 de mayo de 2013). Francisco Hernández (Delitos por internet) - Pido la Palabra - 9 de mayo 2013 [Archivo de vídeo]. Recuperado de: https://www.youtube.com/watch?v=6AbL98Sc7rs

[38] LAVILLA, Milagros. 20 formas más comunes de estafas en Internet y redes sociales. *Webespacio*. Recuperado de: https://www.webespacio.com/formas-comunes-estafas-internet-redes-sociales/

aparición de las nuevas tecnologías, sino que se trata de un tipo defraudatorio que sufrió una adaptación al nuevo contexto.

No obstante, el tipo de fraude nigeriano común es aquél consistente en que el ciberdelincuente se hace pasar por una personalidad famosa y con una suma importante de dinero que no puede utilizar por algún tipo de traba (deudas o imposibilidad de acceder al dinero, entre otras). Por ello, se pide a la potencial víctima que ayude a adelantar una parte de dicha cantidad a fin de que, una vez la persona pueda tener acceso a su dinero, llevarse una comisión por la ayuda prestada, una cantidad, sin embargo, que jamás llegará a cobrar.

Una variante del fraude nigeriano la podemos encontrar en el **fraude de las herencias**[39]. Este consiste en que se le hace creer a la potencial víctima de que existe un familiar lejano y previamente desconocido para la misma que ha fallecido y ha dejado una herencia millonaria de la cual, casualmente, la víctima es el único pariente. Así, se le hace saber que en el caso de que ésta aporte una determinada cantidad, podrá acceder a la totalidad de la herencia. No obstante, este supuesto familiar y esta supuesta herencia son inexistentes y la víctima únicamente verá mermado su capital por el dinero que haya podido aportar para hacerse con ella.

En la misma línea, se encuentran las estafas relacionadas con la **compraventa de objetos demasiado baratos**[40]. A pesar de que en muchas ocasiones se utilice la pertenencia a algún país africano para justificar la falta de presencia física entre el comprador y el vendedor del objeto en cuestión, puede ser posible que se utilicen otros países europeos para la finalidad defraudatoria.

En este tipo de estafa cabrían todo tipo de objetos dentro del tráfico jurídico, pero los dos que más destacan son los coches y los apartamentos (incluso de alquiler en ocasiones). De este modo, la comisión de la misma se llevaría a cabo estableciendo un precio

[39] *Víctimas de estafas por internet ¿Qué hacer?* Vázquez & Apraiz y asociados. Recuperado de: https://www.tuabogadodefensor.com/victimas-estafas-internet/#

[40] *El Instituto Nacional de Consumo pone en marcha una iniciativa contra el fraude en Internet*. (1 de agosto de 2008). Noticias Jurídicas. Recuperado de: http://noticias.juridicas.com/actualidad/noticias/870-el-instituto-nacional-de-consumo-pone-en-marcha-una-iniciativa-contra-el-fraude-en-internet/

inusualmente bajo para las prestaciones o características del objeto en cuestión, hecho que suscita la curiosidad e interés de potenciales víctimas de la estafa.

Así, cuando existe una persona interesada en tal bien, el ciberdelincuente se pone en contacto con dicho individuo y le justifica que la transacción debe llevarse a cabo por medios exclusivamente informáticos y antes de poderlo ver físicamente dado que se encuentra fuera de España y necesita abonar unos gastos para poder desplazarse hasta allí para poderle transmitir la posesión del objeto en cuestión. No obstante, una vez son abonados esos supuestos gastos a los que hace alusión el ciberdelincuente, la víctima no volverá a tener noticias del mismo ni del supuesto bien prometido.

Otro ejemplo defraudatorio lo constituyen las **donaciones**. Este tipo de estafa se caracteriza por apelar al elemento más emocional del ser humano, partiendo de una desgracia provocada por alguna catástrofe natural (tales como tsunamis o terremotos) o enfermedad crónica. De este modo, mediante esta modalidad el ciberdelincuente pide que se aporte por parte de la potencial víctima una cantidad de dinero que supuestamente irá destinada al resarcimiento de los damnificados en la catástrofe natural o para pagar la costosa cura del enfermo terminal, hecho que jamás llegarán a producirse.

Por último, una de las estafas que efectivamente sí que ha aparecido a raíz de las nuevas tecnologías y la frecuente utilización de las mismas por los ciudadanos de a pie es el **virus para estafar al internauta**[41].

A través de esta modalidad, el ciberdelincuente inserta un virus en el sistema informático de la potencial víctima, se hace pasar por un miembro de la autoridad como por ejemplo un policía (hecho que constituye en sí mismo otro tipo delictivo adicional), y hace que le aparezca un aviso en la pantalla indicando que se han detectado archivos ilícitos en el ordenador de la misma (como por ejemplo archivos pornográficos o vulneradores de la Ley de Protección de Datos y/o propiedad intelectual) y que para poder transaccionar este hecho deberá abonarse una determinada cantidad. Posteriormente a este hecho, muchas de las víctimas caen en el engaño fruto del miedo que les produce esta situación y abonan el importe solicitado sin haber existido tan siquiera un ilícito real.

[41]*Las 10 estafas más utilizadas en internet*. (30 de enero de 2016). Unaibenito. Recuperado de: https://www.unaibenito.com/que-no-te-enganen-en-internet-las-estafas-mas-utilizadas-durante-el-2012/

6. ¿POR QUIÉN SE COMETEN LOS DELITOS ECONÓMICOS INFORMÁTICOS?

6.1. El perfil y la organización de los ciberdelincuentes

Al hablar de delitos y del perfil de los delincuentes que los cometen, la imagen que se habitualmente se tiene en mente es la del autor de cualquier otro tipo de ilícito penal tal como un robo o un homicidio. En estos casos se espera un perfil agresivo, conflictivo e incluso sociópata, pero la Inspectora BARRERA[42], a raíz de su experiencia como policía especialista en este tipo de delitos, afirma que esto no es así con carácter general.

De modo habitual, tal como indica la Inspectora, los ciberdelincuentes económicos -especialmente en los delitos de estafa informática- son individuos especializados en los delitos que están cometiendo dado que representan su fuente principal de ingresos (la actividad con la cual "*se ganan la vida*", en palabras de la Inspectora). El objetivo, el fin último, es obtener una cantidad de dinero con ello, lo que provoca que muchos de los delincuentes se hayan centrado en ser expertos en este campo y maximizar así los potenciales beneficios económicos a obtener.

De este modo, como indica VELASCO[43], el "*romántico hacker"* que existía en los inicios de estos delitos (e incluso antes de que se tipificaran los mismos), ha ido ocupando una menor proporción de la totalidad de ciberdelincuentes a medida que profesionales organizados y especializados van tomando el control de este campo.

A pesar del análisis individual de los ciberdelincuentes que se pueda realizar, cabe decir que esta no es la forma habitual de actuar en este tipo de ilícitos penales. En los delitos económicos informáticos, si bien es cierto que existen algunos individuos que prefieren actuar por su cuenta cometiendo el acto ilícito de forma particular desde el inicio de la exteriorización del primer acto hasta la consumación del mismo, la mayoría de estos profesionales especializados a los que hacíamos referencia supra se trata de verdaderas

[42] GARCÍA, Isabel. Cibercrimen: "En España solo se resuelve el 3% de los ciberdelitos denunciados". (24 de abril de 2018). *Nueva tribuna*. Recuperado de: https://www.nuevatribuna.es/articulo/sociedad/cibercrimen-ciberseguridad-ciberdelincuente-ciberatracador-mujeres-hackers-ransanwed-wenacraid-pentesting/20180424183449151198.html

[43] VELASCO NÚÑEZ, Eloy. *Delitos cometidos a través de internet*. Op., cit.

organizaciones ordenadas y jerarquizadas destinadas única y exclusivamente a cometer este tipo de delitos, tal como se ha observado por parte del Cuerpo Nacional de Policía[44].

6.2. La organización delictiva en el ámbito legal

A la vista de las evidencias concernientes a la organización y estructuración de este tipo de delincuentes, el Tribunal Supremo ha establecido una jurisprudencia -ya consolidada- acerca de los requisitos o características exigidas por el mismo para entender que una determinada estructura organizativa es, en puridad, una **organización delictiva**[45]:

a) **Actuación conjunta de una pluralidad de personas**, elemento que otorga el carácter de organización.

b) **Relación entre las personas que cometen el acto ilícito**.

c) **Reparto de funciones** entre los distintos miembros que actúan organizadamente.

d) **Base estructurada y jerarquizada de manera más o menos formal**, que es propiciada por el reparto de funciones dado que permite que exista categorías muy diferenciadas y con diferentes niveles de responsabilidad.

e) **Pertenencia y participación continuada de los distintos sujetos y no participación ocasional**, elemento que permitiría diferenciar la organización de una simple colaboración puntual entre un conjunto de personas sin afán de crear una estructura organizada destinada a cometer delitos.

f) **Red con cierta vocación de continuidad**. A pesar de ello, tal como apunta VELASCO[46], no se exige que la organización goce de una "*duración ni estabilidad determinada*", sino que en relación con la característica inmediatamente anterior, únicamente se requiere que las conductas delictivas se prolonguen en el tiempo, evitando castigar como organizaciones delictivas aquellas asociaciones puntuales entre los diferentes individuos infractores.

[44] Andalucía es digital. (10 de mayo de 2017). *Claves para estar preparados frente a los delitos en Internet*. [Archivo de vídeo]. Minuto 22:35. Recuperado de: https://www.youtube.com/watch?v=kYoYYwiilm4
[45] España. Tribunal Supremo (Sala Penal, Sección 1ª). Sentencia núm. 486/2009, de 8 de mayo.
[46] VELASCO NÚÑEZ, Eloy. *Delitos cometidos a través de internet*. Op., cit., p. 259.

g) **Comisión de los ilícitos independiente de la actuación individual de cada uno de los integrantes del grupo**. Esta característica representa quizá la más abstracta de todas, ya que realmente lo que se pretende es que esta organización calificada como delictiva alcance a ser una "*empresa criminal*" como indica VELASCO[47], lo que supondría que realmente lo relevante aquí no es la actuación que lleve a cabo cada uno de los individuos, sino la actividad de la empresa en sí autónomamente considerada.

h) **Medios materiales idóneos, relevantes y extraordinarios**.

i) **Mayor facilidad de comisión del delito y capacidad de lesión del bien jurídico protegido**, hecho que dificulta elementos tales como la prevención de la comisión de los delitos como la persecución de los mismos.

Además del pronunciamiento del Tribunal Supremo, VELASCO[48] indica que tanto la Unión Europea como la Fiscalía General del Estado han elaborado una serie de instrucciones con diez indicadores relacionados con las organizaciones delictivas que, además de integrar parte de los elementos observados por el Tribunal Supremo, añaden los suyos propios:

a) Los **actos delictivos** que se cometan deben revestir del carácter de **graves**.

b) Los **actos delictivos** se deben llevar a cabo de manera **transnacional** o que representen una gran movilidad dentro del territorio estatal.

c) En la realización de la conducta típica se debe emplear **violencia o intimidación de carácter grave**, en su defecto.

d) En la comisión del acto delictivo deben haberse utilizado medios apropiados para crear "***estructuras económicas o comerciales***".

e) En el desarrollo de la comisión delictiva se deben haber llevado a cabo **actividades de blanqueo de capitales** con el fin de último de integrar en el tráfico legal el dinero proveniente de la misma.

[47] VELASCO NÚÑEZ, Eloy. *Delitos cometidos a través de internet*. Op., cit., p. 259.
[48] CASAS HERRER, Eduardo. *La red oscura: En las sombras de internet: el cibermiedo y la persecución de los delitos tecnológicos.* Editorial La esfera de los libros. 2017. p. 173 y 174.

f) En el transcurso del *iter criminis* deben haberse empleado **influencias sobre personas pertenecientes a diferentes ámbitos de poder** tales como la política o las Administraciones Públicas.

g) En el objetivo a conseguir a través de la comisión delictiva debe aparecer como **finalidad última y principal la de obtener ciertos beneficios** con carácter recurrente o, en su defecto, **influencia en alguna de las esferas** mencionadas en el elemento inmediatamente anterior.

6.3. Roles en la estafa por internet

Una vez se ha podido apreciar que la forma natural de organización de los ciberdelincuentes la configura la creación de entes criminales u "**organizaciones delictivas**", cabe resaltar que, como en toda estructura organizada y jerarquizada, existen una serie de roles que determinan cómo opera la organización y marca qué funciones y qué categoría ocupa cada uno de sus integrantes.

Al respecto, tampoco existe una única clasificación y clara determinación de los **roles** que sea igual para todas las organizaciones delictivas, del mismo modo que tampoco existe una estructura única que opere en el resto de organizaciones estructuradas y jerarquizadas.

De este modo, se deberá atender a las distintas clasificaciones que existan doctrinalmente. En este caso, la clasificación tomada fue expuesta por el miembro de la Unidad de Investigación Tecnológica del Cuerpo Nacional de Policía y miembro permanente del Grupo de Expertos en Identificación de Víctimas de la Interpol, Eduardo Casas Herrer[49].

En la cúspide de las estructuras organizadas de carácter delictivo se encuentran los **jefes o directores**. Con ellos se origina y se pone en marcha todo el entramado delictivo organizado, dado que son aquellos individuos que detectan las vulnerabilidades de los usuarios en la red y logran encontrar la manera de sacar un beneficio -normalmente económico- de dichos puntos críticos.

[49] CASAS HERRER, Eduardo. *La red oscura*. Op., cit., p. 174, 175, 176 y 177.

No obstante, con la mera detección de oportunidades "de negocio" no es posible que se lleve a cabo el fin delictivo para el cual se crean este tipo de organizaciones, sino que es necesario que dentro de la misma existan **programadores informáticos** –también llamados "*hackers*"- que hallen la manera técnica de llevar a cabo y explotar las oportunidades detectadas por los jefes de la organización. La función de estos individuos es la de aplicar sus conocimientos informáticos para la creación de programas que ayuden a lograr el fin delictivo propuesto.

En el siguiente nivel organizativo se encuentran los **distribuidores** de los programas informáticos creados por los *hackers* para que lleguen a las potenciales víctimas del ataque informático que se quiera llevar a cabo. A pesar de que todos los niveles dentro del esquema organizativo sean importantes para que el delito se pueda llegar a consumar, los distribuidores representan un escalafón básico e imprescindible para poder lograrlo, dado que si no se lleva a cabo un buen "*marketing*" del producto -en este caso del programa delictivo- las potenciales víctimas no llegarán a entrar en contacto con él y no se podrán obtener los beneficios ilícitos previstos.

Unido de manera necesaria a la distribución se encuentran los **redactores** del mensaje utilizado para hacer que las potenciales víctimas entren dentro de la esfera de la estafa informática, ya sea accediendo a un hipervínculo o realizando directamente los desplazamientos patrimoniales viciados propuestos en dicho mensaje. No obstante, esta figura no se encuentra presente dentro de todas las organizaciones delictivas, dado que va muy unida a la forma escogida para llevar a cabo la comisión de la estafa informática.

Una vez decidido la modalidad defraudatoria a cometer y creado y distribuido el programa informático para llevarla a cabo, existe el nivel de **agentes de contacto** continuo con la potencial víctima. La tarea de estos individuos consiste, fundamentalmente, en llevar a cabo todos los trámites y gestiones necesarias para lograr que el cliente realice la transmisión patrimonial deseada. Este punto es realmente relevante, dado que dichos agentes deberán lograr que la víctima confíe en él para que efectivamente se produzca la ganancia patrimonial.

En el nivel inferior de toda la estructura jerarquizada están los llamados "**muleros**", nombre proveniente de su gran similitud con los individuos encargados de transportar estupefacientes en el delito de tráfico de drogas. Así, estos individuos se encargan de aprehender el dinero proveniente del ilícito penal depositado en una cuenta y transferirlo a otra diferente propiedad de los órganos superiores de la trama criminal a cambio de una comisión sobre el importe total que consiga transferir (entre un 5 y un 10%, aunque según VELASCO este importe ha llegado hasta el 50% en algunos casos[50]).

Las personas encargadas de llevar a cabo esta función, tal como expone CASAS[51], representan la parte más débil de todo el entramado criminal. Esto puede darse por múltiples factores y uno de ellos lo representa el hecho de que, en muchas ocasiones, el individuo que ostenta la categoría de mulero no es consciente que lo es ni que forma parte de una organización delictiva, sino que piensa que se trata de un empleo de "intermediario financiero"[52].

Es en este último eslabón en el que recaen la mayor parte de las sanciones penales existentes alrededor de las organizaciones criminales dedicadas a cometer delitos por internet. En este sentido debe ponerse de manifiesto que, en muchas ocasiones, es el único individuo que se encuentra residiendo en España, dado que los demás eslabones delictivos se encuentran en el extranjero, usualmente en Europa del Este como se apuntaba en un inicio.

No obstante, cuando se ha venido enjuiciando por el Tribunal Supremo la actuación de los muleros, no ha existido una uniformidad ni una coherencia en el pronunciamiento de las sentencias a lo largo de los años, dado que han existido condenas por varios delitos: de estafa, de blanqueamiento de capitales y de receptación. Es por ello que el propio tribunal ha indicado que se debe evitar la "*excesiva rigidez*"[53] y considera que se debe analizar cada caso concreto para poder llegar a la mejor decisión posible.

[50] VELASCO NÚÑEZ, Eloy. *Delitos cometidos a través de internet*. Op., cit., p. 322.
[51] VELASCO NÚÑEZ, Eloy. *Delitos cometidos a través de internet*.
[52] Andalucía es digital. (10 de mayo de 2017). *Claves para estar preparados frente a los delitos en Internet*. [Archivo de vídeo]. Minuto 19:57. Recuperado de: https://www.youtube.com/watch?v=kYoYYwiilm4
[53] España. Tribunal Supremo (Sala Penal, Sección 1ª). Sentencia núm. 834/2012, de 25 de octubre.

7. PROBLEMÁTICAS ACTUALES Y FUTURAS DE LOS DELITOS ECONÓMICOS INFORMÁTICOS

7.1. Problemáticas actuales

Las problemáticas actuales que rodean a los delitos económicos informáticos son, en gran parte, problemas estrictamente jurídicos motivados, en parte, por la reciente aparición e implantación de estos tipos delictivos.

Para llevar a cabo un análisis de alguna de estas problemáticas, se procederá a dividir las mismas en dos grandes grupos: 1) Problemáticas generales; y 2) Problemáticas específicas. En este sentido, al hablar de problemáticas generales se hará referencia a aquellos obstáculos que pueden ser aplicables a todo tipo de delitos económicos informáticos y, al hablar de problemáticas específicas, la atención se centrará en aquellos elementos conflictivos que se pueden encontrar en el delito económico informático más relevante, la estafa.

No obstante, aquellas problemáticas que serán expuestas a continuación de ninguna manera constituyen un numerus clausus de supuestos conflictivos existentes alrededor de los delitos económicos informáticos, sino que se expondrán aquellos que de manera más recurrente se han plasmado en la doctrina, en la jurisprudencia y en la sociedad.

7.1.1. Problemáticas generales

Uno de los elementos relevantes a considerar cuando se está haciendo referencia al posible enjuiciamiento de un delito económico informático y que no en todas ocasiones se tiene en cuenta, es la posibilidad de que el delito se encuentre **prescrito**, es decir, que haya pasado un plazo de tiempo determinado que imposibilita que ese delito pueda ser perseguido y castigado por razones de seguridad jurídica.

La regulación de la prescripción se encuentra en el artículo 131 del Código Penal y ofrece una serie de plazos de prescripción en función de la pena establecida en el tipo penal que se quiera enjuiciar. A pesar de no poder analizar aquí en profundidad todos los plazos de prescripción existentes para los múltiples delitos que han sido nombrados con

anterioridad, sí que cabe poner el énfasis en un dato que ha sido detectado por diversos autores doctrinales, entre ellos VELASCO[54], como es el hecho de que la mayoría de los delitos informáticos establecidos en el Código Penal son castigados con una pena baja y esto provoca que la prescripción de estos delitos también suceda en un lapso corto de tiempo. Es por ello que en muchas ocasiones se intenta llevar a cabo una acumulación de tipos delictivos regulada en el artículo 300 de la Ley de Enjuiciamiento Criminal para que la prescripción se vea inexorablemente alargada.

No obstante lo anterior, la prescripción no es un plazo fijo y continuo, sino que puede ser interrumpida. Es en este sentido que el Tribunal Supremo[55] ha puesto de relieve que esta interrupción en el caso de los delitos económicos informáticos se da siempre y cuando los escritos de denuncia o querella presentados para el futuro enjuiciamiento de un hecho contengan datos que permitan la identificación suficiente de los culpables del delito, elemento que no parece fácilmente alcanzable dado el carácter usualmente anónimo de este tipo de delitos expuesto con anterioridad.

El segundo elemento general a tener en cuenta que se halla ligado con esta última apreciación de la identificación del autor delictivo y es el hecho de que **si no hay autor del delito que sea conocido, la causa se archiva**.

Este punto se encuentra así estipulado en el artículo 284.2 de la Ley de Enjuiciamiento Criminal a raíz de su reforma en el año 2015[56]. En este sentido, lo que ocurre en este caso es que en el caso de que el autor de los hechos que se denuncian ante la policía no esté identificado, esa misma denuncia no se traslada a los juzgados, sino que permanece en dependencias policiales y se archiva.

Uno de los motivos que puede explicar esta regulación es la propia configuración del proceso penal. En un procedimiento sancionatorio de esta tipología, lo que se prevé es la existencia de un sujeto activo (el que realiza el delito, el autor) y un sujeto pasivo (el que sufre los daños del delito, la víctima) para que el sujeto activo pueda ser juzgado por su

[54] VELASCO NÚÑEZ, Eloy. *Delitos cometidos a través de internet*. Op., cit., p. 49.
[55] VELASCO NÚÑEZ, Eloy. Delitos cometidos a través de internet. Op., cit., p. 66.
[56] Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Boletín Oficial del Estado, España, 5 de octubre de 2015.

conducta ilícita hacia el sujeto pasivo. De este modo, si no se conoce el sujeto activo, no podrá iniciarse este procedimiento porque la finalidad última del procedimiento penal que es la de imponer un castigo al sujeto activo por la conducta llevada a cabo se verá frustrada.

No obstante, esta práctica impuesta por la legislación vigente ha sido objeto de muchas críticas por muchos operadores jurídicos, en especial el Ministerio Fiscal que ya en su Memoria del año 2017 reflejó que el 80% de las denuncias que se presentaban por los ciudadanos no pasaban de dependencias policiales a las judiciales y, consecuentemente, no se podían investigar, tal como pone de manifiesto BARRERA[57].

El último de los elementos a analizar es la gran **dificultad existente para posibilitar la acumulación de delitos**, es decir, lograr atribuir a un mismo autor varios hechos delictivos que aumenten la pena impuesta al sujeto activo.

Mediante tal objetivo lo que realmente se pretende es que al sujeto activo se le acaben imputando una multiplicidad de delitos para evitar los plazos de prescripción relativamente cortos a los que se ha hecho referencia *supra*. De este modo, tal como aparece regulado en el artículo 132 del Código Penal, el plazo de prescripción empezaría a computar "*desde el día en que se realizó la última infracción, desde que se eliminó la situación ilícita o desde que cesó la conducta*".

No obstante, esto no siempre es una tarea fácil. Uno de los elementos que dificultan enormemente este cometido es la infinidad de modus operandi existentes, ya que esto provoca que sea prácticamente imposible identificar a un autor por las características de la comisión del delito como ocurre en la gran mayoría de los delitos del Código Penal.

[57] GARCÍA, Isabel. Cibercrimen: "En España solo se resuelve el 3% de los ciberdelitos denunciados". (24 de abril de 2018). *Nueva tribuna*. Recuperado de: https://www.nuevatribuna.es/articulo/sociedad/cibercrimen-ciberseguridad-ciberdelincuente-ciberatracador-mujeres-hackers-ransanwed-wenacraid-pentesting/20180424183449151198.html

7.1.2. Problemáticas específicas

Como ya se ha puesto de relieve con anterioridad, aquí se abordarán aquellas problemáticas que rodean a los delitos económicos informáticos más importantes, habituales y crecientes del ordenamiento jurídico-penal, las estafas informáticas.

Un primer elemento de carácter fáctico vendría dado por la existencia, en ocasiones, de **estafas de poca cuantía**, es decir, que el importe defraudado por parte del sujeto activo al sujeto pasivo representa una cantidad realmente irrisoria.

Esta problemática no esconde algo más allá de la propia interpretación literal de las palabras que lo forman, ya que simplemente se quiere hacer referencia a que existen estafas por importe de 1€, e incluso céntimos, que provocan cinco tipos de reacciones por parte de los afectados.

En primer lugar, existen aquellas personas que no son conscientes tan siquiera de que han sido estafados, ya que la cantidad es tan sumamente reducida que no la notan en el saldo de sus cuentas corrientes y, en ocasiones, nunca llegan a tener conocimiento de ello.

En segundo lugar, estarían aquellas personas que sí notan que les falta esa cantidad de dinero en su cuenta corriente pero que intentan pensar que quizá sea algún tipo de pago que debía efectuar y el cual no recuerdan o cualquier otra cosa similar. Estas personas, ya sea por desconocimiento o por exceso de confianza, no llegan a plantearse la posibilidad de que exista una vulnerabilidad en su sistema informático.

El tercer lugar lo ocuparían los individuos que, a pesar de saber de la existencia de la falta de esta cantidad en su cuenta y de que no es achacable a ningún pago consentido que haya realizado, llegan a pensar que dada la escasa cuantía de la estafa esto no sería sancionable penalmente.

En cuarto lugar se encuentran aquellas personas que, siendo conscientes de que les falta una cantidad en su cuenta y que ellos no han realizado dicho pago, son plenamente conscientes de que lo que se ha llegado a cometer en ese caso particular es un ilícito penal, denunciable y sancionable, por tanto. No obstante, poniendo en una balanza los trámites

por los cuales va a tener que pasar y aquel importe que va a ser capaz de recuperar (así como las probabilidades de que efectivamente se detecte al culpable y se condene al mismo al retorno de dichas cantidades), determina que no merece la pena pasar por todo ello, con lo que no presentan denuncia alguna al respecto.

El quinto y último lugar lo ocuparían aquellas personas que, a diferencia de los individuos anteriormente expuestos, son conscientes de la falta de dinero en sus cuentas, de que esa cuantía faltante no es consecuencia de ningún pago consentido que haya llevado a cabo, de que esa acción constituye un ilícito castigado penalmente y, finalmente, de que esa acción debe y va a ser denunciada ante las autoridades competentes.

A pesar de ello, la gran parte de los sujetos pasivos reaccionan según lo expuesto en las cuatro primeras reacciones, ya que solamente una pequeña parte de ellos reacciona de una manera contundente y efectiva ante este tipo de conductas, lo que provoca un margen de impunidad para aquellos ciberdelincuentes que se dedican a realizar una cantidad ingente de ataques informáticos defraudatorio de poca cuantía para eliminar o reducir el riesgo en su persona e incrementar la efectividad de los mismos.

Un segundo elemento en cierto modo problemático que atañe sobre todo al delito de estafa informática es la **desconfiguración de los tipos delictivos tradicionales** para poder dar cabida a nuevas realidades legislativas, es decir, la modificación o extensión de elementos configuradores del delito en cuestión para evitar la impunidad de ciertos comportamientos vinculados con las nuevas tecnologías.

En este sentido, uno de los elementos configuradores y definitorios del delito de estafa lo constituye el *engaño bastante* para producir error en otro, tal como aparece reflejado en el artículo 248.1 del Código Penal. Tanto es así, que uno de los primeros elementos que se analiza a fin de poder delimitar si se está ante un delito de estafa o ante otro tipo delictivo de carácter económico, es precisamente la existencia de un engaño bastante y suficiente para que se produzca la transferencia patrimonial perjudicial para el sujeto pasivo.

No obstante, con la aparición de las nuevas tecnologías y, con ellas, nuevas conductas merecedoras de sanción penal, el concepto de estafa se ha visto expandido para dar

respuesta a estas nuevas modalidades, produciéndose así la desconfiguración del tipo que se anunciaba.

De este modo, estas nuevas modalidades delictivas aparecen enumeradas en el apartado 2 del mismo artículo 248 del Código Penal relativo a la estafa. Se trata, por lo tanto, del delito de estafa cometido mediante manipulación informática (apartado a), la fabricación, introducción, posesión o facilitación de programas informáticos para la comisión de una estafa (apartado b) y, finalmente, la utilización de tarjetas de crédito, débito o cheques de viaje provocando un perjuicio en el titular de los mismos (apartado c).

En estas tres modalidades delictivas correspondientes a los delitos de estafa especiales, a diferencia de lo que ocurre con el tipo básico o común de estafa del primer apartado del artículo 248 del Código Penal, se elimina la referencia a la existencia de un engaño en el sujeto pasivo para entender consumadas dichos actos ilícitos.

De este modo, se produce la desconfiguración del propio delito de estafa común o tradicional, ya que uno de sus elementos fundamentales (el engaño bastante) desaparece para lograr dar cabida y respuesta a nuevas modalidades delictivas y evitar que ciertas conductas con evidente reproche penal queden impunes.

Por último, tendríamos la tesitura ante la que se encuentran los juzgados cuando deben enjuiciar estos hechos delictivos, consistente en que realmente **la sanción se acaba imponiendo al "último mono"**, es decir, a los individuos que componen el último escalafón de todo el entramado delictivo y que, en ocasiones como ya hemos indicado *supra*, desconocen completamente que están llevando a cabo un acto delictivo.

No es poco habitual toparse en la jurisprudencia con sentencias dictadas condenando a los muleros de la organización delictiva, lo realmente poco frecuente es que se acaben detectando quiénes configuran los máximos responsables de la trama y se les acaben imputando los delitos correspondientes. En este sentido, con ello no solo se están dejando en libertad a ciberdelincuentes que deberían ser enjuiciados por sus hechos, sino que también se está desaprovechando la oportunidad de poder seguir el rastro de todo lo que hacen los muleros para poder llegar hasta los organizadores de toda la trama y desarticularla desde arriba.

Así, por mucho que se llegue a sancionar al individuo que meramente traspasa fondos de una cuenta a otra para blanquear el dinero de procedencia ilícita, no se estará poniendo fin a la actividad delictiva de la organización, ya que son fácilmente sustituibles.

7.2. Problemáticas futuras

A pesar de que existan problemáticas que afectan más al corto plazo como las examinadas *supra*, existen muchas más como las que se pasarán a analizar sucintamente a continuación que afectan no solo a la realidad actual, sino que tienen mucho que ver con elementos que obstaculizarán la buena marcha del enjuiciamiento de estas nuevas realidades delictivas que seguirán creciendo de manera exponencial.

Para realizar el presente análisis, se cree conveniente agrupar estas diferentes problemáticas en cuatro grandes grupos: usuarios; justicia; recursos y obstáculos operativos.

7.2.1. Usuarios

En este grupo, se pasará a analizar únicamente una problemática, dado que esta es tan significativa que, cualitativamente, tiene un peso realmente superior a varias de las problemáticas aquí analizadas si se consideraran conjuntamente: el **miedo al daño reputacional y la culpabilidad de la víctima**.

Como se puede observar, existe una doble vertiente al tratar este punto y esto vendría dado por el hecho de que este tipo de ataques pueden sufrirlo tanto personas físicas (individuos o personas aisladas) como jurídicas (empresas u organizaciones en general).

En este sentido, cuando se hace referencia al daño reputacional se estaría hablando de cómo afectan los delitos económicos informáticos en las personas jurídicas. Los administradores de las mismas, tras sufrir un ataque informático de carácter económico (aunque también se han producido casos en otro tipo de ataques informáticos como por ejemplo la “fuga de datos”), rehúsan la posibilidad de ponerlo en conocimiento de las autoridades por miedo a que la sociedad u otras empresas tengan conocimiento de ello ya

que consideran que puede mostrarse como un elemento de "debilidad" de la misma o falta de seguridad.

Del mismo modo, en las personas físicas, este daño reputacional no tiene tanto sentido como si se hace referencia a la culpabilidad. En estos casos, lo que suele ocurrir con las víctimas es que, lejos de considerarse a sí misma como sujeto pasivo de un delito económico informático, tiende a culpabilizarse por sus actos, toda vez que cree que ha sido objeto de dicho ataque por su propio actuar y su propia falta de diligencia.

Todas estas barreras "emocionales" únicamente favorecen la perpetración de delitos económicos informáticos con mayor abundamiento y, en ocasiones, aumentan el riesgo de que puedan volver a ser víctima de los mismos por la impunidad que detectan los ciberdelincuentes al cometer dichos ataques contra esos mismos sujetos pasivos.

Por todo ello, se puede apreciar que esta problemática tiene una vertiente notoriamente transversal, toda vez que puede magnificar o reducir sensiblemente el problema de enjuiciamiento existente en cuanto a los delitos económicos informáticos se trata.

7.2.2. Justicia

En este grupo quedan englobadas aquellas problemáticas que, si bien ya han venido siendo patentes en la investigación y enjuiciamiento de otros tipos delictivos tradicionales y no necesariamente tecnológicos como los aquí analizados, en esta ocasión pasan a agravar un problema ya existe y, por ello, sus carencias se hacen más visibles.

Con ello, en primer lugar, se está haciendo referencia al hecho innegable de que **la realidad va siempre por delante de la justicia**. Este fenómeno no es propio de los delitos informáticos ya que se da en la mayoría de los actos ilícitos del Código Penal, pero sí que adquiere una relevancia notoria cuando nos estamos refiriendo a ellos.

El motivo es que aunque en un delito tradicional la realidad pueda cambiar y haga que la justicia se deba adaptar a la misma, en el caso de los delitos informáticos estos cambios representan auténticos retos para el legislador, ya que no solo debe saber cómo reflejar correctamente los tipos en el texto para evitar posibles vacíos futuros, sino que primero

debe entender a la perfección el funcionamiento de los cambios para asegurarse de que realmente se está acotando correctamente la nueva configuración del tipo delictivo.

Además de ello, adicionalmente al hecho de que la justicia nunca puede ponerse por delante de los delincuentes y, en ocasiones, tan siquiera a la par que los mismos, en el momento que consigue entrar en juego, es cuando más patente se hace **la lentitud de la justicia.** Esta, a su vez, tendría una doble vertiente: 1) En el mundo jurídico y 2) En el mundo judicial. En un primer sentido, la lentitud jurídica vendría inexorablemente ligada al hecho innegable de que la realidad siempre se encuentra un paso por delante de todo aquello que se pueda llegar a prever legislativamente. En un segundo sentido, estaría la lentitud en el ámbito judicial. Con ello se quiere hacer referencia a que no únicamente existe lentitud en poder prever los tipos delictivos adecuados en el texto penal sino que, una vez previstos, el lapso de tiempo que media entre la identificación del culpable y el enjuiciamiento cierto del mismo es innecesariamente largo, seguido de muchos trámites y, en ocasiones, muchas trabas.

7.2.3. Recursos

Pero, cuando se están analizando las problemáticas concernientes a los delitos económicos informáticos (y a los delitos informáticos en general), no se debe caer en el error de considerar que las carencias existentes solo dependen del mero devenir de la investigación o del enjuiciamiento sino que, en muchas ocasiones, los obstáculos son meramente materiales como sería el caso de los recursos.

En este sentido, en primer lugar se encontraría la **falta de personal** para perseguir esta tipología de delitos. En este sentido, sí que es remarcable el aumento progresivo que ha existido a nivel estatal, europeo e internacional de número de efectivos destinados tanto a la persecución (policías e investigadores) como a el enjuiciamiento de los mismos (fiscales y jueces). No obstante, dicho aumento de individuos cuya principal tarea viene siendo enfocada a este tipo de delitos, parece crecer a un ritmo mucho menor al que lo hace la comisión de delitos económicos informáticos.

De este modo, a pesar de que parece haber una consciencia también creciente sobre la necesidad de prestar atención y dedicar esfuerzos y recursos a este tipo de delitos, cabe

poner de manifiesto que esta asignación de recursos aún no es totalmente eficiente. Prueba de ello puede encontrarse en el hecho de que aún muchos de estos actos ilícitos siguen quedando impunes por falta de una adecuada investigación sobre los mismos.

Así las cosas, a pesar de que se aumentaran los efectivos para la investigación y enjuiciamiento de esta tipología delictiva, seguiría existiendo otro problema que a continuación se expondrá, la **falta de especialización de los efectivos**.

Cuando se trata de delitos tradicionales, cuyo ámbito de ocurrencia es el mundo físico y tangible conocido por todos, no parece difícil poder afirmar la necesidad de dotar a los investigadores y enjuiciadores de los mismos de unos conocimientos suficientes para poder llevar a cabo correctamente su tarea, sino sus cometidos quedarían vacíos de contenido.

No obstante, cuando de lo que se trata es de dar respuesta a actos ilícitos cometidos en el mundo virtual, más novedoso y por lo tanto menos conocido, resulta extraño la dificultad que existe para crear conciencia de que estos conocimientos aplicados al medio en el que se actúa son extremadamente necesarios del mismo modo que lo son en los delitos tradicionales y, en ocasiones, incluso más por la gran complejidad de los asuntos y el contexto en sí mismo.

De este modo, se podría dar la tesitura de que existan efectivamente el número idóneo de efectivos para investigar y enjuiciar los delitos económicos informáticos (aunque hoy en día esto aún no sea así) pero que los mismos no supieran y, por lo tanto, no pudieran, actuar contra los mismos. Esto conllevaría un malgasto ingente de recursos económicos por el mantenimiento de puestos de trabajo a los cuales no se les dota de los conocimientos necesarios para desarrollarse con normalidad, eficacia y eficiencia.

En un paso posterior a la elevación de número de efectivos encaminados a investigar y enjuiciar los delitos informáticos y a la especialización de los mismos, se encontraría la imposibilidad de respuesta a la **falta de una adecuada asignación de recursos** ya que, en ocasiones, resultan claramente insuficientes.

No se debe olvidar que los delitos económicos informáticos tienen una particularidad de la que no gozan todos los delitos tradicionales, la utilización de mecanismos informáticos. Esto provoca que para realizar cualquier investigación, por reducida que esta sea, se requiera de unas mínimas infraestructuras que posibiliten el acceso a los documentos y rutas mediante los cuales ciberdelincuentes realizan los actos ilícitos.

Con ello no se está pensando en grandes y complejas investigaciones que necesiten de programas específicos y costosos (aunque se hayan dado casos), sino en las más nimias investigaciones como por ejemplo poder dar con el propietario de una IP determinada identificada como la perteneciente al ciberdelincuente.

Visto esto, parece comprensible y razonable pensar que, si hasta la propia identificación del ciberdelincuente en casos sencillos necesita de la aportación de cierto capital para poderse llevar a cabo de manera satisfactoria, la persecución de los delitos económicos informáticos en general necesitará de una considerable asignación de recursos públicos si realmente se quiere poner fin a este tipo de delincuencia.

7.2.4. Obstáculos operativos

Íntimamente ligado con los defectos jurídicos a la hora de enjuiciar concretamente cada uno de los delitos que se cometen, tenemos los aspectos problemáticos ligados con el contexto jurídico en el que se encuentran estos delitos.

De este modo, el primero de ellos serían los diferentes **vacíos operativos y jurídicos existentes**. En este sentido, se está haciendo referencia a que, no todos los actos que son reprochables socialmente lo son penalmente. Con ello se viene a decir que existen muchos comportamientos no deseables que se han cometido y, por diferentes vacíos jurídicos, no se han podido llegar a enjuiciar, ya sea porque no se puede llegar a identificar al responsable o porque no se ha podido dar cabida de la actuación dentro del texto penal, entre otros muchos ejemplos existentes. Del mismo modo, hay vacíos operativos que dificultan esta tarea, y el ejemplo más representativo de ello es cuando no se permite la investigación o el enjuiciamiento de un supuesto delito por el carácter trasfronterizo de este tipo de modalidades delictivas que encuentran innumerables obstáculos con las legislaciones de los diferentes países.

Una vez puesto de relieve la existencia de vacíos generales operativos y jurídicos en un contexto más general, cabe hacer mención a tres obstáculos operativos más específicos al respecto para poder circunscribir mejor la problemática.

En este sentido, y volviendo brevemente a las problemáticas concernientes a los recursos, a pesar de que se llegaran a resolver en algún punto y se alcanzaran los niveles óptimos para poder enfrentarse a la delincuencia organizada de carácter cibernético, hay un elemento obstaculizador que también debe tenerse en cuenta y que, en parte, es propiciado por mucho de los analizados, como es el hecho de que las **posibilidades de investigar en red son reducidas**.

Como se ha puesto de manifiesto, este poco margen de actuación investigadora dentro de los medios informáticos puede venir propiciado por muchos factores. Algunos de ellos pueden ser la falta de efectivos, la falta de especialización o incluso la falta de recursos. Sin embargo, también puede entenderse posible que la propia complejidad tecnológica unida con la destreza de alguno de los ciberdelincuentes, creen la barrera definitiva para una investigación y enjuiciamiento fructíferos.

En este sentido se está pensando en todos aquellos supuestos en los que los ciberdelincuentes utilizan sistemas de encriptación, rutas secretas, medios de eliminación de rastro, entre otros, que quedan fuera del conocimiento y alcance de muchos -o en ocasiones de todos- los sujetos encargados de la persecución de los ilícitos.

Quizá en algunos casos esto pueda tener solución relativamente "simple" como puede ser la mayor formación y especialización de los efectivos como se ha puesto de relieve *supra*, pero en otras ocasiones no hay solución posible, ya que simple y llanamente son mecanismos inventados por los propios ciberdelincuentes que tendrían que ser conocidos por los investigadores y, posteriormente, estudiados para poderse detectar la manera correcta de poner fin a los mismos, posibilidad que no en todos los delitos existe.

Dicho esto, solucionada la situación de los recursos, aún existiría una problemática más por resolver: la **larga duración de las investigaciones policiales** en los delitos económicos informáticos, tal como parece indicar BARRERA[58].

Lo que apunta la Inspectora es que las investigaciones en esta tipología delictiva se alargan durante muchos años, unos cuatro aproximadamente y que, durante todo ese periodo de tiempo, van apareciendo muchas más víctimas del mismo autor que se está investigando en ese momento.

De este modo, sí que cabe destacar que las investigaciones en este campo no resultan tan conocidas como las llevadas a cabo en los delitos tradicionales, hecho que provoca que muchos de los mecanismos utilizados por los investigadores para dar con los autores sean aún tan novedosos que incluso en muchas ocasiones pueden llegar a ser ineficaces e, incluso, ineficientes.

Por otro lado, tampoco se puede olvidar el hecho de que a pesar de que los investigadores puedan utilizar y desarrollar técnicas más o menos actualizadas, los ciberdelincuentes también están continuamente mejorando sus sistemas de encubrimiento del delito a fin de evitar ser rastreados por la red, con más o menos acierto según los casos.

Por último, y como colofón de todas las problemáticas que se han puesto de relieve, nos encontraríamos la **baja ratio entre la cantidad de denuncias interpuestas concernientes a delitos económicos informáticos y la cantidad de casos resueltos** a tal efecto.

Tal como se avanzaba, las cifras en relación a la ciberdelincuencia son llamadas "cifras negras" porque no hay forma posible de determinarlas con claridad y precisión. Además, esto complica enormemente la realización de estadísticas y provoca que no siempre se encuentren datos completamente actualizados. No obstante todo lo anterior, sí que existen ciertas estadísticas llevadas a cabo por investigadores del campo de los delitos informáticos que pueden ayudar a establecer una imagen representativa acerca de la problemática del esclarecimiento de los hechos reportados.

[58] Andalucía es digital. (10 de mayo de 2017). *Claves para estar preparados frente a los delitos en Internet*. [Archivo de vídeo]. Minuto 22:17. Recuperado de: https://www.youtube.com/watch?v=kYoYYwiilm4

Para poder tener una mejor visión de las mismas, es necesario dividir esta última problemática, a su vez, en tres fases diferenciadas del procedimiento: i) Fase previa; ii) Fase policial; iii) Fase intermedia.

En primer lugar, en la **fase previa**, se debe tener en cuenta que no todo lo que se reporta a las autoridades competentes es efectivamente todo lo que pasa, aunque en este extremo los delitos informáticos se comportan exactamente igual que los delitos tradicionales. De este modo, la Inspectora BARRERA[59], estima entre un 5-15% de la cantidad de incidentes que se reportan en relación al total de incidentes acaecidos en un territorio.

No obstante, a medida que van pasando los años, esta cantidad de incidentes se han visto aumentados de forma exponencial aunque, tal como indica la propia Inspectora, las denuncias en torno a ellos no han experimentado el mismo crecimiento aunque se desconoce totalmente el motivo de ello[60].

Una vez interpuesta la denuncia ante las autoridades competentes y nos encontramos en la **fase policial**, este no es el último paso para poder llegar a enjuiciar a un ciberdelincuente, ya que se debe tener en cuenta que, interponer la denuncia no es equivalente a obtener una solución al problema. Tanto es así que en el año 2015, de cada 1000 denuncias únicamente se llegaba a esclarecer 1, tal como también indicaba BARRERA[61].

Como último paso de todo el entramado enjuiciador de las modalidades delictivas que se cometen lo representa el paso de las diligencias policiales a las judiciales, es decir, la **fase intermedia**, en el cual las autoridades policiales traspasan toda la información a los órganos judiciales para que puedan proseguir con la investigación y/o enjuiciamiento correspondientes.

[59] Andalucía es digital. (10 de mayo de 2017). *Claves para estar preparados frente a los delitos en Internet*. [Archivo de vídeo]. Minutos 9:28. Recuperado de: https://www.youtube.com/watch?v=kYoYYwiilm4
[60] Andalucía es digital. (10 de mayo de 2017). *Claves para estar preparados frente a los delitos en Internet*. [Archivo de vídeo]. Minutos 10:15. Recuperado de: https://www.youtube.com/watch?v=kYoYYwiilm4
[61] Andalucía es digital. (10 de mayo de 2017). *Claves para estar preparados frente a los delitos en Internet*. [Archivo de vídeo]. Minutos 10:38. Recuperado de: https://www.youtube.com/watch?v=kYoYYwiilm4

A pesar de ello, tal como se indicaba en la Memoria de la Fiscalía de 2017[62], existe una gran traba legislativa para que se produzca este último paso, consistente a la regulación de la Ley de Enjuiciamiento Criminal acerca de la determinación del sujeto activo de la infracción, cifrándose así en un 80% de denuncias interpuestas aquellas que no logran pasar a dependencias judiciales y se archivan en manos de las autoridades policiales.

Todo ello únicamente representa una pequeña muestra de algunos de los problemas y disfunciones formales y materiales que presenta actualmente la investigación y enjuiciamiento de los delitos económicos informáticos (y de los delitos informáticos, en general). Con todo ello, resulta claramente comprensible este atraso si se tiene en consideración el atraso general que existe a nivel tecnológico. No obstante, estos elementos tan controvertidos deberán verse reducidos de manera significativa en los próximos años si no se quiere que estos representen un reclamo para los delincuentes por ver una modalidad delictiva de más fácil comisión y de menor riesgo personal y patrimonial.

[62] Citada por GARCÍA, Isabel. Cibercrimen: "En España solo se resuelve el 3% de los ciberdelitos denunciados". (24 de abril de 2018). *Nueva tribuna*. Recuperado de: https://www.nuevatribuna.es/articulo/sociedad/cibercrimen-ciberseguridad-ciberdelincuente-ciberatracador-mujeres-hackers-ransanwed-wenacraid-pentesting/20180424183449151198.html

CONCLUSIÓN

A la vista de todo lo expuesto, si a alguna conclusión no controvertida se puede llegar en el presente trabajo, es el carácter sustancial a la par que desconocido de los delitos económicos informáticos.

A partir de aquí, todas las conclusiones que se pueden extraer pecan de ser controvertidas dado que, al ser un tema tan novedoso, amplio e incierto, existen muchas posturas sobre sus elementos esenciales sin existir una verdad absoluta al respecto, al menos por el momento.

¿Qué?

Al inicio de este estudio, se abordaba el concepto de delito informático en general, punto esencial para poder abordar los siguientes interrogantes y configurar un mapa general sobre los ejes centrales de este tipo de delito usual a la par que desconocido. En este sentido, y después de haber efectuado el presente análisis, concluyo que existirían dos tipos de definiciones para conceptualizar el delito informático: 1) Aquellos tipos delictivos cuyo elemento principal para la comisión del ilícito penal lo constituye la afectación a medios tecnológicos y/o informáticos; y 2) Aquellos tipos delictivos la consumación del cual no gira alrededor de la afectación de elementos tecnológicos pero, a pesar de ello, se realizan a través de los mismos.

¿Cuándo?

Una vez quedó definido en la medida de lo posible lo que se podía entender como delito informático en general, pasó a analizarse cuándo un delito informático podía llegar a ostentar la etiqueta de delito "económico". De nuevo, al igual que ocurría con la definición de delito informático, bajo mi punto de vista concluyo que existen dos posibles definiciones para la conceptualización del delito económico informático: 1) Aquellos tipos delictivos encuadrados en el Título XIII dedicado a los delitos contra el patrimonio y el orden socioeconómico; y 2) Aquellos tipos delictivos dentro de los cuales la finalidad lucrativa forma parte de los mismos independientemente de la intensidad de la misma.

¿Dónde?

Abarcada la conceptualización de ambos términos esenciales para el estudio, se entró en una cuestión que, a simple vista, puede no gozar de demasiada trascendencia práctica. No obstante, a la vista del estudio realizado, puedo concluir y concluyo que, tanto en términos jurídicos como prácticos, la territorialidad ciertamente representa un reto que abordar y al cual prestar atención en aras de una mejora en la investigación y el enjuiciamiento de los delitos económicos informáticos. De este modo, sí que es cierto que el Tribunal Supremo ha dejado clara su postura aceptando la tesis de la ubicuidad ampliamente extendida en el derecho penal (admitiendo, por lo tanto, el enjuiciamiento en cualquiera de los países en los que se cometa o reciba el hecho delictivo en cuestión), pero también lo es que los problemas prácticos de cooperación judicial han ganado terreno y que aún distan de resolverse.

¿Cómo?

Este apartado que se dedicaba a los diferentes modos de comisión de los delitos económicos informáticos quizá sea el apartado más abstracto y más impreciso de todo el análisis efectuado. Esto es porque, a pesar de que se intenten sistematizar aquellos modos de proceder más habituales o más comunes entre los individuos y las empresas, resulta prácticamente imposible recogerlos en su totalidad. De este modo, al respecto puedo concluir que, si bien existen técnicas muy frecuentes entre los ciberdelincuentes que se repiten con mayor asiduidad que otros, también lo es que resulta técnicamente imposible recopilarlas todas dada la exhaustividad virtual y el avance constante y desenfrenado de la tecnología.

¿Por quién?

La resolución de esta pregunta quizá haya provocado en el lector la misma reacción de sorpresa que se me presentó en el momento de analizar la información existente en este punto. Siempre se nos ha presentado la imagen de un individuo solitario con dotes informáticas, el típico “hacker”. No obstante, como se pudo observar, se puede concluir sin reparo que, a pesar de que estos individuos existan y estén presentes, estos no representan el gran grueso de los individuos que efectivamente los cometen. De este

modo, son auténticas organizaciones delictivas las que llevan el mando de las grandes operaciones de delitos económicos informáticos y que, dado los recursos, oportunidades y posibilidades que tienen a su alcance, pueden provocar los ataques económicos informáticos más devastadores para la sociedad.

Problemáticas

Como punto final de este análisis, se ha creído necesario hacer referencia a problemáticas tanto presentes como futuras que presentan los delitos económicos informáticos. De este modo, resulta ciertamente difícil hacer una conclusión acerca de cuáles representan las problemáticas más relevantes que se deben tener en cuenta a la hora de enfrentarse a los delitos económicos informáticos. No obstante, sí que se puede hacer una aseveración francamente honesta en relación con este punto: quizá es más fácil hablar de todos los elementos que configuran los delitos económicos informáticos en sí, que intentar abarcar todos los problemas y retos que presentan estos tipos delictivos, ya que son tantos y tan cambiantes que al analizar uno de ellos quizá habrían aparecido ya tres más.

Con todo lo expuesto, puede verse que los delitos económicos informáticos no constituyen en absoluto una nimiedad o un tema carente de importancia, más bien al contrario. Espero que con el presente trabajo haya logrado arrojar un rayo de luz (a la par que de esperanza), a la conceptualización general de qué son estos “nuevos” delitos que entran pisando fuerte y que están aquí para quedarse. Con ello, significará que lo único que se puede hacer al respecto es intentar analizar más en profundidad cada uno de los aspectos que los configuran para poder entender mejor la manera de prevenirlos, enjuiciarlos y, aunque pueda sonar utópico, erradicarlos.

Quizá los delitos económicos informáticos puedan pasar ciertamente desapercibidos en algunos aspectos en el presente, pero de bien seguro que condicionarán el futuro. Por ello, únicamente se puede esperar a que ese futuro llegue, aunque siempre es mejor que lo haga habiéndolo previsto.

8. LEGISLACIÓN, JURISPRUDENCIA, BIBLIOGRAFÍA Y WEBGRAFÍA

8.1. Legislación

Unión Europea. (26 de enero de 2001). *Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos.* Bruselas.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Boletín Oficial del Estado, España, 5 de octubre de 2015.

8.2. Jurisprudencia

España. Tribunal Supremo (Sala de lo Penal, Sección 1ª). Auto de 22 de febrero de 2018 (Rec. 21048/2017).

España. Tribunal Supremo (Sala de lo Penal, Sección 1ª). Sentencia núm. 533/2007 de 12 de junio.

España. Audiencia Provincial de Logroño (Sala Penal, Sección 1ª). Sentencia núm. 233/2014, de 16 de abril.

España. Tribunal Supremo (Sala Penal, Sección 1ª). Sentencia núm. 486/2009, de 8 de mayo.

España. Tribunal Supremo (Sala Penal, Sección 1ª). Sentencia núm. 834/2012, de 25 de octubre.

8.3. Bibliografía

CASAS HERRER, Eduardo. *La red oscura: En las sombras de internet: el cibermiedo y la persecución de los delitos tecnológicos.* Editorial La esfera de los libros. 2017.

PÉREZ MACHÍO, ANA ISABEL. *Delincuencia Informática. Tiempos de Cautela y Amparo*. Thomson Reuters Aranzadi. Navarra. 2012.

POVEDA CRIADO, Miguel Ángel. *Delitos en la red*. Editorial Fragua. Madrid. 2015.

QUINTERO OLIVARES, Gonzalo (Director). *Monografías. La reforma penal de 2010: análisis y comentarios.* Editorial Thomson. 2010. y España. Tribunal Supremo (Sala Penal, Sección 1ª). Sentencia núm. 506/2015, de 27 de julio y 3537/2007, de 12 de junio.

Unión Europea. (2017) Informe SOCTA (Serious and Organised Crime Threat Assessment): *Crimen en la era de la tecnología*.

VELASCO NÚÑEZ, Eloy. *Delitos cometidos a través de internet*: *Cuestiones procesales*. Editorial La Ley. Madrid. 2010.

8.4. Webgrafía

ASHTON, Kevin. (3 de julio de 2010). The "Internet of the Things" thing. RFID Journal. Recuperado de:

http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf

El 80% de los delitos en internet son estafas y el 10% pornografía infantil. (7 de mayo de 2015). La Vanguardia. Recuperado de:

https://www.lavanguardia.com/tecnologia/20150506/54431079001/el-80-de-los-delitos-en-internet-son-estafas-y-el-10-pornografia-infantil.html

MARTÍNEZ, María José. (28 de febrero de 2017). *El 5% de los delitos se cometen por internet y redes sociales*. Córdoba: Cadena Ser. Recuperado de:

https://cadenaser.com/emisora/2017/02/28/radio_cordoba/1488277241_095891.html

Facultad de Informática - Universidad Complutense de Madrid. (21 de enero de 2015). *Delitos en internet*. Recuperado de:

https://www.youtube.com/watch?v=o7u0T7cpyJQ

GARCÍA, Isabel. Cibercrimen: "*En España solo se resuelve el 3% de los ciberdelitos denunciados*". (24 de abril de 2018). Nueva tribuna. Recuperado de:

https://www.nuevatribuna.es/articulo/sociedad/cibercrimen-ciberseguridad-ciberdelincuente-ciberatracador-mujeres-hackers-ransanwed-wenacraid-pentesting/20180424183449151198.html

Injurias o calumnias en Internet y Phishing, los delitos informáticos más comunes. Robo de identidad y estafa, los que más han aumentado. (20 de octubre de 2014). Noticias Jurídicas. Recuperado de:

http://noticias.juridicas.com/actualidad/noticias/4135-injurias-o-calumnias-en-internet-y-phishing-los-delitos-informaticos-mas-comunes-robo-de-identidad-y-estafa-los-que-mas-han-aumentado/

Los delitos con internet y las redes sociales suben un 52%. (11 de septiembre de 2018). Diario de Burgos. Recuperado de:

https://www.diariodeburgos.es/noticia/ZB62F8BE4-F63F-D2CA-C76B2012B3B6133E/Los-delitos-con-internet-y-las-redes-sociales-suben-un-52

Ministerio del Interior. (2018). *Infracciones penales registradas en Comunidades Autónomas, provincias, islas, capitales y localidades con población superior a 30.000 habitantes.* Recuperado de:

http://www.interior.gob.es/documents/10180/8736571/informe+balance+2018+3%C2%BA%20trimestre.pdf/4169ea84-3a74-48f1-913a-86869a8525be

Andalucía es digital. (10 de mayo de 2017). *Claves para estar preparados frente a los delitos en Internet*. [Archivo de vídeo]. Recuperado de:

https://www.youtube.com/watch?v=kYoYYwiilm4

Pido la palabra. (15 de mayo de 2013). *Francisco Hernández (Delitos por internet) - Pido la Palabra - 9 de mayo 2013* [Archivo de vídeo]. Recuperado de:

https://www.youtube.com/watch?v=6AbL98Sc7rs

La legislación española debería modificarse para luchar mejor contra los ciberdelitos. Comillas Universidad Pontificia. Recuperado de:

https://www.comillas.edu/es/noticias-comillas/3723-la-legislacion-espanola-deberia-modificarse-para-luchar-mejor-contra-los-ciberdelitos

ORTIZ PRADILLO, Juan Carlos. (23 de mayo de 2016). Determinación de la jurisdicción y competencia para la investigación y enjuiciamiento de los daños informáticos. Madrid. Recuperado de:

https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/ponencia%20Ortiz%20Pradillo%20Juan%20Carlos.pdf?idFile=cd54640d-efbe-4839-bb98-27f9b0c17d67

ALONSO LECUIT, Javier. (5 de diciembre de 2017). *Relanzamiento del Plan de Ciberseguridad de la UE*. Real Instituto Elcano. Recuperado de:

http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciberseguridad/ari97-2017-relanzamiento-plan-ciberseguridad-ue-union-europea

España, tercer país del mundo más afectado por 'phishing' en el tercer trimestre de 2018. (30 de noviembre de 2018). Portaltic. Madrid. Recuperado en:

https://www.europapress.es/portaltic/ciberseguridad/noticia-espana-tercer-pais-mundo-mas-afectado-phishing-tercer-trimestre-2018-20181130165759.html

LAVILLA, Milagros. 20 formas más comunes de estafas en Internet y redes sociales. *Webespacio*. Recuperado de:

https://www.webespacio.com/formas-comunes-estafas-internet-redes-sociales/

Víctimas de estafas por internet ¿Qué hacer? Vázquez & Apraiz y asociados. Recuperado de:

https://www.tuabogadodefensor.com/victimas-estafas-internet/#

El Instituto Nacional de Consumo pone en marcha una iniciativa contra el fraude en Internet. (1 de agosto de 2008). Noticias Jurídicas. Recuperado de:

http://noticias.juridicas.com/actualidad/noticias/870-el-instituto-nacional-de-consumo-pone-en-marcha-una-iniciativa-contra-el-fraude-en-internet/

Las 10 estafas más utilizadas en internet. (30 de enero de 2016). Unaibenito. Recuperado de:

https://www.unaibenito.com/que-no-te-enganen-en-internet-las-estafas-mas-utilizadas-durante-el-2012/