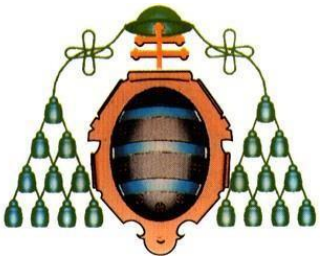

# UNIVERSIDAD DE OVIEDO

## Facultad de Derecho

Máster en Abogacía

## TRABAJO FIN DE MÁSTER

# LOS DELITOS COMETIDOS A TRAVÉS DE LAS NUEVAS TECNOLOGÍAS Y SU PROBLEMÁTICA PROCESAL.

Realizado por: Javier Somiedo Barrientos

Convocatoria: Enero de 2020

## RESUMEN

El trabajo se centra fundamentalmente en exponer el concepto de delito informático con sus principales características, e intenta desarrollar los principales tipos de conductas delictivas cometidas a través de las nuevas tecnologías. Asimismo, pretende exponer las principales problemáticas que se derivan en torno a las referidas conductas, más concretamente en lo relativo a su persecución y castigo judicial y a la determinación de la jurisdicción y competencia de los tribunales, intentando poner de relieve el influjo que las nuevas tecnologías plasman en el derecho, y las dificultades de este para adaptarse a las mismas y dar una respuesta adaptada a la realidad actual.

## ABSTRACT

The essay focuses mainly on exposing the concept of computer crime with its main characteristics, and attempts to develop the main types of criminal conduct committed through the new technologies. It also seeks to highlight the main problems arising in connection with the conduct in question, more specifically with regard to its prosecution and judicial punishment and the determination of the jurisdiction and jurisdiction of the courts, trying to highlight the impact of new technologies on the law, and the difficulties of the law in adapting to them and in responding to current realities.

# ÍNDICE

# INTRODUCCIÓN

El presente trabajo pretende exponer una realidad jurídica que ha introducido importantes cambios en el campo del derecho penal y procesal: los delitos cometidos a través de las nuevas tecnologías.

Así, se estudiará qué se entiende por el concepto de delito informático, así como sus principales características, fundamentando el análisis en la aportación de distintos autores y en la propia legislación española, intentando dar una respuesta a una cuestión controvertida y ausente de unanimidad. Seguidamente se desarrollarán las principales conductas delictivas llevadas a cabo a través de los medios informáticos, centrando la atención fundamentalmente en el delito de estafa informática con sus respectivas variantes y características y en aquellas conductas delictivas cometidas por medio de las redes sociales, plasmando la creciente influencia que las mismas están teniendo en el campo del derecho y de la sociedad, sin olvidar el examen que se hará relativo a las conductas que atenten contra la intimidad y seguridad informática en internet, basando el estudio en hechos tales como la interceptación de comunicaciones en la red, el espionaje o el intrusismo informático.

De este modo, se intentará representar la importante influencia que las nuevas tecnologías y su utilización están causando en el ámbito del derecho penal, apareciendo conductas antijurídicas novedosas y que hacen necesaria la intervención del legislador para adaptarse a los cambios producidos en la sociedad con el objetivo de dar respuesta a esos cambios, y de la propia jurisprudencia, cubriendo lagunas existentes en la legislación y que requieren una respuesta ante los importantes desafíos a los que se enfrenta y se enfrentará el derecho en este ámbito.

Enlazado con lo anterior, se representarán las principales problemáticas a las que se enfrenta el derecho procesal penal, evidenciando las carencias tanto técnico-policiales como jurídicas existentes para combatir esta clase de delitos, y poniendo de manifiesto la difícil convivencia entre las nuevas tecnologías y el derecho, consecuencia fundamental de la capacidad del primero para sobrepasar las tradicionales formas de investigación y castigo de los actos contrarios a derecho habidos en una sociedad.

Sin olvidar esto último, se analizarán los principales instrumentos de los que se dispone en la actualidad para el trabajo procesal, esto es, los medios procesales consistentes en la entrada y registro, la intervención de las comunicaciones y la prueba pericial, sin perjuicio de la manifiesta necesidad de que los mismos avancen y se adaptan al contexto actual, para después describir las fases procesales existentes para la investigación y castigo de la delincuencia informática desde una perspectiva técnico-policial, la fase inicial, la fase de investigación y la fase incriminatoria, sirviendo estas de base para la actuación de los Tribunales de Justicia.

Finalmente se estudiará una de las cuestiones que se revelan más complejas, y no es sino la determinación de la jurisdicción y competencia de los Tribunales en el ámbito de los delitos cometidos a través de las nuevas tecnologías, en este punto, se expondrán dos cuestiones fundamentales, la determinación de la competencia judicial desde el punto de vista internacional, con los problemas que se derivan y las soluciones aportadas, y la determinación de la competencia judicial desde el punto de vista interno, recogiendo en ambos casos las principales aportaciones de los autores, de la legislación y de la jurisprudencia para dar respuesta a una cuestión procesal que se manifiesta como fundamental, y es determinar el Tribunal que será el competente para perseguir y castigar las conductas antes descritas.

En definitiva, se intentará poner de relieve el impacto que las nuevas tecnologías están causando en el derecho penal y procesal, evidenciando la necesidad de que el derecho avance a mayor velocidad y se adapte con éxito a los desafíos que presentan las sociedades actuales donde las nuevas tecnologías lo invaden prácticamente todo.

# 1. EL DELITO INFORMÁTICO

## 1.1. QUÉ SE ENTIENDE POR DELITO INFORMÁTICO

El avance de la sociedad y por ello de la informática, está poniendo de manifiesto de forma clara la elevada dependencia existente entre las empresas, la Administración y la propia sociedad en la eficacia y seguridad de las TIC, esto es, las Tecnologías de la Información y la Comunicación. A modo de ejemplo podría destacarse que la mayoría de las transacciones económicas empresariales se efectúan por medio de ordenadores, la producción de una determinada compañía se subordina a un sistema informático que procesa sus datos o un gran número de datos personales se encuentran recogidos electrónicamente.

Esta interconexión manifiesta entre la sociedad y las TIC revela el gran impacto que los delitos informáticos pueden causar, y por ello la importancia que adquiere la seguridad que han de ostentar los mismos con el objetivo de obstaculizar las conductas delictivas llevadas a cabo por estos medios, así como la necesidad de tipificación de aquellos hechos que puedan ser constitutivos de sanción penal.[1]

La abundancia de conductas de carácter ilícito en internet hace complicado que pueda establecerse una definición acerca de lo que debe entenderse por delito informático. Diferentes autores han intentado ofrecer definiciones sobre el delito informático destacando la recogida por José Antonio Cruz de Pablo que dice así: ``*Por delito informático podrá entenderse aquéllas conductas típicas, antijurídicas, culpables y debidamente sancionadas por el ordenamiento jurídico penal para cuya ejecución se valen de ordenadores o cualquier otro mecanismo electrónico o informático, bien como medio, bien como fin, o mediante el uso indebido de los mismos´´*.

A pesar de que la mencionada definición pudiera resultar completa ha de destacarse que los avances tecnológicos, y la aparición de nuevas formas delictivas, consecuencia de ese avance, hacen necesaria una permanente revisión de cualquier definición relativa

[1] Davara Rodríguez, M., ``Delitos Informáticos´´, *Cizur Menor: Thomson Reuters Aranzadi.* Navarra, 2017, p. 20.

al delito informático, ya que lo que en un momento actual pudiera considerarse ajustado quedará obsoleto resultado de la velocidad con la que avanzan las nuevas tecnologías.[2]

Además de la complejidad para la definición de estos delitos basada en ese notable avance tecnológico, no ha de olvidarse una circunstancia especialmente relevante en este ámbito y no es otra que la falta de definición específica sobre este tipo de delitos en la legislación penal. El Código Penal referencia el término ``delitos informáticos´´ en torno a las consecuencias accesorias que puedan derivarse de la comisión de un delito, así puede destacarse el artículo 127.1 de este cuerpo legal que recoge: ``*Toda pena que se imponga por un delito doloso llevará consigo la pérdida de los efectos que de él provengan y de los bienes, medios o instrumentos con que se haya preparado o ejecutado´´*.

De modo complementario el artículo 127 bis afirma: ``*El juez o tribunal ordenará también el decomiso de los bienes, efectos y ganancias pertenecientes a una persona condenada por alguno de los siguientes delitos cuando resuelva, a partir de indicios objetivos fundados, que los bienes o efectos provienen de una actividad delictiva, y no se acredite su origen lícito´´*. En el apartado c) de este mismo artículo se recoge como una de las conductas delictivas la comisión de delitos informáticos.[3]

Ello pone de manifiesto que no existe una tipificación formal del delito informático, el elemento esencial estaría basado en analizar la utilización de las TIC en la comisión de un delito, consecuencia de ello se deriva que en el Código Penal la expresión ``delitos informáticos´´ no se recoge para tipificar una acción que deba tratarse de forma independiente con un apartado propio en el texto legal, sino con el objetivo de resaltar la utilización de las TIC en la comisión de un delito. Es por ello que la expresión delitos informáticos se refiere a una serie de acciones u omisiones que ya sean de forma dolosa o imprudente se encuentran penadas por la Ley, y en donde ha tenido relación en su comisión, de forma directa o indirecta, un bien o servicio informático.[4]

Centrando la atención de nuevo en establecer una definición concreta de lo que ha de entenderse por delito informático, podría afirmarse de forma previa que estos delitos

[2] Cruz de Pablo, J., ``Derecho Penal y Nuevas Tecnologías´´, *Difusión jurídica y temas de actualidad*. Madrid, 2006, pp. 20-21.
[3] Davara Rodríguez, M., ``Delitos Informáticos´´, *Cizur Menor: Thomson Reuters Aranzadi*. Navarra, 2017, p. 22.
[4] Ibid., p. 23.

se configuran por cualquier actividad ilegal conocida, esto es, una conducta típica tipificada en el Código Penal como podría ser un robo, hurto o fraude, siempre que en la referida conducta intervenga de forma directa y protagonista algún elemento TIC.[5]

El Convenio Sobre la Ciberdelincuencia del Consejo de Europa, suscrito en Budapest el 23 de Noviembre de 2001, define en su preámbulo al delito informático como ``todo acto dirigido contra la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos´´.[6]

Autores como Camacho Losa consideran que el delito informático se basa en ``*toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas´´.*[7]

Los delitos informáticos constituyen un elemento de dificultad notable para saber quién cometió la infracción penal, consecuencia de una serie de peculiaridades tales como la facilidad para borrar pruebas o la capacidad que proporciona el mundo de internet para huir de las identificaciones y con ello encubrir los hechos, además la comisión de estos delitos no requiere de la presencia física de su autor. Circunstancias estas que más adelante se abordarán en este trabajo pero que resulta procedente destacar en estos momentos en los que se intenta alcanzar una aproximación a una idea de delito informático.

Otras peculiaridades destacables de esta clase de delitos radican en la falta de conexión entre acción, tiempo y espacio, el anonimato que protege al delincuente, la dificultad de recabar pruebas sobre los hechos delictivos o el procesamiento y enjuiciamiento de los mismos.

[5] Ibid., p.25.
[6] Instrumento de Ratificación del Convenio sobre Ciberdelincuencia, Budapest, 23 de noviembre de 2001, publicado por el BOE nº226, 17 de septiembre de 2010, preámbulo.
[7] Camacho Losa, L., ``El delito Informático``, *Camacho Losa.* Madrid, 1987, p. 25.

## 1.2. CARACTERÍSTICAS BÁSICAS

Los delitos informáticos presentan una serie de características básicas y comunes que los diferencian de manera clara y evidente de la mayoría de conductas delictivas recogidas en la legislación penal.

Una de las referidas características se basa en la falta de conexión existente entre tiempo y espacio, estos delitos pueden ser llevados a cabo por una persona que se encuentre separada del lugar donde son cometidos y realizando una actividad distinta e incluso incompatible con los hechos delictivos en el momento en que estos se producen consecuencia de la posibilidad que ofrecen las tecnologías de la comunicación de actuar sobre programas informáticos que son programados para llevar a cabo su función en un momento temporal posterior, pudiendo elevarse a meses de diferencia entre la acción de programación y la producción del resultado, posibilitando de esta manera que el autor ya no se encuentre en el mismo lugar de la comisión y por ello resulte especialmente complejo conectar la acción de un sujeto con la producción de un resultado que pudiera derivarse en infracción y por ello susceptible de sanción.[8]

Esta circunstancia manifiesta la dificultad que ofrecen estos delitos para localizar la actividad delictiva y relacionarla con los hechos, ocultando en muchos casos el sujeto que ha llevado a cabo la acción.

Otro hecho relevante a destacar descansa en la facilidad para encubrir el hecho, una de las vías para hacerlo se basa en la posibilidad para modificar un programa para que lleve a cabo una actividad ilícita que beneficie al que ejecuta dicha acción, programando el programa para que sea modificado automáticamente cuando se haya llevado a cabo el hecho de forma que aparente total normalidad y ninguna apariencia de haber sido intervenido para ocasionar algún ilícito. Ello permite evitar que se detecte la comisión de un hecho delictivo y la forma de llevarlo a cabo por lo que habría que resignarse al resultado de la acción para ser conscientes que la misma se ha cometido.[9]

[8] Davara Rodríguez, M., ``Delitos Informáticos´´, *Cizur Menor: Thomson Reuters Aranzadi*. Navarra, 2017, p. 40.
[9] Idem.

En consecuencia, el resultado parece obvio y no es sino la dificultad para conectar la determinada persona que ha cometido el hecho con este mismo y por ello establecer la relación de causalidad típica del Derecho Penal que genere una implicación del sujeto activo y una correspondiente sanción penal.

La facilidad para borrar las pruebas es otra de las características ya que existe una gran facilidad para hacer que las mismas desaparezcan y con ello dificultar la detección de la acción. Son varios los ejemplos a destacar en este punto, uno de ellos proviene de la pertenencia que se repite en ocasiones del sujeto activo a una empresa determinada que cuenta con un sistema informático a través de cual se lleva a cabo la acción lo que permite el borrado de pruebas. En otras ocasiones el borrado de pruebas se deriva de la posibilidad que ofrecen los propios programas informáticos de hacer desaparecer mediante su manipulación actividades, operaciones o procesos llevados a cabo a través de estos.[10]

La cuestión de la intangibilidad constituye una de las principales problemáticas a las que se enfrenta el derecho penal para proceder a la tipificación de los delitos informáticos. Tradicionalmente se protegía bienes de carácter tangible, pero las nuevas tecnologías y su evolución manifiestan la necesidad de tener presente por la legislación penal valores inmateriales y de la información que se constituyan como bienes jurídicos protegidos, permitiendo de tal modo fijar uno de los elementos del tipo penal y con ello una acción antijurídica y por tanto sancionable por el derecho penal.[11]

El anonimato se presenta como la principal característica que obstaculiza la persecución de estas conductas y es que para llevar a cabo estas acciones no se requiere de la utilización de un sistema informático propio como podría ser un ordenador personal, sino que basta con utilizar cualquier tipo de ordenador, ello unido a la existencia de mecanismos que eliminan la identificación vía informática. [12]

[10] Davara Fernández, M., ``Delitos Informáticos´´, *Cizur Menor: Thomson Reuters Aranzadi*, Navarra. 2017, p. 41.
[11] Ibid., p. 42.
[12] Idem.

# 2. PRINCIPALES TIPOS

## 2.1. LA ESTAFA INFORMÁTICA

El delito de estafa informático presenta diversas variantes y ejemplos de conductas delictuales, una de ellas sería el delito de ``fraude de pago anticipado´´ o también denominado la ``estafa en el pago por anticipado´´. En este tipo de estafas interviene un elemento denominado ``spam´´ que no es sino un correo fraudulento de carácter electrónico. Para los casos en los cuales el resultado de las estafas den lugar a una merma económica se estaría hablando de ``scam´´ y en los supuestos en los que no mediara dicho perjuicio económico se estaría ante el denominado ``hoax´´. En el primero de los casos la conducta antijurídica tendría por objeto una finalidad de carácter lucrativo, un aprovechamiento económico derivado de la acción llevada a cabo, mientras que en el segundo de ellos el objeto principal no residiría en alcanzar dicho perjuicio.[13]

Este tipo de conductas suelen tener bastante presencia en la práctica y se dan con relativa frecuencia, un ejemplo concreto podría ser el supuesto en el que a través de las aplicaciones de venta online de varias clases de artículos, fundamentalmente de ropa de segunda mano el sujeto que procede a realizar la compra no ingresa de forma real el importe del objeto, sino que insta al vendedor al acceso a una determinada página como podría ser un servicio de mensajería donde supuestamente aparecerá la realización efectiva del ingreso pero en dicha página preparada a fin de engañar al vendedor se le informa de la necesidad de proceder a un determinado pago de la operación de venta como podría ser los gastos de transporte para obtener la cantidad objeto de venta, ello implica que el sujeto pasivo realiza un pago y no recibe el importe que le corresponde por lo que el autor de la estafa consigue su objetivo, en este caso mediando un elemento lucrativo, ejemplo que encajaría en el antes mencionado ``scam´´.

Otro tipo de conducta enmarcada en la estafa informática seria aquella mediante la cual la propia víctima hace llegar al defraudador los elementos sobre los cuales se lleva a cabo la conducta fraudulenta, el denominado ``phishing´´ sería un ejemplo, este

[13] Serrano Ferrer, M., ``El reflejo de las nuevas tecnologías en el derecho penal´´, *Cizur Menor: Thomson Reuters-Aranzadi,* Navarra. 2016, pp. 71-72.

término aplicado a la práctica consiste en recabar contraseñas ajenas para proceder a realizar la acción que conllevaría la estafa. El proceso sería el siguiente, el autor del hecho manda diversos correos vía electrónica a usuarios de banca on-line con enlaces cuyo acceso genera una página web creada al fin de proceder a la estafa y en donde el cliente puede ser engañado con facilidad ya que la apariencia es prácticamente idéntica a la original de la entidad, dicho acceso permite conseguir las contraseñas, claves de acceso, así como los datos bancarios de las víctimas con el fin posterior de disponer de los fondos de dichos clientes, conducta esta que igual que la anterior presenta una clara finalidad lucrativa.[14]

Pueden destacarse variedad de sentencias del Tribunal Supremo con un componente explicativo del método phishing como podrían ser: STS 23/07/2019 siendo ponente el Sr. Eduardo de Porres que recoge en su FJ 4: ``*en el mes de octubre de 2008, antes de los días comprendidos entre el 16 y 21 de dicho mes, persona o personas desconocidas a través del método phishing comenzaron a enviar a una serie de clientes de Caja Madrid, emails por medio de una aplicación web o dirección mendaz porque, aparentemente, estos correos electrónicos provenían de dicha entidad bancaria, de tal modo que, creyendo aquéllos que la web era la auténtica de su banco, facilitaron los datos que les solicitaron y las contraseñas o claves secretas, logrando acceder a sus distintas cuentas bancarias online´´*. Igualmente puede destacarse la STS 20/04/16 siendo ponente el Sr. Miguel Colmenero Menéndez de Luarca que establece: ``*el acusado, de acuerdo con el coacusado rebelde y utilizando el método phishing, es decir, remitiendo un correo simulado la página web de la entidad Banco Popular, consiguió que un familiar de Marcelina Loreto facilitara la clave secreta de la cuenta nº NUM042, abierta en una sucursal de Zaragoza, consiguiendo de esta forma ejecutar una transferencia de 4.100 euros que se ingresó en la cuenta abierta en Bankinter nº NUM043, abierta en una sucursal de Valencia a nombre de Franco Nemesio, persona inexistente´´*.

Una de las más explícitas en cuanto a su concepto sería la SAP La Rioja 16/04/2014, que en su FJ 2 desarrolla: ``*el phishing es 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*

[14] Ibid., p. 74.

*tarjetas de crédito u otra información bancaria). El estafador conocido como phisher, envía a numerosas personas correos electrónicos masivos en los que se hace pasar por una empresa de confianza (por ejemplo, una entidad bancaria, o una compañía telefónica, etc); otras veces lo hace mediante la creación de páginas web que imitan la página original de esa entidad o empresa de reconocido prestigio en el mercado; en ocasiones también se realiza por medio de llamadas telefónicas masivas realizadas a numerosos usuarios en las que se simula ser un empleado u operador de esa empresa de confianza. En todo caso, siempre se trata de una aparente comunicación oficial que pretende engañar al receptor o destinatario a fin de que éste le facilite datos bancarios o la tarjeta de crédito, en la creencia de que es a su entidad bancaria u a otra empresa igualmente solvente y conocida a quien está suministrando dichos datos. Finalmente, en otras ocasiones el sistema consiste simplemente en remitir correos electrónicos que inducen a confianza (simulando ser de entidades bancarias) que cuando son abiertos introducen troyanos en el ordenador del usuario, susceptibles de captar datos bancarios cuando este realiza pagos en línea. En todo caso, fuera cual fuere el modus operandi elegido, el objetivo son clientes de banco y servicios de pago en línea´´.*

En consecuencia puede apreciarse como la propia víctima de la conducta delictiva interviene de forma directa y trascendente en la comisión del hecho, claro está, que lo hace de forma inconsciente ya que de lo contrario estaría atentando contra sus propios intereses. El elemento base del engaño consistiría en conseguir aparentar una comunicación que podría calificarse de oficial, segura, familiar, en definitiva que transmita al perjudicado que puede confiar en ella y por ello acceder a suministrar los datos demandados en la misma con el resultado conocido, esto es, la producción de la acción típica antijurídica.

Del ``phishing´´ pueden derivarse otras conductas como es el ``smishing´´ pero en este caso el medio a través del cual se realiza la acción antijurídica no es el mismo, se estaría ante la utilización de mensajería móvil, mensajes SMS como medio comisivo.

Otra variante más sería el ``pharming´´, consistente en alterar las direcciones DNS encargadas de llevar a los usuarios a las páginas que desean ver. La clave de esta conducta radica en que el defraudador consigue que las páginas a las que se accede no se correspondan con las pretendidas por el usuario, sino con otras creadas para hacerse

con datos de carácter confidencial que guardan relación fundamentalmente con banca on-line.[15]

Este tipo de acciones se enmarcarían en el artículo 248.2 a) del CP que reza así: ``*Se consideran reos de estafa los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro´´*. Destacar en este extremo que en el encaje del método phishing en este precepto es apoyado por reiteradas sentencias del Tribunal Supremo entre las que puede destacarse la STS 25/10/2012 siendo ponente el Sr. Manuel Marchena Gómez que recoge: ``*el phishing, es decir, la obtención fraudulenta de claves personales de acceso pertenecientes a usuarios de la banca on-line adquiere tratamiento jurisprudencial como estafa informática del artículo 248.2 del Código Penal´´*.

Otra de las conductas mediante la cual se procede a llevar a cabo una estafa informática consistiría en la técnica de clonación de tarjetas mediante el sistema ``skimming´´ y ``de siembra´´. El primero de ellos consiste en lo siguiente: Se procede a la sustitución de la banda magnética de una tarjeta de crédito o de débito falsa por una verdadera cuyos datos son alcanzados a través de lectores preparados a tal fin. El objetivo pretendido consiste en llevar a cabo adquisiciones de bienes en establecimientos comerciales haciendo uso de la tarjeta manipulada aparentando por ello ser el titular legítimo pudiendo incluso disponer de fondos a través de entidades de crédito.

Apoyando lo anterior puede destacarse la STS 19/11/2014 siendo ponente el Sr. Manuel Marchena Gómez que recoge: ``*se describe el llamado skimming como la manipulación de los datos de las pistas de la banda magnética de la tarjeta genuina una vez haya sido copiada, alterando los datos concernientes al nombre del titular para finalmente grabarlos a una tarjeta, emitida originalmente por una entidad bancaria que coincide con el nombre de la persona que va a pasar la tarjeta´´*.

El proceso de ``siembra´´ consiste en lograr el número PIN y la propia tarjeta de crédito de aquella persona que se sitúa en el cajero para retirar dinero, de modo que situándose a una distancia suficientemente cercana se alcance a percibir el número

[15] Fernández Teruelo, J., ``Derecho Penal e internet´´, *Lex Nova,* Valladolid. 2011, p. 38.

secreto para justo después distraer a esa persona en el momento en que la tarjeta sale del cajero, circunstancia esta aprovechada por un tercero para sustraer la tarjeta original y sustituirla por otra distinta, de forma que la víctima sólo es consciente del hecho cuando procede en otra ocasión a realizar la misma operación y no se encuentra posibilitada para ejercerla debido a que la tarjeta no es la misma, esto es, la original. Del lado contrario los sujetos autores del hecho antijurídico se hacen con la tarjeta original y su clave pudiendo disponer de los fondos de esta. En el momento en que estas tarjetas pierden validez consecuencia de alcanzar el límite de disposición en efectivo son utilizadas como base para producir otras nuevas y volver a llevar a cabo nuevas operaciones como la descrita.[16]

La clonación de tarjetas apoyaría su carácter antijurídico en el artículo 248.2 b) del CP cuyo tenor literal es el siguiente: ``*Se consideraran reos de estafa los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo´´*.

Además de la mencionada clonación de tarjetas otro método de acción delictual común se trata del denominado ``lazo libanés´´ que consiste en lo siguiente: Se hace uso de un frontal de plástico con una ranura que, consigue prácticamente imitar a la ranura existente en el cajero automático de modo que el original queda cubierto por este último, el frontal superpuesto lleva adherida una cinta en forma de lazo (de ahí el nombre ``lazo libanés´´) con la extensión necesaria para que la tarjeta entre de forma completa y no sea posible recuperarla, todo ello sin que sea apreciable el modo en que se ha llevado a cabo. Este tipo de conductas suelen reproducirse en aquellas zonas con elevado número de turistas, y en épocas dónde precisamente estos acuden a las ciudades con mayor asiduidad.[17]

Los mensajes electrónicos se configuran como una vía de acción para cometer una estafa informática, un ejemplo claro sería la denominada ``estafa nigeriana´´ basada en el envío de una gran cantidad de e-mails que ofertan a los remitentes vías varias para ganar dinero entre las que se destacan premios de lotería o a través de mensajes de correo electrónico donde se informa al destinatario que se le hará un cargo a su tarjeta

[16] Serrano Ferrer, M., ``El reflejo de las nuevas tecnologías en el derecho penal´´, *Cizur Menor: Thomson Reuters-Aranzadi,* Navarra. 2016, pp. 77-78.

[17] Ibid., p. 80.

crediticia por una adquisición que nunca ha tenido lugar, en el mismo mensaje se adjunta una dirección de teléfono para resolver posibles dudas cuya llamada genera una conexión internacional en la que se mantiene a la espera por un tiempo considerable a los afectados.

## 2.2. DELITOS EN REDES SOCIALES

En primer lugar cabe destacar que las Redes Sociales se configuran como un elemento más de las TIC y en consecuencia traen consigo uno de los principales problemas de ellas y no es sino la falta de seguridad. Las conductas dolosas, es decir, con ánimo de causar daño llevadas a cabo a través de las redes sociales pueden agruparse en tres grandes grupos que son los siguientes:

- Conductas que conllevan actos de acoso.
- Ejercicio de la libertad de expresión hasta límites que pueden suponer ejercer acciones de odio y de violencia.
- Actuaciones que dan lugar a injurias y calumnias

### 2.2.1. GROOMING

El término ``grooming´´ hace referencia a aquellas conductas de un adulto por medio de la Red con el objeto de hacerse con el afecto o la intimidad de un menor de edad, con una elevada carga afectiva a través de la cual se alcanza la desinhibición del joven que consiente determinados actos en un marco de alto contenido de carácter sexual que, abre una serie de vías tales como el abuso sexual del adulto sobre el menor, introducir a este en la prostitución, exhibicionismo o proceder a la distribución de material pornográfico.[18]

La STS 21/03/2017 siendo ponente el Sr. Francisco Montarde Ferrer refiere: *´´el grooming, término de origen inglés se refiere a la acción deliberada de un adulto que pretende acosar y/o abusar sexualmente de un niño/a adolescente a través de internet.*

[18] Davara Fernández, M., ``Delitos Informáticos´´, *Cizur Menor: Thomson Reuters Aranzadi*, Navarra. 2017, p. 155.

*Para conseguir su objetivo, los groomers crean perfiles falsos en redes sociales u otras plataformas de chat similares inventándose una vida o persona que no son. Además de entablar conversaciones por tiempos prolongados, el propósito del diálogo es establecer confianza y pedir al menor contenido sexualmente explícito. Las fotos y medios eróticos son el principal medio de acción del Grooming, este primer paso puede producir un primer encuentro físico, lo que desenlaza en un acoso moral, o algo peor como una violación o un asesinato. Asimismo, una vez que la víctima decide compartir material a través de engaños, el groomer comienza a chantajear al menor, amenazándolo con publicar sus fotos y videos si no entrega más o se niega a un encuentro personal´´.*

Igualmente destacar la STS 24/02/2015 siendo ponente Juan Ramón Berdugo Gómez de la Torre que establece: ``*el término Child Grooming se refiere, por tanto, a las acciones realizadas deliberadamente con el fin de establecer una relación y un control emocional sobre un menor con el fin de preparar el terreno para el abuso sexual del menor´´.*

Esta conducta encontraría encaje penal en el artículo 183.ter del CP que establece:

1. ``*El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometido. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño´´.*
2. `` *El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años´´.*

Del contenido de las sentencias expuestas puede extraerse que el ``Grooming´´ se configuraría como una vía de actuación tendente a la producción de acción delictivas consistentes en abusos y agresiones sexuales a menores de dieciséis años, mediando un elemento de engaño, el menor actúa de forma espontánea y confiada consecuencia entre otros motivos del desequilibrio existente entre las partes, es decir, entre un adulto y un menor de edad, pudiendo el primero actuar dolosamente con el objetivo de que se acceda a sus pretensiones.

Esta conducta delictiva adquiere un importante componente psicológico, ya que la capacidad del adulto para manipular al menor y por ello que este lleve a cabo actos que puedan comprometerle en adelante será fundamental, de igual modo que el ``phishing´´ antes analizado, el engaño que media entre el sujeto activo y el perjudicado determinará que la acción delictiva se lleve a término y por ello que la víctima sufra las consecuencias.

### 2.2.2. SEXTING

El ``Sexting´´ se trata de una conducta consistente en el envío por medio de teléfono móvil de imágenes de carácter fotográfico, así como vídeos de contenido sexual llevados a cabo normalmente por el propio usuario.

Una de las principales características de esta conducta radica en que, en un primer momento, no media coacción alguna para realizarse la imagen y enviarla sino que se entiende como una acción voluntaria y deseada hecha en beneficio de la pareja o un grupo de amigos a modo de ejemplo.

La principal problemática del ``sexting´´ radica en el momento en el cual la imagen, vídeo enviado por su autor en un círculo de confianza y seguridad sale del mismo llegando el contenido a terceras personas, apareciendo en móviles de infinidad de sujetos, pueden llegar a ser miles o incluso millones, consecuencia de la elevada capacidad de difusión de que gozan las redes sociales. Plataformas como Facebook o YouTube permiten que en cuestión de minutos una imagen o un video puedan ser vistos en diferentes países propagándose de forma vertiginosa.[19]

[19] Ibid., pp. 164-166.

Las razones por las cuales el contenido desborda el ámbito de confianza del autor puede deberse a una imprudencia propia del mismo, es decir, un envío erróneo a una persona equivocada que posteriormente difunde el contenido o incluso un envío doloso por parte de una persona del círculo de confianza del autor.

Las consecuencias para la persona que sufre esta conducta pueden ser muy perjudiciales, fundamentalmente desde un una órbita psicológica ya que un contenido multimedia, ya que sea vídeo o imagen que comprometa a la persona en cuestión puede provocarle un estigma social importante, que se genere una respuesta negativa en la sociedad.

Una variante del ``Sexting´´ sería el ``Sexcasting´´, en este caso, el principal elemento característico de esta conducta encuentra lugar en el uso de la webcam para la grabación de contenidos sexuales y difusión de los mismos por e-mail, Redes Sociales u otra vía que permitan las nuevas tecnologías.

### 2.2.3. CIBERBULLYNG

El ``Ciberbullyng´´ o también denominado ciberacoso constituye una de las principales conductas dolosas cometidas a través de las Redes Sociales, generalmente cuando estas tienen lugar sobre los menores. Consiste en una práctica de carácter punible basada en el uso de medios informáticos para realizar un abuso de un menor a otro, la propia definición desvela que se trata de una práctica que afecta de forma muy notable a los menores.[20]

Para que tenga lugar el cibercaso, para que se ponga en práctica se requiere que el autor de la conducta y la víctima de la misma tengan la misma edad, o una edad muy similar, equiparable. La clave del ciberacoso radica en el ejercicio de un acoso psicológico entre iguales.

Por lo expuesto podría considerarse al ciberbullyng como ``*el acoso que un menor ejerce sobre otro de su misma franja de edad en entornos digitales tales como Redes Sociales, correo electrónico o SMS y constituye una de las principales lacras sociales que ha generado el uso irresponsable de la red´´*.

[20] Ibid., p. 168.

En la práctica esta conducta consistiría en la plasmación en el mundo digital del acoso que tiene lugar en el ámbito escolar pero en este caso la acción se vería agravada por unas circunstancias tales como una mayor exposición temporal, un anonimato o una usurpación de identidad.[21]

Ha de destacarse que el acoso siempre ha existido en un ámbito escolar pero la aparición y desarrollo de las nuevas tecnologías ha fomentado la aparición de una figura que es propia de la sociedad actual y no es otra que el ciberacoso con efectos en muchos casos más dañinos que el acoso tradicional debido a los elementos característicos de este tipo de conductas y que se han comentado anteriormente.

Por las propias características de esta práctica, el ciberacoso tiene lugar de forma muy mayoritaria en ámbitos escolares como colegios o institutos y provoca en la persona que lo sufre consecuencias muy perjudiciales para su salud mental.

### 2.2.4. SEXTORSIÓN

Consiste en una actividad que guarda una importante relación con el sexting, y es que unas fotografías o vídeos obrantes en una persona equivocada pueden provocar consecuencias altamente perjudiciales para el autor de las mismas, entre ellas podría destacarse la posibilidad de extorsionar, chantajear a la persona que aparece en ellas. Podría definirse la Sextorsión como el chantaje en el que un sujeto hace uso del contenido de imágenes o videos de contenido sexual para conseguir algo de la víctima, llevando a cabo amenazas consistentes en la posible publicación de los contenidos sexuales si no se accede a la petición del chantajista.[22]

La STS 23/07/2018 siendo ponente el Sr. Vicente Magro Servet establece: ``*Ante la proliferación de los casos de abusos sexuales por internet sin consentimiento de las víctimas y con el empleo de la extorsión de divulgar imágenes o vídeos de las víctimas se ha empezado a utilizar el término sextorsión, para calificar este tipo de actos de delitos de abusos sexuales cometidos por internet y con la extorsión que lleva implícita la falta de consentimiento de las víctimas. Como en este caso aquí analizado, el autor*

[21] Davara Fernández, M., ``Delitos Informáticos´´, *Cizur Menor: Thomson Reuters Aranzadi*, Navarra. 2017, p. 169.
[22] Ibid., p.170.

*del delito de abuso sexual online infecta primero el ordenador de su víctima mediante un virus que le permite acceder a sus contenidos, captando imágenes y/o vídeos que puedan comprometer su intimidad si se divulgaran. Generalmente el modus operandi consiste en la mecánica por la que el autor del delito envía un correo electrónico a su víctima con un enlace atractivo para ella, y al pinchar en el mismo se descarga el malware en su ordenador. Con ello, el criminal ya tiene acceso a sus contenidos y podrá descargarse archivos e imágenes o vídeos, que constituye luego la extorsión, lo que lleva a calificar los actos como sextorsión´´.*

Se pone de manifiesto nuevamente como la propia víctima puede determinarse como un elemento básico para garantizar la producción del delito, dicho de otro modo, si la persona que recibe el correo electrónico no hubiera pinchado en el enlace habido en el mismo, el delincuente no hubiera podido acceder a sus contenidos privados y posteriormente utilizarlos en forma de extorsión, por lo que se reitera como muy necesario una prudente utilización de los medios informáticos para evitar hechos como los descritos.

El artículo 197.7 del Código Penal recoge la tipificación de esta clase de conductas, afirmando lo siguiente:

``*Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa´´.*

### 2.2.5. PORNO VENGANZA

El porno venganza se trata de un término consistente en la publicación o divulgación de contenidos sexuales en Internet o a través de las Redes Sociales sin que medie aprobación del sujeto que aparece en las imágenes. Los contenidos suelen ser colgados en la red social por personas que, han mantenido algún tipo de relación con la persona que se ve afectada, ya sea de pareja o de amistad o incluso profesional y en consecuencia tienen acceso al mismo.[23]

Estas acciones encontrarían cabida en el artículo 197.7 del Código Penal, artículo arriba desarrollado y que resultaría de aplicación tanto para la sextorsión como para el porno venganza.

### 2.2.6. ACOSO INCESANTE: STALKING

Una de las principales diferencias entre este delito y los anteriores radica en que en este caso, no se trataría de una conducta vinculada exclusivamente a las Redes Sociales o tan siquiera a internet, ya que el acoso reiterado puede tener lugar por muy diversas vías, pero no cabe duda que el uso de las nuevas tecnologías constituye una herramienta fundamental para llevar a cabo estas acciones de acoso por lo que resultaría procedente enmarcar el stalking dentro de aquellos delitos cometidos por medio de internet.[24]

Este delito ha sido introducido en el Código Penal recientemente, en concreto en el año 2015 y se encuentra tipificado en el artículo 172 ter 1 de este texto legal que recoge lo siguiente:

``*Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:*

- *La vigile, la persiga o busque su cercanía física.*
- *Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.*

[23] Ibid., p.177.
[24] Ibid., p. 178.

- *Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contratare servicios, o haga que terceras personas se pongan en contacto con ella.*
- *Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella´´.*

La conducta requiere que tenga lugar una maniobra o estrategia permanente tendente a perseguir a una determinada persona y que se encuentre formada por varias acciones encaminadas a alcanzar un determinado objetivo que les vincule entre ellas por lo que no basta con que la conducta sea insistente o reiterada, sino que se requiere de la estrategia anterior. Un acoso concreto, a pesar de haber tenido lugar en dos o tres veces no encontraría encaje penal, se requiere una persistencia en el acoso y ante la resistencia u obstrucción de la víctima se persista en la actitud.[25]

La STS 12/07/2017 siendo ponente el Sr. Joaquín Giménez García establece: ``*el legislador al tipificar el nuevo delito de acoso y hostigamiento -Stalking- lo hace considerándolo como una variante del delito de coacciones al quedar fuera del ámbito de las coacciones, las conductas de acecho permanente o intento de comunicación reiterada que sin llegar a las coacciones, si tienen la entidad suficiente como para producir una inquietud y desasosiego relevante penalmente y que por ello no debe quedar extramuros de la respuesta penal al producir tal situación de acoso una alteración grave de su vida cotidiana, estableciéndose un tipo agravado para los casos en los que el sujeto pasivo, el que sufre el acoso es de las personas a las que se refiere el art. 173 CP, entre las que se encuentra el hecho de someter a esta situación a quien sea, o haya sido el cónyuge o persona ligada con él por análoga relación de afectividad´´.*

*´´El nuevo delito se vertebra alrededor de cuatro notas esenciales, que la actividad sea insistente, que sea reiterada, como elemento negativo del tipo se exige que el sujeto activo no esté legítimamente autorizado para hacerlo, que produzca una grave alteración de la vida cotidiana de la víctima. Puede afirmarse que la expresión insistente y reiterada equivale a decir que se está ante una*

[25] Cámara Arroyo, S. ``La primera condena en España por acecho o Stalking´´ Firma Invitada. Dialnet. 2016.

*reiteración de acciones de la misma naturaleza que se repiten en el tiempo, el tipo penal no concreta el número de actos intrusivos que puedan dar lugar al tipo penal, pero podemos afirmar que el continuo de acciones debe proyectarse en un doble aspecto: repetitivo en el momento en que se inicia, reiterativo en el tiempo (al repetirse en diversas secuencias en tiempos distintos). A ello debe añadirse la consecuencia de que ello produzca una grave alteración en la vida cotidiana, por tal debe entenderse algo cualitativamente superior a las meras molestias´´*

*``Por lo anterior se está ante un delito de resultado en la medida en que se exige que las referidas conductas causen directamente una limitación trascendente en alguno de los aspectos integrantes de la libertad de obrar del sujeto pasivo´´.*

*``El análisis de cada caso concreto, a la vista de las acciones desarrolladas por el agente con insistencia y reiteración, y por otra parte a la vista de la idoneidad de tales acciones para alterar gravemente la vida y tranquilidad de la víctima nos conducirá a la existencia o no de tal delito de acoso´´.*

Del estudio de la doctrina y de la jurisprudencia analizadas puede extraerse que para determinar la existencia o no de una conducta de ``stalking´´ o acoso incesante habrá que analizar el contexto, las acciones del sujeto activo, los casos en concreto para discernir si se están produciendo acciones que merezcan reproche penal, basando la investigación en revelar la existencia de una estrategia tendente a producir en la víctima alteraciones tales que limiten su vida cotidiana, que la perturben, de modo que se compruebe que las acciones no consisten en meras molestias compatibles con un día a día relativamente normalizado.

### 2.2.7. ENALTECIMIENTO DEL ODIO Y EL TERRORISMO POR MEDIO DE LAS REDES SOCIALES

Se trata en este caso de una cuestión controvertida debido a que en ocasiones no se encuentra del todo delimitada la frontera entre el ejercicio del derecho a la libertad de expresión y a la libertad ideológica y la posible comisión de un delito de apología del terrorismo. En este sentido han fallado los tribunales destacando la STS 3113/2016, de 13 de julio de 2016, que se pronunció sobre un caso de un usuario de la red social Twitter que publicó una serie de mensajes de apoyo a la banda terrorista ETA, entendiendo que se estaba humillando a las víctimas de los atentados de esta organización.

En lo tocante a la libertad ideológica que había esgrimido la defensa del acusado, la sentencia establece lo siguiente:

``*Es claramente un plus cualitativamente distinto del derecho a expresar opiniones arriesgadas que inquieten o choquen a sectores de una población, porque la Constitución también protege a quienes la niegan- STC 176/1995-, y ello es así porque la Carta Magna no impone un modelo de ``democracia militante´´. No se exige ni el respeto ni la adhesión al ordenamiento jurídico ni a la Constitución. Nada que ver con esta situación es la alabanza de los actos terroristas o el ensalzamiento de los verdugos que integran la médula del delito del art. 578 del Código Penal como elemento positivo, pero que excluye la incitación directa o indirecta a la comisión de hechos terroristas, como elemento negativo´´.*

El fundamento de derecho cuarto de la sentencia desarrolla lo siguiente:

``*No se trata, con toda evidencia, de prohibir el elogio o la defensa de ideas o doctrinas, por más que éstas se alejen o incluso pongan en cuestión el marco constitucional, ni, menos aún, de prohibir la expresión de opiniones subjetivas sobre acontecimientos históricos o de actualidad. Por el contrario, se trata de algo tan sencillo como perseguir la exaltación de los métodos terroristas, radicalmente ilegítimos desde cualquier perspectiva constitucional, o de los asuntos de estos delitos, así como las conductas especialmente perversas de quienes calumnian o humillan a las víctimas al tiempo que incrementan el horror de sus familiares. Actos todos ellos que*

*producen perplejidad e indignación en la sociedad y que merecen un claro reproche penal´´.*

Igualmente resulta procedente traer a colación la STS 224/2010, de 3 de marzo de 2010, que recoge:

``*El ejercicio de la libertad ideológica o de la libertad de expresión, no obstante, su reconocimiento como derechos fundamentales, pueden servir de cobertura a la impune realización de actos o exteriorización de expresiones que contengan un manifiesto desprecio hacia las víctimas del terrorismo, en tal grado que conlleve su humillación*.

*De hecho, como dijimos en la STS 539/2008, de 23 de septiembre, determinadas restricciones a la libertad de expresión pueden ser no sólo legítimas, sino hasta necesarias ante conductas que puedan incitar a la violencia o, como sucede en la humillación a las víctimas, provocar un especial impacto sobre quien la sufre en un contexto terrorista´´.*

En definitiva, la jurisprudencia del Tribunal Supremo se inclina por proteger la dignidad de las víctimas del terrorismo, así como a los familiares y personas allegadas a estas y su sufrimiento personal, en contraposición con el ejercicio del derecho a la libertad ideológica o de expresión, ejercicio que llevado al extremo puede y de hecho causa un grave perjuicio para aquellas personas que han sufrido, sufren o pueden sufrir actos de carácter terrorista.

La cuestión se revela como muy controvertida y prácticamente siempre que se pronuncian los Tribunales hay reacciones en uno y otro sentido, pero podría considerarse pertinente la vía adoptada por el Tribunal Constitucional, esto es, en aquellos concretos casos en los que el ejercicio de la libertad de expresión atente contra colectivos, personas vulnerables por los perjuicios que han sufrido, se proteja a las mismas, aún cuando se limite la libertad de expresión.

Aquellas conductas consistentes en llevar a cabo actos de enaltecimiento del terrorismo se encuentran claramente tipificadas en el artículo 578 del CP cuyo tenor literal dice así:

``*El enaltecimiento o la justificación públicos de los delitos comprendidos en los artículos 572 a 577 o de quienes hayan participado en su ejecución, o la realización de*

*actos que entrañen descrédito, menosprecio o humillación de las víctimas de los delitos terroristas o de sus familiares, se castigará con la pena de prisión de uno a tres años y multa de doce a dieciocho meses. El juez también podrá acordar en la sentencia, durante el periodo de tiempo que él mismo señale, alguna o algunas de las prohibiciones previstas en el artículo 57.*

*``Las penas previstas en el apartado anterior se impondrán en su mitad superior cuando los hechos se hubieran llevado a cabo mediante difusión de servicios o contenidos accesibles al público a través de medios de comunicación, internet, o por medio de servicios de comunicaciones electrónicas o mediante el uso de tecnologías de la información´´*

*``El juez o tribunal acordará la destrucción, borrado o inutilización de los libros, archivos, documentos, artículos o cualquier otro soporte por medio del que se hubiera cometido el delito. Cuando el delito se hubiera cometido a través de tecnologías de la información y la comunicación se acordará la retirada de los contenidos´´.*

## 2.3. DELITOS CONTRA LA INTIMIDAD Y SEGURIDAD INFORMÁTICA EN INTERNET

### 2.3.1. APROPIACIÓN DE CORREO ELECTRÓNICO E INTERCEPTACIÓN DE COMUNICACIONES EN LA RED

El artículo 197 del Código Penal sanciona las conductas de apoderamiento e interceptación de comunicaciones en la red con el objetivo de descubrir secretos o vulnerar la intimidad de un tercero sin su consentimiento, estableciendo:

``*El que, para descubrir los secretos o vulnerar la intimidad de otro, si su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación será castigado con la pena de prisión de uno a cuatro años y multa de doce a veinticuatro meses´´.*

Una de las principales problemáticas que se derivan de este delito radica en la determinación de la frontera de la privacidad que se protege, es decir, determinar cuál es el punto exacto a partir del cual se lleva a cabo un quebrantamiento de la privacidad reprochable penalmente. Se debe tener presente una disyuntiva consistente en saber si se requiere de la existencia de un perjuicio apreciable de la intimidad de la víctima o si, en cambio, es suficiente un simple acceso a la información privada de la misma con la intención de vulnerar su intimidad, aunque el mismo no sea especialmente dañino ni relevante para la víctima desde la perspectiva de su intimidad. Con carácter mayoritario se ha optado por la segunda vía, fundamentalmente porque el Código Penal protege además de la intimidad el secreto de las comunicaciones.[26]

No obstante, no hay unanimidad en esta cuestión y la jurisprudencia se manifiesta contradictoria entre sí, con resoluciones de los Tribunales en una u otra vía, afirmando en algunos casos que el tipo penal no puede englobar el acceso sin consentimiento a

[26] Fernández Teruelo, J., ``Derecho Penal e internet´´, *Lex Nova,* Valladolid. 2011, p.181.

informaciones con carácter anecdótico o banal, requiriéndose que el contenido del secreto esté basado en elementos propios de la intimidad personal.[27]

En referencia a la cuestión concerniente a la legitimidad o ilegitimidad y, dentro de ella, su potencial condición delictiva, de la interceptación de correo electrónico de los trabajadores de una determinada empresa por medio de los responsables de control de la misma, con carácter mayoritario se niega la existencia de responsabilidad de carácter penal por posible comisión de un delito contra la intimidad, o de otro tipo.[28]

La jurisprudencia más reciente establece que la empresa debe fijar el modo de uso de los medios informáticos y comunicar a los empleados la existencia de medios de control relativos a su uso. El control empresarial quedaría por ello restringido a la comprobación del uso de los medios informáticos para uso personal, sin que sea posible indagar en el discernimiento específico de cada uno de los usos.[29]

Podría destacarse como interesante al respecto lo establecido en la STS 26/09/2007 siendo ponente el Sr. Aurelio Desdentado Bonete. Se refiere: ``*Con respecto al control del uso del ordenador facilitado por el empresario al trabajador, si el medio informático se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado una expectativa razonable de intimidad en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso Halford) y 3 de abril de 2007 (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo para la protección de los derechos humanos´´*.

Establece además la misma Sentencia: ``*El empresario tiene que controlar el uso del ordenador, porque en él se cumple la prestación laboral y, por tanto, ha de comprobar si su uso se ajusta a las finalidades que lo justifican, ya que en otro caso estaría retribuyendo como tiempo de trabajo el dedicado a actividades extralaborales. El control de los ordenadores se justifica también por la necesidad de coordinar y garantizar la continuidad de la actividad laboral en los supuestos de ausencias de los trabajadores´´*.

[27] Ibid., p. 182.
[28] Ibid., p. 183.
[29] Ibid., p. 184.

De las sentencias analizadas puede concluirse que el empresario encuentra facultad para llevar a cabo controles en los ordenadores que utilizan los trabajadores en su puesto laboral, garantizando que de los mismos se hace uso para funciones estrictamente laborales y no de ámbito privado, el empresario puede comprobar que el tiempo de trabajo se utiliza para ello precisamente y no para otras cuestiones de ámbito personal, de modo que al realizar estas comprobaciones no se vulneraría la intimidad de los trabajadores y por ello no se produciría ilícito penal.

### 2.3.2. ESPIONAJE INFORMÁTICO

Las acciones relativas al espionaje informático encontrarían encaje penal en el artículo 197.2 del CP, que castiga el apoderamiento, utilización o modificación, sin autorización, en perjuicio de tercero, de datos reservados de carácter personal o familiar de otra persona hallándose estos registrados en ficheros o soportes informáticos. Igualmente destaca que el precepto que se castigará a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

Del tenor de la ley se extraen algunas características como: El apoderamiento y el acceso. En el primero de los casos, la doctrina se inclina por entender que se exige aprehensión material, mientras que en el acceso bastaría con una simple vista que no haya sido consentida, requiriéndose que ambas acciones hayan tenido lugar sin consentimiento, es decir, de forma ilícita.[30]

La principal controversia radicaría en el término ``datos de carácter personal o familiar´´ recogido en el precepto, en este sentido, la jurisprudencia entiende que bastaría con que se trate de datos que no se encuentran en poder de cualquiera, y que el sujeto no quiere que se divulguen.

[30] Ibid., p. 190.

### 2.3.3. INTRUSISMO INFORMÁTICO

El intrusismo informático encuentra encaje en el artículo 197.3 del CP. ``*El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con la pena de prisión de seis meses a dos años´´.*

Este tipo de delito adquiere la condición de delito ``barrera´´ u ``obstáculo´´[31] , de modo que se impide el acceso carente de aprobación a datos, programas o sistemas informáticos ajenos, en el sentido en que dicho acceso se configura como un elemento imprescindible para la producción de lesiones fundamentalmente sobre la intimidad y el patrimonio.

La punibilidad alcanza al acceso a datos o programas ajenos por medio de sistemas informáticos y el mantenimiento en los mismos sin consentimiento.

Un elemento llamativo del tipo tiene lugar en lo referido a la afirmación de ``*se mantenga dentro del mismo´´*, es decir, al sistema informático. El profesor Fernández Teruelo entiende que se está ante una ``forma omisiva propia´´, entendida esta como la obligación que tiene el sujeto de evacuar el sistema en cuanto deje de tener autorización para ello y, en cambio, permanece en el mismo sin abandonarlo. Ello conllevaría la existencia de dos elementos precedentes como son la existencia de una autorización previa de acceso y la consiguiente pérdida de esta.[32]

[31] Ibid., p. 198.
[32] Ibid., p. 201.

# 3. PROBLEMÁTICA EN LA PERSECUCIÓN Y CASTIGO DE LA DELINCUENCIA INFORMÁTICA

## 3.1. ASPECTOS COMUNES EN LA DIFICULTAD DE PERSECUCIÓN

La delincuencia informática presenta una serie de problemas de índole procesal entre los que pueden destacarse, la determinación de la jurisdicción nacional competente, la falta de homogeneidad de tipificación, la existencia de espacios de impunidad o la escasa colaboración de las víctimas en la denuncia de este tipo de conductas. Otras características a tener en cuenta podrían ser la obligación de especialización y concertación de carácter policial, la necesidad de contar con medios técnicos que hagan posible una satisfactoria investigación, la problemática derivada de la obtención de fuentes de prueba o las consecuencias transfronterizas de aquellas sentencias condenatorias, fundamentalmente en lo concerniente a su aplicación.[33]

La dificultad de persecución es consecuencia fundamental del funcionamiento de los procesos informáticos, y sobre todo de Internet. Esta última presenta una serie de características que indicen de forma directa en un proceso de carácter judicial, tales circunstancias serían:

- Se configura como una red, organización global, con vías de comunicación digitales, que obstaculiza el control fronterizo y el emplazamiento territorial de las acciones llevadas a cabo.
- La estructura de Internet promociona un elevado grado de oscurantismo en las conexiones y por ello incide en el anonimato de los sujetos intervinientes en la red, con la consiguiente dificultad para descifrar la identidad de los mismos y su posterior rastreo.
- La falta de homogeneidad legal en el ámbito internacional hacen complicado determinar la responsabilidad consecuencia de actos de carácter ilícito.

[33] Flores Prada, I., ``Criminalidad informática´´, *Tirant lo Blanch,* Valencia. 2012, pp. 300-301.

- El escaso grado de denuncias, que pone en evidencia el marco de desconocimiento del que en abundantes ocasiones son titulares las víctimas de este tipo de delitos.[34]

Circunstancias todas ellas que evidencia de forma clara la problemática que aportan las nuevas tecnología en ámbito legal, fundamentalmente en el penal y procesal.

Unido a lo anterior podría destacarse la necesidad incipiente de especialización en la investigación criminal, en la actualidad hay una serie de carencias en el ámbito policial y judicial que impiden un desarrollo favorable en la investigación y castigo de la delincuencia informática, algunas de ellas serían:

- Incremento de unidades policiales formadas en la investigación de estas conductas.
- Refuerzo de los procedimientos de concurso, convergencia internacional entre las fuerzas y cuerpos de seguridad de diferentes Estados, con creación de elementos de coordinación entre todos ellos.
- Formación de fiscalías específicas para la persecución de los delitos informáticos.
- Reformas legislativas y procesales que permitan una mayor agilidad y eficacia en la investigación y persecución.
- Acuerdos entre diferentes Estados para incrementar la necesaria cooperación judicial trasnacional en este tipo de ilícitos.[35]

Analizando de forma concreta algunos de los principales problemas en la investigación informática van a destacarse:

La conservación de los datos de tráfico, la identificación del usuario y el registro domiciliario.

Respecto del primero de ellos, debe destacarse que los datos de tráfico en ocasiones no son localizables, las investigaciones policiales ponen de manifiesto que en la mayoría de las investigaciones no se hallan señales concretas de un posible ilícito, lo que hace necesario la indagación de otras vías para alcanzar a determinar la autoría del mismo. El delincuente a la hora de cometer el delito procura en la gran mayoría de los casos borrar el rastro, de forma que cuanto más tiempo permanezcan los datos informáticos conservados en la red, mayor

[34] Ibid., p. 310.
[35] Ibid., p. 311-312.

posibilidad habrá de seguir una vía de investigación, por lo que se hace necesario fijar unos plazos de conservación que impidan la exención del delito.[36]

En lo relativo a la identificación del usuario, la asociación de éste con el equipo presenta importantes problemas, a modo de ejemplo, podría destacarse los supuestos de existencia de equipos de titularidad empresarial al que puede acceder cualquier persona sin ninguna clase de impedimento. Si un ordenador de empresa es utilizado por varios de sus trabajadores se haría muy complicado descifrar cuál de ellos podría haber cometido un hecho delictivo por vía informática.[37]

Otro caso sería el relativo a la existencia de varios ordenadores puestos a disposición de varios usuarios con carencia absoluta de control, como podría ser el supuesto de aulas informáticas en colegios, institutos o universidades que facilitan el acceso a los estudiantes. [38]

Parecido a este último caso es aquel consistente en el acceso a un sistema informático a través de los cibercentros, que presencian una importante ausencia de regulación y por ello dan absoluta libertad de acción, no tiene lugar ningún tipo de identificación lo que favorece evidentemente el anonimato. Igualmente el uso de los dispositivos WiFi permite que cualquier sujeto pueda conectarse en un lugar cercano al punto concreto de recepción disponiendo de anonimato, un ejemplo sería el caso en que una persona accede al interior de una cafetería que dispone de este tipo de servicios, conectándose desde su ordenador personal, garantizándose el anonimato en sus acciones a través de la red informática. [39]

En lo tocante al registro domiciliario, el principal problema radica en determinar el elemento o el grado a través del cual se está legitimado para poder llevar a cabo el mismo, un registro domiciliario puede llegar a conculcar un derecho fundamental, en concreto el de la inviolabilidad del domicilio, de manera que se trata de una medida compleja, cuya puesta en práctica requiere una aprobación sustentada en una justificación y una proporcionalidad.[40]

La jurisprudencia del Tribunal Constitucional se ha pronunciado al respecto, destacando la STC 49/1999, de 5 de abril de 1999 que recoge: ``*si la medida se*

[36] Velasco Núñez, E., ``Delitos contra y a través de las nuevas tecnologías´´, *Consejo General del Poder Judicial, Centro de Documentación Judicial,* Madrid. 2006, pp. 121-122.
[37] Ibid., p. 123-124.
[38] Ibid., p. 124.
[39] Idem.
[40] Velasco Núñez, E., ``Delitos contra y a través de las nuevas tecnologías´´, *Consejo General del Poder Judicial, Centro de Documentación Judicial,* Madrid. 2006, p. 126.

*autoriza por ser necesaria para alcanzar un fin constitucionalmente legítimo, como –entre otros-, para la defensa del orden y prevención de delitos calificables de infracciones punibles graves, y es idónea e imprescindible para la investigación de los mismos´´.*

Es decir, la Sentencia refiere que la posible restricción de un derecho fundamental como podría ser en este caso la inviolabilidad del domicilio únicamente tendrá legitimidad constitucional si ha habido una autorización judicial que tenga por objeto prevenir y perseguir conductas delictivas de carácter grave.

Teniendo presente que la única vía de obtención de indicios de prueba para incoar y continuar una investigación referente a este tipo de delitos es el domicilio en que se encuentra el equipo que ha servido de base para cometer el ilícito, el juicio de proporcionalidad exigible, también de idoneidad y necesidad quedarán vinculados al grado de gravedad del delito.[41]

Por lo que respecta a la duración del registro, ha de destacarse que en la mayoría de los casos es elevada, consecuencia del importe número de acciones que debe llevarse a término para esclarecer la posible comisión de un delito informático, tales como el volcado y análisis de la información intervenida, de modo que genera un importante perjuicio para la persona que se ve afectada por dicho registro.[42]

[41] Ibid., p. 127.
[42] Idem.

## 3.2. INSTRUMENTOS PROCESALES PARA SU INVESTIGACIÓN

### 3.2.1. ENTRADA Y REGISTRO

Sobre la medida de entrada y registro, debe establecerse que la intromisión en la privacidad del domicilio del investigado ha de tener lugar consecuencia de un auto judicial fundamentado jurídicamente, requisito indispensable para lograr una salvaguarda de una intervención imparcial de la jurisdicción, tal y como exige la Ley de Enjuiciamiento Criminal en su artículo 558.

En el auto se deberá expresar los indicios existentes que justifiquen la puesta en práctica de la medida, así como el domicilio a registrar, fundamentando las razones que apoyen que sea imprescindible y proporcionado vulnerar la intimidad domiciliaria del investigado.[43]

Además se exige que la medida de entrada y registro tenga lugar bajo fe pública, con la consiguiente intervención del Letrado de la Administración de Justicia que velará por una buena praxis en torno al manejo de los elementos delictivos (ordenadores, discos duros, fotografías, etc.), acreditando que se procede al precinto de los objetos requisados, y que serán una base para la prueba en el juicio.[44]

Para llegar al contenido de un ordenador situado en un domicilio privado, se configura como principal garantía judicial precisamente el auto de autorización de entrada y registro ya que este faculta la entrada en un sitio cerrado donde tenga lugar el ejercicio de la vida privada, el registro de todos los elementos del domicilio, y en especial de aquellos necesarios para la investigación judicial.[45]

---

[43] Velasco Núñez, E., ``Delitos contra y a través de las nuevas tecnologías´´, *Consejo General del Poder Judicial, Centro de Documentación Judicial,* Madrid. 2006, p. 284.
[44] Idem
[45] Velasco Núñez, E., ``Delitos contra y a través de las nuevas tecnologías´´, *Consejo General del Poder Judicial, Centro de Documentación Judicial,* Madrid. 2006, p. 287.

Se debe analizar ahora una cuestión controvertida y es la relativa a la necesidad o no de mandamiento judicial para proceder a adoptar la medida en una empresa, en un despacho profesional o en la Administración.

Estudiando el primero de los supuestos, el relativo a la entrada y registro en una empresa, suele estimarse que las misma, en su actividad de desarrollo mercantil, no se encuadra en espacios de realización de vida personal o familiar, motivo por el cual no se requeriría consentimiento judicial para llevar a cabo la medida, pero las características de este tipo de delitos y de procesos conllevan que en los registros se incauten elementos antes mencionados como ordenadores, discos duros, fotografías que implica que pueda quebrantarse la privacidad del usuario, por lo que se considera recomendable que la medida se lleve a cabo bajo mandamiento judicial, a pesar de que no sea específicamente necesario.[46]

Con respecto a los despachos profesionales y la las dependencias de la Administración, en los casos de despachos para el ejercicio de profesiones liberales se requiere de mandamiento judicial, es decir, no es posible prescindir del mismo para los supuestos en los que medie secreto profesional (despacho de abogados, de un psicólogo, etc.), de igual modo ocurre en los casos de dependencias administrativas donde se lleva a cabo la función pública.[47]

### 3.2.2. INTERVENCIÓN DE LAS COMUNICACIONES

Para proceder a llevar a cabo una intromisión en el secreto de las comunicaciones del investigado se requiere el cumplimiento de una serie de requisitos o condiciones previas como son:

- Una solicitud al Juez que deberá hacerse por los Cuerpos policiales o la parte que se haya personado en el procedimiento, con referencia explícita a las personas que hayan podidos participar en los acontecimientos que puedan ser objeto de investigación, un relato de los sucesos acontecidos y de los indicios existentes.
- Existencia de autorización judicial por auto motivado.

[46] Velasco Núñez, E., ``Delitos contra y a través de las nuevas tecnologías´´, *Consejo General del Poder Judicial, Centro de Documentación Judicial*, Madrid. 2006, pp. 284-285.
[47] Art. 564 LECrim.

- Realizar un correspondiente control temporal de la medida acordada.[48]

Una cuestión concerniente a la intervención de las comunicaciones radica en la intervención judicial para determinar la validez de los datos de tráfico en los casos en los que estos se consiguen por otras vías que no sean la judicial, al respecto ha de destacarse que no resulta obligada la intervención judicial, pero es obligatorio que las vías que han permitido la consecución de los datos de tráfico, no se hayan alcanzado mediando mala fe, aunque las mismas impliquen servirse de acciones espontáneas del investigado.[49]

La STC 18/09/2002 siendo ponente el Sr. Vicente Conde Martín de Hijas establece: ``*Al ser la intervención de las comunicaciones telefónicas una limitación del derecho fundamental al secreto de las mismas, exigida por un interés constitucionalmente legítimo, es inexcusable una adecuada motivación de las resoluciones judiciales por las que se acuerda, que tiene que ver con la necesidad de justificar el presupuesto legal habilitante de la intervención y la de hacer posible su control posterior en aras del respeto del derecho de defensa del sujeto pasivo de la medida, habida cuenta de que, por la propia finalidad de ésta, dicha defensa no puede tener lugar en el momento de la adopción de la medida´´*

`` *Se trata de determinar si en el momento de pedir y adoptar la medida de intervención se pusieron de manifiesto ante el Juez, y se tomaron en consideración por éste elementos de convicción que constituyan algo más que meras suposiciones o conjeturas de la existencia del delito o de su posible comisión, y de que las conversaciones que se mantuvieran a través de la línea telefónica indicada eran medio útil de averiguación del delito, el secreto de las comunicaciones no puede ser desvelado para satisfacer la necesidad genérica de prevenir o descubrir delitos o para despejar las sospechas sin base objetiva que surjan de los encargados de la investigación´´*

``*Una medida restrictiva del derecho al secreto de las comunicaciones sólo puede entenderse constitucionalmente legítima, desde la perspectiva de este derecho fundamental, si se realiza con estricta observancia del principio de proporcionalidad,*

[48] Velasco Núñez, E., ``Delitos contra y a través de las nuevas tecnologías´´, *Consejo General del Poder Judicial, Centro de Documentación Judicial*, Madrid. 2006, pp. 292.
[49] Ibid., p. 295.

*es decir, si, como ya hemos tenido ocasión de señalar, la medida se autoriza por ser necesaria para alcanzar un fin constitucionalmente legítimo, como, entre otros, para la defensa del orden y prevención de delitos calificables de infracciones punibles graves y es idónea e imprescindible para la investigación de los mismos´´.*

La existencia pues de autorización judicial para intervenir las comunicaciones se revela como fundamental, ello unido a una justificación de la medida, dicho de otro modo, el juez tendrá que argumentar las razones y fundamentos que habilitan adoptar una medida que puede provocar restricciones a un derecho fundamental con lo que ello supone, de modo y manera que debe existir una base de investigación previa suficientemente trabajada y sólida para proceder a la adopción de la intervención de las comunicaciones, actuando siempre bajo el principio de proporcionalidad, siendo la intervención necesaria para la continuación y buen término de la investigación y para lograr una salvaguarda del orden y prevención de los actos antijurídicos graves.

### 3.2.3. PRUEBA PERICIAL

En los delitos informáticos, especialmente en aquellos relativos a la estafa informática, tras la detención del disco duro del ordenador que se investiga, resulta necesario proceder a llevar a cabo un análisis pericial sobre el contenido del mismo, comprobando una serie de elementos constitutivos de la acción ilícita.

La prueba pericial lleva a cabo por organismos oficiales, fundamentalmente por las Fuerzas y Cuerpos de Seguridad del Estado, poseen presunción de imparcialidad, la defensa no obstante, se encuentra facultada para plantear una pericia alternativa o incluso impugnar la oficial en su escrito de calificación, teniendo presente que en los casos en que la defensa no se pronuncie sobre la pericial inicial, esta puede elevarse a prueba documental.[50]

Destacar igualmente que el informe pericial debe constar de unas bases mínimas para ser válido y tenido en cuenta como prueba en el proceso, estos requisitos básicos son:

- Relato de objetos sometidos a examen.

[50] Ibid., p. 307.

- Operaciones llevadas a cabo por medio del propio informe.
- Conclusiones.[51]

# 4. LA INVESTIGACIÓN DEL DELITO INFORMÁTICO

## 4.1. LA INVESTIGACIÓN

### 4.1.1. FASE PREVIA

La fase previa comienza a desarrollarse a través de la puesta en conocimiento del delito, la actuación que se lleva a cabo posteriormente es única, se procede al reconocimiento visual del lugar donde se hayan cometido los hechos para proceder al aislamiento del mismo y en concreto del equipo informático mediante el cual se hayan cometido los supuestos actos delictivos con el objeto principal de búsqueda de indicios de una acción antijurídica que permitan incoar una vía de investigación.[52]

En la mayoría de los casos se suele reclamar el apoyo de los Administradores del Sistema que tienen un elevado grado de conocimiento del equipo informático y de los servidores de la Red y sirven de ayuda para ubicar los vestigios del delito de forma más acelerada.

Los mencionados servidores de Red suelen custodiar un registro de hechos que tiene lugar en el sistema, donde se acopian los datos de tráfico de las conexiones establecidas, constituyéndose por ello como una de las principales vías de investigación.[53]

En esta fase, se acreditará, comprobará la existencia o no de una acción delictiva, pretende comprender qué ha ocurrido, en qué se ha basado el delito.

[51] Idem
[52] Velasco Núñez, E., ``Delitos contra y a través de las nuevas tecnologías´´, *Consejo General del Poder Judicial, Centro de Documentación Judicial*, Madrid. 2006, p. 111.
[53] Ibid., p. 112.

### 4.1.2. FASE INDAGATORIA

Esta fase se conforma por una parte técnica y otra policial. Se interesa conocer como se ha cometido el ilícito, determinar las conexiones que guarden relación con el delito y analizar los datos de tráfico para localizar el equipo informático y posteriormente encuadrar al titular de la conexión.

Una problemática que se plantea en la práctica en reiteradas ocasiones en esta fase radica en la complejidad que conlleva determinar la comunicación delictiva por la cual se ha llevado a cabo la acción antijurídica, por el contrario, suelen encontrarse meros indicios que posibilitan indagar en otras comunicaciones ramificadas y que pueden guardar relación con el delito. [54] Resulta crucial en este punto que el sujeto autor del hecho haya cometido errores a la hora de llevarlo a cabo, a modo de ejemplo, en un supuesto de creación y propagación de un virus informático, en su código de programación suelen incluirse apodos o sobrenombres que permiten rastrear en la Red esa nomenclatura y así poder identificar una comunicación. Dicha comunicación puede llevar a los investigadores a determinar un equipo informático utilizado por ese sujeto en la red.

Emplazado el equipo y determinado el abonado, se persigue la identificación del usuario del ordenador, para ello se seguirá la denominada ``*prueba de indicios´´* [55] , que servirá de base para asociar el usuario con el acto antijurídico, y con ello establecer la posible responsabilidad penal. Sobre los indicios se requiere que sean varios, estén acreditados y guarden una conexión exacta entre ellos mismos y la acción base de la responsabilidad penal.

La pluralidad de indicios exigidos para cumplir con la prueba antes referenciada se suelen integrar con los datos de tráfico o IP y aquellos que se consigan a través de la intervención del sistema informático, por lo que este último se configura como un elemento clave para alcanzar una satisfactoria indagación informática con la consiguiente incriminación.[56]

La STS 18/02/2015 siendo ponente la Sra. Ana María Ferrer García establece: ``*El valor como prueba de cargo de la prueba de indicios ha sido admitido tanto por el*

[54] Ibid., p. 113.
[55] Ibid., p. 115.
[56] Idem

*Tribunal Constitucional como por este Tribunal Supremo, a falta de prueba directa de cargo también la prueba indiciaria puede sustentar un pronunciamiento condenatorio, sin menoscabo del derecho a la presunción de inocencia´´.*

*``Sobre la naturaleza y estructuración de la prueba indiciaria tiene establecido el Tribunal Constitucional que el razonamiento o engarce lógico entre los hechos base y los hechos consecuencia ha de estar asentado en las reglas de criterio humano o en las reglas de experiencia común. El control de constitucionalidad de la racionalidad y solidez de la inferencia en que se sustenta la prueba indiciaria puede efectuarse tanto desde un doble canon: el de su lógica o cohesión, y el de su suficiencia o calidad concluyente. Con arreglo al primero la inferencia será irrazonable si los indicios acreditados descartan el hecho que se hace desprender de ellos o no llevan naturalmente a él. Desde el canon de su suficiencia o calidad concluyente no será razonable la inferencia cuando sea excesivamente abierta, débil o imprecisa. Son los órganos judiciales quienes, en virtud del principio de inmediación, tienen un conocimiento cabal, completo y obtenido con todas las garantías del acervo probatorio. Por ello se afirma que sólo se considera vulnerado el derecho a la presunción de inocencia en este ámbito de enjuiciamiento cuando la inferencia sea ilógica o tan abierta que en su seno quepa tal pluralidad de conclusiones alternativas que ninguna de ellas pueda darse por probada´´.*

La prueba de indicios se revela pues como pertinente en base a lo establecido tanto por la doctrina del Tribunal Supremo como por el Tribunal Constitucional, de forma que es posible constituirla como base en la fase indagatoria, y en efecto asociar un usuario con el acto antijurídico para determinar posteriormente la posible responsabilidad de carácter penal. Ello sin olvidar claro está que los mismos han de llevar al hecho antijurídico de forma natural, debe haber en consecuencia un encadenamiento entre los hechos base y las consecuencias que estos provocan.

### 4.1.3. FASE INCRIMINATORIA

En la fase incriminatoria se integran tres elementos fundamentales, estos son: la intercesión de los equipos informáticos, el respectivo dictamen incriminatorio y en caso de proceder la puesta a disposición judicial del sujeto causante del delito.

La intervención de la prueba tendrá lugar a través de un registro domiciliario, que tiene por finalidad intervenir todos aquellos elementos de carácter informático que puedan encerrar señales de ilegalidad, lograr las evidencias necesarias que conecten equipo y usuario, así como intervenir todos los instrumentos de la acción antijurídica para su decomiso. Cuando se haya procedido a la intervención del sistema informático habrá que realizar un examen del mismo, para ello resulta especialmente necesario proceder a una copia de la información, manteniendo la original, circunstancia que favorece el principio de contradicción de la prueba.[57]

El proceso de análisis sirve de base para ubicar, determinar y consolidar las certezas que se hallen para erigir la prueba de indicios y para vincular equipo informático, usuario e indicios.

Las investigaciones tienen por objeto establecer el delincuente y garantizar y presentar las pruebas del delito. La investigación de carácter informático se funda en identificar unas comunicaciones antijurídicas o ramificadas de la acción delictiva que permitan localizar el equipo informático por lo que se ha cometido la acción. Asociar equipo a usuario autor del delito se basa en un procedimiento complejo consistente en reunir un número importante de pequeños indicios que en su total constituyen una prueba. [58]

La totalidad de los indicios obtenidos en los diferentes estudios, tendrán que ser reflejados un informe que de forma razonada, concluya en una imputación de una acción antijurídica concreta a una persona determinada.[59] La base de esta fase incriminatoria consiste en la obtención y aseguramiento de las pruebas del delito

[57] Velasco Núñez, E., ``Delitos contra y a través de las nuevas tecnologías´´, *Consejo General del Poder Judicial, Centro de Documentación Judicial,* Madrid. 2006, pp. 116-117.

[58] Ibid., p. 119.
[59] Ibid., p. 120.

## 4.2. JURISDICCIÓN Y COMPETENCIA DE LOS TRIBUNALES

El fenómeno de Internet ha introducido significativos cambios en la sociedad, uno de ellos se basa en la utilización de este medio como un mecanismo de comunicación global, que hace que expanda su influjo con carácter plurijurisdiccional, es decir, sobre multitud de espacios territoriales. Las fronteras de los Estados suponen una evidente traba para incoar un proceso judicial sobre los autores de los delitos cometidos a través de internet, ya que este medio se conforma como un ámbito sin fronteras para los ciberdelincuentes, mientras que aquellos funcionarios (Cuerpos y Fuerzas de Seguridad, Fiscalía, Judicatura) encargados de perseguir y castigar los referidos delitos encuentran su actuación limitada a un campo de actuación concreto, que no es sino el del Estado al que pertenecen.[60]

El nacimiento y desarrollo del ciberespacio ha excedido los fundamentos de ubicación delictiva clásicos, fundamentados básicamente en el principio de territorialidad. En el ámbito físico, la acción delictiva tiene lugar en un emplazamiento más o menos concreto, lo que permite determinar una jurisdicción competente para entablar un proceso judicial, en este caso penal, pero por el contrario, en el espacio digital no se tiene en cuenta el espacio físico como tal, sino la Red de Internet con sus respectivas ramificaciones.[61]

La determinación de la Jurisdicción y Competencia de los Tribunales se configura como una cuestión controvertida, que ha dado lugar a diversas teorías tanto en la doctrina como en la jurisprudencia. Una de las vías propuestas que diversos autores consideran ajustada y razonada consiste en la determinación del juez nacional como juez global en el ámbito de los delitos informáticos, es decir, para ciertas conductas delictivas, diversos Estados conforman a los jueces nacionales como jueces universales, de modo que la competencia de estos engloba a cualquier acción antijurídica llevada a cabo en cualquier lugar del mundo sin tener presente el país de origen de su autor. En nuestro país este hecho tiene lugar a través de lo dispuesto en el art. 23.4 LOPJ que capacita a los jueces españoles para actuar sobre unos determinados delitos cuya comisión agrede bienes protegidos básicos (genocidio, terrorismo, prostitución, entre

[60] Flores Prada, I., ``Criminalidad informática´´, *Tirant lo Blanch*, Valencia. 2012, p. 313.
[61] Climent Barberá, J., ``La justicia penal en internet´´, *Cuadernos de Derecho Judicial.* 2001, p. 657.

otros). Ello aplicado al campo de Internet supondría establecer el principio de universalidad de castigo y persecución, donde se determinarían una serie de conductas delictivas de carácter informático, seleccionadas por su gravedad y efecto universal, pero esta vía no se entiende como válida para aplicarla en el ordenamiento jurídico español.[62]

La imposibilidad de aplicación del referido principio trae consecuencia fundamentalmente en el art. 24.3 de la LOPJ que recoge una restricción para la aplicación del principio de justicia penal universal, determinando que este principio sólo puede ser aplicado a una serie concreta de delitos, además de que la misma ley exige que para que puedan ser competentes los tribunales españoles, deberá confirmarse que sus autores se encuentren en España, que haya afectados de nacionalidad española, o se demostrase algún nexo relevante con nuestro país. [63]

Se considera que salvo supuestos muy concretos, la competencia de la jurisdicción española para incoar un procedimiento sobre delitos cometidos a través de internet que hayan tenido lugar más allá de las fronteras nacionales deberá configurarse sobre la base de lo establecido en el art. 23.2-3 LOPJ, lo que quiere decir, acciones delictivas llevadas a cabo por nacionales, o cometidas contra intereses nacionales.[64]

La principal problemática que se manifiesta consiste en determinar la jurisdicción nacional que resulta prioritaria ante actos delictivos de carácter informático que traigan causa en diversos países (nacionalidad del autor, lugar de ubicación del servidor, lugar de ubicación del terminal), y que producen efectos en infinidad de ellos. [65]. En estos casos, ``*la competencia, suele atribuirse a los Tribunales del Estado que, practicando su autoridad sobre el fundamento de la buena fe, y asegurando a los acusados y a las víctimas los derechos fundamentales a un juicio justo, se encuentren en las mejores condiciones de celebrar el juicio, valorando una serie de elementos como:*

- *Obligaciones existentes entre diferentes Estados*
- *Naturaleza y gravedad del delito*
- *Lugar de comisión*

[62] Pérez Machío, A., ``Dos problemas particulares de cara a la persecución de los delitos informáticos´´, *Thomson Reuters Aranzadi.* 2010, p. 250.
[63] Flores Prada, I., ``Criminalidad informática´´, *Tirant lo Blanch,* Valencia. 2012, p. 319.
[64] Idem.
[65] Choclán Montalvo, J., ``Fraude informático y estafa por computación´´, *Cuadernos de Derecho Judicial, CGPJ.* 2001, p. 309

- *Nacionalidad del autor*
- *Nacionalidad de las víctimas*
- *Intereses nacionales afectados*
- *Disponibilidad de las pruebas materiales del delito*
- *Residencia del acusado*
- *Lugar donde se encuentren los testigos o las víctimas´´*[66]

Dentro de la problemática que se plantea con la concurrencia de varias jurisdicciones nacionales, uno de los casos más ilustrativos que manifiestan los obstáculos existentes para configurar la competencia judicial internacional, afianzando la sujeción de la resolución judicial sobre las partes cuya nacionalidad no sea la misma que la del Tribunal que se considera competente, es la sentencia del Tribunal de Gran Instancia de París de mayo del año 2000, en un caso de objetos relacionados con el nazismo y distribuidos a través de la plataforma yahoo.com. La sentencia dictaminó que la referida plataforma debía impedir el acceso a ciudadanos franceses, consecuencia basada en que la distribución de propaganda nazi es considerada como delito en Francia, pero la principal controversia radicaba en que la referencia estadounidense de la misma plataforma no impidió el acceso a la ciudadanía gala debido a que la conducta tipificada como delito en Francia no lo estaba en Estados Unidos, es decir, la conducta no era contraria a derecho en el país en que la plataforma encontraba su sede. Durante el proceso la compañía americana ``yahoo´´ se personó en la justicia de los Estados Unidos, consiguiendo de sus Tribunales la declaración de no ejecución de la decisión judicial adoptada por el Tribunal parisino fundamentado en que la justicia francesa no se deduce competente para reglar actividades de una compañía americana. [67]

Para proceder a establecer la competencia judicial de los tribunales españoles en aquellas acciones antijurídicas llevadas a cabo a través de Internet, donde la determinación del lugar comisivo resulta notablemente complejo consecuencia de la disgregación territorial de la mayor parte de los componentes del ilícito, la jurisprudencia ha optado por aplicar la teoría de la ubicuidad para acoger a los tribunales españoles como competentes en el ámbito jurisdiccional, cuando alguno de

[66] Prada, I., ``Criminalidad informática´´, *Tirant lo Blanch*, Valencia. 2012, p. 321.
[67] Ibid., p. 323.

los elementos básicos del delito (acción ejecutiva, consecuencias producidas, beneficio de los autores) hayan encontrado su comisión en España.[68]

En este sentido hay que destacar lo el Acuerdo del Pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo de 3 de febrero del año 2005 sobre el mencionado principio. El acuerdo dice así: ``*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´´.*

Este acuerdo del Pleno del Tribunal Supremo ha asentado la aplicación de la teoría de la ubicuidad en nuestros tribunales, y la jurisprudencia con carácter muy mayoritario se ha basado en ello para resolver los problemas que surjan para determinar la competencia de los tribunales españoles en los delitos cometidos a través de internet donde medie dispersión territorial de los elementos del mismo.

Ahondando en lo anterior puede traerse a colación la STS de 12 de julio de 2009 788/ 2009 siendo ponente el Sr. Maza Martín, FJ 2 letra B) que establece: ``*en el motivo segundo en concreto, cuestiona la competencia de los Tribunales españoles para conocer de los delitos enjuiciados, pero, al margen de la inoportunidad de plantear una cuestión semejante a través del cauce de la infracción de Ley en lugar de otros posibles planteamientos más idóneos, como la vulneración del Juez legalmente predeterminado, lo cierto es que al resultar de aplicación, para la determinación de la jurisdicción nacional competente, el principio de "ubicuidad", según el cual puede atribuirse aquella a cualquiera de los órganos territoriales de los lugares donde se cometieron actos ejecutivos del delito y en este caso, como con tanto acierto indica el Fiscal en su escrito de impugnación del Recurso, gran parte de esos actos ejecutivos de los delitos de las defraudaciones se han cometido en nuestro país, entre otros los estrictamente consumativos de los ilícitos como el hecho de quedar el dinero defraudado a disposición del sujeto activo precisamente en España, es evidente la competencia de nuestros Tribunales para conocer de este enjuiciamiento´´.*

En la presente sentencia puede apreciarse como los Tribunales españoles, más en concreto el Tribunal Supremo aplica el principio de ubicuidad teniendo en cuenta la

[68] Idem

posibilidad de aplicar la competencia judicial a uno de los órganos territoriales de los lugares donde se hayan cometido actos del delito en cuestión.

Ha de destacarse que las acciones delictivas llevadas a cabo haciendo uso de los medios informáticos además de suponer una fuente de problemas competenciales de carácter internacional como se ha expuesto, también suponen una problemática en lo relativo a la competencia judicial interna. [69] La determinación de la jurisdicción nacional constituiría el primer tránsito para configurar el órgano competente en materia de delincuencia informática, y es que una vez se ha establecido que a modo de ejemplo resultan competentes los tribunales españoles se requiere determinar el concreto órgano judicial que conocerá del delito y ello puede derivar en dificultades en el ámbito de la competencia territorial.

La Ley de Enjuiciamiento Criminal hace referencia al lugar de comisión delictiva como fuero general y prioritario para la especificación del órgano judicial que resultará territorialmente competente, pero en el campo de internet los nexos existentes en el mundo físico entre acción y espacio territorial donde se lleva a cabo desaparecen, por lo que habrá que atender a otros criterios competenciales para este tipo de delitos, aportando fueros que se basen en el modo de actuación digital (ubicación física de terminales) o centralizando la competencia en órganos de carácter nacional como podría ser la Audiencia Nacional.[70]

Sentado lo anterior debe destacarse que tanto la doctrina como la jurisprudencia se inclinan por la aplicación de las normas competenciales vigentes, que en el ámbito de la competencia territorial fija que se determinará analizando el caso en concreto tomando como base las teorías de la actividad, resultado y ubicuidad, optando fundamentalmente por la aplicación de esta última tal y como ocurría en el campo de la competencia judicial internacional. En base a ello y para determinar la competencia judicial interna, se atenderá al contenido de la teoría que recoge que ``*el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo, resultando competente cualquiera de ellos, y de competencia preferente el que primero haya iniciado las actuaciones´´*. [71]

[69] Fernández Teruelo, J., ``Derecho Penal e internet´´, *Lex Nova,* Valladolid. 2011, p.28.
[70] Ibid., pp. 24-25.
[71] Prada, I., ``Criminalidad informática´´, *Tirant lo Blanch*, Valencia. 2012, pp. 329-330.

Ejemplificando la puesta en práctica de lo anterior cabe destacar la SAP de Barcelona, de 29 de enero de 2008, siendo ponente la Sra. Ana Rodríguez Santamaría, en su FJ segundo establece: ``*para evitar discusiones de foro (que sólo favorecen el anonimato delincuencial y la demora en la persecución de estos delitos, que por su naturaleza precisan de la rápida actuación del investigador), el Tribunal Supremo, ha considerado que el delito informático, de tracto mutante e itinerante, y que establece sus efectos en múltiples ubicaciones geográficas, se produce (y por lo tanto es competente) en todos y cada uno de los sitios donde se manifiestan sus efectos, lo que incluye tanto el lugar de la acción como el del resultado. Esa opción por el llamado principio de la ubicuidad, se reflejó a partir del acuerdo no jurisdiccional del pleno del Tribunal Supremo de fecha 3/02/2005, según el cual: 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 y además en este caso sin duda lo fueron los Juzgados de Barcelona al versar la investigación con una página web alojada en el dominio de Vesatec, empresa formada entre otros por el aquí condenado´´.*

De ello se desprende que tanto para la determinación de la competencia judicial internacional como para la competencia judicial interna, se atenderá al principio de ubicuidad consecuencia fundamentalmente del acuerdo del Pleno del Tribunal Supremo mencionado, y que es de aplicación por la jurisprudencia de los Tribunales españoles para resolver los conflictos competenciales que surgen en los delitos informáticos.

# 5. CONCLUSIONES

1.- El concepto de delito informático entraña una realidad compleja de analizar, y es que a pesar de las diferentes aportaciones de autores que se han comentado o del propio Convenio sobre la Ciberdelincuencia del Consejo de Europa, el elemento fundamental a tener en cuanta radica en que no existe una tipificación formal en la legislación penal, la normativa se centra en la influencia que las nuevas tecnologías tienen en la comisión de una conducta delictiva, es decir, en la comisión de un ilícito penal perpetrado haciendo uso de elementos informáticos, donde ha tenido relación en su comisión, de forma directa o indirecta, un bien o servicio informático, pero no obra una definición concreta en el Código Penal, de modo que para alcanzar una respuesta a la cuestión relativa a qué se entiende por delito informático, habrá que buscar un equilibrio entre las aportaciones de la doctrina y la influencia que los elementos de las TIC (Tecnologías de la Información y la Comunicación) tienen en la comisión de una conducta reprochable penalmente.

2.- Respecto a las principales características que presentan esas conductas delictuales cometidas por medios informáticos se destaca la falta de conexión existente entre tiempo y espacio, la dificultad para localizar la actividad delictiva, la facilidad para encubrir el hecho o la intangibilidad que presentan estas acciones, circunstancias todas ellas que implican importantes dificultades para el derecho fundamentalmente en el campo de la persecución y castigo.

3.- La estafa informática se configura como una de las principales vías de acto antijurídico perpetrado haciendo uso de los medios informáticos, presenta una importante variedad de conductas, muchas de ellas con una finalidad eminentemente lucrativa, de entre las analizadas en el presente trabajo, podría resaltarse el ``phishing´´ ya que en la práctica resulta una de las más asiduas y por ello más usuarios de internet se ven afectados, el carácter lucrativo de la misma es claro ya que uno de los elementos básicos consiste en hacerse con los datos bancarios del usuario para posteriormente disponer de los fondos, mediante técnicas bastante sofisticadas y que en reiteradas ocasiones consiguen su objetivo y en consecuencia la consumación del hecho delictivo, por lo que resulta muy importante actuar con la debida diligencia y precaución cuando

se hace uso de los medios informáticos, en particular, si se aportan datos determinantes para provocar un perjuicio económico.

4.- Además de la estafa informática, los delitos cometidos en redes sociales se manifiestan como otro de los medios comisivos más habituales, de entre todos los tipos analizados, uno de los que resulta más controvertido sería el enaltecimiento del odio y terrorismo a través de las redes sociales, este carácter controvertido no resulta caprichoso, sino basado en la dificultad práctica de delimitar la frontera entre el ejercicio del derecho a la libertad de expresión e ideológica y la posible comisión de un delito de apología del terrorismo. La solución se encuentra fundamentalmente en la Jurisprudencia, en las sentencias de los Tribunales, al respecto se destaca que estos optan mayoritariamente por ofrecer una protección a la dignidad de las víctimas en contraposición con un ejercicio podría decirse que excesivo de la libertad de expresión y que en consecuencia atentaría contra la mencionada dignidad, por lo que se busca un equilibrio entre ambos derechos, inclinando la balanza los Tribunales por sancionar aquellas conductas que lleven a odio o apología del terrorismo, protegiendo con ello a las víctimas, como se pone de manifiesto a través de las sentencias analizadas, por lo que en ocasiones se opta por restringir la libertad de expresión, cuando esta pueda conllevar incitación al odio o violencia.

5.- Los principales ilícitos cometidos mediante los medios informáticos no acaban aquí, y es que además de la referida estafa informática o los delitos perpetrados haciendo uso de las redes sociales, ha de destacarse los cometidos atentando contra la intimidad y seguridad informática en internet, de entre ellos el más relevante podría ser el apoderamiento de correo electrónico e interceptación de comunicaciones en la red, donde se castiga fundamentalmente la vulneración de la intimidad de una persona, el principal punto destacable en este aspecto deriva de la problemática respecto a establecer el límite a través del cual se considera que se vulnera la intimidad de una persona, y es que la repuesta no está clara debido a que los Tribunales en ocasiones exigen un plus en el contenido de la información interceptada para que pueda considerarse de entidad suficiente y no meros datos banales que no implican perjuicio a la persona afectada mientras que en otras ocasiones se inclinan por no elevar ese límite, de modo que es más sencillo incurrir en la comisión de un delito.

6.- En lo relativo a los principales problemas existentes en la persecución y castigo de la delincuencia informática pueden destacarse que internet se configure como una red global que obstaculiza el control fronterizo y el emplazamiento territorial de las acciones llevadas a cabo, el anonimato que ofrece, la falta de homogeneidad legal en el ámbito internacional o el escaso grado de denuncias, circunstancias ellas que evidencian la problemática que aportan las nuevas tecnologías en el ámbito penal y procesal, destacando como posibles soluciones para mejorar el papel del derecho en este ámbito, el incremento de unidades policiales formadas específicamente para la investigación de estos delitos, formación de fiscalías específicas para la persecución de los delitos informáticos, o acuerdos entre los Estados para incrementar la necesaria cooperación judicial trasnacional.

7.- Sobre los principales instrumentos de los que dispone el derecho procesal para hacer frente a estas conductas delictivas ha de destacarse la entrada y registro, la intervención de las comunicaciones y la prueba pericial. De entre ellos, la entrada y registro presenta algunas particularidades, y es que esta medida requiere en la mayoría de los casos de autorización judicial, pero no siempre ocurre así, ha de diferenciarse entre la adopción de la medida en un domicilio particular, donde es obligada la autorización, una empresa donde es recomendable pero no obligada la mencionada autorización o en dependencias de la administración, así como en despachos profesionales donde sí se requiere mandamiento judicial, sin la posibilidad de prescindir del mismo como ocurre en el caso de las empresas. Cuando se hace referencia a despachos profesionales se destacan aquellos en los que media la existencia de secreto profesional, destacando como ejemplos una clínica de un psicólogo o un despacho de abogados.

8.- Las fases procesales estudiadas en el trabajo se basan en un campo técnico-policial, las mismas son, la fase previa, la fase indagatoria y la fase incriminatoria. Las tres tiene en común que sirven de base para el posterior trabajo de los Tribunales de Justicia con el objetivo de que estos posean toda la información necesaria sobre el autor o autores del delito, la forma en que se ha perpetrado, las vías por las cuales se ha cometido, pruebas y demás elementos necesarios para garantizar un reproche penal a una conducta contraria a derecho. En muchas ocasiones y dado su carácter técnico, se recaba el apoyo de administradores del sistema informático, de expertos para una labor que se manifiesta como compleja y fundamental en el ámbito procesal penal.

9.- Centrando la atención en la cuestión relativa a la jurisdicción y competencia de los Tribunales, esta se revela como una de las circunstancias más complejas en lo relativo a los delitos cometido por medio de las nuevas tecnologías, ello consecuencia de una serie de características como el hecho de que internet expanda su influjo con carácter plurijurisdiccional, sobre multitud de espacios territoriales, excediendo por ello de los fundamentos tradicionales de ubicación delictiva, basados en el principio de territorialidad, y es que en el mundo físico, el acto delictivo tiene lugar en un emplazamiento más o menos concreto del territorio por lo que se hace relativamente sencillo determinar la jurisdicción y competencia de los Tribunales, circunstancia esta que resulta mucho más compleja en el campo de los delitos cometidos mediante las nuevas tecnologías.

10.- Pueden destacarse dos vertientes a la hora de determinar la jurisdicción y competencia, una relativa a la competencia judicial internacional y otra a la competencia judicial interna. Respecto de la primera de ellas se han propuestas diversa teorías, optando los Tribunales españoles por la aplicación del principio de ubicuidad para determinar la jurisdicción nacional competente, consecuencia del Acuerdo del Pleno no Jurisdiccional del Tribunal Supremo de 3 de febrero del 2005, cuya conclusión fundamental a extraer se basa en que la competencia de los Tribunales pueda atribuirse a cualquiera de los órganos territoriales de los lugares donde se cometieron actos ejecutivos del delito, el delito se entenderá cometido en todas las jurisdicciones en las que se haya llevado a cabo algún elemento del tipo, por lo que el Juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será competente para la instrucción del caso.

11.- Con respecto a competencia judicial interna, ha de destacarse que al igual que la determinación de la competencia judicial internacional, ésta también presente problemas, y es que una vez determinada la jurisdicción nacional competente, habrá que establecer qué concreto órgano judicial conocerá del delito, por lo que pueden surgir problemas en el ámbito territorial, para la resolución de estos problemas, tanto doctrina como jurisprudencia optan por el mismo principio que se aplicó en el ámbito de la competencia judicial internacional, esto es, el principio de ubicuidad, de modo que el primer órgano judicial que haya iniciado las actuaciones de entre alguna de las jurisdicciones en las que se haya cometido algún elemento del tipo, será el competente.

12.- Todo lo anteriormente expuesto, lleva a concluir que el fenómeno de las nuevas tecnologías está causando un importante impacto en el mundo del derecho, evidenciando la necesidad de este de adaptarse a esta realidad que con mucha probabilidad irá a más en el futuro expandiendo de forma creciente su influencia, por lo que el derecho penal y procesal ha de garantizar que su uso no suponga una fuente de comisión delictiva, incrementando los medios técnicos, policiales y jurídicos para su prevención y su posterior persecución y castigo en los casos en los que lo anterior no haya sido posible.

# BIBLIOGRAFÍA

Camacho Losa, Luis, El Delito Informático, Camacho Losa, Madrid, 1987.

Cruz de Pablo, José Antonio, Derecho Penal y Nuevas Tecnologías, Difusión Jurídica y Temas de Actualidad, Madrid, 2006.

Davara Rodríguez, Miguel Ángel, Delitos Informáticos, Cizur Menor- Thomson Reuters-Aranzadi, Navarra, 2017.

Fernández Teruelo, Javier Gustavo, Derecho Penal e Internet, Lex Nova, Valladolid, 2011.

Flores Prada, Ignacio, Criminalidad Informática, Tirant lo Blach, Valencia, 2012.

Serrano Ferrer, María Pilar, El Reflejo de las Nuevas Tecnologías en el Derecho Penal, Cizur Menor- Thomson Reuters- Aranzadi. Navarra, 2016.

Velasco Núñez, Eloy, Delitos contra y a través de las Nuevas Tecnologías, Consejo General del Poder Judicial- Centro de Documentación Judicial, Madrid, 2006.

# FUENTES NORMATIVAS

Instrumento de Ratificación del Convenio sobre Ciberdelincuencia, Budapest, 23 de noviembre de 2001, publicado por el BOE nº 226, 17 de septiembre de 2010.

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

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

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.

## FUENTES DOCUMENTALES

Cámara Arroyo, Sergio, La Primera Condena en España por acecho o Stalking, Cuadernos de Criminología- Revista de Criminología y Ciencias Forenses, 2016.

Climent Barberá, Juan, La Justicia Penal e Internet, Cuadernos de Derecho Judicial, 2001.

Choclán Montalvo, José Antonio, Fraude Informático y Estafa por Computación, Cuadernos de Derecho Judicial- CGPJ, 2001.

Pérez Machío, Ana Isabel, Dos Problemas Particulares de Cara a la Persecución de los Delitos Informáticos, Derecho Penal Informático, 2010.

## FUENTES JURISPRUDENCIALES

Acuerdo del Pleno no Jurisdiccional de la Sala Segunda del Tribunal Supremo de 3 de febrero de 2005.

Sentencia Tribunal Constitucional, 49/1999, de 5 de abril de 1999.

Sentencia Tribunal Constitucional, 167/2002, de 18 de septiembre de 2002.

Sentencia Tribunal Supremo, 966/2006, de 26 de septiembre de 2007.

Sentencia Tribunal Supremo, 788/2009, de 12 de julio de 2009.

Sentencia Tribunal Supremo, 224/2010, de 3 de marzo de 2010.

Sentencia Tribunal Supremo, 834/2012, de 25 de octubre de 2012.

Sentencia Tribunal Supremo, 771/2014, de 19 de noviembre de 2014.

Sentencia Tribunal Supremo, 72/2015, de 18 de febrero de 2015.

Sentencia Tribunal Supremo, 97/2015, de 24 de febrero de 2015.

Sentencia Tribunal Supremo, 327/2016, de 20 de abril de 2016.

Sentencia Tribunal Supremo, 3113/2016, de 13 de julio de 2016.

Sentencia Tribunal Supremo, 174/2017, de 21 de marzo de 2017.

Sentencia Tribunal Supremo, 554/2017, de 12 de julio de 2017.

Sentencia Tribunal Supremo, 377/2018, de 23 de julio de 2018.

Sentencia Tribunal Supremo, 379/2019, de 23 de julio de 2019.

Sentencia Audiencia Provincial de Barcelona, 95/2008, de 29 de enero de 2008.

Sentencia Audiencia Provincial de La Rioja, 77/2014, de 16 de abril de 2014.