## 1. Introducción

El presente trabajo tiene como objeto de estudio la figura de los delitos informáticos, su conceptualización tanto en el ordenamiento jurídico nacional como a nivel doctrinal, puesto que resulta necesario para estudiar este hecho delictivo tan habitual en nuestra actualidad apreciar si se deben de configurar como una categoría penal propia o si por el contrario los delitos informáticos resultan un mero medio por el cual se desarrollan las figuras delictivas más tradicionales de nuestro ordenamiento a través de las redes informáticas, aprovechando los progresos en el campo de las TIC y la facilidades del anonimato para cometerlos.

Además, analizaremos las características esenciales comunes a estos tipos delictivos para complementarlas con un análisis jurisprudencial cuya función en este proyecto es servir de antesala para denotar cuestiones o características esenciales de los tipos delictivos más habituales en la práctica diaria, los bienes jurídicos afectados, así como circunstancias relevantes para su resolución.

Para concluir, analizaremos cuestiones sobre la competencia de los tribunales nacionales en el enjuiciamiento de estos tipos delictivos, concretamente un estudio de las teorías doctrinales más relevantes para determinar la competencia atendiendo a la idiosincrasia de los delitos informáticos, así como un análisis sobre la normativa, convenios y doctrina sobre la problemática para enjuiciar estos hechos en supuestos en los que la acción y resultado se dan en diferentes países.

## 2. Los delitos informáticos en el C.P

### 2.1 El concepto de delito informático

Los delitos informáticos en nuestro ordenamiento jurídico han sido fruto de un constante estudio y mutabilidad en lo relativo a su conceptualización por parte del estudio doctrinal, como consecuencia de la rápida y constante evolución de los medios digitales en la sociedad. En un principio, la propia denominación del "delito informático" ha sido objeto de discusión al considerarse la figura de los ciberdelitos como aquellas conductas criminales más estrechamente relacionadas con las redes telemáticas que los delitos informáticos, figura más ajustada a la comisión de tipos delictivos empleando las tecnologías de la información y la comunicación. [1]Así pues, la postura mayoritaria de la doctrina ha considerado a los delitos informáticos más como una categoría o elemento funcional más que un tipo penal propiamente desarrollado, configurándose éstos como meros delitos tradicionales instrumentalizando el uso de la informática como modus operandi para cometer el tipo delictivo clásico[2].

En esta vertiente, autores españoles como Camacho Losa han señalado con anterioridad, que a falta de una definición satisfactoria de delito informático debería considerarse al mismo como *"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 indirecta a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas"*[3] o González Rus que opta por considerar esta clase delictiva como un conjunto de

[1] Hernández Díaz Leyre (2010) "Derecho penal Informático". *Eguzkilore núm 23*. Págs.228 y ss.

[2] Möhrenschlager, M. (1992). "*Delincuencia informática"*. *Promociones y Publicaciones Universitarias, PPU*

[3] Losa Camacho. (1987) "El Delito informático", *Gráficas Condor S.A* Págs. 25 y ss.

delitos heterogéneos clasificables en dos categorías en función de bien jurídico afectado la intimidad personal y los patrimoniales[4]

Sin embargo, esta postura adolece de no abarcar tanto a los dispositivos informáticos como objeto del delito, sino que no logra abarcar todas las opciones que han ido desarrollándose con el paso del tiempo, por lo que no podemos aceptarla cómo una definición correcta de los mismo.

Actualmente se le ha dado una mayor consideración al conjunto de conductas enmarcadas en el concepto de delito informático, esto debido a que además de proteger bienes jurídicos tradicionales se ha apreciado la necesidad de proteger bienes jurídicos eminentemente informáticos como puede ser la información o los datos informáticos en sí mismos[5], junto a esta noción es importante complementarla con las diferentes modalidades en las que se puede manifestar y que serán objeto de estudio más adelante en lo relativo a la clasificación de los mismos.

## 2.2 Características comunes de los delitos informáticos

Si bien la definición conceptual de los delitos informáticos ha sido problemática para la doctrina penal, se ha llegado a un claro consenso en las características comunes tradicionales de los delitos informáticos que han perdurado hasta la actualidad, siendo estas características comunes:

### 2.2.A) **La permanencia del hecho**

Resulta la característica principal de este tipo delictivo, pues habida cuenta de la estructura rígida que supone el procesamiento de datos informáticos de encontrarse una vulnerabilidad, nada impide al autor del hecho aprovecharse constantemente de ella.

---

[4] González Rus, "Precisiones conceptuales y político-criminales sobre la intervención penal en Internet", *Cuadernos Penales José María* Lindón (2007) pág. 14 y ss.

[5] Enrique Rovira del Canto. (2002). "Delincuencia Informática y fraudes informáticos". Granada, *Editorial Comares*.

Sobre este punto Alastuey Dobon[6] indica el efecto continuado propio de este tipo de delincuencia que propicia que se dé un alto porcentaje de delitos continuados en la sanción de estos tipos delictivos, sin embargo no debemos pasar por alto que dadas las opciones que ofrece la informática y la automatización de acciones mediante comandos de código, se pueda dar un automatismo del hecho delictivo, por el cual mediante la injerencia de "*Spyware o Troyanos*" el sistema informático infectado sea vulnerado automáticamente con una única comisión en lugar de múltiples comisiones en el tiempo. Esto nos lleva a la conclusión lógica de diferenciar estos tipos delictivos en modalidades de comisión instantánea de efectos permanentes.

### 2.2.B) Extensa y elevada lesividad

Es gracias a la característica de la permanencia y a la constante evolución de los medios informáticos que ha llevado a un constante aumento de los delitos informáticos, si bien sobre todo en su vertiente económica-patrimonial[7], como recoge el estudio sobre la ciberdelincuencia en España en el año 2019 se reportaron 218302 hechos delictivos un 35.8% más de incidencia que el año pasado, de estos tipos en nuestro país, correspondiendo a su vertiente económica patrimonial un 88.1% de los mismos.

En este aspecto autores nacionales como Rovira del canto[8] consideran que supone un riesgo de afectación grave de los sistemas informáticos y la seguridad y fiabilidad de la información de graduar esta clase de delitos en función del perjuicio económico, pues de lo contrario se propiciaría una situación idílica para el surgimiento de delincuencia económica informática propia de delitos bagatela,

---

[6] Alastuey Dobon M.ª C. "Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial". Zaragoza (1994)

[7] Estudio sobre la cibercriminalidad en España (2019) http://www.interior.gob.es/documents/10180/9814700/Estudio+sobre+la+Cibercriminalidad+en+Espa%C3%B1a+2019.pdf/24bd3afb-5a8e-4767-9126-c6c3c256982b fecha de última revisión 20/11/2021

[8] Enrique Rovira del Canto. (2002). "Delincuencia Informática y fraudes informáticos". Granada, *Editorial Comares.*

es decir, de escasa cuantía pero afectando gracias a las posibilidades del medio informático a una multiplicidad de víctimas.

### 2.2.C) Dificultades de averiguación y comprobación

Consecuencia del objeto del delito informático, esto es, la información y los datos informáticos se da pues la falta de capacidad para visualizar los datos directamente almacenados en los dispositivos sino a través de la interpretación que hace dicho dispositivo y su configuración gráfica que podemos apreciar a través de la pantalla hacen que sea dificultoso o imposible discernir una manipulación o alteración de los datos por el usuario medio, siendo además posible borrar las huellas de cualquier intrusión en el sistema operativo tras cometer la acción delictiva lo cual al sumar el anonimato de la autoría genera una severa complicaciones a la hora de investigar o sancionar estos hechos, lo que en consecuencia nos deriva a la siguiente característica

### 2.2.D) Alto volumen de "cifra negra" o no reportaje

Un alto volumen de cifra negra de casos, que quedan sin investigar o ser sancionados debido a factores como pueden ser la mencionada dificultad de averiguación o comprobación, el desconocimiento de la víctima de la comisión de los hechos o mismamente la no denuncia de los mismos autores como Alaustey Dobon, Camacho Losa o Jay J. Becker inciden respectivamente, sobre cómo la víctima desconoce la comisión de estos hechos, así como que su descubrimiento suele ser de forma accidental o como sólo se ponía en conocimiento de las autoridades un 14%[9] del total de todos los delitos informáticos. Este alto volumen de casos es agravado tanto por la posibilidad de la transfrontericidad de la comisión de los hechos, o la indicada posibilidad de distanciamiento temporal en

[9] Becker J: "The investigation of Computer Crime" (1980) https://www.ojp.gov/pdffiles1/Digitization/51999NCJRS.pdf fecha de última revisión 20/11/2021 Págs. 17 y ss

la comisión de los hechos quedando un vacío sancionador al no darse tipos penales abstractos sino de resultado en la tipificación de estos hechos ilícitos.

## 3. Estudio jurisprudencial de los delitos informáticos en el ordenamiento nacional

A fin de analizar la figura de los delitos informáticos en nuestro ordenamiento jurídico, es precioso un enfoque de estudio desde la perspectiva práctica de la jurisprudencia nacional. Por ello se va a desarrollar en el siguiente punto un análisis de los casos seleccionados y que a su vez sirven de referencia para el estudio en los siguientes puntos, relativos a la tipicidad y competencia. Las siguientes sentencias elegidas se estudiarán en función a los bienes jurídicos afectados a la par que en orden cronológico.

### 3.1 Sentencia 18/2008 de la Audiencia Provincial de Pontevedra

En el presente proceso, R. mayor de edad y sin antecedentes penales previos, a fin de menoscabar el patrimonio ajeno, realizó diversos ataques informáticos sobre el ordenador de la empresa de arte de la que fuera trabajador, dicho ataque informático ocasiono la pérdida de los datos de contabilidad de la citada empresa, así como el bloqueo del sistema operativo y la inutilización de los programas del mencionado ordenador.

Por estos hechos fue condenado a un delito continuado de daños a la pena privativa de libertad de veinte meses de prisión, así como pena de multa de dieciséis meses, dicha condena fue confirmada en el recurso de apelación instado por la defensa del acusado al no poder probarse que el ordenador empleado por el acusado, don R., fuera una herramienta empleada por un tercero para perjudicar a don R.

### 3.2 Sentencia 17/2015 de la Audiencia nacional

En el presente procedimiento se enjuicia a una comunidad de acusados como responsables de crear, orquestar y distribuir una “botnet”, esto es, una red de sistemas que se conecta a otros ordenadores a efectos de infectarlos mediante un virus informático para que éstos ejecuten las órdenes que se le indique desde el sistema central de control de la

botnet, permitiéndoles así poder alquilar a terceros estos ordenadores infectados para poder realizar ciberataques.

Así pues, en un periodo de tres años pudieron infectar aproximadamente 24000 sistemas informáticos, causando aproximadamente 3 millones de euros en concepto de daños. Los acusados fueron condenados como culpables de un delito continuado de daños a la pena de un año de prisión con inhabilitación especial para el ejercicio del derecho de sufragio pasivo, así como a pena de multa de doce meses a razón de tres euros de cuota diaria (1080 euros).

### 3.3 Sentencia 14/2016 de la Audiencia Nacional

En este procedimiento se da pie al enjuiciamiento de una pluralidad de acusados como responsables de un delito de continuado de estafa en concurso medial con un delito de daños informáticos, falsedad en documento mercantil, pertenencia a organización criminal, así como contra la intimidad. En este procedimiento fue probado que los diferentes acusados crearon y distribuyeron un software "ransomware" el cual bloqueaba el terminal informático infectado dicho software impedía todo acceso a los datos del terminal, manipulándolo para que apareciera en pantalla un mensaje indicando los métodos para pagar por recuperar el terminal informático en cuestión, haciéndose pasar en este caso por la policía española.

Una vez obtenido el dinero de las víctimas las cuales pagaban bajo la concepción de que se trataba de una multa, procedían a extraer la información bancaria de la cuenta empleada para el pago de dicha "multa" y con ello se solicitaba la emisión de tarjetas bancarias que eran enviadas a países de Europa del este para su uso.

### 3.4 Sentencia 39/2016 del juzgado de lo penal núm. 3 de Gijón

En el presente procedimiento el juzgado se pronuncia sobre la imputación de los tres acusados de pertenencia a organización criminal y delito continuado de daños al supuestamente ser los cabecillas de la red Anonymous en España y que con ocasión de las elecciones locales y autonómicas del año 2011 y a fin de entorpecer el proceso electoral llevaran a cabo ataques de denegación de servicio al entorno informático de la junta electoral, el congreso de los diputados y las webs del sindicato UGT. Los acusados

llevaron a cabo supuestos ataques a los elementos lógicos de los dominios web anteriormente mencionados, sin autorización de los afectados y causando supuestamente daños "graves", el problema para el tribunal radica en que el tipo penal que recoge esta figura delictiva no llega a determinar criterios para objetivar dicha gravedad del daño, en este procedimiento se absolvió a los acusados dado que los daños ocasionados fueron a ojos del tribunal "*se produjo una interrupción intermitente de la página que quedó fuera de servicio en intervalos de minutos y el problema quedó resuelto en una hora, que el correo siguió funcionando y que los perjuicios derivados de los hechos inicialmente estimados en setecientos euros no eran tales porque el trabajo lo realizó un empleado en nómina al que no se le abonó cantidad alguna por dicho servicios*."

### 3.5 Sentencia 326/2019 del Tribunal Supremo

En el presente proceso, el alto tribunal resuelve sobre los diferentes recursos casacionales alegados por las partes sobre un procedimiento de fraude informático sobre "Bitcoins" donde M. pactó con diferentes personas que se le entregaría una cantidad concreta de Bitcoins con el fin de que invirtiera con ellos y llevarse una comisión de las ganancias. Si bien fue condenado como reo de un delito continuado de estafa, lo verdaderamente importante de esta sentencia yace en el análisis del alto tribunal sobre la naturaleza del Bitcoin como activo patrimonial inmaterial, lo cual a efectos de responsabilidad patrimonial sugiere el propio tribunal que " las víctimas de la estafa no fueron despojados de bitcoins que deban serles retornados, sino que el acto de disposición patrimonial que debe resarcirse se materializó sobre el dinero en euros que, por el engaño inherente a la estafa, entregaron al acusado para invertir en activos de este tipo. Por otro lado, tampoco el denominado bitcoin es algo susceptible de retorno, puesto que no se trata de un objeto material, ni tiene la consideración legal de dinero"

### 3.6 Sentencia 42/2006 del Juzgado de lo Penal de Badajoz

En este procedimiento se condenó a C. mayor de edad y sin antecedentes penales como culpable de un delito de revelación de secretos del artículo 197 del C.P tras llevar a cabo una intrusión en la red interna de administración del sistema de juego de una

empresa obtiene acceso al código binario de dicho sistema, así como a los correos electrónicos de los administradores de la empresa y amenazó con su difusión si no se le reactivaban su cuenta en dicho juego. El tribunal condenó a C. como responsable de revelación de secretos por intrusión informática a la pena privativa de libertad de 1 año de prisión.

### 3.7 Sentencia 201/2018 de la Audiencia Provincial de Lleida

En el presente procedimiento se absolvió a la acusada G. Mayor de edad y sin antecedentes penales de los delitos de descubrimiento y revelación de secretos, así como subsidiariamente de daños informáticos por el que fue condenada en primera instancia, tras haber modificado la contraseña del correo electrónico de la asociación en la que colaboraba como voluntaria y eliminado en torno a 3000 correos de dicha cuenta, sin embargo tras analizarse la gravedad de los hechos y habida cuenta de la ausencia de trascendencia penal, de los hechos objeto de enjuiciamiento, se dictó una sentencia no condenatoria.

### 3.8 Sentencia 267/2020 del Juzgado de lo Penal, Valencia de 24 de septiembre de 2020

En este proceso se enjuicia y se condena a los acusados S. y JC. Como responsables respectivamente de sendos delitos continuados de falsedad documental en concurso medial de un delito continuado de descubrimiento y revelación de secretos. Los acusados emplearon una herramienta informática "Keylogger" para obtener las contraseñas de sus profesores a fin de obtener acceso a la plataforma e intranet universitaria para alterar las calificaciones obtenidas en diversas asignaturas y prácticas.

Esta herramienta permitió a los acusados grabar las pulsaciones ejercidas sobre el teclado que empleaban los profesores para adquirir de forma dolosa y sin riesgo todos los datos que fueran insertados en ese teclado sin consentimiento o conocimiento de las víctimas.

### 3.9 Sentencia 70/2020 del Tribunal Supremo

En el presente proceso se da la culminación del iter procesal por el que fuera juzgado C., mayor de edad y sin antecedentes penales, al delito de revelación de secretos no haber lugar al recurso de casación de C. el cual es imputado un delito de revelación de secretos al reenviar fotografías en las que la víctima aparece desnuda y fueron transmitidas por esta a C. con pleno consentimiento suyo, no así con consentimiento para ser reenviadas, la sentencia se pronuncia sobre el recurso de casación interpuesto por la defensa al considerar la condena no ajustada a derecho al condenarle por un delito de revelación de secretos en lugar de uno de sexting, sin embargo, el alto tribunal tras analizar las fotografías y apreciar la ausencia de connotación sexual más allá del simple desnudo así como la única remisión de las fotos a un tercero, resuelve el tribunal que no se ha dado lugar a un daño a la intimidad de la víctima.

### 3.10 Sentencia 22/2021 (2959/2021) de la Audiencia Nacional

En el presente procedimiento se resuelve sobre las actuaciones de los acusados S y Z por dirigir una organización criminal dedicada a la extracción fraudulenta de dinero de entidades bancarias de diferentes países, empleando sistemas de malware que introducían en los terminales informáticos de los trabajadores de los bancos afectados, a través de engaño burdo vía correos electrónicos, haciéndose pasar por organizaciones colaboradoras de la entidad bancaria y engañando a los trabajadores.

De esta manera y empleando el malware mencionado previamente, se emitía la orden a cajeros automáticos para que en determinada hora dispensaran dinero que era posteriormente recogido por miembros del grupo criminal, logrando obtener así un botín de en torno a los cuatro millones de euros. Condenándose a los acusados como responsables de delitos de blanqueo de capital, pertenencia a banda criminal, falsedad en documento público y un delito continuado de estafa informática.

## 3. Cuestiones que considerar sobre la tipicidad de los delitos informáticos

Habida cuenta del estudio jurisprudencial previo, podemos clasificar a los delitos informáticos más habituales en el ordenamiento jurídico español en dos categorías en base al bien jurídico afectado, delitos informáticos económico-patrimoniales y delitos informáticos intrusivos.

### 4.1 Sobre los delitos cibereconómico-patrimoniales

En atención a los delitos informáticos económico-patrimoniales, son el tipo delictivo mayoritario en la realidad jurídica de nuestro ordenamiento[10], y es que todos estos tipos delictivos (Estafa, defraudación, blanqueo de capital, hurto de tiempo, daños informáticos…) tienen una serie de características idóneas para que el sujeto activo acometa la actividad ilegal con relativa impunidad, acorde a la pericia o conocimientos técnicos del sujeto pasivo, ya sea con ánimo de vandalizar los sistemas o terminales informáticos o si mediara una intencionalidad de obtener ganancias a costa de un tercero, procederemos a su análisis a continuación.

### 4.1.A Defraudaciones y estafa informática

Por ejemplo, en lo relativo a las estafas informáticas las sentencias SAN 22/2021 y SAN 14/2016 nos permiten apreciar como el sujeto activo busca conseguir la obtención de un lucro ya fuere empleando ardides psicológicos que pretendan conseguir del sujeto pasivo una reacción puramente emocional para la consecución de sus fines delictivos, o ardides puramente lógico-informáticos que permitan, con la desafortunada ayuda del sujeto pasivo, dar pie a la transferencia de activos económicos.

Sírvase de ejemplo la sentencia SAN 14/2016 donde los sujetos activos buscaban manipular a sus víctimas haciéndose pasar por la autoridad, empleando el engaño y el temor a sanciones económicas o la SAN 22/2021 donde tras aplicando la modalidad de "Phishing" a los empleados de diversas sucursales bancarias y usando comandos lógicos-informáticos a la par que programas de malware se pudo acceder a las cuentas afectadas debido al engaño sufrido por parte de los empleados.

Otra modalidad que caracteriza a la estafa informática es la posibilidad de la comisión de la misma mediante las técnicas de "Pharming" que permiten al sujeto activo manipular el DNS (Siendo éste, el servidor de números de dominio que permite al terminal dirigir las búsquedas del usuario a una página web concreta) pudiendo en este caso el sujeto activo alterarlo para redirigir al sujeto pasivo a una web falsa creada por el activo de cara a hacerse con las credenciales de la víctima.

En definitiva, todas estas variables de la estafa informática vienen a romper con la idea clásica del concepto del tipo delictivo clásico pues como indica la STS de 30 de

[10] https://oedi.es/estadisticas/ (fecha de última revisión 08/03/2022)

junio de 2009 "*sólo puede ser engañada una persona que, a su vez, pueda incurrir en error. Por lo tanto, ni las máquinas pueden ser engañadas, ni el cajero automático ha incurrido en error, puesto que ha funcionado tal como estaba programado que lo hiciera, es decir, entregando el dinero al que introdujera la tarjeta y marcara el número clave. De esa forma, el tipo aplicado requiere valerse "de alguna manipulación informática o artificio semejante" para conseguir una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero*".

Sobre las defraudaciones informáticas, reguladas en los artículo 255 y 256 del código penal, vienen a ser una modalidad de estafa por la cual el sujeto activo se viene a beneficiar de un servicio en perjuicio de la víctima que lo costea, un ejemplo típico pudiere ser un vecino poco ducho en conocimientos informáticos expone su internet vía wi-fi abierta al público, sin contraseña alguna y un tercero se aprovecha de esto obteniendo pleno acceso a internet de forma gratuita, cometiendo así un ejemplo de defraudación de telecomunicaciones recogido en el mencionado previamente artículo 255.

Sirva de ejemplo la SAP 567/2012 de la Audiencia provincial de Cantabria, la cual viene a denotar las diferencias entre los diferentes tipos defraudatorios en las telecomunicaciones; En ella un trabajador al cual se le otorga un teléfono móvil para uso corporativo, el cual conserva después de habérsele dado de baja laboral y con el que factura a coste de la empresa una deuda por valor de 1600 euros, condenándose a el empleado como autor de un delito de apropiación indebida en concurso real con una defraudación por uso indebido del terminal telefónico (256 C.P)

Siendo pues determinante para tipificar correctamente la defraudación, apreciar si el autor de los hechos se ha valido de medios clandestinos u otros mecanismos para realizar la defraudación o si por el contrario ha empleado los terminales sin consentimiento del propietario.

**4.1.B Hurto de tiempo y daños informáticos**

Por otro lado, en lo relativo al llamado "hurto de tiempo" resulta especialmente interesante pues del análisis de la acción típica del mismo podemos apreciar una amplia regulación de la figura delictiva que va a dar pie a consecuencias tanto para el derecho laboral como para el derecho penal; Recogido en el artículo 256 del código penal, se desarrolla indicando *"El que hiciere uso de cualquier equipo terminal de*

*telecomunicación, sin consentimiento de su titular, y causando a éste un perjuicio económico, será castigado con la pena de multa de tres a doce meses"*. Luego el hurto de tiempo no estaría limitado únicamente a supuestos de hacking vulnerando la seguridad del dispositivo, sino el empleo de terminales de trabajo de forma gravosa y diferente al fin para el que les fue autorizado el uso.

En este sentido podemos tomar de ejemplo, mas si bien tiene una naturaleza más laboral, la sentencia del Tribunal Europeo de Derechos Humanos Barbalescu contra Rumanía en la que se desarrolla la potestad del empleador de controlar los dispositivos otorgados para el desarrollo del trabajo del empleado si bien se reconoce como abusivo del derecho fundamental al secreto de las comunicaciones y al respeto de la vida privada del empleado, el control en tiempo real de su correspondencia.

En lo relativo a los delitos de daño informático tal y como hemos apreciado en la SAP 18/2018 la conducta tipificada en el artículo 264 del C.P pena a aquel que daña, borra, deteriora, altera, suprime o impide el acceso a datos, programas o documentos electrónicos sin autorización del titular, sin embargo sigue el principio de Ultima Ratio del derecho penal y no se sanciona únicamente la mera molestia sino a aquel que daña de manera grave, esta diferencia viene a ser especialmente clarificadora y definitoria entre las conductas de "cracking" y "hacking" que tal como hemos analizado en la sentencia 42/2006 caracterizará el "animus damnandi" que el hecho culposo sea propio de una conducta de cracking la cual es un delito de daños informáticos, por ende económico-patrimonial, o una conducta de hacking la cual sería un delito de naturaleza ciberintrusiva.

En esta clase de delitos, podemos apreciar una problemática habitual en el día a día de la práctica jurídica y es que el contrario el legislador no ha desarrollado baremos por los que cuantificar o graduar la gravedad del hecho culposo, teniendo como requisitos para la gravedad de los hechos que se dé un resultado que afecte al patrimonio de la víctima, por lo que esto resulta una tarea especialmente ardua a la hora de objetivar la gravedad de los actos del sujeto pasivo y escasamente compaginable con el principio de seguridad jurídica, quedando pues en manos del juzgador determinar la severidad de las acciones de vandalismo informático del autor.

### 4.2 Delitos Ciberintrusivos

Sobre los delitos ciberintrusivos la doctrina plantea como las nuevas tecnologías han contribuido al surgimiento de una nueva esfera de intimidad para las personas, autores como FERNANDEZ ESTEBAN desarrollan esta idea "[11]*en tanto que la intimidad protege la esfera en que se desarrollan las facetas singularmente reservadas a la vida de la persona —el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo—, la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo, que éste tiene derecho a mantener reservada».*"

Así pues, se da una conexión entre el derecho a la privacidad del individuo, con el "habeas data" esto es en el contexto del derecho y la informática, la denominada libertad informática o derecho a controlar el uso de los datos de naturaleza sensible del individuo (aquellos relativos a su credo, ideología, esfera sexual, vida familiar, salud…) que pueden recogerse y ser tratados por terceros siempre que medie autorización del individuo. Ello hace que podamos clasificar los delitos ciberintrusivos más relevantes en aquellos contra la intimidad, confidencialidad e integridad de datos o sistemas informáticos, así como aquellos contra el habeas data

### 4.2.A) Intrusismo e interceptación de las comunicaciones

En lo que respecta a la concepción más pura y conocida del intrusismo informático, debemos indicar que la estructura tradicional del "hacking" no requiere para su consumación la vulneración efectiva de la intimidad, sino que se dé la plena intromisión e interceptación de las telecomunicaciones (alterando el DNS del rúter o accediendo mediante un troyano "backdoor" al terminal, por ejemplo) mediando ese ánimo de atentar contra la intimidad del agraviado. Se desarrolla en este sentido la doctrina del Alto Tribunal, en sus Sentencias de 30 de abril de 2007 y de 20 de junio de 2003.

La configuración del tipo delictivo del hacking no se configura únicamente para la intrusión de terminales informáticos y es que el legislador ha considerado como la interceptación de cualquier clase de comunicación como propias de este tipo delictivo,

[11] Fernández Esteban, M.L : "Nuevas tecnologías, Internet y derechos fundamentales", Madrid (1998)

incluyendo así la interceptación de mensajes SMS, WhatsApp o medios de comunicación análogos.

A diferencia de cómo hemos visto previamente, el hacking no requiere de causar daños o inutilizar el sistema sino que se persigue castigar el hecho de sortear las barreras de seguridad informática sin mediar consentimiento expreso del sujeto pasivo, requisito de especial relevancia puesto que las prácticas de hacking ético a fin de exponer y solucionar fallos de seguridad son un elemento esencial en la constante evolución y desarrollo de los sistemas de seguridad informáticos, ello acorde al cumplimiento de la Directiva 40/2013 relativa a los ataques contra los sistemas de información.

Merece una mención especial el tipo delictivo del Sexting introducido en la reforma del año 2015 el cual se estructura como la revelación o difusión a terceros de material audiovisual que fue obtenido en el seno de un contexto íntimo y privado, sin consentimiento expreso para difundirlo. Tal y como apreciamos en la STS 70/2020 el estudio de estos hechos delictivos suponen una complejidad que no radica tanto en el aspecto informático de la comisión de los hechos, sino que media en el estudio del consentimiento, la privacidad y la naturaleza de los archivos compartidos, este tipo delictivo no tiene una naturaleza plenamente informática pero dada su relevancia en la sociedad actualmente y su integración en el artículo 197 del Código penal resulta necesario un breve comentario y análisis.

### 4.2.B) Atentados contra el Habeas Data

.

Recogido en el artículo 197.2 del C.P se vienen a sancionar dos modalidades típicas que atentan contra la libertad informática, esto es las acciones de apoderamiento, uso o alteración de datos confidenciales de carácter personalísimo que se encuentren registrados en terminales o soportes electrónico-informáticos, registro público o privado o en cualquier otro tipo de archivo, sin autorización del titular de dichos datos. Por otro lado, también se viene a sancionar a aquel que acceda por cualquier medio a dichos datos y los altere con ánimo doloso de perjudicar al titular o a un tercero.

En este sentido se ha pronunciado el Alto Tribunal en su sentencia 990/2012 indicando que "[12]*los ficheros o registros han de ser de acceso y utilización limitada a personas concretas y con finalidades específicas, siendo indiferente, su naturaleza: personal, académica o laboral, medica, económica, etc... Se trata, en realidad, de informaciones de carácter personal relacionadas más con la privacidad que con la intimidad. No tienen por qué ser informáticos porque se acoge también a cualquier otro tipo de archivo o registro público o privado."* Por ello podemos entender cómo se configura una nueva capa al derecho a la intimidad configurado en el artículo 18 de la Constitución gracias a los avances informáticos.

Resulta además de especial mención como tras la reforma del año 2015, el legislador desarrolla la responsabilidad penal tanto del diseñador como del distribuidor o facilitador de programas informáticos desarrollados con el fin de vulnerar la integridad del sistema informático y comprometer así la intimidad de la víctima, pudiendo ser sujeto activo de este tipo inclusive las personas jurídicas pues si bien si bien en este caso se estaría castigando el acto preparatorio en sí en lugar de la comisión del hecho, debemos considerar cómo media un ánimo de enriquecimiento a la par como facilita a aquellos usuarios "Skiddies" sin conocimientos técnicos de hacking con herramientas para la consecución de sus metas delictivas.

Pero volviendo a la figura del Habeas Data en sí, autores como Barrio Andrés consideran que esta figura surge como consecuencia de la evolución del derecho a la privacidad, que deja de configurarse *"como un derecho negativo de rechazo a las intromisiones para pasar a contemplarse como un derecho positivo, de afirmación de la propia libertad y de limitación sobre el poder informático"*[13]

## 5. Cuestiones relativas a la competencia de los jueces y tribunales españoles en el enjuiciamiento y persecución de los delitos informáticos

[12] STS 990/2012 en su fundamento de derecho primero, así como STS 1328/2009 en su fundamento de derecho sexto

[13] Barrio Andrés M. Ciberdelitos: Amenazas criminales del ciberespacio *editorial Reus* (2017) Págs. 74 y ss.

### 5.1 De las teorías doctrinales para determinar la competencia de los tribunales nacionales

Del estudio previo ha quedado especialmente remarcado que una de las mayores dificultades que se le presenta al ordenamiento jurídico español a la hora de enjuiciar los delitos informáticos, es la transfrontericidad en la comisión de los hechos delictivos, es en los artículos 14 y 15 de la Ley de Enjuiciamiento Criminal en los que se define como fuero principal el lugar de la comisión de los hechos a la par que se complementa con fueros subsidiarios como el del lugar de obtención de pruebas o el lugar de aprehensión del investigado.

En aquellos casos que no se pudiere determinar con exactitud que fuero resulta competente para el enjuiciamiento del reo, disponemos de las diferentes teorías desarrolladas por la doctrina estas son la teoría de la actividad, del resultado y de la ubicuidad.

Sirva de ejemplo el ATS 20590 / 2008, en dicho auto, el Alto Tribunal resuelve una cuestión de competencia planteada por el Juzgado de Instrucción nº4 de Murcia sobre un caso el cual se emplearon imágenes de una menor, residente en Murcia, obtenidas vía webcam por parte del supuesto autor, residente en Guadalajara, en anuncios de naturaleza pornográficos para promocionar una web de dicho contenido.

El Alto Tribunal considera que, dado que la acción típica y los resultados se desarrollan en diferentes regiones, lo adecuado resulta aplicar el criterio de la ubicuidad citando doctrina previa (ATS 1317/2006, ATS 20117/2006…) así como lo recogido en el Pleno de la Sala Segunda del Tribunal Supremo de tres de marzo de 2005 que indica *"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"*.

Sin embargo, la teoría de la actividad es empleada si se dan circunstancias determinadas, por ejemplo en el ATS de 21 de marzo de 2014 se indica "*la determinación de lugar de comisión del delito en el caso de difusión y tenencia de material pornográfico no se hará con base en la teoría de la ubicuidad o la del resultado sino con base en la teoría de la actividad, y ello porque en este tipo de delitos existe gran dificultad para determinar con precisión el lugar de difusión del contenido pornográfico […] en los delitos cometidos a través de internet serán competentes los Juzgados del*

*lugar en el que se hayan introducido en la red los contenidos delictivos".*

Si bien es una solución más residual y limitada a aquellos casos donde se dé plena certeza del lugar donde ha sido difundida la pornografía o información adquirida vulnerando sistemas informáticos, considero que esta solución adolece frente a la constante evolución de las tecnologías de la comunicación, pues con la ayuda de múltiples VPN así como otros programas u ardides lógico-informáticos, es relativamente sencillo inducir a error en la determinación del lugar donde ha ocurrido el hecho delictivo, al poder manipular la dirección IP denotando un lugar diferente a la comisión de los hechos u ocultando los servidores informáticos. Sirva de ejemplo los hechos recogidos en la STS 987/2012 de 3 de diciembre de 2012[14] en la cual un tercero sin identificar accedió al ordenador del acusado, el cual no ostentaba conocimientos de informática avanzados para la comisión de los hechos imputados, para llevar a cabo un hecho típico de estafa y garantizar su impunidad al quedar registrada la IP o identificación del terminal del acusado.

Por otro lado, en cuanto a la teoría del resultado, en lo relativo a los delitos informáticos, su fundamento sería meramente residual, con una función más bien de facilitarse al sujeto pasivo, personarse en el proceso más sin embargo esta idea ya resulta asimilada dentro de la teoría de la ubicuidad por lo que considero que no procede profundizar más en su análisis.

### 5.2 De la normas, convenios y tratados internacionales

Sobre las normas, convenios y tratados en lo relativo a la competencia, debemos indicar que debido a que como hemos visto anteriormente, resulta especialmente problemática la persecución de las conductas delictivas informáticas cuyo iter ejecutorio se desarrolle a lo largo de diferentes países, el legislador ha considerado como necesario configurar la normativa penal en base a la legislación nacional, así como mediante un entorno de colaboración con los diferentes estados mediante convenios internacionales.

Resulta especialmente relevante el convenio sobre la ciberdelincuencia de 23 de noviembre de 2001 de Budapest, en él se recogen un numerus clausus de delitos informáticos, tanto económico-patrimoniales como intrusivos, que los estados parte

[14] STS 987/2012 en su fundamento de derecho cuarto

deberán desarrollar a nivel nacional, así como el deber de desarrollar su legislación procesal para la obtención, custodia y traslado de pruebas en los procedimientos informáticos.

Pero en materia de competencia el tratado en sus artículos 22 y siguientes desarrolla como será de aplicación el principio de territorialidad a la hora de la persecución de los delitos informáticos pero no desarrolla mecanismos para determinar la competencia de darse un conflicto entre dos estados firmantes, limitándose a crear una red de seguridad y consulta bajo principios de cooperación, asistencia y extradición y dejando la resolución de estas cuestiones competenciales al libre designio de los estados firmantes.

En cuanto a la competencia de los tribunales españoles, resulta especialmente complejo sobreponer el concepto tradicional de "auctoritas del Ius puniendi" estatal para la persecución de los hechos criminales cometido en su territorio y/o por sus ciudadanos en un medio que es claramente plurinacional, el desarrollo exponencial del Internet ha ocasionado la puesta en manifiesto de la ausencia de una entidad reguladora con potestad de perseguir los delitos más graves cometidos de forma cibernética.

Sin embargo, autores como Flores Prada consideran que "*Junto a los problemas de sumisión a la competencia, de los que dan buena cuenta las dificultades para conseguir las ratificaciones cualitativamente relevantes del Tribunal Penal Internacional, deben situarse problemas técnicos derivados de la definición de su competencia, del volumen de trabajo que soportaría, de su composición, y de la eficacia de una jurisdicción que nunca sería plenamente universal.*[15]*"* y es que siguiendo con la teoría de Flores Prada, la existencia de los denominados como "Paraísos ciberdelictuales" o aquellos países donde la legislación penal sobre los delitos informáticos es más laxa o nula, genera no solo beneficios para dichos paraísos ciberdelictuales sino una brecha de vulnerabilidad a la esfera cibernética y por ende a todos los usuarios.

Para concluir, autores doctrinales como Diaz Gómez en cambio, optan por una postura más conciliadora, a la par que optimista y consideran que la vía de la Cooperación internacional resulta la hoja de ruta a seguir en el futuro para la persecución de los delitos

[15] Flores Prada I. (2012) Criminalidad informática. Aspectos sustantivos y Procesales. *Editorial Tirant Lo Blanch.* Pág. 311 y ss.

informáticos *"*[16]*La propensión a la cooperación no es ilusoria: cada vez hay más países interesados en formar parte del convenio, cada vez mayor cantidad de Estados reforman su Código Penal introduciendo las infracciones informáticas, progresivamente desaparecen los «paraísos ciberdelictuales» y en definitiva, sucesivamente más gobiernos se dan cuenta de la verdadera necesidad de actuar en esta materia.*

## 6. Consideraciones finales

Como hemos podido apreciar a lo largo de este estudio, los delitos informáticos resultan un reto tanto para el legislador como para la casuística habitual del jurista, pues al ser tanto un medio en constante evolución como un sistema que requiere de amplios conocimientos técnicos, es especialmente complejo aplicar las normas de persecución de los delitos tradicionales en el mundo informático, puesto que no solo nos enfrentamos al problema del anonimato, la elevada cifra negra de delitos informáticos que no se reportan y por ende no puede haber lugar el inicio del iter procesal para la investigación y persecución de estos hechos delictivos, así como la vulnerabilidad de la brecha digital entre aquellos usuarios más duchos en ciberseguridad respecto de los menos hábiles, sino que además debemos de añadir la posibilidad de cometer esta clase delictiva de manera transfronteriza, se propicia así el caldo de cultivo idóneo para la impunidad de los autores de estas afrentas al ordenamiento jurídico.

Sin embargo, considero que gracias a los convenios internacionales y la creación de cuerpos y fuerzas especializados en ciberseguridad, así como a la exponencial colaboración entre los diferentes estados, se está alcanzando un punto de equilibrio entre la potestad de control y persecución de los hechos delictivos en internet y la naturaleza propiamente anarquista de internet como un medio donde el individuo tiene derecho a poder expresarse libremente pero a pesar de ello, la ausencia de un organismo jurisdiccional supranacional con potestad para conocer y enjuiciar de aquellos hechos delictivos más graves, es decir aquellos con mayor relevancia para la comunidad internacional, genera una inseguridad jurídica al no haber una clara figura a la que los

[16] DÍAZ GÓMEZ, A.: El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest, *REDUR* (2010) https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071/3321 (Fecha de última revisión 08/03/2022) Pág. 34 y ss.

estados puedan someter a control los conflictos o cuestiones competenciales, o la persecución de los paraísos ciberdelictuales.

En mi opinión, resulta especialmente necesario la creación de un tribunal supranacional que medie estas disputas entre estados y esté plenamente enfocada en la persecución de los delitos informáticos más relevantes, pues si bien esta idea parece más bien utópica pues supondría la renuncia de autonomía de los estados que prefieren resolver esta problemática por la vía de la cooperación internacional y derivando la potestad de investigación a fuerzas y cuerpos de seguridad especializados.

Pues un organismo jurisdiccional con personal especializado y constantemente supervisando aquellos hechos más graves supondría no solo una menor carga de trabajo para los órganos jurisdiccionales nacionales, sino un alivio a las tensiones en las relaciones diplomáticas entre países reguladores y aquellos que permiten con su laxitud normativa la existencia de los mencionados paraísos ciberdelictuales que suponen una constante vulnerabilidad para el resto de usuarios y un elemento de seguridad jurídica para el ciudadano al ser este Tribunal una capa más de protección sobre la cual poder ejercer el derecho a la tutela judicial efectiva.

## 7. Tabla de Jurisprudencia

- ROJ: STS 694/2003
- ROJ: SJP 9/2006 - ECLI:ES:JP:2006:9
- ROJ: ATS 20117/2006
- ROJ: STS 358/2007
- ROJ: SAP PO 170/2008 - ECLI:ES:APPO:2008:170
- ROJ: ATS 20590/2008
- ROJ: SAP 567/2012
- ROJ: STS 8258/2012 - ECLI:ES:TS:2012:8258
- ROJ: ATS 2258/2014 - ECLI:ES:TS:2014:2258A
- ROJ: SAN 2034/2015 - ECLI:ES:AN:2015:2034
- ROJ: SJP 39/2016 - ECLI:ES:JP:2016:39
- ROJ: SAN 704/2016 - ECLI:ES:AN:2016:704
- ECLI: CE:ECHR:2017:0905JUD006149608
- ROJ: SAP L 500/2018 - ECLI:ES:APL:2018:500
- ROJ: STS 2109/2019 - ECLI:ES:TS:2019:2109

- ROJ: SJP 36/2020 - ECLI:ES:JP:2020:36
- ROJ: STS 492/2020 - ECLI:ES:TS:2020:492
- ROJ: SAN 4567/2021 - ECLI:ES:AN:2021:4567

## 8. Bibliografía


- Becker J: The investigation of Computer Crime (1980) https://www.ojp.gov/pdffiles1/Digitization/51999NCJRS.pdf fecha de última revisión 20/11/2021
- Losa Camacho. (1987) El Delito informático Gráficas Condor S.A
- Möhrenschlager, M. (1992). *Delincuencia informática*. Promociones y Publicaciones Universitarias, PPU
- Alastuey Dobon M.ª C. Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial. Zaragoza (1994)
- Fernández Esteban María Luisa Nuevas tecnologías, Internet y derechos fundamentales, Madrid (1998)
- Enrique Rovira del Canto. (2002). Delincuencia Informática y fraudes informáticos. Granada: Comares.
- González Rus, Precisiones conceptuales y político-criminales sobre la intervención penal en Internet, Cuadernos Penales José María Lindón (2007)
- DÍAZ GÓMEZ, A.: El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest, REDUR (2010) https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071/3321 (Fecha de última revisión 08/03/2022)
- Hernández Díaz Leyre (2010) Derecho penal Informático. Editorial Aranzadi
- Flores Prada I. (2012) Criminalidad informática. Aspectos sustantivos y Procesales. Editorial Tirant Lo Blanch.
- Barrio Andrés M. Ciberdelitos: Amenazas criminales del ciberespacio editorial Reus (2017)
- Estudio sobre la cibercriminalidad en España (2019) http://www.interior.gob.es/documents/10180/9814700/Estudio+sobre+la+Ciberc

riminalidad+en+Espa%C3%B1a+2019.pdf/24bd3afb-5a8e-4767-9126-c6c3c256982b fecha de última revisión 20/11/2021