Universidad Internacional de La Rioja
Máster en el Ejercicio de la Abogacía

Cibercriminalidad: especial referencia al delito de usurpación y suplantación de identidad

Trabajo fin de máster presentado por: Francisco Javier Sánchez Canet
Titulación: Master profesional en el Ejercicio de la Abogacía.
Área jurídica: Penal. (Dictamen Penal teórico).
Directora: María Sonsoles Vidal Herrero-Vior

Ciudad: Valencia
[25-noviembre de 2016]
Firmado por: Francisco Javier Sánchez Canet

I N D I C E

ABREVIATURAS

Art	Artículo
Art(s)	Artículos
Cit.	Citado
Coord.	Coordinador
CP	Código Penal
CE	Constitución Española
Dir	Director
Ibídem	En el mismo lugar
p.	Página
pp.	Páginas
SAP	Sentencia de la Audiencia Provincial
STS	Sentencia del Tribunal Supremo
TS	Tribunal Supremo
Vol.	Volumen
VV.AA	Varios Autores
ss.	Siguientes
TICs	Tecnologías de Información y Comunicación
TFM	Trabajo Fin de Máster
DoS	Denegación del Servicio

PRESENTACION

Debido a la evolución de Internet y de las nuevas tecnologías, han surgido nuevas formas delictivas a través de sistemas informáticos que han tenido que ser considerados por nuestra legislación.
Así, el presente trabajo versa sobre el análisis de los delitos informáticos en España, así como la actual regulación de nuestro Código Penal resultante de la promulgación de la Ley Orgánica 1/2015, la cual ha incrementado notablemente el listado de esta clase de delitos.
Del mismo modo, debido a un interés personal del autor, se aborda especialmente el delito de suplantación de la identidad, así como los medios informáticos que facilitan en gran medida la realización de esta suplantación.
Desarrollamos la figura del agente encubierto en la fase de instrucción sobre esta clase de delitos, ya que, debido a las características de los sistemas informáticos, se requiere una adaptación de esta figura para garantizar el éxito en sus investigaciones.

ABSTRACT

Due to the evolution of the Internet and new technologies, new criminal forms have emerged through computer systems that have had to be considered by our legislation.
Thus, the present work deals with the analysis of computer crimes in our State, as well as the current regulation of our Criminal Code resulting from the promulgation of Organic Law 1/2015, which has significantly increased the list of these types of crimes.
In the same way, due to our personal interest, it deals especially with the crime of impersonation, as well as the computer means that facilitate the accomplishment of this impersonation.
We developed the figure of the undercover agent in the training phase on this class of crimes, because, due to the characteristics of the computer systems, an adaptation of this figure is required to ensure success in their investigations.
.

Capítulo I: Consideraciones generales sobre la Cibercriminalidad

1.1 Introducción

El avance y desarrollo de nuevas tecnologías, así como el desarrollo social, han llegado a abrir un nuevo marco a la criminalidad por medio de la informática, la cual permite la creación de nuevos delitos. Estas circunstancias han llegado a generar el fenómeno que en la actualidad conocemos como cibercriminalidad, lo que ha requerido una actuación y preocupación desde el punto de vista jurídico-penal.

De esta forma, con la aparición en las últimas décadas del crecimiento del fenómeno informático, se ha planteado la cuestión sobre el tratamiento penal de los hechos lesivos que se cometen a través de este medio digital contra determinados bienes jurídicos, surgiendo así el concepto de delitos informáticos y cibercriminalidad[1].

La comisión de estos delitos informáticos ha manifestado una tendencia creciendo durante los últimos años, tanto en términos nacionales como internacionales, lo cual no es de extrañar debido al crecimiento del uso de las Tecnologías de Información y Comunicación (en adelante TICs)[2]. Del mismo modo, el coste total del cibercrimen a nivel mundial asciende hasta los 113 mil millones de dólares y con un total aproximado de 378 millones de víctimas por año[3].

Así, podemos observar la evolución de los hechos delictivos en los últimos años por medio de la siguiente representación:

Elaboración propia. Datos obtenidos del Ministerio del Interior de España. Estudio sobre la cibercriminalidad en España 2015.

Asimismo, es destacable que, en términos nacionales, la mayoría de esta cibercriminalidad se centra en la comisión de fraudes informáticos, seguido de lejos de los delitos relativos a las amenazas y coacciones. De esta manera, para una mayor representación de la situación podemos atender al siguiente gráfico:

[1] MATA Y MARTÍN R. (2003). *Criminalidad informática: Una introducción al cibercrimen*. Actualidad Penal. Nº. 37. Sección Doctrina. Semana del 6 al 12 de octubre de 2003. Editorial la Ley. p. 4.
[2] Ministerio del Interior. (2015). *Estudio sobre la cibercriminalidad en España 2015.*p.3.
[3] NORTON (by Symantec) (2013) *Reporte Norton 2013. p*.10.

Elaboración propia. Datos obtenidos del Ministerio del Interior de España. Estudio sobre la cibercriminalidad en España 2015.

1.2. Concepto y características

En primer lugar, debemos de destacar que no puede existir un concepto legislativo relativo a los delitos informáticos o a la cibercriminalidad, ya que no hay una tipificación penal concreta sobre este tipo de delito. Sin embargo, nuestro Código Penal establece el concepto de delito informático para referirse a la utilización de la informática o de las tecnologías de la información y de las comunicaciones para la producción de un hecho delictivo.

Por ello, no podemos encontrar un apartado en el Código Penal español en el que haga referencia a los delitos informáticos o a la cibercriminalidad, sino que nuestra legislación trata estos hechos delictivos atendiendo a la utilización de las TICs para la comisión de un delito, ya sea por medio de una acción u omisión a través de las facilidades de estos sistemas[4].

Por lo tanto, debemos entender el delito informático como un acto criminoso relacionado con la tecnología informática, por lo que no constituye una nueva categoría delictiva, sino que los hechos delictivos que se comenten o que facilitan para cometerse por medio de sistemas informáticos, son los mismos que vienen realizándose[5].

[4] DAVARA RODRÍGUEZ M.A. (2016). *Los delitos informáticos.* El consultor de los Ayuntamientos. Nº. 15. Sección Zona Local / Nuevas tecnologías. Editorial Wolters Kluwer. pp. 1825-1830. p. 1826.
[5] REYNA ALFARO L.M. (2002). *La criminalidad informática: cuestiones para una reflexión inicial.* Actualidad Penal. Nº. 21. Sección Doctrina. 2002. Tomo 2. Editorial La Ley. pp. 525- 542. p.534.

Debido que para la comisión de estos tipos delictivos requieren la utilización de medios informáticos o telemáticos para su realización, llegan a presentar una serie de características especiales a diferenciación de la comisión de los delitos tradicionales.

De esta forma, entre las características propias que muestran estas acciones delictivas podemos destacar las siguientes[6]:

a) Rapidez y acercamiento en su comisión: Debido a las características y a las facilidades que otorgan los sistemas informáticos, el sujeto activo puede permitir preparar acciones dolosas en perjuicio de un sujeto tercero en tiempo y espacio distante.
b) Facilidad para encubrir el hecho: A causa de las facilidades descritas anteriormente, se permite generar una serie de condiciones beneficiosas para encubrir el hecho delictivo.
c) Facilidad para destruir las pruebas: Es de gran facilidad la eliminación de todas las pruebas relacionadas con el hecho delictivo realizado, lo que hace difícil detectar la comisión del hecho delictivo.

1.3. Bien jurídico protegido

Para tratar de determinar el bien jurídico protegido de los delitos informáticos, debemos de atender primeramente a la teoría del bien jurídico protegido. En primer lugar, el concepto de la seguridad en el ámbito de la informática y en las telecomunicaciones tienen un valor e interés social innegable, no obstante, esta circunstancia no es suficiente para poder elevar este concepto al nivel de bien jurídico protegido.

Debemos recordar que la doctrina jurisprudencial del Tribunal Constitucional establece como punto de partida para la determinación de un bien jurídico que tal bien tenga su origen en la Constitución; sin embargo, determinar la relación entre la Constitución y el bien jurídico protegido en ocasiones puede llegar a ser difícil.

Así, tratando de realizar una búsqueda entre un bien jurídico relativo a la seguridad en los sistemas de información y en relación a los valores constitucionales, la doctrina considera que se debe de atender en primer lugar al artículo 1 de nuestra Constitución de 1978, el cual establece como valores fundamentales la libertad y la justicia. Del mismo modo en su Título Preliminar se determina que los poderes públicos deben de remover todos "*los obstáculos que impidan o dificulten su plenitud*" y a su vez, en su artículo 10, se determina el libre desarrollo de la persona[7].

Tras esta explicación hay que atender a que el desarrollo de la libre personalidad es un concepto muy genérico, por lo que no es irracional considerar que los sistemas informáticos han pasado a formar parte de la realidad y de la vida común de los ciudadanos, donde un ataque contra dichos sistemas llevará consigo una vulneración contra el desarrollo de la personalidad del individuo.

---

[6] DAVARA RODRÍGUEZ M.A. (2016). *Los delitos informáticos.* El consultor de los Ayuntamientos. Nº. 15. Sección Zona Local / Nuevas tecnologías. Editorial Wolters Kluwer. pp. 1825-1830. p. 1828.

[7] GONZÁLEZ HURTADO J.A. (2014). *Un nuevo bien jurídico protegido en el uso y disfrute de la tecnología: la seguridad en los sistemas de información.* La Ley Penal. Nº. 107. Sección Estudios. Marzo-Abril. p.3.

En este sentido, no parece exagerado pensar que la libertad que establece la Constitución va más allá que una simple libertad de circulación o de establecimiento y que se debe de atender como una autentica facultad de determinación personal en todos los ámbitos que puedan desarrollarse sobre el individuo. Por lo tanto, podemos encontrar un nexo constitucional entre la libertad constitucional y el uso de sistemas informáticos[8].

Por otro lado, también se puede tratar de relacionar la seguridad de los sistemas de información con una protección de carácter constitucional a través de la protección del derecho a comunicar o recibir libremente cualquier información a través de cualquier medio, regulado en el artículo 20.1.d) de nuestra Constitución. Así, tal Derecho debe de atenderse en relación a favor de la realidad y sistemas tecnológicos que nos encontramos en la actualidad, por lo que tiene una gran relevancia la protección de los sistemas informáticos que permiten desarrollar este derecho fundamental[9].

No obstante, a pesar de que se pueda dar cierto nexo causal para la determinación de los sistemas informáticos como un bien jurídico protegido, en la práctica, el sistema informático se relaciona con el hecho delictivo como un medio para la comisión de un delito determinado, por lo tanto, el bien jurídico protegido de los delitos informáticos se vincula con el bien jurídico protegido de este último.

Por ello la doctrina considera que la determinación del bien jurídico protegido en los delitos informáticos es una tarea difícil. En este sentido, se pueden diferenciar dos tipos de teorías doctrinales: por un lado, la más clásica y a la que atiende el legislador actual, mediante el cual consideran que el único bien jurídico protegido de los delitos informáticos son los bienes jurídicos tradicionales, donde la única novedad es la utilización de un sistema informático en algún momento del proceso de la comisión delictiva, por lo que no cabe la determinación de un bien jurídico protegido diferente.

Por otro lado, otra parte de la doctrina, considera que los delitos informáticos deben de proteger bienes individualizables y concretos, por lo que propone la creación de un nuevo bien jurídico protegido de carácter colectivo, entendiendo que en los casos en los que se ataca un sistema informático no solo se produce un daño contra un individuo en concreto, sino que se vulnera un bien relacionado con la libertad y seguridad informática, los cuales deben ser protegidos de forma autónoma[10].

1.4. Breve comentario al Convenio Europeo 185/23 de 23 de noviembre de 2001.

El Convenio Europeo 185/23 de 23 de noviembre de 2001, también conocido como el “Convenio sobre la ciberdelincuencia”, ha requerido de cuatro años para su elaboración, mediante el cual, pretenden responder a los desafíos que llega a plantear la denominada criminalidad informática. De esta forma, este Convenio se

[8] Ibídem.
[9] COTINO HUESTO L. (2007). *Retos jurídicos y carencias normativas de la democracia y la participación electrónicas.* Revista Catalana de Dret Públic. Nº. 35. Pp. 75-120.
[10] GONZÁLEZ HURTADO J.A. (2014). *Un nuevo bien jurídico protegido en el uso y disfrute de la tecnología: la seguridad en los sistemas de información.* La Ley Penal. Nº. 107. Sección Estudios. Marzo-Abril. p.3.

convierte en el primer texto legislativo a nivel global que trata de garantizar la seguridad en Internet y en sus usuarios[11].

Por medio de dicho Convenio, los Estados ratificantes pretenden exponer la necesidad de aplicar de forma prioritaria una política penal común para luchar contra la cibercriminalidad, por medio de la adopción de la legislación adecuada y el fomento de la cooperación internacional, teniendo en cuenta todos los cambios que se han provocado por la globalización, la digitalización y el desarrollo de nuevas tecnologías.

De esta forma, el Convenio sobre la ciberdelincuencia trata de dar de una mayor eficacia a las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos, así como tratar de facilitar la obtención de pruebas digitales en los delitos cometidos[12].

Así, el Convenio distingue entre todos los posibles delitos de carácter informático tres categorías principales[13]:

- Infracciones contra la confidencialidad, la integridad, la disponibilidad de datos y sistemas informáticos.
- Infracciones informáticas vinculadas a los delitos de pornografía).
- Infracciones vinculadas a los delitos contra la propiedad intelectual y cuestiones relacionadas.

Del mismo modo, el Convenio pretende fomentar la cooperación internacional entre los Estados miembros estableciendo nuevas reglas de cooperación internacional, así como nuevos procedimientos para facilitar el desarrollo de investigaciones en el marco virtual, tales como[14]:

- Conservación rápida de datos informáticos almacenados.
- Obligación de comunicación y de informar.
- Registro y recogida de datos informáticos almacenados.
- Recogida en tiempo real de datos informáticos.

Por último, y en relación con todo lo anterior, me parece importante destacar la entrada en vigor el pasado mes de julio -en concreto el día 19- de la Directiva 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la UE, más conocida como Directiva sobre ciberseguridad, y cuyo objetivo es "*formalizar un planteamiento global en la UE que integre requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales".*

---

[11] DAVARA RODRÍGUEZ M.A. (2016). *Los delitos informáticos.* El consultor de los Ayuntamientos. Nº. 15. Sección Zona Local / Nuevas tecnologías. Editorial Wolters Kluwer. pp. 1825-1830. p. 1826.

[12] SÁNCHEZ BRAVO A. (2003). *El convenio del consejo de Europa sobre Cibercrimen: Control versus Libertades públicas.* Diario La Ley. Nº. 5528. Sección Doctrina. Abril de 2002. pp.1851-1866. p. 1855.

[13] DAVARA RODRÍGUEZ M.A. (2016). *Los delitos informáticos.* El consultor de los Ayuntamientos. Nº. 15. Sección Zona Local / Nuevas tecnologías. Editorial Wolters Kluwer. pp. 1825-1830. p. 1828.

[14] SÁNCHEZ BRAVO A. (2003). *El convenio del consejo de Europa sobre Cibercrimen: Control versus Libertades públicas.* Diario La Ley. Nº. 5528. Sección Doctrina. Abril de 2002. pp.1851-1866. p. 1860.

Capitulo II: La regulación de la cibercriminalidad en el Derecho nacional y comparado

2.1. Evolución de los delitos informáticos en el Derecho español

En el caso nacional, la regulación de los delitos informáticos o de la cibercriminalidad ha sido escasa hasta su última modificación del Código Penal de 2015, donde la doctrina ha clasificado estas tipologías delictivas, pretendiendo solventar todas aquellas lagunas de punición que se observaban en el Código Penal anterior. Hasta dicha nueva regulación, la doctrina realizó importantes críticas respecto a la legislación sustantiva y a la Ley de protección de datos principalmente[15].

En este sentido, por lo tanto, podemos entender que el legislador actuó con retraso para la regulación de este tipo de delitos en comparación con el resto de países de su entorno. La justificación de este retraso legislativo puede encontrarse en que los países del entorno se encontraban más desarrollados y tenían capacidad para realizar procesos de modificación legislativa para tratar esta nueva clase de delitos, sin embargo, en el caso nacional, a causa de la transición política vivida en la década de los setenta, hizo que se centraran la regulación en aquellas materias de mayor necesidad, dejando la regulación de estos delitos informáticos como un objetivo secundario[16].

Desde un inicio, el legislador ha optado por regular la cibercriminalidad o los delitos informáticos por medio del mismo Código Penal, rechazando la opción de crear una Ley o regulación especial para ellos. Por lo tanto, como venimos señalando, ni el Código Penal de 1995, ni sus constantes reformas, han creado un Titulo o apartado específico para tratar este tipo de delitos, ni para tratar su tratamiento o sanciones, estableciéndose su regulación en diversos capítulos sin ningún vínculo entre ellos, caracterizándose por una inexistencia de título regulatorio y por una dispersión normativa[17].

En cuanto al desarrollo normativo, cabe destacar que en el Código Penal de 1973 no contemplaba la regulación de los delitos informáticos como la conocemos en la actualidad, ya que solamente trataba esta clase de delitos como un ataque a elementos de carácter informáticos, por lo que, en un principio, parece indicar que la responsabilidad por su comisión recaía por medio de la vía civil a través de la reparación del daño causado.

Cabe destacar en el marco del desarrollo de la cibercriminalidad, que existe una gran cantidad de regulación de otros ámbitos jurídicos relacionada con este tipo de delitos, como puede ser el Real Decreto Legislativo 1/1996 de 12 de abril, por el que

---

[15] GONZÁLEZ RUS J.J. (1999). *Protección penal de sistemas, elementos, datos, documentos y programas informáticos.* Revista electrónica de ciencia penal y criminología. Nº. 1.p.14.

[16] GONZÁLEZ HURTADO J.A. (2013). *Delincuencia Informática: Daños informáticos del artículo 264 del Código Penal y propuesta de reforma.* Tesis doctoral. Universidad Complutense de Madrid. p 81 y ss.

[17] BARRIO ANDRÉS M (2011). *Los delitos cometidos en Internet. Marco comparado, internacional y derecho español tras la reforma penal de 2010.*La Ley Penal. Nº. 86. Sección Legislación aplicada a la práctica. Octubre 2011. Editorial La Ley. p. 4.

se aprueba el texto refundido de la Ley de Propiedad Intelectual, el cual se encuentra activo en la actualidad.

Asimismo, es destacable, en este sentido, el Real Decreto 14/1999, de 17 de septiembre, sobre firma electrónica, regulando las materias que puedan surgir sobre esta. Asimismo, este Real Decreto ha sido igualmente reforzado por la Ley 59/2003, de 19 de diciembre, de firma electrónica, la cual añade novedades con el objetivo de dar seguridad a las comunicaciones por Internet, así como el inicio de la regulación de la firma jurídica y la prestación de los servicios de certificación[18].

En esta misma línea, cabe destacar la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, mediante la cual, a través de la regulación de diversos datos y ficheros (independientemente del soporte en que se encontrara), se pretendía proteger el tratamiento de datos personales, con la finalidad principal de proteger su honor, intimidad y privacidad.

Del mismo modo, dicha Ley ha sido desarrollada a través del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de protección de datos de carácter personal, el cual ha establecido medidas de seguridad para aplicar a los sistemas informáticos[19].

También es destacable la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, mediante el cual traba la regulación de los servicios de la sociedad de información y de la contratación por vía electrónica.

En cuanto al Código Penal observamos una gran cantidad de reformas durante los últimos años, debiendo destacarse aquí que por la última reforma -la efectuada por la Ley Orgánica 1/2015- se añaden una gran cantidad de nuevos tipos delictivos informáticos (los cuales desarrollaremos en el siguiente Capítulo)[20].

Esta última reforma en materia sobre los delitos informáticos, se ha llevado a cabo principalmente para proceder a la transposición de la Directiva Europea 2013/40/UE, de 12 de agosto, relativa a los ataques de los sistemas de información y la interceptación de datos electrónicos cuando no se trata de una comunicación personal[21].

2.2. El Derecho comparado.

Por medio del presente capítulo, pretendemos realizar un breve análisis sobre determinados países que sufren esta clase de delitos informáticos. Se mencionan los

[1818] VALDIVIA CHERNOZIOMOVA M. (2011). *Propuesta de modificaciones al tratamiento legal que reciben las conductas delictivas generadas por la criminalidad en Cuba.* Universidad de Sancti Spiritus.p 42.
[19] Ibídem.
[20] DE URBANO CASTRILLO E. (2011). *Los delitos informáticos tras la reforma del CP de 2010.* Revista Aranzadi Doctrinal. Nº. 9/2011. Parte Estudio. p.4.
[21] Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Preámbulo número XII.I

países europeos en concreto y se hace una especial mención a los EE.UU. por ser pionero en la regulación de este tipo de delitos.

2.2.1. Estados Unidos

Estados Unidos tuvo el reconocimiento de ser el primer país en poseer una regulación de ámbito estatal sobre este tipo de delitos, por medio de la aprobación de la Ley denominada "*Couterfeit Acces Device and Abuse Act"* en 1984, la cual supone un éxito respecto a la regulación penal de abusos informáticos[22].

No obstante, tras su entrada en vigor se consideró que se trataba de una Ley de gran importancia, pero insuficiente, por lo que dicha Ley ha ido sufriendo enmiendas al largo de los años con la finalidad de proteger y endurecer sus penas, ampliándose en relación con los tratados internacionales ratificados y adaptándose continuamente a los cambios sociales.

2.2.2 Alemania

En Alemania se aprobó, en fecha de 15 de mayo de 1986, y se encuentran todavía en vigor pese a las modificaciones que ha recibido para su adaptación social[23].
Las conductas que castiga son: Piratería informática (artículo 202.a); Estafa por medio de un sistema informático, (artículo 263 a); Alteración de datos (artículo 303.a); el Sabotaje informático (artículo 303.b); y la utilización abusiva de cheques o tarjetas de crédito (artículo 266b)[24].

2.2.3. Francia

En el Estado francés en fecha de 5 de enero de 1988 se promulgó la Ley 8819, relativa al fraude informático, la cual prevé penas de dos meses a dos años de prisión y multas de 10.000 hasta 100.000 euros, y castiga las siguientes conductas: el acceso fraudulento a un sistema de elaboración de datos; el sabotaje informático; y la falsificación de documentos informatizados[25].

2.2.4. Austria

La regulación de los delitos informáticos se dio por medio de la reforma del Código Penal del 22 de diciembre de 1987, mediante la cual se establecieron los siguientes delitos[26]: destrucción de datos[27] (artículo 126); y la estafa informática (artículo 148),

[22] GONZÁLEZ HURTADO J.A. (2013). *Delincuencia Informática: Daños informáticos del artículo 264 del Código Penal y propuesta de reforma.* Tesis doctoral. Universidad Complutense de Madrid. p 72 y ss.
[23] VALDIVIA CHERNOZIOMOVA M. (2011). *Propuesta de modificaciones al tratamiento legal que reciben las conductas delictivas generadas por la criminalidad en Cuba.* Universidad de Sancti Spiritus. p. 32.
[24] Ibídem.
[25] ESTRADA GARAVILLA M. (2008). *Delitos informáticos.* Universidad Abierto de México. p. 15.
[26] ESTRADA GARAVILLA M. (2008). *Delitos informáticos.* Universidad Abierto de México. p. 14.

en las que sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero, así como se sanciona a los informáticos profesionales que delinquen.

2.2.5. Holanda

La primera regulación en el Estado holandés se dio el 1 de Marzo del año 1993, por medio de la publicación de la Ley relativa a los delitos informáticos, por medio de la cual castigaba conductas relativas al Hacking y Phreacking, así como otras actividades relacionadas como la ingeniería social y la distribución de virus informáticos[28]. Este último delito está penado hasta 4 años de prisión.

2.2.6. Reino Unido

La principal motivación legislativa surgió en el año 1991 por medio de un caso de hacking, por lo que promulgaron la Ley denominada "*Computer Misuse Act*", por medio de la cual, castigaban la comisión de los delitos informáticos con una pena de hasta cinco años de prisión o multas, independientemente si dicho hecho delictivo se hubiera consumado con éxito o no[29].

[27] Se tiene en consideración tanto los datos personales, como los no personales, independientemente del soporte en que se encuentre.
[28] ESTRADA GARAVILLA M. (2008). *Delitos informáticos.* Universidad Abierto de México. p. 17.
[29] Ibídem.

Capítulo III: Tipos de delitos informáticos

3.1. Introducción

Como hemos señalado anteriormente, las formas de delinquir a través de medios informáticos han ido evolucionando en los últimos años, lo que ha requerido de una respuesta legislativa al respecto. De esta manera la última reforma de nuestro Código Penal, realizada por medio de la ya mencionada Ley Orgánica 1/2015, se añaden una gran cantidad de nuevos delitos a los ya existentes, tratándolos como una simple forma de cometer el hecho delictivo a través de un medio informático.

La doctrina ha tratado de clasificar estos novedosos tipos delictivos en tres apartados diferentes, distinguiendo entre: delitos cibereconómicos, delitos ciberintrusivos y delitos de ciberterrorismo[30].

3.2. Los delitos cibereconómicos

Se trata de aquellos delitos en los que el autor busca un beneficio lucrativo por medio del apoderamiento de dinero, activos o patrimonio ajeno por medio de técnicas informáticas. Son los delitos más cometidos dentro del ámbito de la cibercriminalidad, donde un 65% de los delitos informáticos que se denuncian son de esta clase[31].

3.2.1. La estafa informática. (248.2 CP)

Es el delito informático más denunciado en nuestra sociedad y se encuentra regulado en el artículo 248.2 CP, se considera reos de estafa a los siguientes sujetos: *"a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo. c) Los que, utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero."*

La regulación de este precepto se da como una respuesta al uso de nuevas tecnologías para los actos delictivos y su regulación sirvió para finalizar con el debate sobre si una maquina puede llegar a ser engañada[32]. Se trata, por lo tanto, de la comisión de la estafa tradicional realizándose por medio de elementos informáticos o digitales.

De esta forma, por medio de esta regulación, se permite incluir en la tipicidad de la estafa aquellos supuestos en los que una manipulación informática pueda llegar a

[30] VELASCO NUÑEZ E. (2015). *Los delitos informáticos.* SEPÍN Editorial Jurídica. Nº.81. Diciembre 2015. pp. 14-28 .p.16.
[31] Ibidem.
[32] BARRIO ANDRÉS M (2011). *Los delitos cometidos en Internet. Marco comparado, internacional y derecho español tras la reforma penal de 2010.*La Ley Penal. Nº. 86. Sección Legislación aplicada a la práctica. Octubre 2011. Editorial La Ley. p.10.

realizar una transferencia no consentida de activos en perjuicio de un tercero, aceptando diversas formas para su aceptación, como creación de órdenes de pago o de transferencias, manipulaciones de entrada o salida de datos.

3.2.2. La defraudación. (255 CP)

Se trata de una modalidad de la estafa, donde su especialidad y diferenciación con esta consiste en que, mientras la estafa suele consistir en provocar un acto de disposición en beneficio propio o ajeno, en la defraudación se realiza una serie de maquinaciones para beneficiarse, absorber o utilizar de unos servicios de pago (tales como energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos)[33].

De esta forma, atendiendo al artículo 255 CP incurrirán en este delito, quienes defrauden por medio de los siguientes medios: *"(…) 1.º Valiéndose de mecanismos instalados para realizar la defraudación. 2.º Alterando maliciosamente las indicaciones o aparatos contadores. 3.º Empleando cualesquiera otros medios clandestinos."*

3.2.3. Hurto de tiempo (256 CP)

Este tipo delictivo no solamente consiste en utilizar de forma no autorizada terminales tele comunicativos ajenos, sino que, además, debe de causar un perjuicio económico que no puedan encontrarse dentro del uso cotidiano y social[34].

Un caso concreto se encuentra en aquellos casos en los que el coste del servicio de la línea que un usuario paga a la compañía que le suministra el servicio de Internet es utilizado por un empleado de la empresa receptora en otros menesteres de tipo particular de uso, haciendo por ello un gasto económico de la cual la empresa no tiene conocimiento.

Otra modalidad de hurto del tiempo -a la que yo me he atrevido a bautizar como "doble o triple hurto de robo de tiempo"- se realiza cuando la empresa que suministra el servicio de Internet entrega unas claves de acceso al usuario de la misma que es su cliente, pero a la vez este usuario desvela el número secreto de su acceso a Internet a otras personas, las cuales utilizando las mismas claves entran a utilizar dicho servicio, pero que no son clientes de la empresa suministradora de Internet, pero lo usan, por lo tanto se está produciendo un perjuicio económico en la empresa suministradora de Internet.

---

[33] FARARDO CABANA P. (2011). Defraudación de telecomunicaciones y uso no consentido de terminales de telecomunicación. Dificultades de delimitación entre arts. 255 y 256 CP. Un derecho penal comprometido: libro homenaje al Prof. Dr. Gerardo Landrove Diaz. Editorial Tirant lo Blanch. pp 363 y ss.

[34] VELASCO NUÑEZ E. (2015). *Los delitos informáticos.* SEPÍN Editorial Jurídica. Nº.81. diciembre 2015. pp. 14-28. p.20.

De esta forma, la conducta punible que establece el artículo 256 CP se refiere al "*que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, y causando a éste un perjuicio económico".*

3.2.4. Cracking o Daños informáticos (264 CP)

Este delito es comúnmente conocido como "cracking" y se caracteriza porque estos daños no tienen un contenido patrimonial como sucede con el concepto delictivo tradicional de daños.

En primer lugar, debemos de comentar su **conducta básica**, la cual se encuentra regulada en el artículo 264 CP, por medio de la cual se establece que incurrirán en este tipo delictivo el sujeto que *"por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave".*

En este sentido las conductas que engloba estas figuras delictivas recaen en el daño, deterioro, alteración, supresión o imposibilidad de acceso a programas, datos y documentos electrónicos, siempre que lo haga sin autorización, por cualquier medio. En cuanto a la pena aplicable, dicho artículo lo determina con una pena de prisión comprendida entre los seis meses de prisión a los tres años.

Por lo tanto, los elementos principales para incurrir en este tipo recaen sobre la ajenidad y la falta de autorización, Por lo cual, por un lado, el objeto sobre el que recaiga la acción del daño debe de ser ajeno al autor, es decir, el sujeto activo nunca incurrirá en este precepto si realiza estos daños sobre datos, programas informáticos o documentos electrónicos propios; por otro lado, para incurrir en este tipo debe de existir una falta de consentimiento por parte del auténtico propietario de los datos, programas informáticos o documentos electrónicos[35].

Del mismo modo, hay que destacar que estos daños deben de tener unas consecuencias graves para distinguirlo de aquellos supuestos en los que no deben de intervenir el Derecho penal y cuando se realicen contra un objeto de propiedad ajena[36].

No obstante, cabe destacar que nuestro legislador, en el apartado segundo de dicho artículo, ha establecido una serie de casos agravantes (llegando a aplicarse una pena de dos años a cinco y multa del tanto al decuple) en los casos que se den unas determinadas circunstancias[37].

---

[35] GONZÁLEZ HURTADO J.A. (2013). *Delincuencia Informática: Daños informáticos del artículo 264 del Código Penal y propuesta de reforma.* Tesis doctoral. Universidad Complutense de Madrid.p.206 y ss.

[36] VELASCO NUÑEZ E. (2015). *Los delitos informáticos.* SEPÍN Editorial Jurídica. Nº.81. diciembre 2015. pp. 14-28. p.20.

[37] En este sentido, una pena de prisión de dos a cinco años y multa del tanto al décuplo cuando se dan las siguientes circunstancias: Comisión por medio de una organización criminal; Daños de especial gravedad o afectación a un número elevado de sistemas informáticos; Que el hecho haya afectado gravemente al funcionamiento de los servicios públicos esenciales o a la provisión de bienes de primera necesidad; Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea

En segundo lugar, podemos encontrar la conducta denominada **DoS o denegación del servicio**, la cual se encuentra regulada en el artículo 264 bis CP, a tenor del cual establece la conducta relativa sobre quien *"sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno: a) realizando alguna de las conductas a que se refiere el artículo anterior; b) introduciendo o transmitiendo datos; o c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica."*

Por lo tanto, aquellas conductas que obstaculice o interrumpa el funcionamiento informático de un sujeto ajeno, así como el propio en los casos en los que este sea compartido, siempre y cuando este se realice de una forma grave (ya que en caso contrario no podría incurrirse dentro del ámbito penal), sin estar autorizado para ello y siempre que dicha actuación no vaya dirigida a interferir en el orden público (ya que de lo contrario nos encontraríamos ante un delito de desorden público tipificado en el artículo 560.1 del Código Penal[38].

Como ejemplo podemos destacar el denominado *"mail bombing"* o el bombardeo simultáneo de un correo electrónico, por medio del cual se realiza un envío masivo de mensajes a una maquina informática hasta llegar a saturar el servidor.

Del mismo modo, este tipo penal acepta la aplicación de los agravantes que establece el artículo 264.2º CP citado anteriormente, por medio de la cual se aplica la pena superior en grado.

En tercer lugar, encontramos la conducta referida a la **facilitación de la comisión** de los delitos mencionados anteriormente. Este tipo se encuentra en el artículo 264 ter CP y establece la conducta relativa sobre quien trate de facilitar la comisión de los delitos mencionados anteriormente, por medio de la producción, adquisición, importación de *a) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información."*

La característica principal de este tipo delictivo, incide en la responsabilidad civil que puede llegar a derivar, la cual no solamente alcanza el lucro cesante por la interrupción o el daño ocasionado, sino que tiene que tenerse en consideración una gran cantidad de elementos, como las horas de trabajo afectadas, el tipo de actividad y las pérdidas de clientes, posibilidad de recuperación de datos, etcétera.

o de un Estado Miembro de la Unión Europea; El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter. Del mismo modo, en los casos en los que el delito se hubiera realizado de extrema gravedad, se podrá incluso aplicar la pena superior en grado.

[38] VELASCO NUÑEZ E. (2015). *Los delitos informáticos.* SEPÍN Editorial Jurídica. Nº.81. diciembre 2015. pp. 14-28. p.20.

Por lo tanto, la determinación del daño causado por este tipo penal tiene una gran dificultad, ya que no será suficiente indemnización la devolución a la situación previa a dicha interrupción o daño causado[39].

3.2.5. Delitos contra la Propiedad Intelectual e Industrial

Se trata de todas aquellas acciones dirigidas a la reproducción, plagio, distribución o comunicación pública, de una obra literal, artística o científica, su transformación, sin la autorización de los titulares de los correspondientes Derechos[40].

3.2.5.1 Delitos relativos a la propiedad intelectual. (270.1 CP)

Dentro de este tipo de delitos, debemos de atender en primer lugar a la **conducta básica** que establece el artículo 270.1 CP, a tenor del mismo se castiga al sujeto que *"(…)con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios."*

Como se puede observar, se trata de una infracción mercantil criminalizada, donde la deslealtad penada nace de explotar, un producto ajeno o que no se ha cedido, en otras palabras, un producto no autorizado.

De otro lado el articulo 270.2 CP regula la conducta relativa al **acceso de contenido ilegitimo en Internet**, tipificando la siguiente conducta relativa al sujeto que *"(…) en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en Internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios."*

Por medio de este tipo, se pena los servicios de referenciación de contenidos en Internet que puedan llegar a facilitar la localización de contenidos protegidos y ofrecidos de forma ilícita sin ninguna autorización del propietario o cesionario de Derechos.

En estos casos, es necesario un ánimo de lucro por parte del sujeto activo, donde en la práctica es frecuente que dicho lucro se obtenga a través de la publicación de banners publicitarios en la página web donde se publica el contenido. Del mismo

---

[39] VELASCO NUÑEZ E. (2015). *Los delitos informáticos.* SEPÍN Editorial Jurídica. Nº.81. Diciembre 2015. pp. 14-28. p.21.

[40] DE URBANO CASTRILLO E. (2011). *Los delitos informáticos tras la reforma del CP de 2010.* Revista Aranzadi Doctrinal. Nº. 9/2011. Parte Estudio. p.45.

modo, como es lógico, es necesario que dicho acceso al contenido se produzca sin una autorización por parte del titular del producto[41].

En este último caso, el órgano jurisdiccional competente podrá ordenar la retirada de las obras o prestaciones que son objeto de la infracción, asimismo, podrá establecer medidas restrictivas en Internet, como la retirada de contenidos, interrupción de los servicios, el bloqueo a su acceso (en aquellos casos en los que haya reiteración), así como cualquier medida cautelar que tenga por finalidad proteger los Derechos de propiedad intelectual del autor[42].

Cabe destacar que este tipo establece penas de prisión de seis meses a cuatro años, y multas de doce a veinticuatro meses. Sin embargo, en los casos que expone el articulo 270.1 CP, a saber, si la conducta se realiza de una forma ocasional o ambulante, con una distribución al por menor y con un escaso beneficio económico de la actividad, cuando el sujeto activo no actúe en el seno de una organización criminal, ni haga uso de menores, debe de aplicarse una mera pena de multa de uno a seis meses o trabajos en beneficio de la comunidad de treinta y un a sesenta días[43].

Asimismo, el artículo 270.5 CP establece las mismas penas descritas anteriormente a aquellos sujetos que *exporten o almacenen, importen intencionadamente, favorezcan o faciliten la realización de las conductas* anteriores para permitir que un tercero eluda las medidas tecnológicas de protección de propiedad intelectual. En estos casos, el sujeto activo debe actuar siempre con un ánimo de lucro, ya sea directo o indirecto, sin una debida autorización y con una finalidad de destino a la reproducción, distribución o comunicación pública.

Finalmente, es destacable comentar que estas conductas pueden tener unas penas agravadas que ascienden en las penas de prisión de dos a seis años y multa de dieciocho a treinta y meses, así como la inhabilitación especial para el ejercicio de la profesión vinculada en la realización del hecho delictivo por un periodo de dos a cinco años, en los casos que se den alguna de las siguientes circunstancias[44]:

- Especial trascendencia económica.
- Especial gravedad por el número de obras.
- Pertenencia a una organización o asociación (aunque sea transitoria) que tenga como finalidad estos actos.
- Utilización de menores de 18 años para su comisión.

[41] VELASCO NUÑEZ E. (2015). *Los delitos informáticos.* SEPÍN Editorial Jurídica. Nº.81. Diciembre 2015. pp. 14-28. p.22.
[42] Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Artículo 270.3.
[43] Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Artículo 270.4.
[44] Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Artículo 271.

3.2.5.2 Delitos relativos a la propiedad industrial. (274 CP)

Nuestro Código Penal establece unas conductas punibles relativas a la propiedad industrial en los artículos 274 y siguientes del mismo. En este sentido, el tipo básico castiga *"al que, con fines industriales o comerciales, sin consentimiento del titular de una patente o modelo de utilidad y con conocimiento de su registro, fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio objetos amparados por tales derechos."*

En este sentido y en relación con la cibercriminalidad, el legislador castiga todas aquellas conductas independientemente del medio que se haya realizado, lo que incluye la realización a través de cualquier sistema de información[45].

3.2.6. Espionaje informático de secretos de empresa. (278 CP)

La conducta básica de este tipo penal la encontramos en el artículo 278 CP, por medio del cual se refiere al sujeto que *para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197[46] (…)."*

En este sentido, nos encontramos ante un delito que protege el carácter "*intuitu personae"* de determinados elementos significativos y diferenciadores de cada empresa, los cuales se puede representar por medio de datos, documentos escritos, soportes informáticos o similares.

Hay que destacar que no confundir estos elementos con el denominado *know how*, el cual es el conocimiento de la realización de una tarea de forma sencilla y eficiente a causa de la experiencia y que se transfiere justamente entre los cambios del empleador. Del mismo modo, tampoco debemos confundirlo con los denominados *atributos de la libre competencia*, los cuales se obtienen por permanecer en el propio mercado[47]. Sobre su penología, se establece una pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

3.2.7 Falsificaciones de tarjetas bancarias y de transporte. (399.1CP)

La conducta típica en este tipo de delitos se encuentra regulada en el artículo 399.1 bis CP, por medio del cual castiga al sujeto *"que altere, copie, reproduzca o de cualquier otro modo falsifique tarjetas de transporte, tarjetas de crédito o débito, así como cheques bancarios o de viaje.*

Se trata de una figura propia que se diferencia de la estafa informática del artículo 248.2.c) CP, la cual hemos analizado anteriormente. En este sentido, la falsedad de

---

[45] BARRIO ANDRÉS M (2011). *Los delitos cometidos en Internet. Marco comparado, internacional y derecho español tras la reforma penal de 2010.*La Ley Penal. Nº. 86. Sección Legislación aplicada a la práctica. Octubre 2011. Editorial La Ley. p. 16.

[46] En este sentido se refiere al uso de artificios técnicos de escucha, transmisión, grabación reproducción de sonido o de la imagen, o de cualquier otra señal de comunicación.

[47] VELASCO NUÑEZ E. (2015). *Los delitos informáticos.* SEPÍN Editorial Jurídica. Nº.81. diciembre 2015. pp. 14-28. p.22.

tarjetas se debe de entender de una forma amplia, vinculando a aquellas tarjetas de crédito y de debido y de transporte, así como los cheques de viajes.

Del mismo modo, la conducta punible debe de atenderse por un lado desde el punto de vista de la fabricación de la tarjeta, ya sea por medio de la alteración, el copiado o la reproducción a través de la creación de programas informáticos o incorporando identidades ficticias; y, por otro lado, en cuanto a la composición de los soportes físicos de la misma, la cual puede generar suplantaciones de personalidad o la tenencia para su posterior tráfico.

Como se puede observar, esta figura delictiva trata una primera modalidad basada en la "alteración", lo que supone una manipulación material de alguno de los componentes del objeto en cuestión. Por otro lado, se establece una segunda conducta que puede relacionarse con la "copia" o "reproducción" de estos productos, lo que en la práctica se conoce como *skimiming* y supone la duplicación de los datos contenidos en la banda magnética con la finalidad de confeccionar otra que puede ser utilizada sin necesidad de autorización del verdadero titular[48].

Igualmente, debemos atender que el legislador ha establecido un tipo agravado en aquellos casos en los que los efectos falsificadores afecten a una generalidad de personas o cuando se haya realizado a través de una organización criminal que se tenga como finalidad estas actividades[49].

No obstante, hay que distinguir esta conducta con la relativa al uso de tarjetas que son auténticas, pero que son utilizadas de forma no autorizada por un sujeto diferente a su titular, ya que en estos casos nos encontramos ante una estafa regulada en el artículo 248.2 CP.

3.3. Los delitos ciberintrusivos

Son aquellos delitos en los que sujeto activo busca principalmente apoderarse de elementos personales de terceras personas a través de medios tecnológicos[50]. Asimismo, debemos de destacar los siguientes:

3.3.1. Acoso sexual a menores a través de la red. (189 CP)

En primer lugar, podemos hacer mención a la conducta relativa a la **pornografía infantil**, regulada en el artículo 189 CP, así este tipo delictivo pretende proteger el bien jurídico relativo al crecimiento armónico de la sexualidad del menor, como una forma de proteger la defensa de la inocencia y la pureza de la infancia.

Nuestra legislación, castiga todo lo vinculado con la pornografía del menor, desde su elaboración hasta su difusión, favorecimiento o posesión, ya que la finalidad de

[48] AZCONA ALBARRÁN C. D. (2012). *Tarjetas de pago y Derecho penal: Un modelo interpretativo del art. 284.2. c) CP.* Atelier Libros.p.23.
[49] Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Artículo 399 bis.1.
[50] VELASCO NUÑEZ E. (2015). *Los delitos informáticos.* SEPÍN Editorial Jurídica. Nº.81. diciembre 2015. pp. 14-28. p.20.

esta protección se centra en la sexualidad armónica del menor o de aquellas personas que requieran de una especial protección, como es el caso de las personas con discapacidades pese a que superen esta mayoría de edad.

Por ello, debemos entender la pornografía infantil como la participación del menor o de la persona con discapacidad en una conducta sexual explicita o la representación de sus órganos sexuales con un fin sexual[51]. De esta forma, las nuevas tecnologías y el uso de sistemas de información como Internet, son una fácil vía para la distribución de este tipo de contenido pornográfico[52].

En segundo lugar y en relación con la utilización de sistemas informáticos para la comisión de esta clase de delitos, debemos hacer mención al denominado **child grooming**, regulado en el artículo 183 ter CP, por medio del cual castiga al sujeto 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 la finalidad de cometer un delito de abuso sexual o de pornografía, realizando actos materiales que vayan dirigidos al acercamiento de la víctima. En cuanto al bien jurídico protegido, este precepto vuelve a proteger la indemnidad sexual del menor[53].

Por lo tanto, como se puede observar, este tipo penal combina una acción virtual tecnológica con una exteriorización posterior de la conducta. De esta forma, este tipo pretende castigar el abuso de confianza, así como la explotación de la ingenuidad de los menores, la captación de pornografía infantil y el intento de abuso sexual, por lo cual, este precepto puede llegar a plantear problemas de concursos de delitos[54].

3.3.2. El Hacking o Descubrimiento y revelación de secretos. (197 CP)

Su conducta básica se encuentra regulada en el artículo 197 bis del Código Penal, y castiga al a que "(…) *vulnerando las medidas de seguridad y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo".*

Del mismo modo, nuestro legislador, por medio de la reforma de la LO 1/2015 tipifica la facilitación a la producción de programas informáticos o equipos diseñados para cometer tales delitos en el artículo 197 ter CP.

---

[51] Directiva 2011/92/UE del Parlamento Europeo y del Consejo de 13 de diciembre de 2011, relativo a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil. Artículo 2.c).

[52] VILLACAMPA ESTIARTE C; GÓMEZ ADILLÓN M.J. (2016). *Nuevas tecnologías y victimización sexual de menores por online grooming.* Revista electrónica de ciencia penal y criminología. p.2.

[53] BALANZA, M. O., & ROMERO, L. R. (2014). *Amistades peligrosas: el delito de child grooming*. Iuris: Actualidad y práctica del derecho. Nº. 217, pp. 47-53. P.49.

[54] En este sentido Eloy VELASCO, considera que la conducta a través de medios tecnológicos sin llegar a producir un acercamiento, puede derivar en una forma imperfecta de ejecución, así, en el caso de llegar a consumar los delitos relativos a abuso sexual o de pornografía se debería de proceder a castigar por medio de un concurso real; por otro lado, en el caso de contactar por medios tecnológicos y llegar a realizar actos que le lleven a obtener un material pornográfico de la víctima o a que este le muestre contenidos pornográficos en el que se represente a un menor, el autor incurriría en un delito de pornografía infantil.

De esta forma, podemos entender que nos encontramos ante un delito que castiga el acceso no autorizado por medio de la violación de mecanismos de seguridad (en el caso que los hubiera), a los archivos y bases de datos contenidos en los sistemas informáticos ajenos. Se trata, de un delito de carácter informático, así como un medio para cometer otros delitos, haciendo uso de malwares, tales como virus, troyanos, spyware, keyloggers, etcétera[55].

Asimismo, cabe destacar que la novedad en la reforma establece como conducta delictiva tanto la producción y adquisición de dicha información no autorizada para su uso, como la importación o facilitación a terceros sujetos de programas informáticos creados para cometer estos delitos informáticos[56].

3.3.3. Suplantación y robo de la personalidad

En esta apartado solamente queremos hacer mención que este tipo delictivo se encuentra categorizado como un delito ciberintrusivo. No obstante, el estudio de dicho delito se realizará en el Capítulo V, donde profundizaremos sobre todos los elementos del mismo.

3.3.4. El Stalking o el acoso informático. (172 ter CP)

El Stalking se encuentra regulado en el artículo 172 ter CP y es un nuevo delito añadido por la última reforma de nuestro Código Penal a través de la Ley Orgánica 1/2015. Por medio de este delito se pretende proteger diversos bienes jurídicos, como puede ser la libertad de obrar o la libertad de decidir libremente, ya que por medio de estas conductas pueden llegar a afectar a la formación de la voluntad de la víctima[57].

En este sentido, el tipo sanciona a quien "*acose a una persona llevando a cabo de forma insistente y reiterada y sin estar legítimamente autorizado, (…), altere gravemente el desarrollo de su vida cotidianidad".*

Del mismo modo, establece las conductas punibles por las que se puede incurrir en dicho tipo como son: a) Sometimiento a vigilancias, persecuciones o búsqueda de su cercanía física; b) Contacte o trate de contactar por cualquier medio de comunicación o mediante una tercera persona; c) Hacer un uso indebido de datos, contratando productos o servicios, así como hacer que una tercera persona se ponga en contacto con la victima; d) Atente contra su libertad o patrimonio.

Se trata, por lo tanto, de un delito tradicional que puede ser realizado a través de medios informáticos, ya que estos pueden llegar a facilitar su comisión, ya sea a través de redes sociales, sistemas informáticos, teléfonos móviles, etcétera.

---

[55] BARRIO ANDRÉS M (2011). *Los delitos cometidos en Internet. Marco comparado, internacional y derecho español tras la reforma penal de 2010.*La Ley Penal. Nº. 86. Sección Legislación aplicada a la práctica. Octubre 2011. Editorial La Ley. p. 11.
[56] Ibídem.
[57] GALLEGO CENOZ J.(2016). *Primera condena por el nuevo delito de "stalking"*. Revista Aranzadi Doctrinal. Nº.6/2016. Fichas de Jurisprudencia. P.2.

3.3.5 El Ciberbullyng.

Se trata de una forma de maltrato físico, verbal o psicológico que se da entre escolares de forma reiterada en el tiempo, por lo que no debe de confundirse con meros incidentes aislados u ocasionales entre alumnos. Respecto a su contenido está conformado por una serie de actos de hostigamiento como por ejemplo amenazas, agresiones físicas, insultos, vejaciones, humillaciones, coacciones, etc., en aras a aterrorizar a la víctima.
Sus elementos fundamentales son: un desequilibrio de poder entre acosador u acosadores y acosado; intencionalidad o deseo consciente de hacer daño; y, por último, una reiteración en el tiempo.

Respecto al marco legal actual es fundamental la Convención de Derechos del Niño, la Constitución española –especialmente importante es el art. 10.1º CE, ya que se da un atentado contra la dignidad del menor, pero también otros preceptos incardinados dentro de los derechos fundamentales como la libertad, la integridad física, el honor, etc.-, y la legislación educativa. Especial mención también debe de hacerse del art. 172 ter CP que establece penas de prisión de tres meses hasta dos años y multa para las conductas que tipifica como delito. Algunas de esas conductas son: vigilar y perseguir; usar indebidamente datos personales para adquirir mercancías o contactar con terceras personas; o atentar contra su libertad o su patrimonio.

3.4. Los delitos de ciberterrorismo

Por medio de este tipo de delitos, el sujeto activo pretende crear terror y atemorizar a una gran cantidad de sectores de la población por medio del uso de nuevas tecnologías, las cuales aportan una gran cantidad de la información necesaria para planificar y cometer un atentado terrorista, asimismo, suele ser utilizadas para la comunicación entre los terroristas, así como para realizar campañas de propaganda adoctrinamiento[58]. En este sentido, nuestro Código Penal referencia esta clase de delitos por medio de diversas conductas punibles, como son los siguientes:

3.4.1. El adoctrinamiento y adiestramiento. (575 CP)

El Código Penal castiga en el artículo 575 a los sujetos que con la finalidad de cometer un delito terrorista "*reciba adoctrinamiento o adiestramiento"*. De esta forma, incurrirán en este tipo delictivo todos los sujetos que accedan de una manera habitual a servicios de comunicación públicos en Internet, cuyo contenido vayan dirigidos a iniciarse en una organización o grupo terrorista o a colaborar con estos en sus mismos fines.

[58] VELASCO NUÑEZ E. (2015). *Los delitos informáticos.* SEPÍN Editorial Jurídica. Nº.81. diciembre 2015. pp. 14-28. p.23.

3.4.2. El enaltecimiento o justificación del terrorismo. (578 CP)

A través del artículo 578 CP se castigan actos como "*el enaltecimiento o la justificación pública*" de los delitos terroristas[59] "o *de "quienes hayan participado en u ejecución, o la realización de actos que entrañen descrédito, menosprecio o humillación de las víctimas de los delitos terroristas o de sus familiares*".

En este sentido, este tipo penal se puede ejecutar a través 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, donde, en dichos casos, se procederá a aplicar la pena agravada en su mitad superior[60].

3.4.3. Difusión e incitación al terrorismo. (579 CP)

Por medio del artículo 579 CP se castiga todas aquellas conductas en las que se "*difunda públicamente mensajes o consignas que tengan como finalidad o que, por su contenido, sean idóneos para incitar a otros a la comisión de alguno de los delitos*" de terrorismo.

Como venimos apuntando el uso de las TIC's facilitan la comisión de este tipo delictivo. En estos casos, el órgano jurisdiccional competente se encargará de determinar que se retiren dichos contenidos.

Del mismo modo, el Juzgado Instructor podrá establecer medidas cautelares como medidas para la instrucción de la causa, entre las que se puede ordenar a los prestadores de servicios la retirada de tales contenidos ilícitos, así como exigir a los proveedores de servicios electrónicos que impida su acceso y a los motores de búsqueda que eliminen los enlaces a estos[61].

[59] En este caso nuestro Código Penal se refiere a los artículos tipificados en los artículos 572 a 577 CP.

[60] Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Artículo 578.2.

[61] VELASCO NUÑEZ E. (2015). *Los delitos informáticos.* SEPÍN Editorial Jurídica. Nº.81. diciembre 2015. pp. 14-28. p.24.

Capítulo IV: Usurpación y suplantación de la identidad a través de medios informáticos.

4.1. Introducción

La suplantación de la identidad se entiende como la usurpación del estado civil del individuo y se encuentra tipificado en el artículo 401 de nuestro Código Penal, donde a tenor del cual se establece:

> *"El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años".*

El bien jurídico protegido recae sobre el estado civil del otro individuo. Por dicha razón este tipo penal se ha incluido dentro del Capítulo IV, bajo la denominación de "De la usurpación de las funciones públicas y del intrusismo", dentro del Título XVIII del Libro II de nuestro Código Penal.

Finalmente, cabe destacar que este tipo delictivo es frecuente que se dé con la finalidad principal de llegar a cometer un delito diferente posteriormente.

4.1.1 Elemento objetivo del tipo

La conducta punible, por lo tanto, recae sobre la obtención o apoderamiento de datos, informaciones o documentos de un sujeto tercero, para utilizarlos con una finalidad de hacerse pasar por el en los diversos ámbitos de la vida cotidiana[62], en otras palabras, se trata de asumir la personalidad ajena sustituyendo al sujeto en el ejercicio de todos sus derechos.

Este tipo penal posee una doble naturaleza, por un lado, manifiesta un elemento falsario y por otro un elemento atentatorio, ambos contra el estado civil del sujeto pasivo.

No obstante, atendiendo a la jurisprudencia del Tribunal Supremo, a pesar de que, usurpar el estado civil de otras personas lleva siempre consigo la necesidad de utilizar el nombre y apellido de esta, en la práctica, es necesario que se den unos elementos adicionales para incurrir en este tipo penal, sin que sea suficiente la continuidad o la repetición en el tiempo de dicho uso indebido para llegar a incurrir en la usurpación[63].

[62] MUÑOZ, A. G. (2010). *El Robo de Identidad: aproximación a una nueva y difusa conducta delictiva*. Robo de identidad y protección de datos. Editorial Aranzadi. pp. 169-198.
[63] Sentencia del Tribunal Supremo, número 635/2009, de 15 de junio. Así como SAP Sevilla número 46//2015 de 18 de junio, SAP Sevilla 432/2015 de 30 de Julio, SAP Huesca 137/2012 de 7 de septiembre, entre otras.

En este sentido, debemos entender el término de "usurpar" como la acción de "*arrogarse la dignidad, empleo u oficio de otro, y usarlos como si fueran propios*"[64]. Por ello, el sujeto activo debe de realizar una acción que solamente tenga pueda realizar aquellas personas que por sus facultades, derechos u obligaciones corresponden[65].

En esta misma línea, debemos de entender la identidad como el ámbito personal donde cada sujeto, preservando el mundo exterior, encuentra las posibilidades de desarrollo y fomento de su personalidad[66]. Por ello, debemos entender que la identidad de una persona es un elemento esencial y único del sujeto que diferencia a esta del resto.

Por lo tanto, para la consumación de este tipo delictivo, debe de entenderse que se produce en aquellos casos en los que el sujeto activo haya realizado una suplantación completa, es decir, cuando haya realizado todos los actos necesarios que puedan llegar a generar un error sobre terceras personas, haciéndoles creer que el usurpador en realidad es el afectado.

Por todo ello, no es suficiente con utilizar el nombre y apellidos del sujeto pasivo, si no que se requiere que el autor actué de una forma concreta, realizando ciertas acciones que le lleven a generar una apariencia que muestra que el usurpador y usurpado son el mismo sujeto, es decir, llevándose a cabo una usurpación completa de la persona del usurpado[67].

Atendiendo al tenor literal del artículo, podemos entender que no es necesario que se llegue a causar un perjuicio de ninguna clase al sujeto pasivo, sin embargo, la jurisprudencia establece realiza una interpretación a favor de la exigencia de este requisito.

4.1.2 Elemento subjetivo del tipo

Este delito requiere del elemento subjetivo del dolo directo[68], por lo que el sujeto activo debe de conocer las consecuencias de la comisión de su hecho delictivo y pese a dicho conocimiento decide realizarlo[69].

En esta misma línea, cabe destacar que la jurisprudencia exige que la usurpación de identidad tenga como finalidad hacer uso de los derechos y acciones del sujeto suplantado, por lo que se convierte en un elemento imprescindible para incurrir en

---

[64] Real Academia de la Lengua Española. Versión online. Recuperado en: [http://dle.rae.es/?id=bCKNShl]

[65] RODRÍGUEZ RAMOS L. (Dir.) (VVAA) (2009). *Código Penal. Comentado y con Jurisprudencia.* Editorial La Ley. 3º Edición. p.1209.

[66] BAJO M. (1982). *Protección del honor y de la intimidad.* Comentarios a la Legislación Penal. Tomo I. Editorial Erdesa. p. 101.

[67] Sentencia del Tribunal Supremo, número 635/2009, de quince de junio. Así como SAP de Sevilla número 46/2015 de 18 de junio; SAP Sevilla 432/2015 de 30 de Julio; SAP Huesca 137/2012 de 7 de septiembre, entre otras.

[68] FARALDO CABANA P. (2010). *Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico.* Revista de Derecho penal y criminología. 3º Epoca. Nº. 3. pp. 73-134. p.87

[69] COBO DEL ROSAL M (2004). *Instituciones de Derecho penal español Parte general.* Editorial CESEJ. Madrid. 2004. p.187.

dicho precepto penal, del mismo modo, no es suficiente que se dé un simple uso continuado del nombre ajeno, sino que se requiere una que consiste en que la usurpación alcance a la totalidad de las facetas que integran la identidad humana, de forma que el sujeto activo se haga pasar por la víctima en todos sus efectos, como si se tratara de dicha persona[70].

Finalmente, cabe comentar que dicha conducta puede ser objeto de en un error de hecho, como puede ocurrir en aquellos casos en los que el sujeto activo haga uso de un nombre o filiación creyendo que no existen pero que en realidad pertenecen a otra persona. En estos casos no se incurren en la conducta básica del 401 CP ya que excluye el dolo directo que debe abarcar que dicho conocimiento pertenezca a un sujeto en concreto[71].

4.1.3 Sujetos

Dentro de este tipo delictivo podemos encontrar dos sujetos principales, por un lado, se encuentra el sujeto pasivo, el cual es la víctima del delito y se trata de aquel sujeto cuya identidad ha sido usurpada. Por otro lado, se encuentra el sujeto activo, el cual es aquel que realiza la conducta típica y se apropia de la identidad de un sujeto ajeno.

4.2. Formas informáticas para suplantar la identidad.

Podemos encontrar una gran cantidad e innovadoras formas informáticas para llevar a cabo una suplantación de la identidad de un sujeto, los cuales, como ya hemos dicho, en la práctica, suelen utilizarse con la finalidad de comentar posteriormente otra serie de delitos. De esta forma, debemos nombrar los siguientes medios para proceder a realizar una suplantación de identidad y el tratamiento penal que reciben.

4.2.1. El spoofing

El spoofing se trata de una técnica utilizada por los cibercriminales, por medio de la cual actúan en nombre de otros usuarios, utilizando el nombre y contraseña de un usuario legítimo e ingresando en un sistema, donde pueden llegar a realizar acciones en nombre de dicho usuario[72].

Por lo tanto, se trata del robo o de la suplantación de la personalidad de una persona física o jurídica a través de medios informáticos, sin embargo, su particularidad recae en que no requiere de la realización de un engaño previo a la víctima que pretende

---

[70] Sentencia del Tribunal Supremo número 8368/1991, de veintiséis de marzo. Véase también entre otras: SAP Islas Baleares de 4 de diciembre de 2009; SAP de Sevilla de veintitrés de mayo de 2000; SAP de Madrid, de cinco de diciembre de 2000; SAP Albacete de nueve de mayo de 2002.

[71] FARALDO CABANA P. (2010). *Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico.* Revista de Derecho penal y criminología. 3º Época. Nº. 3. pp. 73-134. p.88.

[72] MORAIS GALLEGO J.M. (2006) *Las nuevas tecnologías de la información y de la comunicación. Implicaciones legales.* Revista galega de Ensino. Vol. 14. Nº. 48. Marzo 2006. P. 432.

suplantar. Así, esta forma de suplantación requiere una actuación muy técnica y con unos elevados conocimientos en materia informática[73].

De esta forma, podemos destacar diversas formas de suplantación a través de la modificación de diversas formas, como son[74]:

- **IP Spoofing**: En estos casos, la suplantación de la identidad se inicia en el "host"[75], donde el sujeto activo procede a sustituir la IP[76] de origen por otra que desea suplantar, de esta forma, el host que se suplanta recibe una serie de paquetes de respuesta que no han sido solicitados.

- **ARP Spoofing:** Se trata de la suplantación de la identidad por medio del "ARP"[77], por medio de la cual se produce el envío de mensajes al ARP falsos, por lo que hace que se cambie la MAC del atacante y la antigua IP de la víctima. De esta forma, todos los contenidos e información que iba a recibir la víctima, proceden a remitirse al sujeto activo del delito, de esta forma, este último puede decidir si espiar a la víctima, modificar dichos contenidos o proceder a incomunicarla asignándole un MAC inexistente.

- **DNS Spoofing:** Es el cambio de la relación de un nombre de un dominio por una IP falsa. Estos ataques se realizan por medio de la falsificación del dominio de un DNS[78] que muestra alguna vulnerabilidad.

- **Web Spoofing**: Es la suplantación de una página web real, la cual se realizar estableciendo una ruta de la conexión de la víctima por medio de una página web falsa hacia otras páginas web, con la finalidad de obtener información de dicha víctima. De esta forma, esta página web actúa como modo de "proxy"[79], donde obtiene información que le comunica la víctima. Cabe destacar que no debe de confundirse este método con el denominado "phising", ya que este último se encarga de suplantar realmente la página original, mientras que el "Web Spoofing" se encarga de actuar de intermediador entre ambos.

- **Mail Spoofing:** Se trata de la utilización de un servidor de "SMTP"[80] para enviar correos electrónicos con un remitente falso.

En cuanto a la punibilidad y tratamiento penal del spoofing, debemos decir que se trata, por lo tanto, del primer paso para la dinámica comisiva, por medio de esta

[73] LORES, Y. V. (2013). *Seguridad Informática en la formación de profesionales*. Serie Científica-Universidad de las Ciencias Informáticas. Vol. *6. Nº.*5. p.22.
[74] VILLALÓN HUERTA A. (2002)*. Seguridad en Unix y Redes. Versión 2.1.* GNU Free Documentation License. p.298 y ss.
[75] Se trata del servidor donde se hospedan las direcciones IP.
[76] Se trata de la identificación que recibe un sistema informático por medio de la asignación de la red.
[77] Procede de las siglas en inglés de Addres Resolution Protocol y se encarga de convertir la identifiacción de IP en la identificación MAC.
[78] Procede de las siglas en inglés de Domain Name System y se trata de un sistema para dispositivos conectados por medio de redes IP.
[79] Se trata del sistema que sirve como intermediario entre dos sistemas informáticos.
[80] Se trata de un protocolo que actúa sobre los elementos de salida de los correos electrónicos.

suplantación de la personalidad se produce un acomodamiento para la realización de diversos tipos penales[81].

En un principio, parece que el *spoofing* se puede llegar a sancionar a través de un delito de usurpación del estado civil tipificado en el artículo 401 CP, sin embargo, debemos de recordar que este exige una continuidad en cuanto la suplantación de personalidad, por lo que la jurisprudencia no llega a aceptar esta modalidad delictiva.

No obstante, esta circunstancia puede variar en aquellos casos en los que la suplantación se realice sobre la personalidad de una institución pública, por lo que el articulo a aplicar se centra en el 402 CP, donde a tenor del cual se castiga al que "*ilegítimamente ejerciere actos propios de una autoridad ejerciere actos propios de una autoridad o funcionario público atribuyéndose carácter oficial, será castigado con la pena de prisión de uno a tres años"*[82].

Sin embargo, otra parte de la doctrina entiende que más que el estado civil, este tipo penal protege un bien jurídico protegido centrado en la fe pública, basando en la confianza de la comunidad en la correcta identificación de las personas[83].

En esta misma línea, la doctrina a tratado esta práctica informática delictiva considerando que puede llegar a vulnera otros tipos penales diferentes al artículo 401 y 402 CP. De esta forma, otros autores entienden que se puede llegar a constituirse un delito de falsedad en documento mercantil.

En este sentido, el problema incide en que se puede llegar a entender como documento, donde la doctrina acepta que el soporte informático puede llegar a integrar el concepto de documento, siempre que este pueda llegar a materializar una declaración de voluntad sobre el sujeto o que tenga un contenido valorable en el tráfico jurídico[84].

Por otro lado, otros autores entienden esta práctica como un delito contra la intimidad en aquellos casos en los que la usurpación se produzca sobre datos o claves bancarias. Esta conducta se encuentra tipificada en el artículo 197.1 CP, por medio del cual se castiga al quien *"para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere (…) mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones (…)"*[85].

---

[81] MIRÓ LLINARES F. (2011). *Memento Práctico. Penal Económico y de la Empresa. 2011-2012.* Editorial Francis Lefebvre. p. 483.

[82] MIRÓ LLINARES F. (2013). *La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phising.* Revista electrónica de ciencia penal y criminología (en línea). Nº.15-12. pp. 12:1-12:56. p. 12:19.

[83] FARALDO CABANA P. (2010). *Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico.* Revista de Derecho penal y criminología. 3º Epoca. Nº. 3. pp. 73-134. p. 83..

[84] DE LA MATA BARRANCO. N.J. (2007). *Cuadernos penales José María Lidón. Delitos e informática: Algunos aspectos. Número 4.* Edita. Universidad de Deusto. Bilbao. p. 59.

[85] FLORES MENDOZA F. (2014). *Respuesta Penal al denominado robo de identidad en las conductas del Phishing Bancario.* Estudios penales y criminológicos. Vol. 48. pp. 301-340. p. 313 y ss.

4.2.2. El phishing

El phishing, también conocido como la pesca de incautos, se trata de la suplantación de la identidad por medio de Internet, a través de la cual se persigue apropiarse de datos confidenciales de los usuarios para poder lograr un lucro en contra del patrimonio de la víctima o de un tercero. Por lo tanto, esta técnica consiste en la obtención de información de carácter personal por medio de engaños realizados a la víctima[86].

Esta modalidad de suplantación ha sido definida como una especia de mecanismo criminal que hace uso de una ingeniería social y elementos técnicos para inducir a error a la víctima. En este sentido, la ingeniería social se produce cuando se hace uso de la identidad personal de otro sujeto (es decir, por medio del "spoofing") por medio de la falsificación de sitios web, con la finalidad de dirigir a sus usuarios para que confíen en la veracidad de dicha web y publiquen sus datos personales[87].

En esta misma línea, se entiende esta conducta como una suplantación de la identidad, con la finalidad de cometer posteriormente un delito diferente (principalmente el de estafa). En este sentido, en el **phishing tradicional**, el sujeto activo, denominado como "phiser", se hace pasar por una empresa o persona de confianza por medio de una comunicación oficial electrónica, de esta forma y tras obtener la confianza de la víctima por medio de su inducción a error, procede posteriormente a apoderarse de un patrimonio ajeno[88].

Cabe destacar otro método popular del phishing denominado "**Cross Site Scripting**" donde el sujeto activo hace uso del propio código de programa de una entidad bancaria o servicio por el que se hace pasar, por medio el usuario inicia sesión en la propia página del banco o servicio, donde la URL y los certificados de seguridad se muestran como correctos, no obstante, el usuario recibe un mensaje donde le informan de que tiene que proceder a verificar sus cuentas, remitiéndole a una página web falsa que simula la oficial para que la víctima comunique sus datos personales.

Por otro lado, podemos destacar otra modalidad de "phishing" que recibe el nombre de "**Spear Phishing**", el cual toma como víctimas a usuarios de bancos y servicios de pago en línea, en los que el autor crea y envía emails a dichas victimas haciéndose pasar por dicha entidad de servicios con la finalidad de obtener su información personal.

En cuanto a su punibilidad y tratamiento penal del phishing, hay que destacar en primer lugar que es una tarea muy complicada. En este sentido, a pesar de que esta conducta suponga una suplantación de identidad por medios informáticos, en la práctica es frecuente castigar esta conducta informática por medio de la estafa

---

[86] OXMAN N. (2013). *Estafas informáticas a través de Internet: Acerca de la imputación penal del "phising" y el "pharming".* Revista de Derecho de la Pontificia Universidad Católica de Valparaiso. Nº. XLI. pp. 211-262. p. 215.

[87] MIRÓ LLINARES F. (2013). *La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phising.* Revista electrónica de ciencia penal y criminología (en línea). Nº.15-12. pp. 12:1-12:56. p. 12:7.

[88] Ibídem.

informática, tipificada en el artículo 248.2. CP[89], centrándose principalmente en el elemento objetivo del engaño y la inducción a error que se dan por medio de esta práctica informática[90].

Sin embargo, una parte minoritaria de la doctrina entiende el phishing no puede llegar englobarse dentro del tipo de la estafa en atención al concepto manipulación informática que realiza la jurisprudencia[91] , donde entienden que el sistema informático debe de actuar "*a impulsos de una actuación ilegítima que puede consistir en la alteración de los elementos físicos de aquellos que permiten su programación, o por la introducción de datos falsos".*

Por lo tanto, esa parte de la doctrina entiende que no puede caber la conducta del phishing dentro de este tipo penal, ya que no llega a producirse una alteración de elementos físicos, ni la programación, ni introducción de elementos falsos para producir dicha manipulación informática.

Considerando que por medio del phishing el autor se apropia y hace uso de las claves para realizar una disposición patrimonial por medio de la red, sin que llegue a alterarse su programación, del mismo modo, entienden que para que se incurra en esta conducta, se debe de dar estas alteraciones[92].

4.2.3. El Pharming

El pharming consiste en la manipulación de las direcciones DNS o en los elementos de los equipos de los propios usuarios, por medio de la cual permite al autor redirigir un nombre de dominio a otro ordenador diferente, con la finalidad de engañar al usuario.

En este sentido, el pharming ataca a los servidores DNI; con la finalidad de cambiar la correspondencia numérica de los usuarios que lo utilicen. De esta forma, al cambiar este código el usuario puede considerar que se encuentra en una página web determinada, cuyo contenido es veraz y oficial, sin embargo, en la realidad, el sujeto se encuentra en una página web que ha sido creado por el delincuente, mediante la cual pretende obtener la información de la víctima[93].

Podemos observar diversos tipos de esta práctica delictiva, como puede ser los siguientes[94]:

- **Pharming local:** Se trata de la introducción de un malware en el sistema informático de la víctima, por medio de la cual se alterar los registros de los nombres que se encuentran en dicho sistema.

[89] MIRÓ LLINARES F. (2011). *Memento Práctico. Penal Económico y de la Empresa. 2011-2012.* Editorial Francis Lefebvre. p.484 y ss.
[90] Véase el apartado 4.2.1 relativo a la Estafa informática del presente trabajo.
[91] En este sentido, STS 539/2015 de 1 de octubre, STS 663/2009 de 30 de mayo.
[92] FERNÁNDEZ TERUELO, J. G. (2011). *Derecho penal e Internet: Especial consideración de los delitos que afectan a jóvenes y adolescentes*. Lex Nova. Valladolid. p.44.
[93] RECOVERY LABS. *Fraude en Internet: Del phishing al pharming.* Laboratorio de Recuperación de Datos Informáticos. p.2.
[94] Ibídem.

- **Drive-by:** Se produce un ataque contra el "Firewalls", con la finalidad de cambiar la dirección del servidor DNS de la víctima por el servidor DNS del sujeto activo.

- **DNS poisoning:** Hace uso de la vulnerabilidad de los servidores DNS sobre su control del cache de las direcciones de las páginas web.

En cuanto a su punibilidad, debemos de destacar que el pharming tiene un gran conjunto de similitudes con phishing, por lo que su tratamiento penal no varía en este sentido. De esta forma, se debe de castigar como un delito de estafa informática, tipificada en el artículo 248.2 CP[95].

[95] MIRÓ LLINARES F. (2011). *Memento Práctico. Penal Económico y de la Empresa. 2011-2012.* Editorial Francis Lefebvre. p.484 y ss.

Capítulo V: El agente encubierto en Internet

5.1. Concepto

De forma general podemos entender al agente encubierto como aquel funcionario de la Policía que se encarga de infiltrarse en organizaciones criminales con la finalidad de desarticularlas. No obstante, este concepto ha ido evolucionando y adaptándose a las nuevas circunstancias sociales, como son los avances tecnológicos, que conllevan nuevas técnicas de investigación, como son la interceptación de las comunicaciones, el uso de aparatos de video vigilancia, etcétera.

Como venimos señalando, la comisión de delitos informáticos ha mantenido una tendencia alcista en los últimos años, por lo que es necesario crear una nueva figura que trate de indagar y descubrir los delitos cometidos en la Red.

Por esta razón, el agente encubierto debe de trasladar sus actuaciones a Internet, donde debe de cambiar sus características y su modo de actuación para adaptarse a tales entornos virtuales sin llegar a perder su esencia[96]. De esta forma, el agente encubierto trata de infiltrarse en la Red para actuar desde una clandestinidad y bajo la sujeción de la ley.

Asimismo, podemos entender al agente encubierto en Internet como aquel empleado o funcionario público que, por decisión de una autoridad judicial, se infiltra en la Red, con el objetivo de obtener información sobre autores de determinados delitos que se llegan a producir por medio de la Red y que generan una elevada alarma a nivel social[97].

5.2. Regulación del agente encubierto en Internet

La regulación del agente encubierto se encuentra en el artículo 282 bis de la Ley de Enjuiciamiento Criminal, a tenor de la cual, se establece que el Juez puede autorizar a funcionarios de la Policía Judicial, a través de una resolución fundada y teniendo en cuenta la necesidad a los fines de investigación sobre la delincuencia organizada, a actuar bajo una identidad diferente, con lo que pueden adquirir, transportar los objetos, efectos e instrumentos del delito y diferir la incautación de estos.

De esta forma, el procedimiento del agente encubierto debe actuar tras una autorización previa por parte del Juez de instrucción correspondiente, la cual es fundamental para el procedimiento, ya que de no existir esta se podría llegar a vulnerar los derechos fundamentales del sujeto activo, por ello, siempre debe de existir esta autorización previa y un control posterior por parte del juez que la haya otorgado.

Así, por medio de esta autorización, el agente encubierto recibirá una identidad falsa por parte del Ministerio del Interior en un plazo de seis meses con carácter

[96] BUENO DE MATA F. (2012). *El agente encubierto en Internet: Mentiras virtuales para alcanzar la justicia.* Los retos del Poder Judicial ante la sociedad globalizada. Actas del IV Congreso Gallego de Derecho Procesal. pp. 295-306. p.296.
[97] Ibídem.

prorrogable por la que se le dotará de una identidad falsa que puede llegar a utilizar dentro de los foros o webs que deba investigar[98].

Cabe destacar que esta identidad falsa en la Red es muy distinta respecto a los requisitos que puede llegar a exigir una nueva identidad para la investigación de aquellos delitos que se cometen fuera del ámbito de los sistemas informáticos, ya que se elimina la parte física de la infiltración del agente encubierto.

En este sentido, el primer problema lo encontramos en que dicho artículo limita la actuación del agente encubierto aquellos delitos realizados a través de la delincuencia organizada. Asimismo, se establece un sistema de números clausus sobre los delitos que puede llegar a aceptar la participación de un agente encubierto, lo que llega a generar una gran cantidad de problemas prácticos[99].
Como se puede observar, esta regulación limita en gran medida las actuaciones por parte del agente encubierto en los delitos informáticos, ya que no se llegan a establecer todos aquellos delitos que pueden ser cometidos a través de la Red.

En general, la investigación que puede realizar un agente en la Red no puede llegar a vulnerar los derechos fundamentales del sujeto activo, ya que dicho agente se centra la persecución de pistas y rastros informáticos que el delincuente abandona, por lo que no se trata de información privada ni intima. Por lo cual, dicha información que el sujeto activo realiza por medio de su telecomunicación no puede considerarse formalmente protegida, cuyo secreto debe guardarse, ni se trata de datos protegidos automatizada mente[100].

Por ello, dicha exposición del delincuente supone una cesión de su información, por lo que su investigación no supondría la vulneración e los derechos fundamentales del infractor, ya que el autor decide hacer público la información y el contenido en la Red, teniendo estos, por lo tanto, un acceso libre.

No obstante, hay que insistir que en aquellos casos en los que se puede llegar a afectar algún derecho fundamental, el agente encubierto debe de solicitar al órgano judicial competente las autorizaciones necesarias.

En la práctica, el derecho fundamental que puede llegar a vulnerar esta actuación del agente encubierto en Internet versa sobre el derecho al secreto de las telecomunicaciones, el cual puede llegar a afectar en muchas ocasiones por medio de la investigación del agente encubierto sobre los correos electrónicos o chats

---

[98] BUENO DE MATA F. (2012). *El agente encubierto en Internet: Mentiras virtuales para alcanzar la justicia.* Los retos del Poder Judicial ante la sociedad globalizada. Actas del IV Congreso Gallego de Derecho Procesal. pp. 295-306.

[99] En este sentido, el artículo 282 bis.4 establece los siguientes delitos: a) Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos. b) Delito de secuestro de personas. c) Delito de trata de seres humanos d) Delitos relativos a la prostitución. e) Delitos contra el patrimonio y contra el orden socioeconómico. f) Delitos relativos a la propiedad intelectual e industrial. g) Delitos contra los derechos de los trabajadores. h) Delitos contra los derechos de los ciudadanos extranjeros. i) Delitos de tráfico de especies de flora o fauna amenazada) Delito de tráfico de material nuclear y radiactivo. k) Delitos contra la salud pública. l) Delitos de falsificación de moneda y de falsificación de tarjetas de crédito o débito o cheques de viaje. m) Delito de tráfico y depósito de armas, municiones o explosivos. n) Delitos de terrorismo. o) Delitos contra el patrimonio histórico.

[100] VELASCO E. (2010). *Diligencias de investigación penal.* Delitos cometidos a través de Internet. 1º Edición. Editorial La Ley. Junio 2010. p.70.

privados del investigado, así como aquellos datos privados que se han revelado durante las conversaciones cerradas del mismo[101].

Por lo tanto, en estos casos, una correcta autorización judicial llega a cubrir la actuación del agente encubierto que obtiene dicha información protegida, por lo que dicho agente se encontrará exento de responsabilidad por sus actuaciones investigadoras.

5.3. Modo de actuación del agente encubierto en Internet

Como ya hemos comentado anteriormente, el agente encubierto debe de actuar bajo una autorización judicial en los casos en los que se requiera, con la finalidad de no vulnerar ningún derecho fundamental del sujeto activo[102].

Posteriormente a tal autorización, el agente encubierto recibirá una identidad falsa, la cual se centrará en la creación de un perfil falso que le permita acceder a foros y páginas webs sin mostrar su verdadera identificación en la Red, de esta forma, el agente encubierto debe de ganar la confianza de tales cibercriminales y tratar de recabar toda la información y documentación necesaria para poder imputar posteriormente a dicho sujeto. Por lo tanto, cabe destacar que todos los elementos relativos a la identidad falsa del agente deben de ir encaminado a familiarizarse con los cibercriminales.

Asimismo, todos los datos que deba de facilitar para acceder a tales webs o foros serán facilitados por el mismo Ministerio del Interior, con la finalidad de llevar un control del agente encubierto, de esta forma[103].

No obstante, el principal problema de estos agentes se encuentra en que, en algunas ocasiones, los cibercriminales, solicitan contenidos de carácter ilícito y relativo a sus actuaciones delictivas a los usuarios que se comunican en la Red con la finalidad de confiar en él[104]. El problema principal, incide en que la remisión de este contenido por parte del agente encubierto puede hacer que tales objetos lleguen a ser redistribuidos por toda la Red.

En este caso, la figura del agente encubierto encuentra su primer problema legal, ya que el agente no puede proceder a distribuir dichos contenidos ilícitos. Por lo que, en aras de solventar dicha situación, se ha propuesto que dicho materia sea

---

[101] VELASCO E. (2010). *Diligencias de investigación penal.* Delitos cometidos a través de Internet. 1º Edición. Editorial La Ley. Junio 2010. p.710.

[102] BUENO DE MATA F. (2012). *El agente encubierto en Internet: Mentiras virtuales para alcanzar la justicia.* Los retos del Poder Judicial ante la sociedad globalizada. Actas del IV Congreso Gallego de Derecho Procesal. pp. 295-306. p.301 y ss.

[103] BUENO DE LA MATA F (2012). *Un centinela virtual para investigar delitos cometidos a través de las redes sociales: ¿deberían ampliarse las actuales funciones del agente encubierto en Internet?* El proceso penal en la sociedad de la información: Las nuevas tecnologías para investigar y probar el delito. 1º Edición. Editorial La Ley. Madrid. Junio 2012. p.6.

[104] En este caso, podemos ejemplificarlo con el caso de los pederastas, los cuales solicitan contenidos de este tipo a los usuarios con los que se comunica para confiar de que se encuentra ante alguien con los mismos gustos que ellos.

"camuflado", los cuales aparentemente pueden simular que su contenido es objeto de delito, sin embargo, su completamente licito[105].

Del mismo modo, otra de las soluciones puede recaer en establecer un filtro para que este contenido no pueda distribuirse desde otro sistema informático que no sea propiedad de los órganos y miembros que llevan tal investigación.

Así, en tales circunstancias, parece reflejar la figura del agente encubierto puede encontrarse que colisiona con el agente provocador, sin embargo, atendiendo a la Sentencia del Tribunal Supremo número 793/2013 de 28 de octubre, se establece el verdadero contenido de dicho agente provocador el cual trata de inducir a realizar una determinada acción ilícita a alguien que no tenía intención de realizarla.

En esta misma línea jurisprudencial, podemos nombrar igualmente la Sentencia del Tribunal Supremo número 359/2014 de 13 de mayo, la cual establece no puede existir delito provocado cuando el agente encubierto tiene indicios de la existencia de una actividad delictiva previa y su actuación se centra en obtener información y pruebas al respecto.

Por lo tanto, al existir una relación previa con el investigado y comprobar que se ha llegado a producir un determino delito, el hecho de que el agente encubierto remita contenido ilícito al cibercriminal, no podría originar en dicho sujeto activo el nacimiento de la voluntad para la realización de un hecho delictivo, ya que esta voluntad ha existido previamente y de forma independiente a la infiltración del agente[106].
En esta misma línea, consideramos importante comentar aquella situación que puede llegar a producirse cuando el agente encubierto descubre nuevos delitos a los que estaba investigando en el ejercicio de su investigación. En estos casos, debemos recordar que el agente encubierto actúa tras una autorización judicial para realizar unas actuaciones concretas tras una identidad falsa, por medio de la cual le va a otorgar una cobertura en la actuación engañosa e investigadora del agente.

Así en estos casos, la doctrina entiende que dicha autorización judicial previa le da permisibilidad al agente encubierto de todas las actuaciones que pueda llegar a derivarse de la identidad supuesta del agente, a pesar de que tales actuaciones puedan suponer una limitación de los derechos fundamentales del investigado. Pero hemos de reseñar, que en aquellos casos en que dicha actuación en el descubrimiento de nuevos delitos suponga un "plus de lesividad" sobre el investigado, la actuación del agente no podrá verse amparada por la autorización previa que le permite actuar con una identidad falsa, sino que se requerirá una autorización judicial previa que justifique la restricción del derecho fundamental concreto[107].

---

[105] Siguiendo en el ámbito de la pederastia, podemos ejemplificarlo con el envío de material pornográfico en el que aparezcan actores y actrices que simulen ser menores de edad, sin embargo, en la realidad son adultos.
[106] BUENO DE LA MATA F (2012). *Un centinela virtual para investigar delitos cometidos a través de las redes sociales: ¿deberían ampliarse las actuales funciones del agente encubierto en Internet?* El proceso penal en la sociedad de la información: Las nuevas tecnologías para investigar y probar el delito. 1º Edición. Editorial La Ley. Madrid. Junio 2012. p. 7.
[107] ZAFRA ESPINOSA DE LOS MONTEROS R (2010). El policía infiltrado: los presupuestos jurídicos en el proceso penal español. Editorial Tirant lo Blanch. p.348.

En este caso, el requisito de la autorización judicial adicional se dará en los supuestos en los que el agente encubierto deba de realizar una intervención de las comunicaciones privadas del investigado, en los demás supuestos en los que el descubrimiento de nuevos delitos se produzca por su normal actuación que la faculta su identidad supuesta, no se requería ningún requisito adicional, ya que este nuevo delito se ha descubierto por medio de un nexo causal necesario por la actuación del agente.

5.4. El agente encubierto en Internet en la lucha contra el terrorismo yihadista.

El terrorismo yihadista se ha convertido en la actualidad en una amenaza real que atenta contra los principios básicos que rigen en un Estado de Derecho [108], en este sentido, hay que destacar que esta clase de terrorismo encuentra una importante particularidad en su carácter transnacional o global, que hacen que esta forma de violencia no solamente tenga unos efectos sobre un Estado en concreto, sino que se produce una amenaza a nivel internacional, lo que provoca una alta imprevisibilidad[109].

Sin embargo, una de las características más llamativas del terrorismo yihadista se centra en su alto uso de Internet y redes sociales más importantes como son Facebook, Twitter y YouTube, así como en gran cantidad de blogs. Realmente estos instrumentos no solamente son utilizados para ampliar su publicidad, sino que tratan de buscar unos objetivos principales como son[110]:

- El reclutamiento de nuevos miembros yihadistas por medio de campañas de publicidad.
- La incitación al terrorismo a través de la provocación pública.
- La radicalización de usuarios virtuales por medio del adoctrinamiento para su conversión en reclutas.

Como se puede observar, el agente encubierto en Internet tiene una importante función en la lucha contra el terrorismo yihadista por medio de su investigación en la red. De esta forma, la función de esta figura se centra en la búsqueda de todo rastro online que pueda publicar esta organización terrorista, para posteriormente proceder a su cierre y bloqueo.

Sin embargo, en la práctica es frecuente que, tras dicho cierre, los administradores o creadores de tales webs terroristas modifiquen el nombre de su página web o de su Red social y se establezcan en otro alojamiento para continuar con sus actividades delictivas.

[108] MUSACCHIO V. (2005). Instrumentos de lucha contra el terrorismo en Derecho Penal Europeo. Actualidad Jurídica Aranzadi. Nº 665. p.6.
[109] CANO PAÑOS M.A. (2009). Perfiles de autor del terrorismo islamista en Europa. Revista electrónica de ciencia penal y criminología. 11. Vol. 7.p.2
[110] LEJARZA ILLARA (2015). Terrorismo islamista en las redes – La yihad electrónica. IEEE. Instituto Español de Estudios Estratégicos. (100/2015). P.4.

Capitulo VII: Conclusiones

1. Se observa un crecimiento de la cibercriminalidad y de los delitos informáticos en términos nacionales e internacionales a causa del crecimiento del uso y desarrollo de las TICs.
   No existe un concepto legislativo sobre la cibercriminalidad o sobre los delitos informáticos, ya que nuestro Código Penal entiende esta clase de delitos como una modalidad de realización de un hecho delictivo por medio de TICs en los delitos tradicionales. En este sentido, consideramos que, debido a la constante evolución de esta clase delictiva, en el futuro tal vez sería conveniente establecer un apartado concreto donde se englobe todas las conductas posibles.

2. Hay una problemática respecto a la determinación del bien jurídico protegido. Por un lado, parte de la doctrina y la legislación considera que el único bien protegido se centra en aquellos bienes jurídicos tradicionales que se vulneran por la utilización de un sistema informático durante la comisión del hecho delictivo. Por otro lado, otra parte de la doctrina entiende que los delitos informáticos deben de proteger bienes individualizables y concretos, por lo que es necesario determinar un bien jurídico protegido en relación con la libertad y la seguridad informática.
   Se entiende que los delitos informáticos hacen uso de tecnología y sistemas tecnológicos para cometer un determinado hecho delictivo, sin embargo, consideramos que en la actualidad los sistemas informáticos han llegado a convertirse en una herramienta personal y necesaria en nuestra vida cotidiana, por ello, entendemos que hay que atender también a la seguridad informática como bien jurídico protegido. Por dicha razón, tal vez podría castigarse como agravante el uso de sistemas informáticos para la comisión de un hecho delictivo, ya que su conducta puede llegar a atentar contra dos bienes jurídicos diferentes.

3. Es de gran importancia el Convenio Europeo 1853/23 conocido como el “Convenio sobre la ciberdelincuencia”, el cual supone un instrumento de lucha y de cooperación internacional en la cibercriminalidad.

4. La legislación española ha actuado con retraso en materia de regulación de los delitos informáticos en comparación con los países de nuestro entorno a causa de una falta de desarrollo histórico de nuestra Estado.
   A pesar de que la cibercriminalidad se regula principalmente en nuestro Código Penal, encontramos una gran cantidad de diversa normativa que ha ido desarrollando esta clase de delitos -como la Ley de Propiedad Intelectual o la Ley de Protección de Datos de Carácter Personal-.
   La doctrina diferencia los delitos informáticos en tres tipos principales en función de su naturaleza: Los delitos cibereconómicos, los delitos ciberintrusivo y los delitos de ciberterrorismo.

5. Se puede observar una alta regulación penal de estas conductas, sin embargo, en algunos casos, como en los delitos cibereconómicos se podría dar una respuesta por medio de otras vías, como es el caso de la administrativa o civil.

6. Como se puede volver a observar con la clasificación de esta clase de delitos, el legislador no concede a los delitos informáticos un bien jurídico protegido determinado, sino que lo vincula como un medio para cometer delitos tradicionales por medio de sistemas informáticos.

7. El delito de suplantación de identidad regulado en el artículo 401 CP*, se* entiende como un delito instrumental para llegar a cometer posteriormente otro diferente, como es el caso de la estafa, falsedad documental, etcétera.
   A pesar de que no lleguen a imputarse por medio del artículo 401 CP, existe una gran cantidad de medios informáticos para llegar a suplantar la identidad de un sujeto a través de la red, como es el caso del spoofing, el phising y el pharming.

8. Consideramos que en la práctica los usuarios virtuales no son realmente conscientes de los riesgos que conlleva el uso de estos sistemas informáticos, por lo que entendemos que sería conveniente tratar de impedir o reducir dichos riesgos por medio de la prevención primaria del delito y fomentar la conciencia de estos usuarios para que actúen con una mayor diligencia.

9. La regulación actual del agente encubierto no puede llegar a cubrir las necesidades para la investigación de los delitos informáticos. En este sentido, consideramos que la utilización de una numeración cerrada de los supuestos en los que quepa la actuación del agente encubierto, limita en gran cantidad la lucha contra estos delitos informáticos, por lo que sería beneficioso una modificación legislativa que tenga en cuenta el carácter de anonimato que otorga la Red y la necesidad de investigar estos delitos por medio de un agente encubierto en la red.

10. La actuación del agente encubierto en la Red por la que distribuye contenidos de carácter ilícito con la finalidad de investigar a los cibercriminales, no puede llegar a considerarse como un delito de provocación, ya que dicho agente no llega a afectar a la voluntad de delinquir del sujeto activo, debido a que tal voluntad ya existía de forma previa a la intervención del agente encubierto.

Bibliografía

Manuales y Artículos

- AZCONA ALBARRÁN C. D. (2012). *Tarjetas de pago y Derecho penal: Un modelo interpretativo del art. 284.2. c) CP.* Atelier Libros.
- BAJO M. (1982). *Protección del honor y de la intimidad.* Comentarios a la Legislación Penal. Tomo I. Editorial Erdesa.
- BALUJA, W. (2009). Los ataques spoofing. Estudio de sus manifestaciones más comunes. Revista Ingeniería Eléctrica, Automática y Comunicaciones. Vol. 22. Nº. 2. p. 3.
- BARRIO ANDRÉS M (2011). *Los delitos cometidos en Internet. Marco comparado, internacional y derecho español tras la reforma penal de 2010.*La Ley Penal. Nº. 86. Sección Legislación aplicada a la práctica. Octubre 2011. Editorial La Ley.
- BUENO DE LA MATA F (2012). *Un centinela virtual para investigar delitos cometidos a través de las redes sociales: ¿deberían ampliarse las actuales funciones del agente encubierto en Internet?* El proceso penal en la sociedad de la información: Las nuevas tecnologías para investigar y probar el delito. 1º Edición. Editorial La Ley. Madrid. Junio 2012
- CANO PAÑOS M.A. (2009). Perfiles de autor del terrorismo islamista en Europa. Revista electrónica de ciencia penal y criminología. 11. Vol.7 p. 2
- COBO DEL ROSAL M (2004). *Instituciones de Derecho penal español Parte general.* Editorial CESEJ. Madrid. 2004.
- COTINO HUESTO L. (2007). *Retos jurídicos y carencias normativas de la democracia y la participación electrónicas.* Revista Catalana de Dret Públic. Nº. 35. pp. 75-120.
- DAVARA RODRÍGUEZ M.A. (2016). *Los delitos informáticos.* El consultor de los Ayuntamientos. Nº. 15. Sección Zona Local / Nuevas tecnologías. Editorial Wolters Kluwer. pp. 1825-1830.

- DE LA MATA BARRANCO. N.J. (2007). *Cuadernos penales José María Lidón. Delitos e informática: Algunos aspectos. Número 4.* Edita. Universidad de Deusto. Bilbao.
- DE URBANO CASTRILLO E. (2011). *Los delitos informáticos tras la reforma del CP de 2010.* Revista Aranzadi Doctrinal. Nº. 9/2011. Parte Estudio
- ESTRADA GARAVILLA M. (2008). *Delitos informáticos.* Universidad Abierto de México.
- FARALDO CABANA P. (2010). *Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico.* Revista de Derecho penal y criminología. 3º Epoca. Nº. 3.
- FERNÁNDEZ TERUELO, J. G. (2011). *Derecho penal e Internet: Especial consideración de los delitos que afectan a jóvenes y adolescentes*. Lex Nova. Valladolid.
- FLORES MENDOZA F. (2014). *Respuesta Penal al denominado robo de identidad en las conductas del Phishing Bancario.* Estudios penales y criminológicos. Vol. 48. pp. 301-340.

- GALLEGO CENOZ J. (2016). *Primera condena por el nuevo delito de "stalking"*. Revista Aranzadi Doctrinal. Nº.6/2016. Fichas de Jurisprudencia. p.2.
- GONZÁLEZ HURTADO J.A. (2013). Delincuencia Informática: Daños informáticos del artículo 264 del Código Penal y propuesta de reforma. Tesis doctoral. Universidad Complutense de Madrid.
- GONZÁLEZ HURTADO J.A. (2014). *Un nuevo bien jurídico protegido en el uso y disfrute de la tecnología: la seguridad en los sistemas de información.* La Ley Penal. Nº. 107. Sección Estudios. Marzo-abril.
- GONZÁLEZ RUS J.J. (1999). *Protección penal de sistemas, elementos, datos, documentos y programas informáticos.* Revista electrónica de ciencia penal y criminología. Nº. 1.
- LORES, Y. V. (2013). *Seguridad Informática en la formación de profesionales*. Serie Científica-Universidad de las Ciencias Informáticas. Vol. *6. Nº.*5.
- LEJARZA ILLARA (2015). Terrorismo Islamista en las redes – La yidad electrónica. IEEE. Instituto Español de Estudios Estratégicos. (100/2015). p.4
- MATA Y MARTÍN R. (2003). *Criminalidad informática: Una introducción al cibercrimen*. Actualidad Penal. Nº. 37. Sección Doctrina. Semana del 6 al 12 de octubre de 2003. Editorial la Ley.
- MINISTERIO DEL INTERIOR. (2015). *Estudio sobre la cibercriminalidad en España 2015.*
- MIRÓ LLINARES F. (2011). *Memento Práctico. Penal Económico y de la Empresa. 2011-2012.* Editorial Francis Lefebvre.
- MIRÓ LLINARES F. (2013). *La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phising.* Revista electrónica de ciencia penal y criminología (en línea). Nº.15-12. pp. 12:1-12:56.
- MORAIS GALLEGO J.M. (2006) *Las nuevas tecnologías de la información y de la comunicación. Implicaciones legales.* Revista galega de Ensino. Vol. 14. Nº. 48. Marzo 2006.
- MUSACCHIO V. (2005). Instrumentos de lucha contra el terrorismo en Derecho Penal Europeo. Actualidad Jurídica Aranzadi, Nº 665. p.6
- MUÑOZ, A. G. (2010). *El Robo de Identidad: aproximación a una nueva y difusa conducta delictiva*. Robo de identidad y protección de datos. Editorial Aranzadi. pp. 169-198.
- NORTON (by Symantec) (2013) *Reporte Norton 2013.*
- OXMAN N. (2013). *Estafas informáticas a través de Internet: Acerca de la imputación penal del "phising" y el "pharming".* Revista de Derecho de la Pontificia Universidad Católica de Valparaiso. Nº. XLI. pp. 211-262.
- RECOVERY LABS. *Fraude en Internet: Del phishing al pharming.* Laboratorio de Recuperación de Datos Informáticos.
- REYNA ALFARO L.M. (2002). *La criminalidad informática: cuestiones para una reflexión inicial.* Actualidad Penal. Nº. 21. Sección Doctrina. 2002. Tomo 2. Editorial La Ley. pp. 525- 542.
- RODRÍGUEZ RAMOS L. (Dir.) (VVAA) (2009). *Código Penal. Comentado y con Jurisprudencia.* Editorial La Ley. 3º Edición.
- SÁNCHEZ BRAVO A. (2003). *El convenio del consejo de Europa sobre Cibercrimen: Control versus Libertades públicas.* Diario La Ley. Nº. 5528. Sección Doctrina. Abril de 2002. pp.1851-1866.
- VALDIVIA CHERNOZIOMOVA M. (2011). Propuesta de modificaciones al tratamiento legal que reciben las conductas delictivas generadas por la criminalidad en Cuba. Universidad de Sancti Spiritus.

- VELASCO NUÑEZ E. (2010). Diligencias de investigación penal. Delitos cometidos a través de Internet. 1º Edición. Editorial La Ley. Junio 2010.
- VELASCO NUÑEZ E. (2015). Los delitos informáticos. SEPÍN Editorial Jurídica. Nº.81. diciembre 2015. pp. 14-28.
- VILLALÓN HUERTA A. (2002). *Seguridad en Unix y Redes. Versión 2.1.* GNU Free Documentation License..

Legislación Nacional:

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 14/1999, de 17 de septiembre, sobre firma electrónica.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de protección de datos de carácter personal.
- Real Decreto Legislativo 1/1996 de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.

Legislación Internacional:

- Convenio Europeo 185/23 de 23 de septiembre de 2001
- Directiva 2016/1148 del Parlamento Europeo y del Consejo de 6 de Julio de 2016 sobre ciberseguridad.

Jurisprudencia

A) Sentencias del Tribunal Supremo.

Sentencia del Tribunal Supremo número 8368/1991, de 26 de marzo.
Sentencia del Tribunal Supremo, número 663/2009, de 30 de mayo.
Sentencia del Tribunal Supremo, número 635/2009, de 15 de junio.
Sentencia del Tribunal Supremo, número 739/2013, de 28 de octubre.
Sentencia del Tribunal Supremo, número 359/2014, de 13 de mayo.
Sentencia del Tribunal Supremo, número 539/2015, de 10 de octubre.

B) Sentencias de la Audiencia.

Sentencia Audiencia Provincial de Sevilla de 23/5 del 2.000.
Sentencia Audiencia Provincial de Madrid de 5/12 del 2000.
Sentencia Audiencia Provincial de Albacete de 9/5 del 2002.
Sentencia Audiencia Provincial de Huesca 137/2012 del 7 de septiembre.
Sentencia Audiencia Provincial de Sevilla 46/2015 del 18 de junio.
Sentencia Audiencia Provincial de Sevilla 432/2015 de 30 de julio.