FACULTAD DE DERECHO

UNIVERSIDAD DE LEÓN

CURSO 2020/2021

ASPECTOS TÉCNICOS DEL DELITO DE PHISHING

VINCULADOS A LOS ELEMENTOS DEL ORDENAMIENTO JURÍDICO

GRADO EN DERECHO

AUTORA: D. BLANCA IRIS SANTOS SÁNCHEZ

TUTOR: D. JOSÉ MANUEL ALIJA PÉREZ
COTUTOR: D. JUAN CARLOS MARÍA CANTILLO ARCÓN

Tabla de contenido

ÍNDICE DE ABREVIATURAS

Art/s	Artículo/s
Coord/s	Coordinador/es
BJP	Bien Jurídico Protegido
BOE	Boletín Oficial del Estado
CE	Constitución Española
CP	Código Penal
Dir/s	Director/es
DM	Decisión Marco
Ed	Edición
EEUU	Estados Unidos
INCIBE	Instituto Nacional de Ciberseguridad
LO	Ley Orgánica
LOPJ	Ley Orgánica del Poder Judicial.
NNUU	Naciones Unidas
Núm.	Número
OEDI	Observatorio Español de Delitos Informáticos
ONU	Organización de las Naciones Unidas
SAP	Sentencia de la Audiencia Provincial
SA	Sujeto Activo
SP	Sujeto Pasivo
STS	Sentencia del Tribunal Supremo
TIC/s	Tecnología/s de la Información y Comunicación
TJUE	Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
VPNs	Virtual Private Network

UE	Unión Europea
URL	Uniform Resource Locator (Localizador de Recursos Uniforme)

"CICERÓN: DUOBUS MODIS FIT INIURIA, AUT VI AUT FRAUDE."

RESUMEN

El incesante avance tecnológico, y la intromisión de estos en la vida cotidiana de las personas, hacen del ciberespacio el hábitat delictivo idóneo[1] para perpetrar diferentes ataques a bienes jurídicos protegidos tradicionalmente, demostrando la vulnerabilidad de los usuarios frente a los ataques ejecutados a través del ciberespacio y multiplicando las oportunidades de los delincuentes.[2]Convirtiéndose en el 10% de las infracciones penales denunciadas[3], en 2019 se cerró el año con 218.302 delitos cometidos en internet con un aumento del 35,8% en relación con el 2018.

El Derecho Penal ha sabido responder a este novedoso problema: la"ciberdelincuencia"[4], creando tipos nuevos o adaptando los que ya se encontraban en el CP, el delito que incumbe este trabajo está recogido en el art.248.2 denominándose estafa informática.Ésta modalidad tiene una serie de subterfugios técnicos que la caracterízan, adquiriendo especial importancia la ingeneria social.

Palabras clave: Ciberespacio, Ciberdelincuencia, Phishing, delitos informáticos.

[1] GABINETE DE COORDINACIÓN Y ESTUDIOS. SECRETARÍA DE ESTADO DE SEGURIDAD: *Estudio sobre la Cibercriminalidad en España* [Link][10/03/2021]

[2]OBSERVATORIO ESPAÑOL de DELITOS INFORMÁTICOS:*Estadisticas de evolución* [Link] [16/02/2021]

[3] LÓPEZ FONSECA, Oscar:*Los ciberdelitos son ya el 10% de las infracciones penales conocidas.* [Link] [24/04/2021]

[4] *Sobre la diferencia entre el delito informático (que se vale de elementos informáticos para la perpetración y el Ciberdelito (que se refiere a una posterior generación delictiva vinculada a las TIC en el que interviene la comunicación telemática abierta, cerrada o de uso restringido)*Vid.ROMEO CASABONA, Carlos: *De los delitos informáticos al cibercrimen, una aproximación conceptual y político-criminal*. Granada: Comares, 2006.pág.1-42.

ABSTRACT

The incessant technological advance, and the interference of it in the daily lives of people, make cyberspace the ideal criminal habitat to perpetrate different attacks on traditionally protected legal assets, demonstrating the vulnerability of users to attacks carried out through cyberspace and multiplying the opportunities for criminals. Becoming 10% of the criminal offenses reported, 2019 ended the year with 218,302 crimes committed on the internet, an increase of 35.8% compared to 2018.

Criminal Law has been able to respond to this novel problem: "cybercrime", creating new types or adapting those that were already in the CP, the crime that this work is responsible for is included in article 248.2 called computer scam. This modality has a series of technical subterfuges that characterize it, social engineering acquiring special importance.

Keywords: Cyberspace, Cybercrime, Phishing, computer crimes.

OBJETO DEL TRABAJO

En un contexto social donde la tecnología es un condicionante vital, la hiperconectividad y la globalización a través de la red es algo inevitable, no es de extrañar que el ciberespacio se haya convertido en un foco de delincuencia.[5] Así, internet es considerado como "el corazón de un nuevo paradigma socio técnico que constituye, en realidad, la base material de nuestras vidas y de nuestras formas de relación, trabajo y comunicación. Lo que hace el internet es procesar la virtualidad y transformarla en nuestra realidad, constituyendo la sociedad red, que es la sociedad en la que vivimos"[6] .

Esta sociedad se encuentra al alcance de todos por el simple hecho de tener acceso a un Smartphone, una Tablet, un ordenador o cualquier otro dispositivo electrónico. Estos dispositivos no son, en términos morales, ni buenos, ni malos, sino meros instrumentos que cumplen su función; al igual que todas las innovaciones. Por un lado, solventan problemas de la sociedad y la ayudan en su desarrollo, y por el otro, pueden ser un instrumento para cometer acciones punibles causando daños y perjuicios a terceros.[7]

Los riesgos ya no están limitados espacial, temporal y socialmente, tampoco son imputables por las reglas vigentes de causalidad, culpabilidad y responsabilidad; así BECK, en su obra "*La metamorfosis del mundo"* describe nuestra sociedad como una "sociedad del riesgo"[8]. El avance vertiginoso hacia las TICs vinculadas no solo a la informática y al internet, sino también a las tecnologías disruptivas[9], como son el blockchain, la robótica o la inteligencia artificial[10],van abriendo paso a un nuevo concepto: "los datos personales son el petróleo del siglo XXI"[11]. Al igual que las grandes empresas como Google, Amazon, Facebook etc., se han dado cuenta de esto, creando un sistema complejo de ingeniería social basada en la recopilación de datos personales con

[5] ALMENAR PINEDA, Francisco: *Ciberdelincuencia, Teoría y práctica.* Oporto: Jurúa, 2018.pág.18-20.
[6]CASTELLS OLIVAN, Manuel: *La galaxia de internet, reflexiones sobre internet, empresa y sociedad.* Barcelona: Plaza & Janes, 2001. pág.38.
[7]BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos.* Madrid: Wolters Kluwer, 2018.pág.17- 19.
[8] ULRICK BECK: Riesgo digital ,el fracaso de las instituciones funcionales. En: *La metamorphosis del mundo.* Barcelona: Paidós, 2017.pág.163-173.
[9] Vid. CHRISTENSERN, Clayton: *The innovator's dilemma: when the technologies cause great firms to fail*. Boston: Harvard Business Review Press, 1997.
[10] Vid. BARRIO ANDRÉS, Moisés: *Derecho de los Robots.* Madrid: Wolters Kluwer, 2018.
[11] WEIGEND, Andreas: [18/02/2021][Link] Experto internacional de Big Data y analítica de consumo, Ex Chief Scientist de Amazon.

fines comerciales; los ciberdelincuentes no se quedan atrás, saben cómo aprovechar esta ingeniería social y lucrarse con ella.

Esta ingeniería social que se menciona consiste en un conjunto de técnicas realizadas por un tercero o cibercriminal, que obliga a los usuarios o futuras victimas a hacer o no hacer una determinada conducta, basada en el engaño, que individualmente y sin esa incidencia del tercero, no les hubiese surgido hacer, consiguiendo así el envío de datos sensibles o la infección de sus computadoras, entre otros. Los sistemas de detención son cada vez más complejos, implementando mejores medidas que los hacen más difíciles de vulnerar, por lo que los hackers buscan el "eslabón perdido". Este eslabón es el ser humano, que, debido a la poca sensibilización de la sociedad respecto a los malos usos de los dispositivos electrónicos, crea peligros potenciales con acciones tan simples como el acceso a redes sociales o las compras online. De esta forma se comparten datos personales, de carácter económico y confidencial, que antes de la aparición de las TICs eran prácticamente imposible de conseguir para los delincuentes[12].

El Derecho Penal y procesal penal se han visto involucrados al surgir este tipo de delincuencia, suponiendo su comparación con los delitos tradicionales, un gran reto. No obstante, como una primera afirmación, se podría decir que, "todo lo que es ilegal en el mundo real lo es en el virtual, las conductas no quedan exentas por el hecho de pasar por la red. Es por ello, que se exige una respuesta penal específica para estas conductas, la cual se debe abordar tanto a nivel nacional como supranacional".[13]

La actividad delictiva en la red abarca multitud de formas diferentes y que están en constante evolución, algunos ejemplos son: el acceso e interceptación ilícita, la interferencia en los datos y en el sistema, la falsificación informática, el fraude, delitos sexuales, contra la propiedad industrial e intelectual, contra el honor, contra la salud pública, amenazas y coacciones. Los datos que nos proporciona la OEDI señalan que cada año se incrementan los delitos informáticos, teniendo en 2011 una incidencia de 37.458 casos y cerrando el 2019 con 218.302 casos, siendo los de mayor relevancia los denominados fraudes informáticos[14].

[12]Vid. THE OPEN WEB APPLICATION SECURITY PROJECT: [09-03-21][Link]INZUNZA ROJAS, Gustavo Eduardo: *Ingeniería social, hacking psicológico*. [09/03/2021][Link]

[13] Vid BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pág.27-30/ ALMENAR PINEDA, Francisco:*Ciberdelincuencia… ob. cit.*pág.20-21.

[14] OEDI: [30/04/2021][Link]

Dentro de estas nuevas figuras delictivas se ha de considerar el phishing como una de las de mayor impacto económico y social, ya que a pesar de remontarse su origen a veinticinco años atrás, se encuentra en constante evolución[15] y con mayor relevancia social.

El objeto fundamental de este trabajo se centra en la investigación del "phishing" y el como se adecuan sus aspectos y dinámica al tipo de delito de estafa informática, llevado a cabo a través de las TICs. Desde un punto de vista general, se analizarán las clases de phishing y las diferentes formas de entrada de los ciberdelincuetes en nuestros dispositivos.

[15] ALMENAR PINEDA, Francisco: *Ciberdelincuencia… ob. cit.*pág.60 / ALMENAR PINEDA, Francisco: *El delito de hacking.* Oporto: Jurúa, 2018.pág. 40-41.

METODOLOGIA

En el proceso de elaboración de este documento he trabajado en dos disciplinas transversales por un lado el derecho como parte integrante de las ciencias sociales, que estudia los hechos, procesos y grupos en los que participa el hombre en sociedad y tiene su particularidad como disciplina científica, esto es la dogmática jurídico penal, que lo obliga a una delimitación concreta de su objeto de estudio. Por otro lado, está fundamentado en la Informática Jurídica como parte de la ciencia del tratamiento racional y automático de la información de contenido jurídico.

1.-Seleccion del tutor, tema y puntos clave a tratar.

En un primer momento, se eligió al profesor que ejercería como tutor del presente trabajo, comunicándole el deseo de abordar cuestiones relacionadas con la ciberdelincuencia. Posteriormente, entre tutor y estudiante, se elaboró una lista conjunta sobre los posibles temas a tratar y con miras a elegir el delito informático más apropiado, debido a la amplia gama que existe. A continuación, la estudiante diseñó una propuesta de trabajo para que fuera supervisada, y es en este momento cuando el tutor sugirió centrarse en el delito de *phishing.* Después de varias reuniones con el tutor y debido a que era necesario una mayor incidencia en el ámbito penal, la estudiante contactó con el departamento de derecho penal y con el decano para la asignación de un cotutor que pudiese solventar los problemas en el marco legal que se estaban planteando. Teniendo así un tutor en materia técnica informática y un cotutor en materia legal, dejando clara la transversalidad del estudio.

2.-Fuentes de información y documentación.

Tras las pertinentes correcciones y sugerencias, el cotutor indicó la bibliografía necesaria para la elaboración del documento final, dotando a la estudiante de la doctrina pertinente para la realización del estudio. Procediendo así a la lectura de los libros recomendados y a la normativa legal relacionada. El tutor dotó a la estudiante de los documentos necesarios en materia técnica, y las páginas web relacionadas con la cuestión y datos estadísticos del OIDE.

3.-Redaccion del texto.

Una vez realizada la fase anterior, la estudiante realizó una reflexión de los aspectos estudiados y procedió en virtud de los mismos, a redactar el presente documento con la mayor coherencia posible, tomando como hilo conductor la estafa informática y la figura delictiva del phishing, que se introduce a través de la LO 5/2010 y se reforma mediante la LO 1/2015, y con base en el método interdisciplinar expuesto. Finalmente fue enviado el documento en un primer lugar al tutor para que corrigiese los aspectos técnicos, y una vez realizada la corrección se procedió a enviarle al cotutor, en diferentes ocasiones el documento elaborado por epígrafes, en los que, él, expuso fallos y brindó orientaciones sobre su subsanación. Tras seguir las últimas directrices dadas y con la aprobación del tutor y cotutor, fue objeto de depósito el mismo, para la posterior exposición.

PARTE CENTRAL DEL TRABAJO

1.-INTRODUCCIÓN

La transcendencia del Internet en la esfera privada y profesional de los individuos que integran la sociedad no es algo que nos encuentre por sorpresa hoy en día.[16] Esta herramienta nos ha permitido acceder a la información prácticamente en tiempo real, y es proporcionada por diferentes emisores, pudiendo mostrarnos diferentes perspectivas de un mismo hecho. El ciudadano es consciente del gran poder que supone el uso y empleo de la información, por lo que se ha convertido en un arma eficaz a nivel defensivo y ofensivo.[17] La tecnología y el internet nos ha facilitado la forma de vida, pero también es claro que el internet no solo abarca nuestra esfera personal y laboral, sino que forma parte de la globalización mundial. Estos dispositivos almacenan gran cantidad de información personal, quedando nuestra privacidad expuesta[18]. Esta continua conexión nos da la sensación de sentirnos más seguros[19],cuando realmente lo que está sucediendo es que cada vez somos más vulnerables.

Los delitos tradicionales, en un contexto en el que más del 50% de la población mundial es usuaria en la red, se han visto modificados por actividades que utilizan las herramientas informáticas para cometer los ilícitos o que van en contra de los propios sistemas informáticos, elaborándose categorías penales novedosas y muy relevantes en la actualidad, como son el phishing, el hacking, el cracking, el childgrooming o el cyberbulling entre otros. Delitos especiales que han ido evolucionando a lo largo de los años y han aumentado en este último año debido a la pandemia C-19.

Durante el año 2020 con la pandemia por el virus C-19, el phishing constituyó un gran impacto económico y social, debido al drástico cambio de nuestro estilo de vida, con un estado de alarma por crisis sanitaria, y las restricciones de movilidad, el "mundo real" paso a ser durante unos meses una completa "realidad virtual".[20] Bajo ese contexto, las

---

[16]COLÁS TURÉGANO, Asunción: Los delitos de género entre menores en la sociedad tecnológica. En CUERDA ARNAU, MªLuisa(dir.)/FERNÁNDEZ HERNÁNDEZ,Antonio(coord.): *Menores y redes sociales: ciberbullying, ciberstalking, cibergrooming, pornografía, sexting, radicalización y otras formas de delincuencia en la red* .ValenciaTirant lo Blanch, 2016. pág.67-116.

[17]BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.* pág.17- 19.

[18] OFICINA DE CIBERSEGURIDAD DEL INTERNAUTA: *La Ciberseguridad es una responsabilidad de todos: el IoT y sus riesgos[15/02/2021][Link] y Tu casa inteligente es cibersegura [15/02/21][Link]*

[19]ALMENAR PINEDA, Francisco: *Ciberdelincuencia… ob. cit.* pág.17-19.

[20]RIVERA BEIRAS, Iñaki: *Pandemia, derechos humanos, sistema penal y control social (en tiempos de coronavirus).*Valencia: Tirant Humanidades, 2020.pág.19-38. /Vid.: SÁNCHEZ ARJONA, Mercedes

relaciones laborales, sociales y económicas se realizaban de forma remota desde nuestros domicilios, compras mediante plataformas virtuales y el tiempo extra que nos proporcionó, para navegar aún más por la web, hace que la "zona caliente" en la actividad delictiva se vincule íntimamente con este nuevo estilo de vida. Advirtiendo que este contexto propició el aumento del fenómeno criminal de la ciberdelincuencia, con alertas por parte del equipo del centro criptológico nacional de la aparición masiva de campañas de malware vinculadas al C-19.

Google registro mas de dos millones de sitios web de phishing durante este año, con una media de mas de 58.000 webs de phishing a la semana. El 2020 se acuña como el año mas prolífico de la ciberdelincuencia, con un incremento del 19,91%[21].

En relación desde un aspecto más técnico, saber que el funcionamiento del internet es fruto de un complejo sistema de comunicaciones electrónicas, protocolos y arquitecturas comunes, relativas a la transmisión de datos e interoperabilidad de los sistemas, vinculado todo ello, al carácter transnacional y universal de los medios de comunicación, y el carácter descentralizado de internet; hace que la tarea de renovación legislativa en estos ámbitos del derecho sea cada vez más urgente, ante la ineficacia con la que se da respuesta a las necesidades derivadas de las conductas criminales en la red a través de los mecanismos de tutela actuales[22], además debido a la imposibilidad de un organismo que dirija y gestione la red, se exige una cooperación internacional, y una compatibilidad y coordinación de las normas estatales en esta materia, para así crear una armonización de los ordenamientos jurídicos nacionales [23].A pesar de esta urgencia y necesidad, no debemos olvidar el principio de intervención mínima[24]y de ultima ratio de nuestro

Llorente(dir.)/ MARTÍNEZ-GIJÓN MACHUCA, Miguel Ángel(dir.).:*Pandemia y derecho, una visión multidisciplinar*.Murcia: Ediciones Laborum, 2020.

[21] KELLY,Tom: *How hackers are using COVID-19 to find new phishing victims*.[15/02/21][Link]

[22] BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pág.27-30/ ALMENAR PINEDA, Francisco: *Ciberdelincuencia… ob. cit.*pág. 20-21.

[23] Vid. BARRIO ANDRÉS, Moisés: *Fundamentos del Derecho de Internet.* Madrid: Estudios políticos y constitucionales, 2017.Cap. I y II.

[24] *El principio de intervención mínima, denominado así en nuestra doctrina por* MUÑOZ CONDE, *afecta de forma directa al contenido y extensión del "ius puniendi". Persigue una mayor racionalidad y efectividad por parte del Estado: según este principio, el Derecho penal sólo tutela aquellos derechos, libertades y deberes imprescindibles para la conservación de la paz social, frente a las agresiones más intolerables que se realizan contra el mismo. Por tanto, siempre, que existan otros medios diferentes al Derecho penal para la defensa de los derechos individuales y/o colectivos, éstos serán preferibles, por ser menos lesivos, buscando así el mayor bien con el menor coste. El principio de proporcionalidad sirve para integrar toda una serie de criterios, hasta ahora dispersos, como, la "ultima ratio", el no más daño que utilidad, la construcción de una jerarquía de bienes jurídicos, etc.* MUÑOZ CONDE, Francisco(dir.) / GARCÍA ARÁN, Mercedes(dir.): *Derecho penal, parte general. Valencia:* Tirant lo Blanch, 2015.pág.58-77/ BLANCO LOZANO, Carlos: *Tratado de Derecho Penal Español, tomo I: El sistema de la parte*

Derecho Penal[25]. En relación, debemos mencionar dos reformas esenciales de nuestro ordenamiento jurídico sobre la ciberdelincuencia, la reforma del CP de 1995 en 2010[26] y en 2015[27], ambas vinculadas a la normativa UE[28],en el ámbito de los ciberdelitos y la política criminal llevada a cabo. En este contexto, surge el interés por el estudio del phishing como fenómeno delictivo y su adecuación como delito en el código penal español, el cual es el tema que se pretende desarrollar.

2.- ¿DELITO INFORMÁTICO O CIBERDELITO? Conceptualización.

En relación a este nuevo cauce de ejecución criminal y los problemas que hemos mencionado, que permiten cuestionar los principios tradicionales de la investigación penal, realizaremos una breve introducción relativa al paso de la denominación del delito informático a la de ciberdelito, vinculada a la doctrina.

Esta nueva forma de criminalidad asociada tanto a la utilización como a la realización de conductas criminales sobre los sistemas informáticos, dejaba a la legislación penal española con un vacío, ya que no se recogía en ella ningún ilícito en esta materia; por lo que no es de extrañar que a finales de los ochenta, en España se comenzasen a denominar a estas conductas como "delito informático" [29], denominación que proviene del termino anglosajón: *computer crime*[30], vinculando este término a la nueva forma de criminalidad que se asocia al uso de las redes telemáticas y las conductas contra los sistemas, programas y datos informáticos[31]; siguiendo la corriente Europea de la mano de Ulrich Sieber[32]. No obstante, comenzaría a haber discrepancias sobre esta nueva acuñación,

general. Volumen 1:Fundamentos del Derecho Penal Español, las consecuencias jurídico-penales. Barcelona: Bosch, 2015.pág.88/ LUZÓN PEÑA, Diego- Manuel: *Lecciones de derecho penal, parte general.* Valencia: Tirant lo Blanch, 2016.Pág.42-44.

[25] ROMEO CASABONA, Carlos María/SOLA RECHE, Esteban / BOLDOVA PASAMAR, Miguel Ángel(coord..): *Derecho penal, parte especial.* Granada: Comares, 2016.pág. 254

[26] Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Publicado en el BOE núm. 152, de 23 de junio de 2010

[27] 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. Publicado en el BOE núm. 77, de 31 de marzo de 2015.

[28] Reglamento (UE) 2019/881 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (Reglamento sobre la Ciberseguridad).

[29]ALMENAR PINEDA, Francisco: *Ciberdelincuencia… ob. cit.*pág. 21-23.

[30] Vid. PARKER, Donn B: *Crime by computer.* Nueva York: Charles Scribner´s Sons, 1976.

[31]BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pag.33.

[32]ULRICH SIEBER*: Computerkriminalitat und Strafercht.* Koln: Heymann,1977. Y *The internacional handboolk on computer crime: computer-related economic crime and the infringements of privacy*.Nueva York: John wiley and sons, 1986./ ALMENAR PINEDA, Francisco: *Ciberdelincuencia… ob. cit.*Pág.21-23.

como se puede observar en la obra *"Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las nuevas tecnologías de la información"* de uno de los precursores en España en esta materia, ROMEO CASABONA, quien apunta lo siguiente: "*en la literatura en lengua española se ha ido imponiendo la expresión delito informático, que tiene la ventaja de su plasticidad, al relacionarlo directamente con la tecnología sobre o a través de la que actúa. Sin embargo en puridad no puede hablarse de un delito informático, sino de una pluralidad de delitos, los cuales tienen una única nota común, que es su vinculación de alguna forma con los ordenadores, pero no siendo el bien jurídico agredido siempre de la misma naturaleza ni tampoco la forma de comisión del hecho delictivo tiene siempre características semejantes*"[33] En un principio el término aludía exclusivamente a la comisión de delitos por medio de los ordenadores, pero en la actualidad existen diversos dispositivos electrónicos con los que perpetrar los ilícitos, como son los teléfonos móviles o las tablets.[34]

Como añade DE URBANO CASTRILLO "*se trata de un tipo de delito, ya sea tradicional o propio de la sociedad de la información, propiciado por las tecnologías que esta aporta. El Convenio de Budapest ofrece el concepto de delito informático: como el delito basado tanto en la utilización de determinadas técnicas y modos de proceder informáticos…, como en ciertos contenidos cuya vulneración se ve facilitada por el medio Internet*".[35] Así, las criticas vertidas sobre este término de "delito informático" se deben a la inexistencia de una clase autónoma de delitos informáticos, ya que no se define un BJP común a todos, sino el ámbito de riesgo, requiriendo la adaptación de los tipos penales existentes en aquel contexto, que no serán modificados hasta la reforma del CP del 2015. En contraposición, DAVARA RODRÍGUEZ, defendió el término de "delito informático" definiéndolo como aquel en el que "la realización de una acción, que reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático, ya sea hardware o software" [36]

La perspectiva actualmente debe distinguirse, con la gran evolución de las TIC y la delincuencia vinculada a las mismas, se ha realizado un cambio de denominación debido

[33] ROMEO CASABONA,Carlos María: *Poder Informático y seguridad Jurídica*.Madrid:Fundesco,1987. pág.41.
[34] Vid. POVEDA CRIADO, Miguel Ángel*: Delitos en la red.* España: Fragua, 2015.
[35] DE URBANO CASTRILLO, Eduardo: Los delito informáticos tras la reforma del CP de 2010. *Delincuencia informática: tiempos de cautela y amparo.*2012, ISBN 978-84-9014-273-8.pág.18.
[36]DAVARA RODRÍGUEZ, Miguel Ángel: *Manual de derecho informático.* Pamplona: Aranzadi, 2015. pág.302.

a la evolución criminológica de los comportamientos ilícitos en la red, siendo posible acuñar estas conductas en función de las características del delito: por un lado "ciberdelincuencia" o "delincuencia cibernética" a aquellas conductas en las que para la comisión del delito se utilizan como instrumento los sistemas informáticos, por ejemplo, la compraventa en el comercio electrónico de un coche que en realidad no existe y se queda el delincuente con el dinero de la compraventa sin entregar ningún bien, y por otro lado, "delincuencia informática" para referirse a la conducta delictiva que es perpetrada en sistemas informáticos, por ejemplo, la introducción de un malware en el sistema de una computadora que inutiliza la misma. Resaltar, que lo telemático o cibernético es también informático, pero no en sentido inverso.

Cabe destacar, que no existe una categoría autónoma de "delito cibernético" o "delito informático", así el *locus comissi delicti* podría ser la red, la vía pública o un domicilio particular, por eso debería hablarse de delincuencia informática y no "delitos informáticos" como expone BARRIO ANDRÉS[37]. En contraposición, DE URBANO CASTRILLO[38], diferencia: por un lado, los delitos informáticos que en su base son delitos clásicos que se cometen a través de la red, como las amenazas o delitos contra la libertad, intimidad e indemnidad sexual, y, por otro lado, los delitos "stricto sensu" que son aquellos que advierten sobre el intrusismo en los equipos informáticos, fraudes, etc.

En definitiva, el concepto de Ciberdelito engloba tanto delitos específicos de internet como los asistidos electrónicamente, refiriéndose a delitos tradicionales que utilizan los medios electrónicos para realizarlos.[39] Como define JEWKES y YAR[40] el "Ciberdelito es cualquier ilícito penal cometido por medio de, o con asistencia de, sistemas informáticos, redes digitales, Internet y demás TIC". A lo largo de este trabajo, trataremos al Phishing indistintamente con el término Ciberdelito, por ser parte de aquellas conductas delictivas que se aprovechan de la utilización de sistemas informáticos y el empleo del Internet y telecomunicaciones como elemento clave para la comisión delictiva[41]; y con el

---

[37]BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pág.34.

[38] DE URBANO CASTRILLO, Eduardo: Los delito informáticos tras la reforma del CP de 2010. *Delincuencia informática…ob.cit.*Pág.19.

[39] Décimo congrego de NNUU sobre Prevención del Delito y Tratamiento del delincuente, Viena 10 al 17 de abril de 2000 "*por delito cibernético se entiende todo delito que puede cometerse por medio de un sistema o una red informáticos, en un sistema o una red informáticos o contra un sistema o una red informáticos".*

[40] JEWKES, Yvonne / YAR, Majid: *Handbook of internet crime.* Nueva York: Willan, 2009.pág. 105.

[41] *Un concepto amplio de lo que debe entenderse por "Ciberdelito" lo encontramos, por ejemplo, en el Décimo Congreso de las NNUU sobre Prevención del Delito y Tratamiento del Delincuente* (Viena, 10 a 17 de Abril de 2000), *en donde se declara que "por delito cibernético se entiende todo delito que puede*

término de delito informático ya que es la definición que se maneja en nuestro CP, art.127 bis.1.c), y como menciona GIL ANTÓN, comprende "*todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tienen como fin estos bienes*" [42]

3.- ALGUNOS PROBLEMAS JURÍDICO-PENALES DE LA CIBERDELINCUENCIA.

Como hemos apuntado en los epígrafes previos, la comisión de delitos en la red ofrece más facilidades que los sistemas tradicionales[43], la rapidez con la que se pueden eliminar o inutilizar pruebas y el empleo de "personalidades virtuales" que favorecen al enmascaramiento del autor, forman grandes problemas a la hora de enjuiciar estos Ciberdelito.

El primer problema que nos encontramos, es saber quien se encuentra detrás de estas conductas ilícitas, no existiendo un único perfil de ciberdelincuente[44], ya que podría ser cualquier sujeto que delinca utilizando la red, desde adolescentes intentando entrar en las redes sociales de sus compañeros, hasta la persona adulta que comparte pornografía infantil, grupos terroristas buscando adeptos, hacker al que contrata un Estado para atacar infraestructuras de otro Estado y hacerse con información sensible, al igual que en los delitos tradicionales, no existe un perfil exclusivo de criminal físico, excepto delitos de sujeto activo cualificado biológicamente, como sucede en el aborto con la mujer. El único rasgo que tienen en común estos cibercriminales, es la utilización de las TIC como vía para realizar el ilícito. En sus orígenes, la figura de los hackers[45]estaba vinculada a la creencia de que compartir información era un bien poderoso y positivo, existiendo un deber ético entre los hackers de facilitar el acceso, utilizar código abierto y compartir la

cometerse por medio de un sistema o una red informáticos, en un sistema o una red informáticos o contra un sistema o una red informáticos" [Link][18/02/21]

[42]GIL ANTÓN, Ana María: De los delitos contra la intimidad personal y familiar y delito informático, de acuerdo con la reforma operada por la LO 1/2015, de 30 de marzo, de reforma del CP.*Revista Aranzadi de derecho y nuevas tecnologías.* 2015, ISSN 1696-0351, pág.27-57.

[43] Vid., en detalle, BARRIO ANDRÉS, Moisés*: Fundamentos del Derecho de Internet*. Editorial Centro de Estudios Políticos y Constitucionales. Madrid, 2017, pág.38 y ss.

[44] BARRIO ANDRÉS, Moisés: *Fundamentos…ob.cit.*pag. 43 y ss.

[45] *Englobados inicialmente en el concepto de "piratas informáticos", concepto vago e inexacto pero muy extendido popularmente, que comprende a los hackers, coders,crackers, e incluso a los que copian y distribuyen por Internet material protegido por los derechos de autor.*

información que "conseguían".[46]En esos momentos, la delincuencia en internet era muy limitada a expertos en la materia, y se basaba más en una inquietud intelectual por la vulnerabilidad de los sistemas informáticos, manteniéndose por lo general, en el limite de la legalidad, por lo que en muchos casos la calificación penal era de atipicidad. Actualmente siguen existiendo hackers fieles a esa ética, como Anonymous[47], Assange o Snowden. Sin embargo, lo más habitual hoy en día es la existencia de grupos criminales, también denominados black hat, con estructuras muy bien organizadas, cometiendo ilícitos de todo tipo, desde tráfico de órganos, drogas, trata de seres humanos, falsificación de productos y un largo etcétera[48].

Por lo tanto, el anonimato de estos hackers es un grave problema a la hora de perseguir y detectar el ilícito. En principio, la determinación de la persona no resultaría complicada, ya que cada dispositivo electrónico conectado a la red tiene una dirección IP, esta dirección se asemeja al DNI electrónico de cada dispositivo[49], por lo que su detección no sería compleja al ser un dato público[50], el problema resulta cuando se enmascaran mediante técnicas de manipulación las IP o cuando se conectan a través de redes botnet[51], o redes wifi abiertas. Mención especial en este apartado a la red tor, the onion router[52], una red de comunicación superpuesta a internet que permite la ocultación de los usuarios, protegiendo la dirección IP y encriptando el tráfico que circula por ella en capas, como una cebolla, así se mantiene la integridad de la información que viaja por la misma. Se encuentra dentro de la conocida darknet o Deep web[53], aunque la mayor parte de el contenido que circula por la misma es ilegal, venta de estupefacientes, venta de armas, pornografía infantil, contratación de sicario, etc. En un principio esta red estaba creada para navegar por internet libremente, sin el control gubernamental o de empresas de

[46]RAYMOND,Eric: Hacker Slang and Hacker Culture .*The Jargon file* [Link][18/02/2021].

[47] Vid. COLEMAN, Gabriella: *Las mil caras de Anonymous: hackers, activistas, espías y bromistas.* Barcelona: Arpa Editores, 2016.

[48] LÓPEZ LÓPEZ, Antonio: La investigación policial en Internet, estructuras de cooperación internacional. *Revista d'internet, dret i política, monográfico III Congreso internet, derecho y política. Nuevas perspectivas.*2007, SSN 1699-8154, Nº 5.pág.65.

[49] Vid. BARRIO ANDRÉS, Moisés: *Fundamentos…ob.cit.*pág.98 y ss.

[50] En la página web: [Link] [22/5/2021] podemos encontrar cuál es nuestra dirección IP pública de la conexión a Internet, como ejemplo.

[51] *Una Botnet, es el término utilizado para referirse al conjunto de ordenadores infectados que pueden controlarse de forma remota.*

[52] THOMAS LEICHETENSTERM, Christoph Langner: Bajo el radar: teoría y práctica de la red Tor.*Linux magazine.*2012, ISSN 1576-4079, Nº82, pág. 55-59.

[53] REZA REYES, Sandra: Uso ilícito de la red: El caso de la DEEP WEB. En NAVA GÁRCES, Alberto Enrique: *Ciberdelitos.* Ciudad de México: Tirant lo Blanch, 2019.pág. 181-196.

internet.[54] Finalizando este punto y volviendo a la identificación de la IP, el proceso de identificación del titular de la IP sería mediante solicitud al juez, que por mandamiento autorizará a que los proveedores de acceso a internet y operadores de telecomunicaciones informen de todos los datos para la identificación. En el caso de que se reconozca al titular, se realizara la entrada y registro del domicilio del titular, accediendo a su ordenador y obteniendo una copia del mismo, iniciándose así el proceso judicial vinculado al ilícito cometido.[55]

El segundo problema, más característico de este tipo de delitos, está vinculado a la magnitud territorial del internet, unido íntimamente a la globalización, dificultando la determinación del lugar de la comisión del ilícito y la competencia para juzgar[56]. La conducta delictiva navega por el ciberespacio, planteando serios problemas de competencia penal para su enjuiciamiento, ya que se hace difícil el cumplimiento del principio de territorialidad[57] del art.23.1 LOPJ:*"En el orden penal corresponderá a la jurisdicción española el conocimiento de las causas por delitos y faltas cometidos en territorio español o cometidos a bordo de buques o aeronaves españoles, sin perjuicio de lo previsto en los tratados internacionales en los que España sea parte";* Por lo que podemos intuir que en la cibercriminalidad, la legislación penal considerada tradicionalmente como cuerpo legislativo vigente para un estado determinado territorialmente no sería válida[58], al igual que ocurre con la modalidad criminal transnacional. Es importante mencionar también que, gracias a la rapidez con la que viajan los datos, el traslado del material ilícito a otro servidor o plataforma puede ser prácticamente instantáneo, evitando la persecución. Por lo tanto, parece ser que las soluciones a estos problemas planteados podrían buscarse, en primer lugar con la armonización de legislaciones nacionales y mecanismos de cooperación internacional[59]; en segundo lugar, creando cláusulas de extraterritorialidad al igual que en materia de

[54] SANCHIS CRESPO, Carolina: *Fraude electrónico, su gestión penal y civil*. Valencia: Tirant lo Blanch, 2015.pag.55 y ss.

[55] BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pág.44 y ss./ También STS, Sala 2ª, 17 de abril de 2013.

[56] CLIMENT BARBERÁ, Juan: *La justicia penal en internet, territorialidad y competencias penales.* 2001, Número 10, ISBN 84-89230-50-1.pág.14-26.

[57]Vid. ALMENAR PINEDA, Francisco: *Ciberdelincuencia… ob. cit.*pág.36/ BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pág. 51-52.

[58] SEMINARA, Sergio: La piratería su Internet e il diritto penale, *Revista Trimestrale di Diritto Penale dell'Economia*.1997, ISSN 1121-1725,Nº 1-2. pág.111.

[59]El Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, tiene como finalidad armonizar legislaciones nacionales y facilitar su persecución.

genocidio, terrorismo, tráfico de personas, o en materia de cibercriminalidad extraterritorial en corrupción de menores art.189.1b) "*(…)aunque el material tuviere su origen en el extranjero o fuere desconocido";* y en tercer lugar, precisando el lugar en dónde se entiende cometido el delito.

El TS considera que es competente para persecución del Ciberdelito, cometido normalmente desde un lugar que se ignora y produce efectos en diversas ubicaciones geográficas, el juez de todos los lugares donde se manifiesten sus efectos, es decir, tanto el lugar de la acción como el del resultado.[60] A este criterio se le denomina principio de ubicuidad, adoptado a partir del Acuerdo no jurisdiccional del Pleno del TS del 3 de Febrero de 2005, "*el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el Juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para la instrucción de la causa"*[61]. Este principio tiene relevancia no solo a nivel doctrinal y jurisprudencial nacional, sino también en derecho comparado[62]. De acuerdo con esta teoría de la ubicuidad, todos los Estados en los que se han realizado conductas o se produjeron resultados son competentes; por lo tanto, otra posible solución sería el principio de personalidad, en el que es competente aquel Estado del que sea nacional el autor. Esta teoría se vuelve conflictiva en supuestos de coautoría de nacionales de diferentes Estados o si las conductas son lícitas en un Estado pero en otro no (necesaria

[60] MARCHENA GÓMEZ, Manuel: Dimensión jurídico-penal del correo electrónico. *Diario la ley*.2006, Nº 6475.pág. 14 "*La teoría de la ubicuidad, por ejemplo, permitirá entender que la inoculación de un potente virus destructivo mediante el correo electrónico, llevada a cabo desde fuera de España por un no nacional, pero que expande sus nocivos efectos en sistemas informáticos radicados en territorio español, puede ser perseguida en nuestro país, en la medida en que el delito, atendiendo al resultado, también puede reputarse cometido en España. Esa conclusión estaría vedada si entendiéramos aplicable la teoría de la actividad, pues el delito, en la medida en que la acción se habría desarrollado por un extranjero, fuera de nuestro territorio y el delito de daños no se halla en el catalogo de figuras delictivas del art. 23 de la LOPJ, no se entendería cometido en los límites jurisdiccionales españoles*

[61] La postura del TS ha sido adoptada también por autores como RODRÍGUEZ MOURULLO, Gonzalo / LASCURAÍN SÁNCHEZ, Juan Antonio /ALONSO GALLO, Jaime: Derecho penal e internet. En FERNÁNDEZ ORDOÑEZ, Miguel(coord.): *Régimen jurídico de internet.* España: Wolters Kluwer, 2001.pág.265./Y CORCOY BIDASOLO, Mirentxu: Problemática de la persecución penal de los denominados delitos informáticos particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos.*Eguzkilore.*2007, Numero 21. San Sebastián: Cuadernos del Instituto Vasco de Criminología, pág.32.

[62] *Citar en el marco comparado, códigos penales a nivel europeo, como en el CP Alemán "§ 9.1 Lugar del hecho: Un hecho es cometido en el lugar en el que el autor ha actuado o, en los casos de la omisión en que debería haber actuado o en el lugar en el que se ha producido el correspondiente resultado al tipo penal o en el lugar en donde según la percepción del autor ha debido producirse"; que coincide en los mismos términos que en el §67 (2) CP Austriaco.*

la armonización) como los denominados paraísos informáticos, fuera de jurisdicción penal y con legislaciones menos restrictivas.[63]

En conclusión, se podría decir que existen diversos problemas a la hora de establecer la autoría, ya que es difícil llegar a saber quién es el SA del ilícito, además de la dificultad de discernir el lugar de comisión y competencia para juzgar los ciberdelitos, ya que pueden surgir conflictos jurisdiccionales de carácter internacional, por lo que es necesario la cooperación jurisdiccional en el ámbito internacional y de la UE. Sin olvidar que, junto al principio de territorialidad, están los principios de universalidad, protección de intereses del Estado y de personalidad.

4.- MARCO LEGISLATIVO

En relación con el punto anterior no es de extrañar que los Estados comenzasen a ser conscientes de los riesgos y consecuencias que podrían acarrearles las redes de comunicación y sistemas de información, en virtud de esto se potenció una tendencia colaboradora en el ámbito de la ciberseguridad, por ello debemos tratar el marco legislativo desde las perspectivas a nivel nacional y supranacional de los ciberdelitos. Debemos mencionar que la colaboración entre países para la adopción de soluciones de carácter internacional, no es impedimento para que los territorios sigan fomentando las herramientas que les proporcionen seguridad e independencia[64].

Para la regulación de los ciberdelitos a nivel comparado, se utilizan por lo general, dos vías normativas: La primera vía es el recurso de leyes penales especiales, países europeos como Francia y la ley relativa al fraude informático desde 1988 o RU con la Computer Misue Act de 1991. Otros países como EEUU que tiene la Computer Fraud and Abuse Act o en Iberoamérica con la ley chilena, pionera de su entorno. La segunda vía, es la seguida por España, con la tipificación en el propio código penal de estos nuevos delitos. A nivel EU también adoptaron esta vía otros países, como Alemania, Austria, Italia y Portugal. Fuera de EU, tenemos como precursores: Argentina y México. La vía del ámbito procesal, en la mayoría de Estados, ha sido caracterizada por la adaptación de las medidas legislativas recogidas en la legislación procesal penal, vinculándolas específicamente con las TIC.[65]

[63]BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pág. 50 y ss.
[64] FERNÁNDEZ BERMEJO, Daniel / MARTÍNEZ ATIENZA, Gorgonio: *Ciberseguridad, ciberespacio y ciberdelincuencia.* Pamplona: Aranzadi, 2018.pág.88.
[65] BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pág.57 y ss.

Dentro del marco internacional nos encontramos en primer lugar dentro de la esfera de la ONU con el Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos de 1977, también conocido como *Manual Tallin,* y el Programa Global de Cibercrimen de la Oficina de las NNUU contra la droga y el delito (UNODC). Hasta Julio de 2020, nos encontrábamos con el "Acuerdo Privacy Shield"[66], en relación a la transferencia internacional de datos procedentes de Europa, con este acuerdo las empresas norteamericanas, receptoras de datos sensibles transferidos desde Europa, realizaban una auto declaración de adhesión, al denominado "escudo de privacidad"[67], obligándose a cumplir las medidas de seguridad requeridas en la UE, además de estar sujetas al control y vigilancia del departamento de comercio de EEUU. Este acuerdo es similar al antiguo "safe harbor", con la diferencia de que ofrece mayores garantías; tras un fallo del TJUE denominado como sentencia Schrems II[68], del 16 de julio de 2020, se dictamina que el acuerdo Privacy Shield queda anulado, ya que el tribunal entiende que el nivel de seguridad exigido en el reglamento de protección de datos, que entró en vigor en Europa el 25 de Mayo de 2018, no era alcanzado para cubrir a los datos personales que se almacenaban y procesaban en los Estados unidos. A partir de este fallo, la UE recomienda que aquellos que puedan busquen alternativas dentro de la UE para la transferencia de datos, servicios en nube y servidores en terceros países, para asegurarles el cumplimiento del RGPD[69].

Este Reglamento de Protección de Datos, que hemos mencionado en el punto anterior, nace de una reforma por parte del Parlamento Europeo y el Consejo que duró cinco años, previamente la aplicación en esta materia era la Directiva 95/46/CE de 1995, el objetivo de este reglamento es la regulación uniforme del tratamiento de los datos, vinculado sobre todo a la práctica empresarial, relacionada íntimamente a los cambios tecnológicos de los últimos veinticinco años. Los principios reseñables en este reglamento son: la prohibición a priori del procesamiento de datos personales salvo autorización expresa, limitación de la finalidad de la recopilación y edición de los datos, minimización de datos recopilados

[66] Vid. Decisión 2016/1250 de la Comisión que declara el nivel adecuado de protección del esquema del Escudo de Privacidad para transferencias internacionales de datos a EEUU.[Link][24/4/21]

[67] PÉREZ CAMBERO, Raúl: Aspectos más destacables de la Decisión de Ejecución 2016/1250 de la Comisión Europea, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU. *Actualidad administrativa.*2017, ISSN 1130-9946, Nº4.

[68]Vid., Sentencia comentada en Blog derecho internacional dermerule[Link][25/5/2021] / ROYO PÉREZ, Victoria: El TJUE anula el acuerdo entre la UE-EEUU y obliga a revisar las transferencias de datos personales[Link][25/5/2021]

[69] INCIBE: ¿Cómo nos afecta la derogación del escudo de privacidad entre EU y EEUU?[Link][25/5/2021]

por las empresas, transparencia del tratamiento de los datos, y confidencialidad, vinculando este último principio a la obligación explícita de la aplicación por parte de las empresas de técnicas de protección[70].

Continuando con la perspectiva legislativa del marco Europeo, nos encontramos con la Organización para la Seguridad y la Cooperación en Europa (OSCE) dónde se han aprobado diversas normas con la intención de disminuir los riesgos vinculados al uso de la TIC, además de ser intermediarios en la comunicación entre Estados parte de la OSCE y la mejora de las infraestructuras.[71]En el marco del Consejo de Europa nos encontramos con el convenio de Budapest sobre la ciberdelincuencia del 23 de noviembre de 2001, que tiene el triple propósito de armonizar el Derecho penal material, establecer medidas procesales y poner en funcionamiento un régimen rápido y eficaz de cooperación internacional.[72]En lo relativo al espacio europeo, ha sido la primera norma con más relevancia por ofrecer respuesta a los ataques perpetrados contra los sistemas informáticos.[73]En España fue ratificada por la publicación en el BOE el 17 de septiembre de 2010 y entrando en vigor el 1 de octubre de 2010[74]. Ha sido reconocido como el primer tratado internacional sobre ciberseguridad, armonización de leyes nacionales, cooperación y mejora de las técnicas para investigar los ciberdelitos[75]. La armonización del Derecho penal material del Convenio mencionado, se concretó con la Decisión marco 2005/222/JAI [76]del Consejo, del 24 de Febrero de 2005, relativa a los ataques contra los sistemas de información, no obstante al igual que con el convenio las directrices marcadas no son suficientemente restrictivas en conductas relativas a la intrusión en sistemas

[70]REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EU Y DEL CONSEJO DE 27 de abril de 2016 [Link][25/05/2021]

[71] Vid.,entre otros: ASENCIO MELLADO, José María/ FERNÁNDEZ LÓPEZ,Mercedes:*Justicia penal y las nuevas formas de delincuencia.* Valencia: Tirant lo Blanch, 2017.pág.46/ BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pág.59.

[72] FERNÁNDEZ BERMEJO, Daniel / MARTÍNEZ ATIENZA, Gorgonio: *Ciberseguridad…ob.cit.* pág.167-168/ GONZÁLEZ HURTADO, Jorge Alexandre: La seguridad en los sistemas de información como un bien jurídico de carácter autónomo, perspectiva EU y española. *Revista Penal de México*. 2016,ISSN 2007-4700, Nª9 pág. 60-61.

[73]ALMENAR PINEDA, Francisco: *Ciberdelincuencia… ob. cit.*.pág.80.

[74] FERNÁNDEZ BERMEJO, Daniel / MARTÍNEZ ATIENZA, Gorgonio: *Ciberseguridad…ob.cit.* pág.167 .

[75] ALMENAR PINEDA, Francisco: *Ciberdelincuencia… ob. cit.*pág. 80-82 / BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pág.58-59.

[76] La Decisión marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información: *El fin de esta norma consiste en reforzar la cooperación entre las autoridades judiciales y otras autoridades competentes, incluida la policía y los demás servicios represivos especializados de los Estados miembros, mediante la aproximación de su legislación penal en materia de ataques contra los sistemas de información*

informáticos, por lo que los Estados cumpliendo los mínimos de la misma, alejándose del objetivo de armonización y coordinación que se pretendían[77].

Mencionar la Directiva 2016/1148 [78], con esta directiva se pretende garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea, evitando incidentes de seguridad que puedan interrumpir las actividades económicas que se realizan en la UE. En los artículos 14 y 16 de esta directiva, se habla de la seguridad de las redes y sistemas de información para los operadores esenciales y proveedores de servicios digitales. Mencionan a los Estados miembro como los responsables de velar por el cumplimiento de las medidas que se les proporcionan o que se adecúen al riesgo planteado. Además, de a los encargados de adoptar medidas para minimizar o prevenir incidentes que afecten a la seguridad. También, velan por la obligación de los proveedores de servicios digitales de adoptar medidas de seguridad técnicas, organizativas y de gestión de riesgos de la seguridad de las redes y sistemas de información que utilizan, adecuando su actividad al cumplimiento de las normas internacionales, entre otras. Será obligatoria, la notificación a la autoridad competente o al CSIRT (Computer Security Incident Response Teams)[79]

Finalmente, en el marco estatal, nos encontramos con un compendio de normas, de las que caben mencionar:

- Código de derecho de la ciberseguridad:

Ante la ausencia de una sistematización para la ubicación de este tipo de conductas, se crea el código de derecho de la ciberseguridad, que es el compendio de normativa internacional, comunitaria, y nacional, para facilitar a los profesionales la búsqueda de normas relativas a la ciberseguridad.[80] En él se recoge normativa trasnacional, ante la tendencia de colaboración en términos de seguridad.

Los Estados cada vez más conscientes de los peligros de los sistemas de comunicaciones e información, y de las redes, asimismo, de la carencia de normativa que regulase la ciberdelincuencia, por tratarse el espacio virtual de un entorno interactivo, el cual no tiene un espacio físico determinado que únicamente compete a un estado, sino que puede relacionarse con una multitud de ellos.

[77] ALMENAR PINEDA, Francisco: *Ciberdelincuencia*…op.Cit.,pág.84.
[78] Vid. DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016[Link][24/05/2021]
[79] Vid. texto legal del Parlamento Europeo y del Consejo del 6 de Julio de 2016[Link][26/05/2021] a
[80] Código de Derecho de la Ciberseguridad, 2 de julio de 2021[Link][25/05/2021]

Empiezan a crear un marco legal para reducir los potenciales conflictos derivados de la utilización de las TICs, a pesar de que en el marco de la UE la capacidad para legislar en el ámbito del derecho penal es limitada y ha conseguido un competencia parcial, al vincular este tipo de delitos con las actividades comerciales entre los Estados miembro.

Es en este marco dónde crean el Convenio Europeo sobre Ciberdelincuencia[81], la Decisión Marco 2005/222/JAI del consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, y la Directiva 2013/40/UE.

En este código se hace referencia a una serie de leyes, referidas a este tema, como son:

A) Normativas seguridad nacional:

- Ley 36/2015,28 de septiembre, de seguridad nacional [82],con esta ley se pretende mejorar la coordinación de las administraciones públicas para la resolución de problemas que se salen de las categorías tradicionales, como el ciberespacio, facilitando la incorporación de la estrategia de seguridad nacional, 31 de mayo de 2013, dirigido por el presidente del gobierno.
- Orden TIN/3016/2011, de 28 de octubre, crea el comité de seguridad de las tecnologías de la información y las comunicaciones del ministerio de trabajo e inmigración [83], denominado en su art.1 "Comité de Seguridad TIC del Ministerio de Trabajo e Inmigración", el objetivo que se persigue con la creación de este comité es "establecer, gestionar, coordinar y aprobar las actuaciones en materia de seguridad de las tecnologías de la información y las comunicaciones".

B) Normativas de seguridad:

- Ley orgánica 4/2015, 30 marzo, protección de la seguridad ciudadana[84], garantizar la seguridad ciudadana es una de las prioridades de la acción de los poderes públicos, art.149.1.29º CE, por lo que es preciso la incorporación de esta ley en el ámbito cibernético, para poder salvaguardar esa seguridad.
- Ley 5/2014, de 4 de Abril, de Seguridad Privada [85], con esta ley se persigue la aplicación del principio de complementariedad entre la seguridad publica y privada, con el fin de eliminar situaciones de intrusismo tanto de las empresas como del personal.
- Ley 34/2002, 11 de Julio de servicios de la información y comercio electrónico [86], con esta ley se incorpora al ordenamiento jurídico español la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de Junio, relativa a la expansión de las redes de telecomunicaciones y su incorporación a la vida económica y social, la mejora de la eficiencia empresarial, entre otros. El objeto de esta ley es la "regulación del régimen jurídico de los servicios de la sociedad de información y de la contratación por vía electrónica", articulo 1 de la presente Ley.
- *Relacionadas con las telecomunicaciones*, existen las siguientes normas:
- Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido o irregular con fines fraudulentos en comunicaciones electrónicas[87], con este real decreto se pretende eliminar el lucro económico indebido de los usos oportunistas, asegurar el buen uso de los recursos públicos de numeración y la calidad de los servicios de estas comunicaciones, integridad, seguridad de redes y servicios de las mismas.

---

[81]Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. [Link][25/05/2021]

[82]Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. [Link][25/05/2021]

[83]Orden TIN/3016/2011, de 28 de octubre, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración.[Link][25/05/2021]

[84] Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. [Link][25/05/2021]

[85]Ley 5/2014, de 4 de abril, de Seguridad Privada.
[Link] [25/05/2021]

[86] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico [Link][25/05/2021]

[87]Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos en comunicaciones electrónicas [Link][25/05/2021]

- Ley 50/2003, de 19 de diciembre, de firma electrónica[88], se equipara funcionalmente a la firma manuscrita, el objetivo de este decreto es fomentar la incorporación de las nuevas tecnologías a las actividades de ciudadanos, empresas y administraciones públicas. Aporta confianza en la realización de transacciones electrónicas como Internet.
- La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones[89], marco regulador de las comunicaciones electrónicas, explotación de redes y prestación de servicios conforme al art.149.1.21º CE, como bien dice el art.1 de esta Ley.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones[90], con esta ley se pretende que los operadores de telecomunicaciones, retengan los datos generados o tratados en relación con la prestaciones de servicios de comunicaciones electrónicas, posibilitando la disposición de los mencionados a los agentes facultados, en el ámbito de la investigación criminal.
- *Relacionado con la ciberdelincuencia:* Código Penal, Ley Orgánica 5/2000 del 12 de enero Responsabilidad penal del menor, RD la ley de enjuiciamiento criminal.
- *Suplantación de identidad de marca o empresa*, de aprovechamiento ilícito de la misma o infracción a creaciones de autores protegidas por la propiedad intelectual: Derecho marcario o normativa de propiedad intelectual e industrial.

5.-REGULACIÓN CIBERDELITOS EN EL DERECHO PENAL ESPAÑOL.

En el epígrafe anterior expuse los dos tipos de técnicas normativas que se utilizan para la regulación de los ciberdelitos, y que España ha optado, como hemos mencionado, por la tipificación de nuevas figuras delictivas en el CP.[91] A pesar de esto, no se ha dedicado un Título o rúbrica específica para los delitos informáticos, optando por la modificación de los tipos tradicionales, introduciendo subtipos autónomos para penar las nuevas modalidades ilícitas; y la extensión del ámbito de los objetos materiales de los delitos análogos a los nuevos hechos punibles.[92]En este sentido, la reforma del CP por la LO 5/2010 del 22 de junio, fue de las más sustanciosas en materia de delitos informáticos, y con ella el legislador pretendió responder al mandato internacional en relación con el Convenio sobre la Delincuencia de Budapest de 2001[93]. En la misma se han añadido acciones, sustituido elementos y las conductas punibles se han ampliado. Los principales tipos afectados son la intrusión informática del 197.3CP[94], la estafa informática del 248.2

[88] Ley 59/2003, de 19 de diciembre, de firma electrónica. [Link][25/05/2021]
[89] Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.[Link][25/05/2021]
[90] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.[Link][25/05/2021]
[91] BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pág. 57-58.
[92] BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pág.67.
[93]BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pág.67. Vid. Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal
[94] Tras la reforma operada por la LO 5/2010, el artículo 197.3 CP tipifica por primera vez el delito de hacking. Posteriormente, como veremos más adelante se ha vuelto a modificar con la reforma de la LO 1/2015

CP, los daños informáticos o cracking del 264 CP y un delito novedoso como el "childgrooming" o embaucamiento de menores del 183 bis CP.[95]

La siguiente reforma del 2015 CP es una ampliación de la reforma del 2010 motivada por la Directiva 2013/40, ya mencionada en párrafos anteriores[96], la reforma está basada en la adopción de técnicas para un sistema penal más rápido y coherente, la desaparición del libro III relativo a las faltas, una mayor incidencia en materia de tráfico, y la respuesta penal a la delincuencia informática, incidiendo en delitos de pornografía infantil y el castigo correspondiente a las personas que accedan a la misma por medio de las TICs, facultando de forma expresa a jueces y tribunales para la adopción de medidas de bloqueo o retirada de páginas web que alberguen contenido de esta índole[97].

El delito de intrusismo informático cambió su ubicación del 197.3 al 197 bis 1, y se añadieron el delito de interceptación de transmisiones no públicas de datos informáticos, 197 bis 2 y el que castiga la facilitación de instrumentos para la realización de los actos delictivos de los artículos 197.1 y 2, y 197 bis, relativos al descubrimiento y revelación de secretos, delitos contra la intimidad y derechos a la propia imagen[98].

DELITOS INFORMÁTICOS TRAS LA REFORMA DEL CÓDIGO PENAL DE 2015

- Art.187: La inducción a la prostitución de menores por cualquier medio.
- Art.189 se castiga la producción, venta, distribución, exhibición e incluso su posesión, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces.[99]
- Art.169 y ss, se tipifican las amenazas, y en los art.205 y ss las calumnias e injurias, efectuadas y difundidas a través de cualquier medio de comunicación.
- Art.248: Los fraudes informáticos para cuya consecución se manipulen datos o programas.

---

[95] BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pág. 68 .

[96]La aprobación de la Decisión Marco 2005/222/JAI del Consejo, del 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, por parte de la UE; Establece una finalidad principal dual, por un lado, la necesaria armonización de las normas comunes en esta materia para todos los Estados miembros, mediante la definición de ilícitos penales y sus penas, y, por otro lado, reforzar la cooperación entre todos los EM, incluyendo los organismos judiciales y policiales.

La Directiva 2013/40/UE, del Parlamento Europeo y del consejo, del 12 de Agosto de 2013, relativa a los ataques contra los sistemas de información, y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo [Link][25/05/2021], constituye un refuerzo penal a nivel Europeo frente a los ataques a los sistemas de información, con esta directiva lo que se pretende es endurecer las penas del hacking, prevenir este tipo de infracciones y mejorar la cooperación entre las autoridades judiciales y otras autoridades competentes; además de incluir el acceso ilícito e incorporar la interceptación ilegal, ampliando las conductas de la ya mencionada DM 200/222 ./ Vid. GIL ANTÓN, Ana María: De los delitos contra…ob.cit.

/ ALMENAR PINEDA, Francisco: *Ciberdelincuencia… ob. cit.*pág.87// GONZÁLEZ CUSSAC, José Luis(dir.)/ MATALLÍN EVANGELIO, Ángela(coord..)/ GORRIZ ARROYO, Elena(coord..): *Comentarios a la reforma del Código PENAL de 2015.*Valencia: Tirant lo Blanch. pág.663-664.

[97] BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pág.68-69.

[98] COLÁS TURÉGANO, Asunción: Los delitos de género…ob.cit.pág.214.

[99]Vid. LA NUEVA ESPAÑA: *Piden cinco años de cárcel para un lavianés por difundir pornografía infantil por internet*.[Link][27/5/2021]

- Art.263 encontramos el sabotaje informático: la alteración o destrucción de datos, documentos, software que se encuentran almacenados en sistemas o redes informáticas.

La posesión de software informático destinado a cometer delitos de falsedad, por ejemplo, falsificar contratos, el DNI, etcétera.

- En los art.197 a 201se tipifican los delitos de descubrimiento y revelación de secretos a través del acceso y difusión sin consentimiento de sus respectivos titulares de datos registrados en ficheros o soportes informáticos.
- Art.197 bis, primer apartado: El acceso no autorizado a sistemas informáticos o delito de intrusión informática, en este delito se pena el simple acceso, sin ser necesario el acceso a datos. Se castiga el acceso o facilitación del acceso a un tercero, al sistema de información, ya sea a una parte o a su conjunto, vulnerando para ello las medidas de seguridad y sin autorización. En este tipo penal, no hay unanimidad doctrinal en cuanto al BJP ya que una parte se decanta por la intimidad y otros, en cambio, por la seguridad de los sistemas informáticos. Respecto al sujeto activo, debido a los conocimientos de uso de las tecnologías, entenderíamos que sería una persona experta en el uso de las TIC o conocimientos avanzados de las mimas. La pena de prisión iría de seis meses a dos años.
- Art.197 bis, segundo apartado: Figura creada ex novo en la reforma 2015, criminalizando las conductas de interceptación de transmisiones no públicas de datos informáticos. El BJP es la seguridad de los sistemas informáticos.
- Art.197 ter: Se castiga la producción o facilitación a terceros de los instrumentos necesarios para cometer los delitos del art.197; en caso de pertenecer a una organización criminal, tenemos el tipo agravado en el art.197 quater.
- La responsabilidad penal de la persona jurídica y funcionario público, se recogen en los art.197 quinquies y 198, respectivamente.
- Art.201: establece la perseguibilidad de este tipo de delitos de intrusismo informático precisa la previa denuncia de la persona agraviada o, en caso de ser menor de edad o incapaz, de su representante legal o ministerio fiscal, en este último caso.
- Art.270 y ss, se introducen los delitos informáticos relativos a la propiedad intelectual e industrial. Con esta nueva redacción, el legislador pretende blindar y reforzar la seguridad en esta materia, castigando a aquellos que sin autorización previa del titular de derechos de la propiedad intelectual o industrial, facilite el acceso al contenido protegido, mediante links o enlaces para la descarga con fines lucrativos, y al que con ánimo de un beneficio económico fabrique, distribuya, produzca, importe, almacene, ofrezca o comercialice los productos con signos distintivos idénticos a los originales.

Todos estos delitos tienen la misma sanción que sus homólogos no informáticos. Por ejemplo, se aplica la misma sanción para una intromisión en el correo electrónico que para una intromisión en el correo postal. La combinación de esta nueva rama del derecho vinculada a las TIC, con los delitos tradicionales, han ayudado al nacimiento de una nueva disciplina científica objeto de análisis para los juristas. Una parte de la doctrina considera que la reforma comunitaria debería haber sido única y que aportase claridad y orden, para que posteriormente se fuesen desarrollando cuestiones accesorias o técnicas en función de la evolución de las TIC.[100]

[100] ALMENAR PINEDA, Francisco: *Ciberdelincuencia… ob. cit.*pág. 90

6.-ANTECEDENTES DEL PHISHING.

Una vez mencionado el marco legislativo, una breve introducción de los ciberdelitos, y observando la amplia gama sobre las conductas delictivas en la red, pasaremos a profundizar en el delito que concierne a este trabajo: el phishing.

El término phishing nace en el año 1987, Jerry Felix y Chris Hauck son las personas que lo referencian en el documento titulado "Sistemas de Seguridad: La perspectiva de un Hacker", vinculando dicho término con el método de imitación de un organismo o entidad de confianza, por parte de una persona ajena, un tercero, con miras a realizar una estafa.[101]

El primer ataque de phishing tiene lugar a mediados de los noventa, contra la compañía America Online (AOL), proveedora estadounidense de medios y servicios de acceso a internet, debido a su gran interacción social, los hackers fijaron su foco en ella. Los atacantes se hacían pasar por los empleados de AOL y enviaban correos electrónicos a los usuarios, o víctimas potenciales, en los mismos introducían el cebo: "verificar cuenta" o "confirmación de", y solo debían esperar a que los usuarios introdujesen sus claves, para comenzar con el ilícito; el método utilizado en los años noventa no se aleja del que utilizan en la actualidad.[102]

La palabra phishing proviene del inglés, es la contracción de *"password harcesting fhising: cosecha y pesca de contraseñas"*[103]. La etimología de phishing[104] se rige por el verbo fishing (pescar), haciendo una metáfora de la práctica de la pesca y la técnica empleada para cometer el delito, ya que lo que pretende es mediante un "anzuelo" o "señuelo" obtener información especialmente delicada. El cambio del "fis" al vocablo "ph", está relacionado con el término "phreaking" que es el estudio, comprensión y aprendizaje de las nuevas tecnologías; utilizando "ph" para identificar los ataques de estas comunidades de Phreaker o Hacker[105]. Tras esta introducción a esta figura delictiva, sus antecedentes y el significado de su denominación, continuaremos con los aspectos más técnicos de la materia en los siguientes epígrafes.

---

[101] *Vid.*CHARLES, Arthur: *Cyber wars: Hackeos que hicieron temblar el mundo empresarial*. España: Tell, 2019. pág.76-77 / BRIGHT HUB: *Phishing History - The Earliest Phishing Scams*[Link][28/05/2021]

[102] PHISHING [Link][22/02/2021

[103] SANCHIS CRESPO, Carolina: *Fraude electrónico…ob.cit.*pag. 268 y ss.

[104] ETIMOLOGÍA DEL PHISHING [Link][28/05/2021]

[105] Vid. JAKOBSSON, Markus/ MYERS, Steven: *Phishing and Countermesasures: Understanding the Increasing Problem of Electronic Identity Theft.* Nueva Jersey: John Willey & Sons, 2005.

7.-QUÉ ES EL PHISING Y CUALES SON LAS FIGURAS DELICTIVAS (O DELITOS) CON LAS QUE PUEDE RELACIONARSE

Previamente a introducirnos en materia legal, es necesario recordar que el phishing *"no es estrictamente una forma de hackeo: No se subvierte ningún ordenador para que haga algo que en teoría no debería hacer. La subversión se da en el usuario debido a las expectativas que tiene puestas en lo que le muestra el ordenador. De forma subconsciente, el usuario espera, dado que los ordenadores son fiables, que no permitan la aparición de ningún mensaje falso; que, del mismo modo que rechazaba los correos o las páginas web defectuosas, sepa detectar las webs y los correos falsificados. Pero los ordenadores solo hacen lo que se les ordena; si se les dice que muestren un mensaje para engañar al receptor, cumplirán su contenido"*[106]

El phishing es una figura delictiva, que estaría cubierta como modalidad dentro de la estafa que es un tipo penal de delito informático, entendiéndolo como: aquellas conductas ilícitas vinculadas a los sistemas informáticos. El bien jurídico está relacionado con el hecho informático, lo que no quiere decir que cualquier conducta delictiva vinculada a las nuevas tecnologías lesione el bien jurídico que realmente le incumple: el patrimonio, como veremos en los epígrafes siguientes. Lo más común de las conductas vinculadas a la delincuencia informática son, la lesión del bien jurídico tradicional por medio de las nuevas tecnologías.[107]

FLOR define el *phishing* como "una metodología de ingeniería social dirigida a obtener informaciones personales, costumbres o estilos de vida de otras personas, con el fin de acceder a servicios financieros o bancarios *online*, asumiendo virtualmente la identidad del titular de los datos de identificación" y añade posteriormente que a través del mismo "puede realizarse un hurto de datos, un abuso de información personal o un fraude de identidad".[108]Lo que podemos sacar en claro de esta definición es que el phishing es una actividad fraudulenta e ilícita mediante la cual se realizan actos de comunicación vía internet, o se utilizan virus informáticos, con el fin del acceso a datos sensibles de los usuarios. El ilícito penal que vamos a tratar en estos delitos informáticos es la estafa

[106] CHARLES, Arthur: *Cyber wars…ob.cit.*pág77.

[107]MUÑOZ CONDE, Francisco: *Derecho penal, parte especial.* Valencia: Tirant lo Blanch, 2019.pág.392-393. / Vid. Anexo 1: Evolución del Ciberdelito

[108] FLOR, Roberto: Phishing y delitos relacionados con el fraude de identidad: un World Wide Problem en el World Wide. *Robo de identidad y protección de datos*.2010, ISBN 978-84-9903-400-3.pág.83 y 84.

impropia[109] o fraude informático del art.248.2 CP.[110]La decisión de tratar esta figura delictiva como fraude informático es la riqueza descriptiva con la que nos dota este precepto y la que bajo nuestro punto de vista cubre la mayor parte de la figura delictiva, no obstante se hará una referencia a otros tipos penales que también pueden relacionarse con esta este fenómeno, ya que en la actualidad existen múltiples modalidades de phishing diferentes y es posible identificar los componentes intrínsecos esenciales al mismo y las modalidades más habituales. En el mismo sentido, no hay un único tipo de hacker que lo realicen, sino que es una actividad delictiva en la que participan diversos sujetos con actividades encomendadas de distinta naturaleza[111].

Antes de continuar, es importante hacer la referencia mencionada en los otros tipos penales, como son la posible sanción de los actos preparatorios[112] del phishing, como el spoofing o también denominada suplantación de identidad[113]. El spoofing es el primer

[109] Se considera estafa impropia por ser cometida mediante manipulación informática, tradicionalmente se ha considerado que dado que las máquinas no son susceptibles de engaño, quien conseguía obtener algo de una maquina sin las contraprestación establecida que para obtener el bien se exigía por su titular, no cometía una estafa; por ello el legislador en virtud de la generalización de la informática y sus inadecuadas manipulaciones, pretende asimilar estas conductas a la estafa propia, que es el tipo básico del art. 248.1CP, aunque no reúnan sus requisitos/Vid. ÁLVAREZ GARCÍA, Francisco Javier/ VENTURA PÜSCHEL, Arturo / MANJÓN-CABEZA OLMEDA, Araceli: *Derecho Penal Español, parte especial (II).*Valencia: Tirant lo Blanch, 2011.pág.229-230 y 251-252. / QUERALT JIMÉNEZ, Joan J.: *Derecho penal español, parte especial.* Valencia: Tirant lo Blanch, 2015.pág.552.

[110] Entre otros: MUÑOZ CONDE, Francisco: *Derecho penal, parte especial…ob.cit.*pág.393. / MIRÓ LLINARES, Fernando:Cibercrímenes económicos y patrimoniales. En ORTIZ DE URBINA GIMENO, Íñigo: *Memento práctico penal y económico y de la empresa.* Madrid: Francis Lefebvre, 2011.pág. 72 y ss.

[111] *Se ha producido una especialización en los delincuentes que realizan este tipo de estafas, así, no es extraño encontrar grupos de ciberdelincuentes que se organizan diferenciando entre mensajeros, recolectores y cajeros.*/ MYERS, Steven.: Introduction to Phishing. En: JAKOBSSON, Markus/ MYERS, Steven: .: *Phishing and Counter- measures: Understanding the Increasing Problem of Electronic Identity Theft.* Nueva Jersey: John Willey & Sons, 2006.pág. 3/ *Los primeros, bien sean spammers o hackers, remiten un gran número de correos, generalmente a través de bot-nets, es decir, redes de ordenadores comprometidos y controlados por el mensajero. El segundo grupo, el de los recolectores, son hackers que construyen o alteran las webs a las que se dirigen los usuarios victimas de spam y de las que se obtiene información confidencial como nombres de usuario, contraseñas o tarjetas de crédito. Un tercer grupo es el de los cajeros, los cuales obtienen información confidencial de los recolectores y hacen uso de ella, creando tarjetas de crédito para obtener dinero en cajeros, comprar productos en línea, hacer transferencias y, en definitiva, cualquier actividad que permita el lucro esperado.*

[112] *En virtud del art.15CP solo son punibles con carácter general el delito consumado y la tentativa art.16.1CP, fase ejecutiva. Sin embargo, el legislador introduce en ciertos delitos especiales el castigo de la "conspiración, proposición y provocación" , como la tenencia de explosivos del art.568CP*. ARROYO ZAPATERO, Luis/ BERDUGO GÓMEZ DE LA TORRE, Ignacio/ FERRÉ OLIVÉ, Juan Carlos.: *Curso de Derecho Penal, parte general.* Barcelona: Ediciones Experiencia, 2016.pág.480-482.

Nuestro CP prevé en su parte especial los actos preparatorios de conspiración, proposición y provocación de determinados delitos. Los actos preparatorios no son relevantes penalmente, y por lo general no son punibles, exceptuando los que se tipifican de forma expresa y que si llevan una pena asociada como la tenencia de explosivos art. 568CP, se denominan delitos preparatorios.

[113]*El spoofing no solo se utiliza en el phishing, sino que se una práctica habitual de los cibercriminales, no obstante, como indica* FLOR, *todos los informes e investigaciones realizadas por organismos nacionales e internacionales sobre el "hurto de identidad" han incluido los phishing attacks entre las principales*

paso de lo hackers para perpetrar estos delitos informáticos. No es sencillo en términos de calificación penales, no obstante, se podría calificar ese comportamiento bajo el art.401CP *"El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años",* aunque se podría considerar que esta calificación no es posible, por no ser continua la suplantación de identidad. Por el contrario, es entendible que en este artículo se proteja la fé publica, la confianza de la comunidad en la veracidad de identificación de las personas, afectando al bien jurídico colectivo. Otra posible calificación, sería la que se desprende del art.402CP "*El que ilegítimamente ejerciere actos propios de una autoridad o funcionario público atribuyéndose carácter oficial, será castigado con la pena de prisión de uno a tres años".* Este artículo se utiliza en el caso de que la suplantación sea de las entidades publicas estatales, como puede ser la Agencia Tributaria, y estaríamos ante un delito de usurpación de funciones públicas. Otros autores, entienden el delito como falsedad documental[114], pero no tiene mucho alcance[115] debido

técnicas empleadas para realizar el "fraude de identidad" en la sociedad de la información;FLOR, Roberto: Phishing y delitos relacionados…ob.cit. p. 82.

[114] Así lo entiende VELASCO NÚÑEZ, Eloy: Fraudes informáticos en la red, del phishing al pharming. *La Ley penal: revista de derecho penal, procesal y penitenciario.*2007, ISSN 1697-5758 Nº37, pág.61, *hay quien dice que no existiendo en España el delito de suplantación informática de la personalidad, es necesario castigar por este tipo conductas que atacan al bien jurídico de ese delito: "la confianza en las transacciones mercantiles, en este caso, a través de la llamada banca, venta o pago on-line".*

[115] *Podrían excepcionarse aquellos casos en los que lo que se falsee, si pueda considerarse lo que tradicionalmente ha entendido la jurisprudencia como un documento mercantil. Según expresan la STS núm. 35/2010, de 4 de febrero de 2010, en su fundamento quinto, la STS núm. 788/2006, de 22 de junio de 2006, y la STS núm. 764/2008, de 20 de noviembre de 2008, en su fundamento segundo, basándose a su vez en otras resoluciones como la STS núm. 625/1997, de 8 de mayo de 1997, y la STS núm. 1148/2004, de 18 de octubre de 2004, el concepto jurídico-penal de documento mercantil es "un concepto amplio, equivalente a todo documento que sea expresión de una operación comercial, plasmado en la creación, alteración o extinción de obligaciones de naturaleza mercantil, ya sirva para cancelarlas, ya para acreditar derechos u obligaciones de tal carácter, siendo tales no solo los expresamente regulados en el Código de Comercio o en las Leyes mercantiles, sino también todos aquellos que recojan una operación de comercio o tengan validez o eficacia para hacer constar derechos u obligaciones de tal carácter o sirvan para demostrarlas, criterio éste acompañado, además por un concepto extensivo de lo que sea aquella particular actividad. Como documentos expresamente citados en estas leyes figuran las letras de cambio, pagarés, cheques, órdenes de crédito, cartas de porte, conocimientos de embarque, resguardos de deposito y otros muchos: también son documentos mercantiles todas aquellas representaciones gráficas del pensamiento creadas con fines de preconstitución probatoria, destinadas a surtir efectos en el tráfico jurídico y que se refieran a contratos u obligaciones de naturaleza comercial, finalmente, se incluye otro tipo de representaciones gráficas del pensamiento, las destinadas a acreditar la ejecución de dichos contratos tales como facturas, albaranes de entrega u otros semejantes". Añade, sin embargo, la STS 788/2006 de 22 de junio de 2006, en su fundamento primero, que a pesar de esta consolidada jurisprudencia "la moderna jurisprudencia no se ha mostrado insensible al sentido restrictivo del concepto que impera en la praxis mercantilista, habiéndose declarado que el hoy artículo 392 del Código Penal se refiere sólo a aquellos documentos mercantiles merecedores de una especial protección, porque su materialidad incorpora una presunción de veracidad y autenticidad equivalente a un documento público, lo que es la «ratio legis» de la asimilación, de modo que «no es suficiente con que se trate de un documento utilizado en el tráfico mercantil, sino que se requiere una especial fuerza probatoria, como ocurre con las letras de cambio, que sin una protección especial difícilmente podrían ser transmisibles por endoso en la forma habitual». De este modo, pues, y frente a la falsificación de documentos privados tipificada con*

a que una web no entraría dentro del art.26CP donde nos define el tipo de documento como "todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica"[116]. Tampoco podríamos englobarlo dentro del art.274CP por no ser un fin industrial ni comercial, el que pretende el hacker, por lo que quedaría esta conducta de spoofing como atípica en estos últimos dos casos. Otro tipo de calificación en este tipo de delitos spoofing, vinculada a un delito contra la intimidad, es aplicar el art.97.1CP: "El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de (…), mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses", considerando que en el tipo básico podemos percibir como se pretende con este artículo evitar la vulneración de la intimidad de las personas, sobre todo cuando hablamos de claves y operaciones bancarias, pudiendo considerar este tipo de información como personal o privada y queda amparada en la intimidad. En nuestra opinión, es compleja la elección de un precepto u otro para sancionar la conducta, no obstante, parecería mas conveniente optar por el art.197.1 CP, aunque resultare difícil dilucidar si estuviésemos ante un concurso ideal medial entre delito de descubrimiento y el delito patrimonial, en el caso de que el sujeto intercepte la comunicación y consiga la clave de acceso. No obstante, lo normal es la utilización de programas sniffer con el fin de conseguir la clave o que sea la persona la que teclee en el url la información confidencial, por lo que es posible que no entrase dentro de la definición de secreto personal relacionado con la privacidad de la persona[117]. En el caso de apoderamiento masivo de correos electrónicos

carácter residual en el artículo 395 del CP, al que se llega por exclusión de los restantes tipos de documentos (es decir, aquéllos que, reuniendo los requisitos del artículo 26 del CP, no sean públicos, oficiales y mercan- tiles) y que también recoge el artículo 324 de la LECiv, no cualquier documento, ni siquiera aunque se refiera a publicidad de una empresa, debiera reputarse documento mercantil, sino sólo aquel que pueda ofrecer una especial fuerza probatoria. Creo que generalmente no será el caso en los supuestos de web spoofing y de phishing.

[116] En sentido contrario, MATA Y MARTÍN, que considera que "La naturaleza electrónica de la pagina web no introduce dificultades para su calificación como documento, pero lo que puede generar más incertidumbre sobre su carácter son las funciones múltiples de las mismas o si es la pagina web la que directamente constituye un documento o en realidad lo son aquellos que se generen como consecuencia de alguna operación realizada con ella. MATA Y MARTÍN, Ricardo: *El robo de identidad y protección de datos.* Madrid: Marcial pons,2010.pág.216.

[117] En este sentido, se plantea MATA Y MARTÍN, *si es posible la aplicación de este tipo a los casos "en los que es el usuario el que facilita los datos reservados, entrega que realiza ante una petición fraudulenta, como sucede en el phishing o pharming", para posteriormente concluir que no debe aplicarse para estos*

o análogos, considero como lo sugiere MATA Y MARTÍN que podría sancionarse el phishing por el articulo 197.1CP, y en los casos de que los datos pertenezcan a personas jurídicas y empresas, sería posible el art.200 o 278 y ss CP.[118]

En otros, vinculados al phishing, como actos preparatorios tenemos el acceso informático ilícito, tratándolo en el art.197.3CP como intrusismo informático o acceso ilícito al sistema por la vulneración de las medidas de seguridad[119]. También los medios informáticos aptos para la comisión del delito de estafa como: delitos de fabricación, introducción, posesión o facilitación de programas de ordenador del art.248.2b) CP, programas keyloggers o sniffers, con este artículo se pretende una anticipación de la tutela penal a la realización del fraude[120].

Continuando con la figura delictiva de phishing, esta se encuentra formada, por lo general, por tres componentes: MENSAJE, INTERACCIÓN Y ROBO: El mensaje, caracterizados por el uso de ingeniería social, la automatización con el envió de correos masivos, la comunicación electrónica como medio, y la suplantación de entidad o empresa legítima[121]. Pues bien, como hemos dicho, consiste en el envío indiscrimado y de forma masiva de correos electrónicos o mensajes de texto[122] a usuarios de la red, por lo general, aunque hay dos variantes que irrumpen con fuerza: mensajes en redes sociales

---

casos el art. 197, pues la utilización del verbo apoderarse reafirma que "no resulta compatible con una mera conducta pasiva ni con una acción puramente fraudulenta". MATA Y MARTÍN, Ricardo.: *El robo de identidad..., ob. cit.*pág. 212 y 213.

[118] Apunta MATA Y MARTÍN, R.: *El robo de identidad*...ob. cit., pág. 214.

[119]ALMENAR PINEDA,Francisco:El delito…ob.cit.pág.140/ MIRÓ LLINARES, Fernando: Cibercrímenes…ob.cit./COLÁS TURÉGANO,Asunción: Los delitos de género…ob.cit. pág.219/ ROMEO CASABONA,Carlos María (…) Derecho penal, parte especial…ob.cit/ .

DEL CARPIO DELGADO, Juana(coor.) / BOZA MORENO, Elena / DEL VALLE SIERRA LÓPEZ, Mª:*Algunas cuestiones de parte especial tras la reforma de 2015 del Código Penal.* Valencia: Tirant lo Blanch, 2018. Pág.174-175.

[120] "No encontramos ante una considerable anticipación de barreras penales mediante la tipificación de actos que ni siquiera merecen el calificativo de preparatorios, pues son por completo ajenos a los referidos en los art.17 y 18 CP(…) estructuras que son frecuentes en el CP y se plantean posible colisión con el principio de presunción de inocencia" ALVAREZ GARCÍA, Javier/ MANJÓN-CABEZA OLMEDA, Araceli/ VENTURA PÜSCHEL, Arturo: Derecho Penal Español, parte especial. Valencia: Tirant lo Blanch, 2011.pág.254-256.

[121] MICROSOFT SEGURIDAD: *What is social engineering? Social Engineering, Phishing and Email Hoaxes*, julio 2021 [Link][04/06/2021].

[122] *Como sucede en los delitos tradicionales, el phishing ha ido evolucionando a medida que los usuarios van conociendo este tipo de fraudes, pasando ahora a los denominados "smishing", mencionados con anterioridad, donde el mensaje se transmite vía SMS, aprovechando el incremento de las redes sociales como puede ser WhatsApp y que todas las comunicaciones suelen realizarse por este medio, se dota a los SMS de un carácter más formal, aprovechando los phisher para evolucionar en su método de estafa, ya que en un principio solo se buscaban datos bancarios, pero en una sociedad donde los datos son la panacea, buscan todo tipo de información.*

o en videojuegos.[123]En estos mensajes se suplanta la imagen de una entidad u organización conocida por el usuario, ¿porqué? para aportar al usuario la confianza necesaria para vulnerar la primera barrera: la persona[124]. Este señuelo desde un punto de vista técnico es poco sofisticado pero es la ingeniería social la que aprovechándose de las debilidades de las potenciales victimas la que consigue el engaño.[125] Por lo que podríamos enlazar con la definición que Kevin David Mitnick, uno de los hackers estadounidenses más famosos de la historia, afirmó: "*El núcleo principal del phishing es la astucia del creador, con el fin de engañar a un sistema o persona mediante la ingeniería social, Los ingenieros sociales se basan en cuatro puntos básicos para atacarnos*: *Todos queremos ayudar, confianza hacia el otro, no nos gusta decir que no y nos gusta que nos alaben.* Con estas cuatro premisas los hackers, o phishers en nuestro caso, van a conseguir lo que quieren, por eso es muy importante concienciarse e interpretar correctamente las políticas de seguridad, y cumplirlas.[126]

Gracias a estas técnicas de engaño utilizadas por los phishers,[127] el usuario aporta el segundo elemento: la interacción. Lo común en estos correos electrónicos es el uso del "factor miedo", por lo general pueden advertir de un impago o la caducidad de un servicio contratado, o también pueden alegar la necesidad de "por motivos de seguridad"[128], "mantenimiento", "mejora de servicio" etc, en el mismo correo te ofrecerán un enlace para que el usuario a través de él acceda a la página web[129] y "resuelva" los problemas

---

[123]HONG, JASON: The estate of phishing attacks. *Communications of the ACM.*2012, Vol. 5, Nº 1.pág. 74. *En relación con los juegos masivos online, HILVEN y WOODWARD señalan que el valor de una cuenta robada de War of Warcraft es superior al de una tarjeta de crédito, lo que puede ayudar a comprender las complejas consecuencias de esta modalidad de fraude.*

[124]*VELASCO NÚÑEZ, Eloy: Fraudes informáticos…ob.cit.* pág.21.

[125] *Algunos ejemplos de la aplicación de estos principios son los mensajes en los que se requieren actualizaciones de seguridad, se insta a completar información de cuentas para su mantenimiento, incentivos financieros o falsas actualizaciones. Así, podemos encontrar mensajes del supuesto administrador de un sistema advirtiendo sobre un ataque, que debe evitarse instalando urgentemente un "parche", o la notificación de problemas con la autenticación de usuario, cuya solución consiste en la remisión de una nueva contraseña. En otros casos, el mensaje contiene una proposición relacionada con futuras ganancias o* beneficios, que finalmente busca aprovechar el animo de lucro de la victima para provocar ingresos de dinero en cuentas. Las ofertas, premios, promociones o regalos constituyen otro de los reclamos utilizados, junto con la solicitud de ayuda humanitaria para victimas de desastres o situaciones desesperadas.

[126] Vid.Pelicula Trackdown, conocida en España como El asalto final o Hackers 2: Operación Takedown.

[127] PHISHER *: La persona que intenta engañar a un tercero mediante phishing*. Cambridge dictionary [Link][02/02/2021]

[128] *Es en este punto, dónde adquiere relevancia la ingeniería social, aprovechándose el phisher de la debilidad de las personas para proceder con el ataque.* Vid. MICROSOFT SEGURIDAD, *Todo lo que debe saber acerca del phishing*, Julio 2021.[Link][02/02/2021]

[129]*Recordar que el Pharming, ya explicado, puede ser mediante esta técnica de envío de correo o introduciéndose el servidor del usuario y cambiando el DNS o programa host, conduciendo al usuario a*

planteados, mediante el enlace accederá a la página web suplantada de la identidad de confianza. Una vez en la web solicitaran claves de acceso a esa entidad u organización, números secretos e información de tipo personal que al usuario no le extrañará que pidan, ya que es el método que utiliza para acceder con normalidad, es este momento donde comienza la estafa.[130] Es importante mencionar que la técnica por la que el phisher intenta recopilar las contraseñas de los usuarios de internet se denomina *password harvesting*[131] *(cosecha y pesca de contraseñas).*[132]Así mencionar las variantes de phishing utilizadas: **"Pharming, Vishing, Smishing":**

- **Pharming:** El estafador crea una web idéntica y paralela a la entidad que suplanta, redirigiendo a la víctima mediante un correo electrónico con un enlace en el que debe pinchar o bien introduciéndose en el sistema informático del tercero y cambiar las direcciones DNS (domain name server)o archivos *host*[133], para acceder a la supuesta web de la entidad de confianza. Esta técnica está basada en el uso de "redirectores": Utilización de la Red para conseguir el acceso al sistema de nombres de dominio o DNS, y modificar las direcciones del URL e IPs; también al router para modificar el servidor DNS; alterar las direcciones URL e IPs del archivo hosts o la configuración de la DNS dirigiendo a la victima a un servidor DNS controlado por los atacantes. El fin es redirigir a los usuarios a una pagina falsa diseñada por los hackers o scammers, que crean su "granja de victimas"[134], con el fin de obtener datos sensibles al dejar constancia de sus claves de acceso y firma electrónica.
- **Vishing:** Técnica en la que utilizan llamadas telefónicas, con el fin de engañar a la victima usuaria, suplantando a compañías de servicios o de gobierno, para que los usuarios o futuras victimas, revelen información personal o privada. El modus operandi de esta técnica, en primer lugar es el envío de un correo electrónico a la futura victima, suplantando a una entidad, en el mismo, se piden datos sensibles de índole bancaria, como pueden ser el número de la cuenta, número de la tarjeta, fechas de expiración, que debido a algún tipo de fallo deben de volver a introducirse para solventar el problema, añadiendo el deber del cliente a contactar con urgencia a la entidad de confianza; en el correo la

una página que no es la deseada, sino la creada por los phisher o scammers. FERNÁNDEZ TERUELO, Javier Gustavo: *Cibercrimen: Los delitos cometidos a través de Internet: estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red.* Oviedo: Constituio Criminalis, 2007.pág.29 y ss. / VELASCO NÚÑEZ, Eloy: Estafa informática y banda organizada. Phishing, pharming, smishing y muleros. *Ley penal: revista de derecho penal, procesal y penitenciario.*2008, ISSN 1697-5758 Nº49, pág.19-29.pág.21.

[130]VELASCO NÚÑEZ, Eloy: Fraudes informáticos…ob.cit.pág.57 y ss.

[131] "*La recolección de credenciales, también conocida como recolección de contraseñas, es el proceso de recopilar nombres de usuario, contraseñas, correos electrónicos privados y direcciones de correo electrónico válidos a través de violaciones de infraestructura. Las posibles motivaciones para tal violación son muchas: los piratas informáticos podrían vender datos personales y financieros delicados en la web oscura; obtener acceso a la red de una empresa con fines de espionaje corporativo y robar propiedad intelectual u otros activos; o utilizar los datos para malversar dinero".* CREDENTIAL HARVESTING [Link][22/06/2021]

[132] *Para completar el engaño, emplean todo tipo de subterfugios técnicos, como la ofuscación de URL o la utilización de supuestas webs seguras de terceras partes o autoridades de validación, las cuales disponen de medidas de seguridad suplementaria como URL https, o certificados SSL; estas entidades utilizan gráficos e imágenes que son igualmente replicadas por los diseñadores de las falsas webs.*

[133] *El servidos DNS y los programas host contienen las direcciones IPs o secuencia numérica de las direcciones electrónicas o URL de las páginas que se visitan*. Vid.:FERNANDEZ TERUELO, *Cibercimen*, p.30. VELASCO NÚÑEZ, Eloy: Estafa informática…ob.cit.pág.21/ VELASCO NÚÑEZ, Eloy: Fraudes informáticos…ob.cit.p.59 y ss.

[134]VELASCO NÚÑEZ, Eloy: Fraudes informáticos…ob.cit. pág. 59 y ss.

futura victima encontrará un número de teléfono gratuito al que debe contactar para confirmar los detalles que le solicitaban en el correo, una vez efectuada la llamada, la futura victima será atendida por una voz computerizada que le ayudara en el proceso para solventar el problema mencionado en el correo, consiguiendo el ciberdelincuente los datos necesarios para perpetrar el delito. El segundo tipo de vishing es mediante la configuración de un *war dialing*[135] por parte del cibercriminal, para llamar a teléfonos de una zona, en cuanto la llamada es atendida por la víctima, ésta será engañada por una grabación donde se alerta al cliente, normalmente bancario, de que su tarjeta esta siendo utilizada de forma fraudulenta, debiendo de llamar a un numero de teléfono para resolver el problema, iniciándose de nuevo el mismo proceso de petición de datos sensibles bancarios que en el caso anterior. En este tipo de delitos el cibercriminal es denominado como "visher".

- **SMShing:** Utilización de mensajes de telefonía móvil, SMS, donde se solicitan datos para obtener el numero de la tarjeta bancaria, la caducidad de la misma o similares, solicitando que llame a un numero de teléfono o se le redirija a una enlace web para completar los datos que faltan, así consiguen datos sensibles bancarios con el fin de crear tarjetas bancarias falsas (Skimming[136]) para uso personal.[137] Las variantes de este tipo de delito han variado, ahora no solo suplantan entidades bancarias si no que acceden a esos datos con otro tipo de cebos en el mensaje " ha ganado usted x premio", "con motivo del covid-19 el estado dotara a las familias con x cantidad" todos redirigiéndote mediante un enlace para cubrir datos bancarios y poder cobrar las ayudas, o regalos. [138]

Podemos comprobar que, en todas las variantes, la información que pretende el phisher captar es desde personal, como pueden ser dirección de correo electrónico, DNI, datos de contacto, como de acceso a redes sociales, llegando a la más peligrosa que sería la información financiera, con números de tarjeta de crédito, números de cuenta bancarias; causando al usuario un perjuicio.

Por útlimo llegamos al tercer elemento que caracteriza al phishing: El robo (apoderamiento), llegando a la utilización efectiva de la información obtenida, lo normal es que el phisher no explote por sí mismo la información y la revenda a terceros, aunque también existen casos en los que ellos usan directamente los datos de la victima y suplantan su identidad.

En virtud de los datos que hemos ido recopilando a los largo de este epígrafe podríamos decir que: el phishing es un mecanismo criminal basado en la suplantación de una identidad personal de otro (spoofing), mediante el uso de la ingeniería social, conjunto de técnicas psicológicas y habilidades sociales que buscan comprometer la información sensible de un usuario, y subterfugios técnicos que implican la instalación de crimeware

---

[135]."WAR DIALING"[Link][22/02/2021] *referido al sistema de marcación automática de varios números telefónicos, con el fin de encontrar el "punto débil" en la arquitectura de seguridad de las TIC.*

[136] Anexo 4: skimming**Error! Reference source not found.**

[137] *Este tipo de técnicas, podrían entrar en concurso de leyes de falsificación de tarjetas bancarias 399bis CP con la modalidad de estafa 248.2.c) CP.*

[138]OSI: *El fraude de los SMS* [Link][17/02/2021]

en ordenadores personales[139].Y debido a la especialización de los sistemas electrónicos podemos ver que existen diferentes tipos de phishing. El sujeto en estos casos no se denomina hacker sino phisher. Cabe aclarar que es similar al hacking normal, con la diferencia de que no se interactúa con una máquina, sino con una persona o usuario, basándose en la confianza que depositas en ciertos organismos o entidades.

El phishing cada vez es más relevante en nuestra sociedad, por un lado, vinculado a la innovación en el método de entrada, y, por otro lado, debido a las importantes pérdidas económicas que causa, el FBI calculó en su informe anual, que las pérdidas reportadas desde 2019 superaron en 2020 los 4,2 millones de dólares, encontrándose España en la lista del top veinte por número total de víctimas en estos ataques.[140]

8.- ANTECEDENTES LEGISLATIVOS DE LA ESTAFA INFORMÁTICA.

Hemos expuesto en el epígrafe anterior los tipos penales posibles de adecuación del phishing, considerando el más idónea el de la estafa informática 248.2CP. Pero antes de exponer tal tipo penal es necesario hablar del delito de estafa tipo básico art. 248.1 CP y sus antecedentes. A mediados del Siglo XIX, el delito de estafa comenzó a ser objeto de elaboración y tratamiento dogmático. Debemos remontarnos al CP de 1822, en su art.766 que "castigaba al que con algún artificio, engaño, superchería, práctica supersticiosa u otro embuste semejante hubiere sonsacado a otros dineros, efectos o escrituras, o le hubiere perjudicado de otra manera en sus bienes, sin alguna circunstancia que le constituya verdadero ladrón, falsario o reo de otro delito especial, sufrirá la pena de reclusión por el tiempo de un mes a dos años, y una multa de cinco a cincuenta duros, sin perjuicio de la mayor pena que merezca como ladrón, falsario o reo de otro delito, si juntamente lo fuere". Y en el mismo cuerpo legislativo, el art.768 castigaba con una pena mayor a los que habitualmente cometiesen el delito del artículo anterior o art.771 especial protección a los menores o incapaces[141].

El CP español continuó evolucionando, llegando a la LO 8/1983[142], momento en el cual, el legislador definió con exactitud el delito de estafa, introduciendo dos elementos: el engaño bastante y el error. "Art.528: cometen estafas los que con ánimo de lucro utilizan engaño bastante para producir error en otro, induciéndole a realizar un acto de disposición

[139] APWG [Link][17/02/2021]
[140]INTERNET CRIME COMPLAINT CENTER [Link][17/02/2021]
[141] CHOCLÁN MONTALVO, José Antonio: *El delito de estafa.* Barcelona: Bosch, 2009.pág. 21-27.
[142] Ley Orgánica núm. 8/1983, de 25 de junio, BOE 27 junio 1983.

en perjuicio de sí mismo o tercero". Otras LO que introdujeron cambios significativos en este tipo de delitos fueron, la LO 10/1995 en la que se sustituye la rúbrica "de las estafas y otros engaños" a únicamente "estafas", separando este capítulo de los delitos de "propiedad intelectual e industrial". La LO 15/2003, del 25 de noviembre, la LO 5/2010, del 22 de junio y la LO 1/2015, del 30 de marzo, realizan una ampliación de las modalidades de estafa recogidas en el 248.2 y del tipo agravado en el art.250CP.

El CP español actual mantiene la misma definición que la LO 8/1983 como apuntan COBOS GÓMEZ DE LINARES, MUÑOZ CONDE y PÉREZ MANZANO [143], ésta constituye la definición moderna de estafa que de facto ya habían adoptado la doctrina y la jurisprudencia gracias al trabajo previo de ANTÓN ONECA, publicado en 1958[144]; además de introducir en el art.248.2 un nuevo tipo penal: la estafa informática. El delito propio de estafa se encuentra recogido en el art.248.1CP que es aquel en el que se recogen una serie de hechos que tienen como denominador común el que se produce un perjuicio patrimonial mediante una conducta engañosa[145]. El SA de este delito es indeterminado o no cualificado[146] y el BJP es el patrimonio ajeno[147], cuando es atacado por medios insidiosos y fraudulentos, ya que este delito no sólo lesiona o pone en peligro la propiedad, sino otros valores como la posesión o el derecho de crédito.[148] Los elementos esenciales para la existencia de la estafa son: en primer lugar, el ENGAÑO: consiste en hacer creer a alguien algo que no es verdad. La jurisprudencia[149] señala las características que deben poseer, por un lado que sea precedente o concurrente[150] y por

[143] COBOS GÓMEZ DE LINARES, Miguel Ángel: *Las defraudaciones, estafa, apropiación indebida, defraudaciones de fluido eléctrico y análogas.* En: RODRÍGUEZ RAMOS, L.: *Derecho penal, parte especial, tomo II.* Madrid: Servicio de Publicaciones de la facultad de Derecho de la Universidad Complutense de Madrid, 1996.pág.159 / MUÑOZ CONDE, Francisco: *Derecho penal, parte especial.* Valencia: Tirant lo Blanch, 2012.pág. 429 / PÉREZ MANZANO, Mercedes*:* Las Defraudaciones (I). Las Estafas. En BAJO FERNÁNDEZ, Miguel: *Compendio de Derecho penal. Parte especial*. Madrid: Centro de Estudios Ramón Areces,1998, pág. 440.

[144] ANTÓN ONECA, José: *Estafa, nueva enciclopedia jurídica.* Barcelona: Francisco Seix, 1958.pág.56 y ss.

[145] MUÑOZ CONDE, Francisco: *Derecho penal, parte especial…ob.cit.*pág.392.

[146] SERRANO GÓMEZ, Alfonso/ SERRANO MAÍLLO, Alfonso/ SERRANO TÁRRAGA, Mª Dolores/ VÁZQUEZ GONZÁLEZ, Carlos: *Curso de derecho penal, parte especial.* Madrid: Dykinson, 2019.Pág.321./ ZUGALDÍA ESPINAR, José Miguel / MORENO-TORRES HERRERA, Mª Rosa / DE ESPINOSA CEBALLOS, Elena Marín: *Lecciones de derecho penal, parte general.* Valencia: Tirant le Blanch, 2021.pág.221. / MUÑOZ CONDE, Francisco: *Derecho penal, parte especial…ob.cit.*pág.393-395.

[147] STS de 19/04/2002.

[148] SERRANO GÓMEZ, Alfonso(…)*Curso de derecho penal, parte especial…ob.cit.*Pág.321.

[149]STS 1-4-2003.

[150] *La STS 8-2-2002 lo califica como espina dorsal, factor nuclear, alma y sustancia de la estafa, fruto del ingenio falaz y maquinador de los que tratan de aprovecharse del patrimonio ajeno. SUAREZ-MIRA*

otro lado que sea bastante[151]. Este engaño puede ser explícito, haciendo afirmaciones rotundas, o implícito, ocultando el propósito de incumplir pero sin afirmar falsamente[152]. Otro elemento es el ERROR: sucede cuando existe una distorsión entre lo que imagina el SP, sobre quien recae la acción, y lo que sucede en realidad[153]. A continuación, tenemos la DISPOSICIÓN PATRIMONIAL: éste elemento consiste en cualquier comportamiento de la persona inducida a error que ocasione de forma directa un daño patrimonial a sí misma o a un tercero, no siendo necesario que concurran en la misma persona la condición de engañado y de perjudicado [154]. El PERJUICIO PATRIMONIAL: es la disminución del patrimonio de forma lesiva para el perjudicado,[155]que debe ser superior a cuatrocientos euros, debido a que por debajo de esa cantidad constituiría el delito leve del párrafo 2º del art.249 CP. La consumación del delito de estafa se produce con el efectivo perjuicio patrimonial sufrido por la víctima, sin ser necesario que el estafador obtenga el lucro[156].Llegamos a los dos últimos elementos, el DOLO *antecedents*, (conocimiento y voluntad de realizar lo anterior) tiene que anteceder o ser concurrente en la dinámica defraudatoria*[157]*, solo cabe el dolo directo. Y por último el ÁNIMO DE LUCRO como *elemento especial subjetivo del injusto* exigido por el art.248CP, consiste en el deseo, expectativa, de tener cualquier tipo de ventaja, beneficio o utilidad, tanto para el auto del delito como para un tercero. Debe de existir un propósito por parte del infractor de obtener una ventaja patrimonial correlativa al perjuicio típico ocasionado.[158]. Los hechos deben

*RODRIGUEZ, Carlos / PIÑOL RODRÍGUEZ, José Ramón / JUDEL PRIETO, Ángel: Manual de derecho penal, tomo II, parte especial. Madrid: Civitas, 2018.*pág.356.

[151] *Ha de ser suficiente y proporcional para la consecución de los fines propuestos en cualquiera que sea su modalidad. SSTS de 8-2-2002 y 23-10- SUAREZ-MIRA RODRIGUEZ, Carlos(…)Manual de derecho penal…ob.cit.*pág. 356.

[152] SUAREZ-MIRA RODRIGUEZ, Carlos(…)*Manual de derecho penal…ob.cit.*pág.357.

[153] STS 3-4-2001 *Como consecuencia del engaño, tiene lugar la originario o producción de un error esencial en el SP, desconocedor o con conocimiento deformado o inexacto de la realidad, por causa de la insidia, mendacidad, fabulación o artificio del agente, lo que lleva a actuar bajo una falsa presuposición, a emitir una manifestación de voluntad partiendo de un motivo viciado, por cuya virtud se produce traspaso patrimonial /* MUÑOZ CONDE, Francisco*: Derecho penal, parte especial…ob.cit.*pág.*398. /* SUAREZ-MIRA RODRIGUEZ, Carlos(…)*Manual de derecho penal…ob.cit.*pág.357. / ZUGALDÍA ESPINAR, José Miguel(…)*Lecciones de derecho penal…ob.cit.*pág.221

[154] STS 26-9-2002 Vid. SUAREZ-MIRA RODRIGUEZ, Carlos*(…)Manual de derecho penal…ob.cit.*pág 357./ ZUGALDÍA ESPINAR, José Miguel(…)*Lecciones de derecho penal…ob.cit.*pág.221.

[155] Ver STS 23-12-2013 y STS 14-3-2014.

[156] SERRANO GÓMEZ, Alfonso: *Curso de derecho penal…op.Cit.,*Pág.325.

[157] *No se valora penalmente el dolo subsequens, el sobrevenido y no anterior a la celebración del negocio que se trate*. ZUGALDÍA ESPINAR, José Miguel*(…)Lecciones de derecho penal…ob.cit.*Pág.222

[158]ZUGALDÍA ESPINAR, José Miguel(…)*Lecciones de derecho penal…ob.cit.*pág.222-223. / SUAREZ-MIRA RODRIGUEZ, Carlos(…)*Manual de derecho penal…ob.cit.* pág.358.

sucederse progresivamente y de forma encadenada[159], así desde el punto de vista objetivo, el engaño debe desencadenar el error, el error debe de dar lugar a la disposición patrimonial, y la disposición patrimonial debe ocasionar el perjuicio.[160] Entre engaño y perjuicio debe mediar una relación causa-efecto, ya que si falta esa relación no existe la estafa[161]. Desde el punto de vista subjetivo, todos los elementos mencionados deben estar abarcados por el dolo del autor en el mismo orden mencionado [162].

Figura 1: Elementos Estafa tipo básico.

9.-CIBERDELITOS: EL PHISHING COMO DELITO EN NUESTRO CP

Hemos hablado sobre el delito de estafa, la conducta de phishing y sobre la existencia de actos ilícitos que lo acompañan y tienen lugar antes de que se produzca el perjuicio económico, pudiendo ser estos actos sancionados penalmente. Ahora nos dedicaremos a tratar el phishing desde la perspectiva de calificación jurídica como hemos introducido previamente como el delito de estafa informática. La modalidad de estafa impropia o informática del art.248.2.a), surge en relación con una laguna que existía en nuestro ordenamiento jurídico vinculada a la insuficiencia del tipo básico de la estafa para abarcar los desapoderamientos patrimoniales que se realizaban por medio de las TICs,[163] así el término del artículo "manipulación informática" como afirman VIVES ANTÓN o

[159] MATA Y Martín, Ricardo :*cada elemento es presupuesto del siguiente y consecuencia del anterior"* visto en: ZUGALDÍA ESPINAR, José Miguel(…)*Lecciones de derecho penal…ob*..cit. Pág.219
[160] STS 21/9/12 y 17/1/13
[161] MUÑOZ CONDE, Francisco: *Derecho penal, parte especial…ob.cit.*pág.393.
[162] STS 24/9/01 y 21/9/12
[163] SUAREZ-MIRA RODRIGUEZ, Carlos(…)*Manual de derecho penal…ob.cit.*pág359-361.

GONZÁLEZ CUSSAC "sustituye al engaño y el error a los que se refiere la estafa propia, pero se mantendría la naturaleza del fraude".[164]

En nuestro CP no encontramos una lista que especifique las variantes de estafa informática, lo que sí podemos encontrar son delitos que contemplan a la informática como el medio comisivo a través del cual se lesionan distintos bienes jurídicos como el patrimonio o la intimidad y también podemos encontrar delitos que tienen como objeto material los sistemas o soportes informáticos. Debido a que el fraude informático contiene múltiples conductas que causan perjuicio económico en un tercero mediante el uso de los medios informáticos, se debe analizar en primer lugar en que consiste cada conducta y vincularlas a los delitos recogidos en el CP.[165]

Los delitos contra el patrimonio y contra el orden socioeconómico se recogen en el titulo XIII del Libro II del CP, en este título se protegen tanto los intereses patrimoniales en sentido estricto, como los de carácter más amplio referidos al orden económico con transcendencia social. Encontramos así en este contexto, el articulo 248.1 CP, mencionado en el epígrafe anterior, y el articulo 248.2 CP que regula la estafa informática o phishing, en los apartados *a y b,* y la utilización fraudulenta de tarjetas de crédito o cheques de viajes del apartado *c*.

Previo a analizar el art. 248.2 CP, se debe dejar clara la figura del SA [166] que en este delito se le denomina phisher, que en principio puede ser cualquiera, por realizar la acción determinada o porque tiene la tecnología necesaria para la comisión del delito[167]como parece entender la doctrina, sin embargo en nuestra consideración, este se trataría realmente, aunque el tipo no lo exija expresamente, de un tipo de sujeto materialmente

---

[164] *En contra, la opinión de otros autores como* J.JAVIER ÁLVAREZ GARCÍA y la JURISPRUDENCIA *Como la STS 185/2006 avalan que, al faltar el componente más personal de la estafa, como son el engaño y el error, no participa esta figura ubicada en el art.248.2 en la naturaleza del fraude*. ALVAREZ GARCÍA, Javier(…)*Derecho Penal Español…ob.cit.*pág.253.

[165]SANCHIS CRESPO, Carolina*: Fraude electrónico…ob.cit.*pag.102-104/ MUÑOZ CONDE, Francisco: *Derecho penal, parte especial…ob.cit.*pág.392 y ss.

[166] *SA o phisher es la persona responsable de perpetrar el delito. Debido a la complejidad de sus métodos, por lo general, no suele captarse al responsable de estos ataques. Vinculados tenemos a varios sujetos que participan en el entramado de este delito, debido a esos métodos cada vez más complejos, los hackers se especializan en materias muy determinadas para luego unirse y perpetrar el mismo: planteamiento del delito, diseños webs, redacción spam, método de envío de correos masivos, los encargados de realizar las transferencias económicas, y los cibermuleros, personas encargadas de recibir en sus cuentas bancarias los activos monetarios y posteriormente por una transacción económica no electrónica, les hacen llegar a los autores reales de la estafa. Los cibermuleros deben de tratarse con una mención especial, pero debido a la extensión del trabajo no puede ser objeto de estudio en el mismo*. SANCHIS CRESPO, Carolina: *Fraude electrónico…ob.cit.*pág.332.

[167] BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pág.125.

cualificado por sus cualidades y conocimientos especiales, ya que no es realmente cualquiera quien puede manejar los sistemas requeridos para tal actividad. No obstante, se le tratara como no cualificado, puesto que dicho nivel de experticia no alcanza a cumplir con los estándares jurídicos normalmente exigidos por la doctrina penal, para tal denominación, como son la expresión concreta de cualificación o las funciones que lo cualifican[168]. Así procedemos a analizar el articulo en cuestión:

A) A *los que "con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio del tercero"*

En este primer supuesto encontramos la primera peculiaridad de este tipo de estafas, ya que los elementos del tipo básico se dan de una manera diferente: no hay engaño, ni error en el perjudicado[169], estos dos elementos por el contrario son esenciales en el tipo básico. EL engaño representa el específico desvalor de la acción del delito que origina un error esencial en el SP[170].No obstante, a pesar de que su estructura no sea exactamente igual a la del tipo básico, si comparte otros elementos como el BJP: patrimonio[171], del que hablaremos más extensamente en el siguiente epígrafe, y el ánimo de lucro del SA que en ambas debe tener ánimo de lucro ya que es el objetivo que se pretende realizar con al acción.[172] El ánimo de lucro debe concurrir en el momento de la acción y no tiene que prolongarse en el tiempo después de consumarse el delito.[173] El perjudicado o SP, es la persona física o jurídica, titular de la red de informática[174] que ha sido manipulada o el titular de los activos. La estructura típica de la estafa informática es caracterizada por la disposición patrimonial que se consigue por *la manipulación informática* entendiéndola como la introducción clandestina del sistema operativo o datos de un dispositivo electrónico, mediante su modificación, supresión, ocultamiento o introducción de otros

[168] MUÑOZ CONDE, Francisco (…): *Derecho penal, parte general* …ob.cit.pág.258-260.

[169] SERRANO GÓMEZ, Alfonso(…)*Curso de derecho penal, parte especial…ob.cit.*pág.326.

[170] SERRANO GÓMEZ, Alfonso(…)*Curso de derecho penal, parte especial…ob.cit.*pág.322

[171] ALVAREZ GARCÍA, Javier(…)*Derecho Penal Español…ob.cit.*pág.252.

[172]ARROYO DE LAS HERAS, Alfonso: *Los delitos de estafa y falsedad documental.* Barcelona: Bosh, 2005.pág.66./ *No obstante, existen ciertas ocasiones en las que el ánimo de lucro no esta claro, bien sea porque no existió tiempo material suficiente o porque sus expectativas no pudieron prosperar*, ARROYO DE LAS HERAS *dice "el propósito que persigue el sujeto constituye un hecho psicológico, es decir, un hecho íntimo, propio de la conciencia, nunca del todo objetivable, razón por la cual dicho ánimo o propósito deberá deducirse de los datos o circunstancias que concurren en el hecho mismo". Así, deberá tenerse en cuenta el caso y circunstancias concretas.*

[173] Vid.MUÑOZ CONDE, Francisco: *Derecho penal, parte especial…ob.cit.*Cap. XIX.

[174] Titular de la red: no es el propietario de la red, sino el usuario que la esta utilizando en ese momento. QUERALT JIMÉNEZ, Joan J.: *Derecho penal…ob.cit.*Pág. 552.

nuevos para provocar una determinada respuesta del sistema.[175]Se diferencia en el tipo básico de estafa, principalmente en la modalidad engañosa, que en este caso no involucra un error humano sino una manipulación del sistema, así la jurisprudencia entendía que *los aparatos electrónicos no tienen errores como los exigidos por el tipo tradicional de la estafa, es decir, en el sentido de una representación falsa de la realidad. El aparato se comporta según el programa que lo gobierna y, en principio "sin error…",* de ahí el termino manipulación del sistema*[176]*. En cuanto a la referencia *otro artificio semejante*, se vincula al empleo de tecnología informática de última generación.[177] El resultado de esta manipulación o artificio semejante ha de ser la transferencia no consentida de un activo patrimonial en perjuicio de tercero. Se trata de un delito de resultado,[178] por lo que es necesaria la *causación efectiva del perjuicio* como consecuencia de la transferencia no consentida mediante manipulación informática o artificio semejante para que de lugar a la consumación del delito.[179]

Podemos relacionar esta modalidad con el artículo 197, 1º y 2º, es decir, incluyéndose toda manipulación operada tanto sobre «ficheros o soportes informáticos, electrónicos o telemáticos[180]. Constituiría este delito, por ejemplo, el hacker que se introduce mediante su ordenador en el sistema de un banco y realiza transferencias a su favor.[181]

B) "*Los que fabriquen, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo*";

El legislador , en primer lugar lo que pretende con este articulo es anticiparse[182], de forma similar a lo que acontece en los delitos de peligro abstracto, a los actos que se pretenden realizar con los medios informáticos aptos para la comisión del delito de estafa. Lo más sustancioso de este precepto es que no solo abarca las estafas informáticas, sino que abarca también las del apartado 1 ("las estafas previstas en este articulo"), esto es debido

[175] ALVAREZ GARCÍA, Javier(…)*Derecho Penal Español…ob.cit.*pág.252-253.
[176] STS 860/2008,17-12 .
[177] SERRANO GÓMEZ, Alfonso(…)*Curso de derecho penal, parte especial…ob.cit.*pág.327.
[178]QUERALT JIMÉNEZ, Joan J.: *Derecho penal…ob.cit.*pág. 553.
[179] SERRANO GÓMEZ, Alfonso(…)*Curso de derecho penal, parte especial…ob.cit.*pág.327./ ALVAREZ GARCÍA, Javier(…)*Derecho Penal Español…ob.cit.*pág.253
[180]GONZÁLEZ CUSSAC, José Luis / VIVES ANTÓN, Tomás Salvador: *Derecho Penal, parte especial.* Valencia: Tirant lo Blanch, 2019.pág.361.
[181] MUÑOZ CONDE, Francisco: *Derecho penal, parte especial…ob.cit.*pág.393.
[182] SERRANO GÓMEZ, Alfonso(…)*Curso de derecho penal, parte especial…ob.cit.*pág.327.

a que la estafa propia puede realizarse por medios informáticos[183] y existen programas que pueden ayudar al engaño.[184]

Vinculado al término "fabricar" entendemos que es la elaboración o modificación de programas informáticos, por "introducir" se entiende la introducción de estos programas en el mercado negro para comercializarlos, y por "facilitar" vender, aunque también puede ocurrir que el termino facilitar al igual que en el tráfico de drogas, sea a titulo gratuito. La tenencia supone que el sujeto tiene en su poder un programa típico, lo haya producido el o le haya llegado a sus manos por cualquier medio.[185]El SP, al ser un delito de peligro, según cierta doctrina, es la comunidad[186] y el SA puede ser cualquiera que no sea ya autor del fraude informático en cuanto a tenencia ya que la tenencia quedaría consumida en el poseedor del programa, que es quien comete el fraude informático. En el caso de atentados por medios informáticos contra propiedad industrial e intelectual, se rigen por su lex specialis[187].

C) "*Los que, utilizando tarjetas de crédito, 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*". Así, por ejemplo, el uso de los datos de una tarjeta de crédito sin permiso de su titular para comprar una televisión por internet entraría dentro de este apartado.[188]

Este precepto esta específicamente dedicado a las defraudaciones realizadas por tarjetas de crédito, débito o cheques de viajes, el objeto material de los comportamientos no abarca otro tipo de tarjetas como pueden ser las de bus, de centros comerciales o similares. La utilización de estas tarjetas que hayan sido perdidas por le titular, para sacar dinero de un cajero o realizar compras en internet están tipificadas en este articulo ya que se utilizan los datos reales del titular sin su consentimiento.[189]

La pena para este delito de estafa informática es la misma que en el tipo básico: prisión de seis meses a tres años. Lo que se deriva de este artículo es que el legislador pretende

---

[183] QUERALT JIMÉNEZ, Joan J.: *Derecho penal…ob.cit.*pág. 555.

[184] ALVAREZ GARCÍA, Javier(…)*Derecho Penal Español…ob.cit.*pág254.

[185] QUERALT JIMÉNEZ, Joan J.: *Derecho penal…ob.cit.*pág.555.

[186]QUERALT JIMÉNEZ, Joan J.: *Derecho penal…ob.cit.*pág. 554.

[187] ALVAREZ GARCÍA, Javier(…)*Derecho Penal Español…ob.cit.*pág254-255

[188]MUÑOZ CONDE, Francisco: *Derecho penal, parte especial…ob.cit.*pág.393

[189] *Un ejemplo sería el hacerse pasar por un usuario autorizado para operar en su nombre obteniendo un beneficio.*. Acuerdo del Pleno no Jurisdiccional de la Sala 2ª del Tribunal Supremo de 18 de Julio de 2007 *"La firma del ticket de compra, simulando la firma del verdadero titular de una tarjeta de crédito, no esta absorbida por el delito de estafa"*. ARROYO DE LAS HERAS, Alfonso: *Los delitos de estafa…ob.cit*.pág.68./SERRANO GÓMEZ, Alfonso(…)*Curso de derecho penal, parte especial… ob.cit*.pág.328-329/SUAREZ-MIRA RODRIGUEZ, Carlos(…) *Manual de derecho penal…ob.cit* .pág362.

abarcar las nuevas formas de criminalidad vinculándolas a las formas tradicionales, no debemos de olvidar la posibilidad de realizar el tipo básico a través de las nuevas tecnologías lo que no quiere decir que sean ciberdelitos *stricto sensu.* Recordar también, la regulación de dos modalidades impropias en este articulo 248.2, por un lado, la estafa informática del 248.2. a) y b): que entendemos que abarcan la obtención de activos monetarios mediante el acceso fraudulento a los datos sensibles de los usuarios de internet[190].Y por otro la estafa mediante la utilización fraudulenta de tarjetas de crédito o cheques de viaje del apartado 248.2.c) CP.[191]

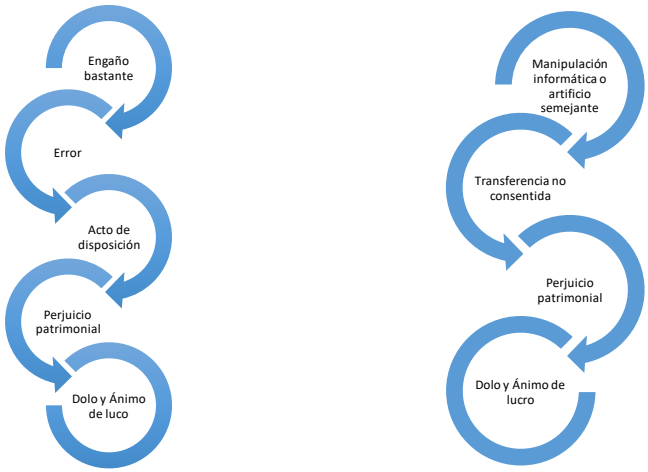

Figura 2.- Tipo básico 248.1CP (*izq*.) y tipo impropio 248.2CP (*dcha*.).

9.1.- Bien Jurídico Protegido.

Los bienes jurídicos son *los presupuestos que las personas necesitan para su autorrealización y desarrollo de su personalidad*[192]*;* el derecho penal elabora un catalogo de bienes con los presupuestos esenciales para la convivencia social que debe proteger y las conductas que los lesionan o ponen en peligro.[193] Los titulares de los BJ pueden ser tanto los individuos, como la sociedad o el Estado. Hemos de aclarar que el BJP trata de un concepto material, que alude a realidades sociales[194] Así llamamos a colación el BJP

[190] *Tribunal Supremo 2 de diciembre de 2014 (RJ 845, 2014 el Alto Tribunal encuadra estas conductas de phishing bancario en el artículo 248.2 a) del Código Penal y explica la actuación del autor en este tipo de delitos de estafa informática.*

[191] BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pág.121-122.

[192]MUÑOZ CONDE, Francisco (…): *Derecho penal, parte general* …ob.cit.pag.59./ LUZÓN PEÑA, Diego- Manuel: *Lecciones de derecho penal, parte general* …ob.cit.pág. 168-170. 2020

[193] DÍEZ RIPOLLÉS, José Luis. *Derecho penal español Parte general*.Valencia:Tirant lo Blanch, 2016. pág.17.

[194] *El BJ posee un componente ideal: respecto al juicio de valor positivo sobre una situación/relación de la realidad social. Este juicio se basa en integrar la relación o situación cuales un lugar determinado*. DÍEZ RIPOLLÉS, José Luis. *Derecho penal…ob.cit.*pág.17.

de la estafa propia del art.248.1 y la impropia del art.248.2 que como hemos dicho en epígrafes previos: es el patrimonio y analizando el concepto de BJ relacionado con el patrimonio, tenemos que el BJ seria la posesión de los bienes materiales en su valoración positiva por la sociedad, y el substrato[195]de ese BJ es el patrimonio individual como realidad social preexistente. Y las formas concretas de manifestación de ese substrato[196] son la capacidad de disposición por sus respectivos poseedores de objetos con valor económico. Por útlimo el objeto material son los objetos con valor económico.[197]

El BJP en las estafas tanto propias como impropias, es en virtud del TS[198], el patrimonio privado ajeno, vinculado tanto al valor de la cosa en concreto, como la protección jurídica que se brinda en relación de una persona con esa cosa[199]. Por otra parte, en el CP se define al patrimonio a efectos del Título XIII, como un conjunto de derechos y obligaciones, referibles a cosas u otras entidades, que tienen valor económico y que deben ser valorables en dinero. [200]La doctrina baraja cuatro conceptos diferentes, en primer lugar, el jurídico "conjunto de derechos patrimoniales de una persona", en segundo lugar el económico, "conjunto de valores económicos de los que dispone una persona", en tercer lugar, y siendo la concepción dominante en nuestra doctrina, se entiende una concepción mixta jurídico-económica de patrimonio, "conjunto de bienes y derechos patrimoniales económicamente valuables y poseídos por el sujeto pasivo en virtud de una relación reconocida por el ordenamiento jurídico", y en último lugar, la personal o funcional "conjunto de bienes de una persona destinados a un determinado fin o dotados de una utilidad concreta para su titular"[201].

Una vez analizado el BJP de la estafa en los dos tipos, me gustaría tratar en este epígrafe otros BJP que pueden verse afectados con el delito informático o phishing, por un lado, tenemos el caso de que el vector de entrada sea abrir un archivo infectado que instale en tu ordenador un malware y por otro la interacción de la persona a clickar en un url, ambas

---

[195] *El substrato del BJ son las situación o relaciones de la realidad social.* DÍEZ RIPOLLÉS, José Luis. *Derecho penal…ob.cit* .pág.17

[196] *Entendiéndolas siempre como materiales, el ataque al BJ debe producir un daño real.*

[197] DÍEZ RIPOLLÉS, José Luis. *Derecho penal…ob.cit* .pág.17

[198] STS 19-4-2002 Vid. VIVES ANTÓN, Tomás Salvador: *Derecho Penal, parte especial…ob.cit*.pág.293-300 y 350.

[199]MUÑOZ CONDE, Francisco: *Derecho penal, parte especial…ob.cit.*pág.392.

[200]MUÑOZ CONDE, Francisco: *Derecho penal, parte especial…ob.cit.*pág.319-324.// VIVES ANTÓN, Tomás Salvador: *Derecho Penal, parte especial…ob.cit*.pág. 293-300.

[201]MUÑOZ CONDE, Francisco: *Derecho penal, parte especial…ob.cit.*pág.344-346 y pág.392-399./ VIVES ANTÓN, Tomás Salvador: *Derecho Penal, parte especial…ob.cit*.pág.350-351./ ARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales…ob.cit.*pág.121-124.

dejan expuestos los datos sensibles del usuario y con ello información de tipo personal. En primer lugar, tenemos el delito de cracking o sabotajes informáticos, regulados en el art.264 a 264 quater CP, que constituye una de las categorías más tradicionales de los ciberdelitos.[202]En este tipo de delitos el BJP es la información contenida en sistemas informáticos, la cual dañan de forma grave quedando inutilizada. En segundo lugar, podríamos estar ante un delito contra la intimidad y la propia imagen del art. 197 al 201 CP, que contiene la tutela penal de los derechos fundamentales a la intimidad y propia imagen de los art.18,1 y 3 CE, y al secreto de las comunicaciones. El BJP en estos delitos es la intimidad o la denominada libertad informática,[203] a la cual acceden y visualizan o escuchan la información privada o restringida de la esfera de la persona.[204] No es de extrañar que en este tipo de delitos, en los que roban datos de tu esfera privada, puedan recopilar imágenes o fotografías personales guardadas en las plataformas y realizar al usuario "sextorsión", utilizando el phishing para realizar un delito contra la libertad e indemnidad sexual de las personas.[205] Los BJP de este tipo de delitos son la libertad e intimidad, y la libertad e indemnidad sexual de la victima[206]. Para finalizar este apartado de BJP diferentes al patrimonio que pueden verse afectados por el delito de phishing, debemos mencionar los delitos de competencia desleal: violación de secretos empresariales del art. 278 CP, el BJP es la capacidad competitiva de la empresa en el mercado o en el interés económico del empresario en el mantenimiento de la reserva.[207] En estos dos últimos tipos de delitos, extorsión y la violación de secretos empresariales, cabe decir que los phisher por lo general recopilan la información al realizar el ataque y posteriormente la venden en la Deep web, a no ser los casos que se les contrate con el fin de conseguir ese tipo de información.[208]

---

[202] GONZÁLEZ RUS, Juan José: Los ilícitos en la Red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes. En: ROMEO CASABONA, Carlos: *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales*.Granada: Comares, 2006.pág.248.

[203] SSTC 254/1993 y 143/1994

[204]VIVES ANTÓN, Tomás Salvador: *Derecho Penal, parte especial…ob.*cit.pág.249-251.

[205] EL COMERCIO: *La 'sextorsión' se dispara en España: el miedo a que publiquen tus vídeos íntimos*[Link][26/06/2021]

[206] *Con el delito de sextorsión pueden verse implicados una serie de ilícitos entre los que se encuentran: extorsión, chantaje, amenazas, explotación sexual, abuso sexual de menores, corrupción de menores, revelación de secretos, daños al honor, interceptación de comunicaciones, producción, tenencia y/o distribución de pornografía infantil. Es un delito en auge y que tendrá mucha repercusión según vayamos avanzando con las TICs.* Vid. DELITO SEXTORSION [Link][26/06/2021]-

[207] VIVES ANTÓN, Tomás Salvador: *Derecho Penal, parte especial…*ob.cit.pág.426-427.

[208]SANCHIS CRESPO, Carolina: *Fraude electrónico…ob.cit.*pág.55-66.

9.2.- Iter criminis del delito de estafa informática.

Hemos explicado la dinámica del phishing y los elementos claves del mismo, pero en este epígrafe debemos de hacer mención a las fases de ejecución del phishing desde un punto de vista más técnico. Una vez explicado el delito de estafa informática art. 248.2 a) y b) vinculándola con la figura delictiva de phishing, los elementos y el BJP, pasaré a analizar el *íter criminis* del mismo. El *iter criminis* tiene dos fases: la fase interna y la fase externa. El derecho penal sanciona las conductas y no los pensamientos, por lo que la fase interna[209] no se castiga ya que consiste en la ideación o el cómo realizar el ilícito, también denominada tentación criminal. A continuación, sucede la deliberación o elaboración del plan y la decisión de poner en práctica el mismo[210]. Vinculada al delito de phishing, podríamos decir que esta fase interna se da cuando se planea el ataque, decidiendo la entidad y empresa que desea suplantar, si el ataque va a ser individual o colectivo, los datos que desea conseguir y el grado de participación de la victima, además del análisis de los medios que tiene a su disposición para realizar el ataque y cumplir su objetivo.

La fase externa[211], en cambio, es la que exterioriza la fase interna, es decir, la realización de los actos planeados en el mundo exterior, esta fase se divide a su vez en: Actos preparatorios, que son los que se presentan antes de la ejecución del delito y se dirigen a facilitarlo, por lo general los actos preparatorios definidos en los art.17 y 18 CP y se exigen que para su punición se prevean expresamente en el delito o grupo de delitos, no obstante el CP prevé actos preparatorios penados específicamente en figuras especiales.[212] Esto es lo que ocurre en el art. 248.2 b) dónde se encuentra que son punibles los actos de: "*fabricación, introducción, posesión y facilitación de programas de ordenador específicamente destinados a cometer una estafa* "así podemos comprobar que en el delito de phishing esta etapa está vinculada la fabricación de los programas que va a utilizar él o va a proporcionar a un tercero para que lo ejecute. A continuación, tenemos los actos de ejecución[213] que son los que aparecen con la exteriorización del pensamiento por medio de conductas con un fin determinado. En el phishing estaría vinculada al envío de correos o mensajes, en esta fase es (dependiendo del tipos phishing) también el

[209] *Principio de impunidad del mero pensamiento: cogitationis poenam nemo patitur. Su impunidad no implica irrelevancia jurídica, ya que pasarán a objeto de valoración jurídico penal en la medida que se realicen actos externos vinculados a ellos*. DÍEZ RIPOLLÉS, José Luis: *Derecho penal…ob.cit.*pág.497.
[210] MUÑOZ CONDE, Francisco (…): *Derecho penal, parte general* …ob.cit.pág 415-418.
[211] MUÑOZ CONDE, Francisco (…): *Derecho penal, parte general* …ob.cit.pág.417-418.
[212] DÍEZ RIPOLLÉS, José Luis. *Derecho penal…ob.cit.*pág.497.-504.
[213]ZUGALDÍA ESPINAR, José Miguel(…)*Lecciones de derecho penal…ob.cit.* pág.208-209.

momento en el que se instala el malware, siendo necesario mencionar la "anatomía del phishing": malware, infección, ejecución, entrada de datos, atacante y servidor legítimo. Siendo importante la entrada del malware en el sistema y la ejecución del código malicioso.

Debemos mencionar antes de seguir con las fases del phishing, la tentativa[214], aclarar que no es una fase individual, sino que se da en la fase de ejecución y tiene una pena atenuada respecto al delito, ésta sucede cuando la ejecución del delito se detiene antes de alcanzar el grado de consumación, es decir, el perjuicio no se ha producido, es en este momento en el que el usuario no ha "mordido el anzuelo", no ha seguido el url proporcionado o no ha accedido al correo o SMS que le han enviado.

Las siguientes partes del delito del phishing, son la recogida de datos, en función del tipo de participación de la víctima. Si son de alta o media participación, tendrán que esperar a que la víctima colabore con la introducción de la información y datos sensibles; en cambio, si son de baja colaboración la tarea se basará en la ejecución del malware para conseguir los datos mencionados. Después de recabar estos datos, tenemos la ejecución del fraude, es el momento en el que el phisher tiene los datos del usuario y su objetivo se ha cumplido, en este momento puede o bien venderlos a un tercero para que efectúe un delito, o bien utilizarlos en beneficio propio. Esto coincide con la consumación del delito[215], una vez realizadas todas las fases[216]. La última fase es la de post-ataque, que es la eliminación del rastro que pudiese inculparle del delito. Sería fase de agotamiento del delito.[217]

9.3.-Dinámica de la estafa informática art.248.2 a) y b) o phishing.

En el epígrafe: 7 *(¿QUÉ ES EL PHISING? Y cuales son las figuras delictivas (o delitos) con las que puede relacionarse)*, mencionamos los elementos en los que se basa el modus operandi de la estafa informática del art.248.2 a) y b) o phishing . Una vez definido el tipo penal en la que la figura delictiva del phishing, consideramos, se encuentra, nos

[214]. DÍEZ RIPOLLÉS, José Luis: *Derecho penal…ob.cit.*pág. 504-520./ ZUGALDÍA ESPINAR, José Miguel(…)*Lecciones de derecho penal…ob.cit.*pág.209-222.

[215] MUÑOZ CONDE, Francisco (…): *Derecho penal, parte general* …ob.cit.pág.412-413.

[216]*La consumación, definida como la producción del perjuicio, no siendo necesario el lucro del autor*. QUINTERO OLIVARES, Gonzalo: *Tomo XXXII Esquemas de la parte especial del derecho penal* (I).Valencia: Tirant lo Blanch, 2011.pág.302.

[217] DÍEZ RIPOLLÉS: José Luis. *Derecho penal…ob.cit* pág.520.

referiremos con ella en lo siguiente del trabajo. Estos elementos, para recordar, son: MENSAJE, INTERACCIÓN Y ROBO.

En este trabajo separaremos los tipos de phishing en dos grupos, en función de la dinámica que utilicen para cometer el ilícito, así nos encontramos, en primer lugar, en función del servicio que ataquen: bancos y cajas, pasarelas de pago online, redes sociales, páginas de compra/venta y subastas, juegos online, soporte técnico y de ayuda de empresa y servicio, almacenamiento en la nube, servicios o empresas públicas, servicios de mensajería, falsas ofertas de empleo. Dependiendo del servicio que estén atacando, los phisher pretenden recopilar diferentes tipos de datos, que se podrán vincular con diferentes tipos de delitos. Podemos mencionar como los más utilizados:

El Phishing Bancario, en el que el objetivo es la obtención subrepticia de claves y contraseñas bancarias de terceros, los objetivos son claros: pin secreto, número de tarjeta de crédito y datos análogos para conseguir el lucro. Las partes que componen este ataque son: en primer lugar la obtención ilícita de datos confidenciales de las cuentas bancarias de las víctimas, una vez conseguidos, el phisher podrá o bien realizar traspasos patrimoniales en línea a otras cuentas bancarias, por lo general sita en el extranjero y abiertas por una tercera persona/miembro, denominados "muleros", o realizar conductas de falsificación de tarjetas bancarias, *skimming*. La última parte por la que pasa esta modalidad es retirar los activos transferidos a las cuentas y a continuación, el envío del dinero a los demás integrantes de la estafa. En este tipo de delitos, en los que normalmente existe un número de miembros determinados que actúan como una organización criminal, podríamos barajar el estar ante la comisión de tipos penales del art.570 bis CP.[218] El phishing bancario se puede identificar también con el "identy related crime"[219].

[218] *La organización criminal parece más adecuada en estos casos que la de asociación ilícita del art. 515 CP, definida por la doctrina y jurisprudencia como la unión de un mínimo dos o tres personas para la realización de alguno de los fines del art. 515, entre los que se encuentra la comisión de delitos (número 1), dotada de una estructura organizativa y de cierta permanencia en el tiempo*. GÓMEZ TOMILLO, Manuel / SÁNCHEZ GARCÍA DE PAZ, Isabel: *Comentarios al Código Penal*. Valladolid: Lex nova 2011.pág. 1795-1922. *Delimita una y otra en atención a si la unión o agrupación de personas concertadas para la comisión de delitos constituye una asociación ilícita o no, pues entiende que las conductas del art. 515 constituyen una manifestación del abuso del derecho de asociación. Planteando diversos criterios y la dificultad para di ferenciarlas*.Vid. MARTELL PÉREZ-ALCALDE, Cristóbal / QUINTERO GARCÍA, Débora.: De las organizaciones y grupos criminales. En QUINTERO OLIVARES, Gonzalo: *La Reforma Penal de 2010: Análisis y Comentarios*. España: Aranzadi, 2010, pág. 360 y ss. / VELASCO NÚÑEZ, Eloy: Delitos informáticos realizados en actuación organizada. En *Diario La Ley* (7743), 2011, pág. 3 [Link][12/04/2021] *Este autor considera que cuando la finalidad de la agrupación es delictiva concurren los tipos del Capitulo IV del Titulo XXII del Libro II del Código Penal.*

[219]NNUU: *Economic fraud and Identity-related crime*.[Link][24/04/2021].

Otro tipo es el Phishing Social que está íntimamente relacionado con las redes sociales, aquí lo que pretenden es suplantar la identidad y obtener información sensible y privada del usuario y sus redes sociales. El método que utilizan para engañar al usuario es una etiqueta en fotos, una solicitud de amistad, o "por motivos de seguridad es preciso que envíen sus claves a: *el URL/LINK que te proporcionen de la plataforma suplantada*". No es de extrañar que, en este tipo de delitos, en los que roban datos de tu esfera privada, puedan recopilar imágenes o fotografías personales guardadas en las plataformas y realizar al usuario "sextorsión", utilizando el phishing para realizar un delito contra la libertad e indemnidad sexual de las personas. Con los ataques a las redes sociales no solo consiguen perpetrar en la esfera privada, si no que también es una vía de acceso para ataques a empresas, utilizando como vector de entrada a los empleados, este tipo de phishing vinculado a las empresas y sus directivos se denominan: "whaling" o "whale phishing"[220] En este tipo de ataques a empresas, utilizando las redes sociales, como el Dropbox o Google Drive[221], con lo que se aseguran una propagación rápida y fácil, mediante el uso de la ingeniería social, gracias a que son canales de tipo personal y que invitan al uso compartido y distribución garantizada. Importante mencionar en este apartado la posibilidad de la adquisición de "kits de phishing industrializados"[222]

Por otra parte, tenemos los tipos de phishing caracterizados por el modus operandi, aunque existen diferentes tipos de acceso a los datos personales, todos tienen los mismos rasgos comunes, variando según la importancia de la interacción del usuario para realizar el delito, o bien el vector de entrada al ordenador del usuario web.

---

[220] *Whaling: práctica dirigida a reducidos grupos de personas y con un perfil determinado, de carácter empresarial, el nombre de "whaling" proviene del inglés y significa cazar ballenas, también se conoce como "Ceo Fraud", en es tipo de ataque los cibercriminales simulan mediante el correo electrónico, ocupar el cargo superior de una empresa u organización, para así atacar a altos ejecutivos u otros trabajadores de la misma, los hackers investigan la vida personal de estos altos cargos, con los recursos en red disponibles como las redes sociales, buscando la estrategia más adecuada. Los ataques se realizan de forma que parezca que las comunicaciones fraudulentas son enviadas por el alto cargo, incluyendo logos empresariales y vínculos a webs fraudulentas. Así, los empleados sienten la necesidad de responder a las solicitudes de un cargo superior en la mayor brevedad posible, saltándose los protocolos de seguridad y cayendo en el "anzuelo" del phisher. Para evitar este tipo de fraudes es muy importante la formación de los empleados y el seguimiento de protocolos de seguridad específicos.[220] La otra variante mencionada es el "spear phishing", variante parecida al "wahling", consiste en la realización por parte del phisher de una averiguación de datos personales o entidades confiables para el usuario mediante el envío de un correo electrónico con el cebo para el posterior ataque, va dirigido a personas especificas o empresas u organizaciones determinadas, el objetivo por lo general es el robo de datos para la posterior reventa.*

[221] INCIBE: *El fraude del ceo* tiene un arma nueva, google drive [Link][28/06/2021]

[222] *Kits de phising, son plantillas elaboradas a gran escala, que facilitan la creación y lanzamiento de campañas maliciosas con más rapidez. Se venden de forma clandestina en la red, y proporcionan las herramientas necesarias para perpetrar los ataques, como herramientas de diseño web y gráficos, contenido de marcadores de posición y correo electrónico masivo u otro software de distribución.*

Los tipos más utilizados son:

- Phishing engañoso-deceptive phising: envío masivo de correos electrónicos, dónde se suplanta una identidad legítima.
- Software malicioso-malware based phishing: instalación de software malicioso en el ordenador de la víctima, utilizando la ingeniería social para engañar a la víctima, o mediante el fallo del sistema de seguridad de la computadora. Los dos tipos más utilizados son:

1) Ransomware: Es un software dañino, normalmente este software es transportado por un troyano en forma de documento adjunto dentro de un e-mail, este software bloquea el acceso al usuario hasta que ceda a sus pretensiones. Tradicionalmente este tipo de software era fácilmente desbloqueado por expertos en la materia, por el contrario, gracias a la evolución de los hackers en esta materia, ahora además de bloquear el sistema, encripta los ficheros de la victima. El hacker pide un rescate económico para desbloquear el sistema y archivos. Este tipo de malware se encuentra entre las cinco primeras amenazas de internet, normalmente el ataque es contra dispositivos con sistema operativo Windows, por ser el más utilizado[223].
2) Keylogger: una posible traducción sería registrador de teclas, este tipo de técnicas utilizan programas que se instalan en los ordenadores o dispositivos móviles, con el fin de grabar lo que escribe el usuario. Es un malware de tipo "demonio", ya que está activo todo el tiempo, pudiendo los atacantes guardar toda la información sensible que deseen. Por lo general, las entidades y organizaciones, como los bancos, han evolucionado en sus sistemas de autenticación para evitar este tipo de ataques, son muchas las que nos piden claves desde un teclado en la pantalla, para que sean pulsados por el ratón. En la variante móvil, también se realiza un registro de notificaciones recibidas y aplicaciones abiertas, ciertos Keyloggers con el mero hecho de instalarlas y activarlas, funcionan sin necesidad de tener el teléfono en modo "root".[224]

- Técnica del intermediario-man in the middle phising: técnica en la que el phisher se posiciona entre el ordenador del usuario y el sitio web legítimo. Técnica basada en leer y modificar los mensajes entre dos usuarios, futuras victimas del ataque, sin su conocimiento. El ámbito de actuación más común es realizar ataques a datos bancarios.[225] Para realizar esta conducta el phisher utiliza, por lo general, cuatro técnicas:

1) ARP Poising o ARP Spoofing: En primer lugar, explicar que la ARP es un protocolo de comunicaciones de la capa red, que será el encargado de encontrar la dirección MAC de una dirección IP. Por lo que este tipo de ataque, es aquel perpetrado contra las redes ethernet, con el fin de atrapar el tráfico que cruza por la LAN y conseguir detenerlo mediante la negación de servicio, modificando la mencionada ARP.
2) Robo de puerto o Port Stealing: En este tipo de ataque el phisher envía muchos "paquetes de capa 2" o "frames ethernet" con la dirección Mac en origen de la víctima y de destino la del phisher. Así, el switch está conectado con el puerto del phisher, para enviarle los paquetes destinados a la víctima. Antes de devolver los paquetes a la víctima, el phisher podrá modificarlos y leerlos.
3) DNS spoofing: Mediante la modificación del ID Spoofing o el caché, el phisher envía respuestas a falsas peticiones de resolución de DNS enviadas por la víctima. En general, el protocolo DNS convierte nombres en direcciones IP.
4) Search engine phishing o DHCP Spoofing: El DHCP es un protocolo de red para asignar una dirección IP a cada dispositivo red, de forma dinámica. En el momento que un dispositivo se conecta a la red, se envía automáticamente una petición al servidor DHCP, como la ubicación de este servidor no es conocida, se envía a todos los dispositivos de la red local, y aquí está el problema, cuando el phisher responde antes que el servidor y le envía información errónea a la víctima, comunicándole que el vector de entrada es él.

[223] SAFETY DETECTIVE: *Ransomware* statistics[Link][22/05/2021]

[224] KEYLOGGER ANDROID: [Link][22/05/2021]

[225] TÉCNICAS DE MAN-IN-THE-MIDDLE:[Link][22/05/2021]

10.-CONCLUSIONES

PRIMERA: Las ventajas que nos ha producido en nuestra vida cotidiana el internet son innumerables, el avance de la tecnología y de la TIC facilitan y favorecen muchos aspectos de la vida de una persona; no obstante, no todo son aspectos favorables, ya que éstos mismos avances facilitan que los delitos tradicionales ahora sean perpetrados también a través de las redes. Esta nueva generación de delitos denominados ciberdelitos o delitos informáticos, fueron abarcados por el legislador con las sucesivas reformas del CP siendo la reforma de 2015 la más sustanciosa en esta materia, abarcando delitos como el que hemos tratado en este documento: phishing.

SEGUNDA: El phishing es el delito de estafa impropia del art. 248.a) y b), también denominado fraude informático. Con este subapartado del art.248, el legislador pretende englobar las conductas que no entran en el tipo penal básico de estafa, por faltar: el engaño y el error, dentro de los elementos esenciales del mismo. Estos dos elementos que "faltan" realmente son sustituidos por: manipulación informática o artificio semejante, estando el engaño y el error vinculados de un mono indirecto, ya que no hay persona que sufra el engaño o artimañas que hacen que caiga en el error, sino que es el sistema informático o la maquina la que será manipulada por el estafador. Esta manipulación en el 248.2 o engaño y error del 248.1, llevan a un mismo fin: transmisión patrimonial a favor del estafador.

TERCERA: Con el término phishing nos referimos a las conductas en las que el SA trata de engañar a la víctima con el fin de obtener datos personales o de carácter sensible, haciéndole creer que la comunicación que está realizando es veraz; mientras que la realidad es que el phisher está realizando una recopilación de datos como números de tarjetas de crédito, claves de acceso o diferentes datos sensibles que le puedan ocasionar algún tipo de beneficio en la deebweb.En la estafa informática o phishing existen multitud de técnicas destinadas al fin de realizar la estafa, los más utilizados son el envío de correos masivos, no obstante tenemos otras variantes como: smishing, vishing, whaling, pharming. Para llevar a cabo el delito son necesarios diferentes programas, que se denominan precursores: keyloggers, programas spyware,programas sniffers,auction fraud y una lista interminable de diferentes malwares.

CUARTA: El phishing. Produce grandes pérdidas económicas, y como hemos observado los datos expuestos en el trabajo, el phishing al igual que los demás delitos informáticos va en aumento. La ingeniería social, como vector de entrada humano es esencial en este

tipo de delitos, cada vez es más sofisticada y personalizada en cada usuario siendo por parte del usuario más complejo de descifrar el que está siendo atacado. Así las personas debemos concienciarnos e instruirnos para evitar este tipo de ataques.

QUINTA: Para finalizar, en mi opinión estos delitos son muy difíciles de abarcar, debido a su cambiante estado y al elevado número de personas que cada día acceden a internet y a redes sociales , lo que propicia que los delincuentes encuentren un mundo en el que delinquir desde sus casas. No obstante, a pesar de que el phishing en España se ha empezado a tratar hace relativamente poco, el legislador ha solventado la inexistencia de engaño y error de manera satisfactoria con el 248.2.a) CP, dando cabida en el ordenamiento a las estafas cometidas mediante sistemas informáticos o a través de internet.

"*Cada época escribe la historia de nuevo. Nadie puede extrañar, pues, que cada época deba escribir de nuevo su ciencia jurídica"*[226]

[226] RADBRUCH, Gustavo: *Filosofía del Derecho*. Madrid: Revista de Derecho Privado, 1959.pág.61.

BIBLIOGRAFÍA

- ALMENAR PINEDA, Francisco: *Ciberdelincuencia, Teoría y práctica.* Oporto: Jurúa, 2018.
- ALMENAR PINEDA, Francisco: *El delito de hacking.* Oporto: Jurúa, 2018.
- ÁLVAREZ GARCÍA, Francisco Javier/ VENTURA PÜSCHEL, Arturo / MANJÓN-CABEZA OLMEDA, Araceli: *Derecho Penal Español, parte especial (II).*Valencia: Tirant lo Blanch, 2011.
- ALVAREZ GARCÍA, Javier/ MANJÓN-CABEZA OLMEDA, Araceli/ VENTURA PÜSCHEL, Arturo: *Derecho Penal Español, parte especial.* Valencia: Tirant lo Blanch, 2011.
- ANTÓN ONECA, José: *Estafa, nueva enciclopedia jurídica.* Barcelona: Francisco Seix, 1958.
- ARROYO DE LAS HERAS, Alfonso: *Los delitos de estafa y falsedad documental.* Barcelona: Bosh, 2005.
- ARROYO ZAPATERO, Luis/ BERDUGO GÓMEZ DE LA TORRE, Ignacio/ FERRÉ OLIVÉ, Juan Carlos.: *Curso de Derecho Penal, parte general.* Barcelona: Ediciones Experiencia, 2016.
- ASENCIO MELLADO, José María/ FERNÁNDEZ LÓPEZ,Mercedes:*Justicia penal y las nuevas formas de delincuencia.* Valencia: Tirant lo Blanch, 2017.
- BARRIO ANDRÉS, Moisés: *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos.* Madrid: Wolters Kluwer, 2018
- BARRIO ANDRÉS, Moisés: *Derecho de los Robots.* Madrid: Wolters Kluwer, 2018.
- BARRIO ANDRÉS, Moisés: *Fundamentos del Derecho de Internet.* Madrid: Estudios políticos y constitucionales, 2017.
- BLANCO LOZANO, Carlos: *Tratado de Derecho Penal Español, tomo I: El sistema de la parte general. Volumen 1:Fundamentos del Derecho Penal Español, las consecuencias jurídico-penales.* Barcelona: Bosch, 2015.
- CASTELLS OLIVAN, Manuel: *La galaxia de internet, reflexiones sobre internet, empresa y sociedad.* Barcelona: Plaza & Janes, 2001.
- CHARLES, Arthur: *Cyber wars: Hackeos que hicieron temblar el mundo empresarial*.España: Tell, 2019.

- CHOCÁN MONTALVO, José Antonio: *Fraude informático y estafa por computación, en CDJ*, núm 10,2001,p.
- CHOCLÁN MONTALVO, José Antonio: *El delito de estafa.* Barcelona: Bosch, 2009.
- CHRISTENSERN, Clayton: *The innovator's dilemma: when the technologies cause great firms to fail*. Boston: Harvard Business Review Press, 1997.
- CLIMENT BARBERÁ, Juan: *La justicia penal en internet, territorialidad y competencias penales.* 2001, Número 10, ISBN 84-89230-50-1.págs.645-663.
- COBOS GÓMEZ DE LINARES, Miguel Ángel: *Las defraudaciones, estafa, apropiación indebida, defraudaciones de fluido eléctrico y análogas.* En: RODRÍGUEZ RAMOS, L.: *Derecho penal, parte especial, tomo II.* Madrid: Servicio de Publicaciones de la facultad de Derecho de la Universidad Complutense de Madrid, 1996.
- COLÁS TURÉGANO, Asunción: Los delitos de género entre menores en la sociedad tecnológica. *Menores y redes sociales: ciberbullying, ciberstalking, cibergrooming, pornografía, sexting, radicalización y otras formas de delincuencia en la red* .2016, ISBN 978-84-9119-780-5, pág.67-119.
- COLEMAN, Gabriella: *Las mil caras de Anonymous: hackers, activistas, espías y bromistas.* Barcelona: Arpa Editores, 2016.
- CORCOY BIDASOLO, Mirentxu: Problemática de la persecución penal de los denominados delitos informáticos particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos.*Eguzkilore.*2007, Numero 21. San Sebastián: Cuadernos del Instituto Vasco de Criminología, pág. 7-32.
- DAVARA RODRÍGUEZ, Miguel Ángel: *Manual de derecho informático.* Pamplona: Aranzadi, 2015.
- DE URBANO CASTRILLO, Eduardo: Los delito informáticos tras la reforma del CP de 2010. *Delincuencia informática: tiempos de cautela y amparo.*2012, ISBN 978-84-9014-273-8, pág. 17-30.
- DEL CARPIO DELGADO, Juana / BOZA MORENO, Elena / DEL VALLE SIERRA LÓPEZ, Mª:*Algunas cuestiones de parte especial tras la reforma de 2015 del Código Penal.*Valencia: Tirant lo Blanch, 2018.

- DÍEZ RIPOLLÉS, José Luis. *Derecho penal español Parte general*.Valencia:Tirant lo Blanch, 2016.
- FERNÁNDEZ BERMEJO, Daniel / MARTÍNEZ ATIENZA, Gorgonio: *Ciberseguridad, ciberespacio y ciberdelincuencia.* Pamplona: Aranzadi, 2018
- FERNÁNDEZ TERUELO, Javier Gustavo: *Cibercrimen: Los delitos cometidos a través de Internet: estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red.* Oviedo: Constituio Criminalis, 2007.
- FLOR, Roberto: Phishing y delitos relacionados con el fraude de identidad: un World Wide Problem en el World Wide. *Robo de identidad y protección de datos.*2010, ISBN 978-84-9903-400-3, pág. 77-120.
- GIL ANTÓN, Ana María: De los delitos contra la intimidad personal y familiar y delito informático, de acuerdo con la reforma operada por la LO 1/2015, de 30 de marzo, de reforma del CP.*Revista Aranzadi de derecho y nuevas tecnologías.* 2015, ISSN 1696-0351, pág.27-57.
- GÓMEZ TOMILLO, Manuel / SÁNCHEZ GARCÍA DE PAZ, Isabel: *Comentarios al Código Penal*. Valladolid: Lex nova 2011
- GONZÁLEZ CUSSAC, José Luis / VIVES ANTÓN, Tomás Salvador: *Derecho Penal, parte especial.* Valencia: Tirant lo Blanch, 2019.
- GONZÁLEZ CUSSAC, José Luis/ MATALLÍN EVANGELIO, Ángela/ GORRIZ ARROYO, Elena: *Comentarios a la reforma del Código PENAL de 2015.*Valencia: Tirant lo Blanch
- GONZÁLEZ HURTADO, Jorge Alexandre: La seguridad en los sistemas de información como un bien jurídico de carácter autónomo, perspectiva EU y Española. *Revista Penal de México.* 2016,ISSN 2007-4700, Nª9, PÁG.59-76.
- GONZÁLEZ RUS, Juan José: Los ilícitos en la Red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes. En: ROMEO CASABONA, Carlos: *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales*.Granada: Comares, 2006.
- HONG, JASON: The estate of phishing attacks. *Communications of the ACM.*2012, Vol. 55, Nº 1, pág. 74-81.

- JAKOBSSON, Markus/ MYERS, Steven: *Phishing and Countermesasures: Understanding the Increasing Problem of Electronic Identity Theft.* Nueva Jersey: John Willey & Sons, 2005.
- JEWKES, Yvonne / YAR, Majid: *Handbook of internet crime.* Nueva York: Willan, 2009.
- LÓPEZ LÓPEZ, Antonio: La investigación policial en Internet, estructuras de cooperación internacional. *Revista d'internet, dret i política, monográfico III Congreso internet, derecho y política. Nuevas perspectivas.*2007, SSN 1699-8154, Nº 5, pág.63-74.
- LUZÓN PEÑA, Diego- Manuel: *Lecciones de derecho penal, parte general.* Valencia: Tirant lo Blanch, 2016.
- MARCHENA GÓMEZ, Manuel: Dimensión jurídico-penal del correo electrónico. *Diario la ley.*2006, Nº 6475, pág.7-14
- MARÍN DE ESPINOSA CEBALLOS, Elena B. / ESQUINAS VALVERDE, Patricia / ZUGALDÍA ESPINAR, José Miguel: *Lecciones de derecho penal, parte especial.* Valencia: Tirant lo Blanch, 2018.
- MARTELL PÉREZ-ALCALDE, Cristóbal / QUINTERO GARCÍA, Débora.: De las organizaciones y grupos criminales. En QUINTERO OLIVARES, Gonzalo: *La Reforma Penal de 2010: Análisis y Comentarios*. España: Aranzadi, 2010
- MATA Y MARTÍN, Ricardo.: *El robo de identidad y protección de datos.* Madrid: Marcial pons,2010.
- MIRÓ LLINARES, Fernando:Cibercrímeneres económicos y patrimoniales. En ORTIZ DE URBINA GIMENO, Íñigo: *Memento práctico penal y económico y de la empresa.* Madrid: Francis Lefebvre, 2011.
- MUÑOZ CONDE, Francisco / GARCÍA ARÁN, Mercedes: *Derecho penal, parte general.* Valencia: Tirant lo Blanch, 2015.
- MUÑOZ CONDE, Francisco: *Derecho penal, parte especial.* Valencia: Tirant lo Blanch, 2019.
- MUÑOZ CONDE, Francisco: *Derecho penal, parte especial.* Valencia: Tirant lo Blanch, 2012.

- MYERS, Steven.: Introduction to Phishing. En: JAKOBSSON, Markus/ MYERS, Steven: .: *Phishing and Counter- measures: Understanding the Increasing Problem of Electronic Identity Theft.* Nueva Jersey: John Willey & Sons, 2006.
- PARKER, Donn B: *Crime by computer.* Nueva York: Charles Scribner´s Sons, 1976.
- PÉREZ CAMBERO, Raúl: Aspectos más destacables de la Decisión de Ejecución 2016/1250 de la Comisión Europea, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU. *Actualidad administrativa.*2017, ISSN 1130-9946, Nº4, pág.
- PÉREZ MANZANO, Mercedes*:* Las Defraudaciones (I). Las Estafas. En BAJO FERNÁNDEZ, Miguel: *Compendio de Derecho penal. Parte especial.* Madrid: Centro de Estudios Ramón Areces,1998,
- POVEDA CRIADO, Miguel Ángel*: Delitos en la red.* España: Fragua, 2015.
- QUERALT JIMÉNEZ, Joan J.: *Derecho penal Español, parte especial.* Valencia: Tirant lo Blanch, 2015.
- QUINTERO OLIVARES, Gonzalo: *Tomo XXXII Esquemas de la parte especial del derecho penal (I).*Valencia: Tirant lo Blanch, 2011.
- RAYMOND,Eric: Hacker Slang and Hacker Culture .*The Jargon file* [Link][18/02/2021].
- REZA REYES, Sandra: Uso ilícito de la red: El caso de la DEEP WEB. En NAVA GÁRCES, Alberto Enrique: *Ciberdelitos.* Ciudad de México: Tirant lo Blanch, 2019.
- RIVERA BEIRAS, Iñaki: *Pandemia, derechos humanos, sistema penal y control social (en tiempos de coronavirus).*Valencia: Tirant Humanidades, 2020.
- RODRÍGUEZ MOURULLO, Gonzalo / LASCURAÍN SÁNCHEZ, Juan Antonio /ALONSO GALLO, Jaime: Derecho penal e internet. En FERNÁNDEZ ORDOÑEZ, Miguel: *Régimen jurídico de internet.* España: Wolters Kluwer, 2001.
- ROMEO CASABONA, Carlos María/SOLA RECHE, Esteban / BOLDOVA PASAMAR, Miguel Ángel: *Derecho penal, parte especial.* Granada: Comares, 2016.pág. 254

- ROMEO CASABONA, Carlos: De los delitos informáticos al cibercrimen, una aproximación conceptual y político-criminal. Granada: Comares, 2006.
- ROMEO CASABONA,Carlos María: *Poder Informático y seguridad Jurídica*.Madrid:Fundesco,1987.
- SÁNCHEZ ARJONA, Mercedes Llorente/ MARTÍNEZ-GIJÓN MACHUCA, Miguel Ángel.:*Pandemia y derecho, una visión multidisciplinar*.Murcia: Ediciones Laborum, 2020.
- SANCHIS CRESPO, Carolina: *Fraude electrónico, su gestión penal y civil*. Valencia: Tirant lo Blanch, 2015.
- SEMINARA,Sergio: La piratería su Internet e il diritto penale, *Revista Trimestrale di Diritto Penale dell'Economia*.1997, ISSN 1121-1725,Nº 1-2. pág.111.
- SERRANO GÓMEZ, Alfonso/ SERRANO MAÍLLO, Alfonso/ SERRANO TÁRRAGA, Mª Dolores/ VÁZQUEZ GONZÁLEZ, Carlos: *Curso de derecho penal, parte especial.* Madrid: Dykinson, 2019.
- SUAREZ-MIRA RODRIGUEZ, Carlos / PIÑOL RODRÍGUEZ, José Ramón / JUDEL PRIETO, Ángel: *Manual de derecho penal, tomo II, parte especial*. Madrid: Civitas, 2018.
- THOMAS LEICHETENSTERM, Christoph Langner: Bajo el radar: teoría y práctica de la red Tor.*Linux magazine.*2012, ISSN 1576-4079, Nº82, pág. 55-59.
- ULRICH SIEBER*: Computerkriminalitat und Strafercht.* Koln: Heymann,1977. Y *The internacional handboolk on computer crime: computer-related economic crime and the infringements of privacy*.Nueva York: John wiley and sons, 1986.
- ULRICK BECK: Riesgo digital ,el fracaso de las instituciones funcionales. En: *La metamorfosis del mundo.* Barcelona: Paidós, 2017.
- VELASCO NÚÑEZ, Eloy: Delitos informáticos realizados en actuación organizada. En *Diario La Ley* (7743), 2011, pág. 3 [Link][12/04/2021]
- VELASCO NÚÑEZ, Eloy: Estafa informática y banda organizada. Phishing, pharming, smishing y muleros. *Ley penal: revista de derecho penal, procesal y penitenciario.*2008, ISSN 1697-5758 Nº49, pág.19-29.

- VELASCO NÚÑEZ, Eloy: Fraudes informáticos en la red, del phishing al pharming. *La Ley penal: revista de derecho penal, procesal y penitenciario.*2007, ISSN 1697-5758 Nº37, pág. 57-66.
- VIVES ANTÓN, Tomás Salvador: *Derecho Penal, parte especial…ob.cit*
- ZUGALDÍA ESPINAR, José Miguel / MORENO-TORRES HERRERA, Mª Rosa / DE ESPINOSA CEBALLOS, Elena Marín: *Lecciones de derecho penal, parte genera.* Valencia: Tirant le Blanch, 2021.

OTRAS REFERENCIAS

- GABINETE DE COORDINACIÓN Y ESTUDIOS. SECRETARÍA DE ESTADO DE SEGURIDAD: *Estudio sobre la Cibercriminalidad en España* [Link][10/03/2021]

- INCIBE: ¿Cómo nos afecta la derogación del escudo de privacidad entre EU y EEUU?[Link][25/5/2021]

- INCIBE: *El fraude del ceo* tiene un arma nueva, google drive [Link][28/06/2021]

- INCIBE: *Protege tu empresa, luchando por la ingeniera social, el firewall humano.* [Link][23/06/2021]

- KELLY,Tom: *How hackers are using COVID-19 to find new phishing victims.*[15/02/21][Link]

- LÓPEZ FONSECA, Oscar:*Los ciberdelitos son ya el 10% de las infracciones penales conocidas.* [Link] [24/04/2021]

- MICROSOFT SEGURIDAD: *What is social engineering? Social Engineering, Phishing and Email Hoaxes,* julio 2021 [Link][04/06/2021].

- OBSERVATORIO ESPAÑOL de DELITOS INFORMÁTICOS:*Estadisticas de evolución* [Link] [16/02/2021]

- OFICINA DE CIBERSEGURIDAD DEL INTERNAUTA: *La Ciberseguridad es una responsabilidad de todos: el IoT y sus riesgos[15/02/2021][Link*

- OFICINA DE CIBERSEGURIDAD DEL INTERNAUTA: *Tu casa inteligente es cibersegura [15/02/21][Link]*

- PHISHER *: La persona que intenta engañar a un tercero mediante phishing*. Cambridge dictionary [Link][02/02/2021]

- RAYMOND,Eric: Hacker Slang and Hacker Culture .*The Jargon file* [Link][18/02/2021].

- ROYO PÉREZ, Victoria: El TJUE anula el acuerdo entre la UE-EEUU y obliga a revisar las transferencias de datos personales[Link][25/5/2021]

- sentencia comentada en Blog derecho internacional dermerule[Link][

- VELASCO NÚÑEZ, Eloy: Delitos informáticos realizados en actuación organizada. En *Diario La Ley* (7743), 2011, pág. 3 [Link][12/04/2021

- Vid. MICROSOFT SEGURIDAD, *Todo lo que debe saber acerca del phishing*, Julio 2021.[Link][02/02/2021]

- BAHILLO,Luis: *historia de internet, como nació y cuál fue su evolución* [Link][24/03/2021

- APWG [Link][17/02/2021]

- INTERNET CRIME COMPLAINT CENTER [Link][17/02/2021]

- OSI: *El fraude de los SMS* [Link][17/02/2021]

- Gustavo Eduardo: *Ingeniería social, hacking psicológico*. [09/03/2021][Link]

- THE OPEN WEB APPLICATION SECURITY PROJECT: [09-03-21][Link]INZUNZA ROJAS.

- BARRY, Leiner: Breve historia de Internet [Link][24/03/2021]

- AMBOAGE SANTOS, Fátima [Link][24/03/2021

- NNUU: *Economic fraud and Identity-related crime*.[Link][24/04/2021].

- OEDI: [30/04/2021][Link]

- KEYLOGGER ANDROID: [Link][22/05/2021]

- SAFETY DETECTIVE: *Ransomware* statistics[Link][22/05/2021]

- TÉCNICAS DE MAN-IN-THE-MIDDLE:[Link][22/05/2021]

- . CREDENTIAL HARVESTING [Link][22/06/2021]

- WEB DE LA EMPRESA SIFT [Link][23/06/2021]

- WEB DEL SISTEMA LYNX [Link][23/06/2021]

- WEB REVELOCK [Link][23/06/2021]

- DELITO SEXTORSION [Link][26/06/2021]

ANEXO JURISPRUDENCIAL

- SENTENCIA PENAL Nº463/2018, Audiencia Provincial de Cantabria, Sección 1, Rec 647/2018 de 17 de diciembre de 2018.

- SENTENCIA PENAL Nº 122/2020, Audiencia Provincial de Tenerife, Sección 6, Rec 882/2019 de 14 de abril de 2020.

- SENTENCIA PENAL Nº848/2019, Audiencia provincial de Barcelona, Sección 10, Rec 280/2019 de 3 de diciembre de 2019.

- SENTENCIA PENAL Nº173/2019, Audiencia Provincial de las Palmas, Sección 6, Rec 1109/2018 de 25 de junio de 2019.

- SENTENCIA PENAL Nº545/2019, Audiencia Provincial de Madrid, Sección 17, Rec 1268/2018 de 11 de Julio de 2019.

- SENTENCIA PENAL Nº 247/2018, Audiencia Provincial de Barcelona, Sección 10, Rec 253/2017 de 19 de marzo de 2018.

- SENTENCIA PENAL Nº473/2015, Audiencia Provincial de Tenerife, Sección 2, Rec 59/2014 de 9 de noviembre de 2015.

- SENTENCIA PENAL Nº451/2014, Audiencia Provincial de Tenerife, Sección 6, Rec 166/2014 de 9 de octubre de 2014.

- SENTENCIA PENAL Nº130/2015, Audiencia Provincial de Granada, Sección 2, Rec 97/2014 de 2 de marzo de 2015.

- SENTENCIA PENAL Nº93/2014, Audiencia Provincial de Zamora, Sección 1, Rec 97/2014 de 31 de octubre de 2014.

- SENTENCIA PENAL Nº580/2014, Audiencia Provincial de León, Sección 3, Rec 855/2014 de 3 de noviembre de 2014.

- SENTENCIA PENAL Nº247/2014, Audiencia Provincial de Alicante, Sección 2, Rec 83/2014 de 7 de mayo de 2014.

- SENTENCIA PENAL Nº226/2013, Audiencia Provincial de Álava, Sección 2, Rec 69/2012 de 4 de Julio de 2013.

- SENTENCIA PENAL Nº333/2012, Audiencia Provincial de Álava, Sección 2, Rec 44/2011 de 31 de octubre de 2012.

- SENTENCIA PENAL Nº334/2012, Audiencia Provincial de Álava, Sección 2, Rec 21/2012 de 31 de octubre de 2012.

- SENTENCIA PENAL Nº162/2014, Audiencia Provincial de Barcelona, Sección 8, Rec 297/2013 de 17 de febrero de 2014.

- SENTENCIA PENAL Nº102/2013, Audiencia Provincial de Ciudad Real, Sección 1, Rec 68/2013 de 11 de Julio de 2013.

- SENTENCIA PENAL Nº96/2013, Audiencia Provincial de Ciudad Real, Sección 1, Rec 49/2013 de 11 de Julio de 2013.

- SENTENCIA PENAL Nº70/2013, Audiencia Provincial de Albacete, Sección 1, Rec 3/2013 de 7 de marzo de 2013.

- SENTENCIA PENAL Nº444/2012, Audiencia Provincial de Madrid, Sección 6, Rec 33/2012 de 24 de octubre de 2012.

- SENTENCIA PENAL Nº644/2010, Tribunal Supremo, Sala de lo Penal, Sección 1, Rec 2766/2009 de 28 de mayo de 2010.

- SENTENCIA PENAL Nº235/2014, Audiencia Provincial de Asturias, Sección 2, Rec 195/2013 de 6 de mayo de 2014.

- SENTENCIA PENAL Nº5/2016, Audiencia Provincial de Valencia, Sección 3, Rec 394/2015 de 4 de enero de 2016.

- SENTENCIA PENAL Nº11/2019, Audiencia Provincial de Burgos, Sección 1, Rec 153/2018 de 14 de enero de 2019.

- SENTENCIA PENAL Nº8/2020, Audiencia Provincial de las Palmas, Sección 6, Rec 442/2019 de 22 de enero de 2020.

Casos suplantación identidad a la agencia tributaria: [LINK][23/05/2021]