CUNEF
COLEGIO UNIVERSITARIO DE ESTUDIOS FINANCIEROS

Máster Universitario en Acceso a la Profesión de Abogado

Título. Estudio práctico del robo de identidad. Especial atención al phishing bancario.

Autor. Nieves de Blas Reig.

Tutor. D. Israel Hernando Aguayo.

Madrid, febrero de 2018.

RESUMEN

El objeto de este trabajo es el estudio del robo de identidad. Antes de adentrarnos en esta figura haremos un estudio de los antecedentes a la protección de datos, para saber cómo surge la necesidad de proteger los datos y documentos que tenemos en internet. Además, veremos cuáles son los posibles derechos de la persona que pueden verse afectados como consecuencia de esta conducta y en particular el derecho a la identidad. El principal problema que nos encontramos en esta materia es la ausencia de regulación por lo que nos ha parecido oportuno analizar las figuras afines que nos encontramos en nuestro Código Penal y que no nos resultan suficientes para dar una protección eficaz ante el robo de identidad. Finalmente, haremos una breve referencia al subtipo de robo de identidad que se conoce como phishing bancario y a los problemas de calificación jurídico penal que presenta.

ABSTRACT

The object of this work is the study of identity theft. Before getting into this figure we will study the background to data protection, to know how the need arises to protect the data and documents we have on the Internet. In addition, we will see what are the possible rights of the person that may be affected because of this behaviour and in particular the right to identity. The main problem we face in this matter is the absence of regulation, which is why we thought it would be appropriate to analyse the similar figures that we find in our Criminal Code and that are not enough to give us an effective protection against identity theft. Finally, we will make a brief reference to the subtype of identity theft that is known as banking phishing and the problems of criminal qualification that it presents.

PALABRAS CLAVE

Suplantación de la identidad, phishing, estafa informática, intimidad, protección de datos.

KEYWORDS

Identity theft, phishing, computer scam, privacy, data protection.

ÍNDICE

PAGINA

1. INTRODUCCIÓN 4
2. ANTECEDENTES JURÍDICOS A LA PROTECCIÓN DE DATOS 5
3. EL DERECHO A LA IDENTIDAD 8
   3.1 CONCEPTO DE IDENTIDAD ELECTRÓNICA O IDENTIDAD DIGITAL 8
   3.2 LA PROTECCIÓN JURÍDICA DE LA INTIMIDAD 10
4. EL ROBO DE IDENTIDAD 12
   4.1 CONCEPTO. 12
   4.2 POSIBLES BIENES JURÍDICOS PROTEGIDOS 15
   4.3 POLÍTICA CRIMINAL EN MATERIA DE ROBO DE IDENTIDAD EN LA UE 17
   4.4. DELITOS A LOS QUE SE RECONDUCEN LAS CONDUCTAS DE ROBO DE IDENTIDAD 18
      4.4.1 Delito de usurpación del estado civil (art.402 CP) 19
      4.4.2 Delito de estafa (art.248 CP) 21
      4.4.3 Delitos contra la intimidad (art. 197 CP y art. 197 Bis CP) 23
5. LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS 26
   5.1 CASOS TRAMITADOS POR LA AEPD 27
6. ESTUDIO DEL PHISHING BANCARIO. 28
   6.1 CONCEPTO 28
   6.2 PRIMERAS APARICIONES DEL PHISHING EN ESPAÑA Y SU EVOLUCIÓN 29
   6.3 CALIFICACIÓN JURÍDICO PENAL DEL PHISHING: EL PHISHER Y EL CYBER-MULER 30
      6.3.1 Problemas de competencia territorial en el phishing 30
      6.3.2 La ignorancia deliberada del mulero informático 32
7. GLOSARIO 32
8. CONCLUSIONES 35
9. REFERENCIAS BIBLIOGRÁFICAS 36
10. LEGISLACIÓN Y JURISPRUDENCIA 39
11. APÉNDICE 42

ABREVIATURAS UTILIZADAS

AEPD = Agencia Española de Protección de Datos.

APWG = Anti-Phishing Working Group.

CE = Constitución Española.

CIFAS= Credit Industry Fraud Avoidance Scheme,

CP = Código Penal.

Coor = Coordinador.

Dir = Director.

EEMM = Estados Miembros.

FJ = Fundamento Jurídico.

LOPD = Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

NU = Naciones Unidas.

SAP = Sentencia de la Audiencia Provincial.

SAN = Sentencia de la Audiencia Nacional.

STC = Sentencia del Tribunal Constitucional.

STS = Sentencia del Tribunal Supremo.

UE = Unión Europea.

1. INTRODUCCIÓN

El tema objeto de estudio es fruto de la evolución social, en este caso del desarrollo de las técnicas de la informática, y su necesariamente aparejado desarrollo normativo. Sin duda, la evolución de las nuevas tecnologías ha supuesto un drástico cambio en la sociedad que el derecho ha tenido que afrontar.

Warren y Brandeis resumían todo esto en su obra diciendo que "es un principio tan viejo como el common law que el individuo debe gozar de total protección en su persona y en sus bienes, sin embargo, resulta necesario, de vez en cuando, redefinir con precisión la naturaleza y la extensión de esta protección. Los cambios políticos, sociales y económicos imponen el reconocimiento de nuevos derechos, y el common law, en su eterna juventud, evoluciona para dar cabida a las demandas de la sociedad"[1]. Estos autores en su artículo "The Right to Privacy", (*Harvard Law Review*, 1980) se referían a medios tecnológicos de incursión en la vida privada como la captura de imagen a distancia y la distribución de estas imágenes en la prensa.

Hoy en día tenemos que hacer frente a un creciente desarrollo de las posibilidades técnicas de la informática, más allá de aquellas a las que hacían referencia Warren y Brandeis, así, comenzaremos nuestro estudio con un breve análisis de este desarrollo y su paralela evolución normativa.

Tristemente, la evolución técnica da lugar a la aparición de nuevas conductas delictivas, entre estas conductas se encuentra la materia que da lugar a nuestro trabajo y que se ha dado en llamar *robo de identidad*.

El estudio de esta conducta reviste especial interés, desde nuestro punto de vista, pues carece de regulación en nuestro ordenamiento jurídico y por ello muchas veces queda impune. A lo largo del presente trabajo trataremos de justificar la necesidad de

---

[1] Warren,S., Brandeis,L.D., *"The right to privacity"*, en Harvard Law Review, vol. 4, núm.5, 1980. Edición Española a cargo de Benigno Pendás y Pilar Baselga, *"El derecho a la Intimidad"*, Madrid: Editorial Civitas. 1995.

una regulación específica para el robo de identidad, como consecuencia del profundo análisis que haremos de esta conducta.

La problemática que supone la ausencia de regulación específica en esta materia ha sido puesta de manifiesto, entre otros, por la Fiscalía General del Estado diciendo: "No podemos acabar este análisis sin referirnos, siquiera someramente, a las cifras que computamos en el apartado <<otras tipologías delictivas>>. Se incluyen en ese epígrafe los procedimientos incoados como consecuencia de denuncias por acciones cometidas a través de las TIC,s y no encuadrables en ninguno de los tipos penales específicamente reseñados, como, por ejemplo, los supuestos finalmente calificados como blanqueo de capitales en las defraudaciones por phishing; determinadas conductas asociadas a la violencia de género cometidas a través de las TIC,s, o incluso denuncias presentadas por comentarios de carácter ofensivos realizados a través de la red y considerados ab initio atípicos. Pero sin duda el volumen mas elevado -y de ahí su mención independiente- son los procedimientos derivados de denuncias por suplantación de identidad en la red que han dado lugar, al menos, a 117 incoaciones en el año 2014. El hecho de que no se haya tipificado expresamente en nuestra legislación esta conducta determina que estos comportamientos, salvo que puedan reconducirse a otros tipos penales como el descubrimiento y revelación de secretos o los delitos contra la integridad moral entre otros, no den lugar a responsabilidad penal y el procedimiento se vea abocado al archivo"[2].

2. ANTECEDENTES JURÍDICOS DE LA PROTECCIÓN DE DATOS

Antes de adentrarnos en la esencia de nuestro trabajo conviene realizar un breve estudio de las nuevas posibilidades técnicas que ofrece la informática y de su paralela evolución normativa.

Podríamos entender que el *Social Security Act*, aprobado por el presidente de los Estados Unidos de América Roosevelt, en el año 1935, es el primer gran proyecto de recogida masiva de datos personales, con él se pretendía el reajuste de datos referentes a los trabajadores como la asistencia médica, las pensiones y otros beneficios. A pesar de

[2] Memoria Fiscalía General del Estado, en el Capítulo III, "*Fiscales especialistas y delegados para materias específicas*", en el apartado relativo a la actividad de la Fiscalía Especial Delegada para la Criminalidad informática, 2015, Pág.599.

los ambiciosos objetivos del proyecto, los escasos medios técnicos de la época hicieron muy difícil que se cumplieran en su totalidad, evidenciando la necesidad de nuevas herramientas técnicas que pudieran afrontar proyectos como este.

Es en 1941 cuando tiene lugar el descubrimiento de Konrad Suze de la primera computadora controlada por programas, la Z3.

Sin embargo, la necesidad de mejorar las técnicas de guerra fue lo que dio lugar al mayor avance en descubrimientos técnicos, así, podemos destacar, en 1943 el descubrimiento por un grupo de expertos al servicio del ejército británico del C*olossus* que perseguía descifrar mensajes secretos de los nazis durante la II Guerra Mundial, en 1945 en Estados Unidos, concretamente en Los Álamos que era el laboratorio donde se estaba desarrollando la bomba atómica, se fabrica el *Eniac (Electronic Numerical Integrator And Calculator),* y en el mismo año John von Neumann formula lo que sería considerado el primer programa de ordenador y establece las primeras bases teóricas de los ordenadores.

Las primeras aplicaciones civiles de la informática tienen lugar en 1950 cuando la multinacional norteamericana Remington Rand entrega el primer ordenador de uso comercial y comienza a fabricarlos en serie. En esta década se empieza a generalizar el uso civil de los ordenadores. En 1952 se empiezan a hacer por ordenador predicciones electorales sobre la candidatura presidencial de Eisenhouer y Stevenson en la cadena televisiva estadounidense CBS, que nuevamente se volverían a realizar en 1960 sobre la candidatura de Kennedy y R. Nixon, siendo en ambos casos acertadas. En 1954 General Electric compra un ordenador *UNIVAC (Universal Automatic Calculator)* para la contabilidad de su empresa, poniendo así de manifiesto el uso empresarial de los ordenadores. Asimismo, seguimos encontrándonos avances con finalidades militares como por ejemplo el *SAGE (Semi Automatic Ground Enviroment)* fabricado por IBM para la defensa aérea de Estados Unidos.

Es otra vez IBM, en el año 1968, quien introduce el primer sistema de gestión de bases de datos, diferenciando entre datos técnicos y datos personales, siendo sin lugar a duda la mayor y mejor aplicación informática del momento.

En España, será en 1962 de la mano de RENFE cuando se empiecen a dar los primeros usos civiles de la informática.

Gracias a estos avances, cada vez se manejaba un mayor uso de datos, personales y técnicos lo cual facilitaba la posible lesión de derechos individuales como consecuencia de un mal uso de los mismos y es Arthur R. Miller, el primer autor en poner de relieve los posibles peligros de la informática para la intimidad en su obra "*Personal privacy in the computer age: the challenge of a new technology and information oriented society"*[3].

[3] MILLER, A.R: *"Personal privacy in the computer age: the challenge of a new technology and information oriented society"*. Michigan Law Review, nº 67 de 1969, págs. 1089-1246.

Por su parte, tras realizar un estudio de las bases de datos más importantes en Estados Unidos, Westin expondrá posibles peligros en esta materia en su obra *"Data banks in a free society"*[4].

La necesidad de una regulación jurídica en esta materia se evidencia con el uso de ordenadores por particulares. Sorprendentemente, no es en Estados Unidos, país pionero en la mayoría de avances informáticos, donde se dicta la primera norma sobre protección de datos, sino que es en Europa, en el Länder alemán de Hesse, donde se publica la *Datenschutz,* de 7 de octubre de 1970 a la que seguirá la *Data Lag* de 1973 en Suecia. Si buscamos el origen de estas normas es inevitable que pensemos en las pretensiones apuntadas por distintos órganos de la Unión Europea.

El Consejo de Europa, en el año 1967, constituyó una comisión consultiva para el estudio de las tecnologías de la información y su potencial lesividad de derechos de las personas. El trabajo de la citada comisión se vio reflejado en la Resolución 509 de 1968 de la Asamblea del Consejo de Europa, cuya finalidad era poner de manifiesto la posible confrontación entre los derechos humanos y los nuevos logros científicos y técnicos. Por su parte, el Comité de Ministros del Consejo de Europa publica dos Resoluciones clave en las que recomienda la toma de precauciones en el uso de datos de carácter personal incluidos en bancos de datos en el sector privado y en el sector público, respectivamente, la primera es la Resolución nº 73 de 26 de Septiembre de 1973, relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector privado y la segunda, es la Resolución nº 74 de 20 de septiembre de 1974, relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público.

En Estados Unidos, en 1974, entra en vigor la *Privacy Act,* que será el verdadero precedente en normas sobre protección de datos de carácter personal.

La auténtica revolución tecnológica llega con ARPANET que era una red de computadoras creada por encargo del Departamento de Defensa de los Estados Unidos para ser un medio de comunicación entre las diferentes instituciones académicas y estatales. En 1970 ya ofrecía correo electrónico y transferencia de ficheros dentro de Estados Unidos apareciendo en 1973 las primeras conexiones internacionales.

La red ARPANET fue mejorando y posibilitando la conexión y transmisión de datos entre una multiplicidad de ordenadores. El funcionamiento de ARPANET, así como el de INTERNET se basa en protocolos, es decir en conjuntos de reglas que estandarizan procedimientos repetitivos. El 1 de enero de 1983 se implanta el protocolo TCP/IP, que sustituye el anterior protocolo NCP, y separa la parte militar, que se denominó Milnet y da lugar a INTERNET, que coexistió con ARPANET hasta 1990, en 1991 aparece la World Wide Web. Poco a poco, se generalizó su uso hasta integrarse en la vida de los

[4] REBOLLO DELGADO, L.; SERRANO PÉREZ, M.; *"Introducción a la protección de datos"*, Dykinson,S.L, 2008, nota al pie núm.5.

ciudadanos como medio de intercambio de información de datos y como medio de comunicación.

Con todo esto, las posibles lesiones de derechos fundamentales que se pueden producir como consecuencia de un mal uso de los avances técnicos traspasaban las fronteras estatales lo que hizo que la intervención jurídica necesitase transformarse en una regulación universal que planteó y que como veremos sigue planteando muchas dificultades.

3. EL DERECHO A LA IDENTIDAD

3.1 CONCEPTO DE IDENTIDAD ELÉCTRONICA O IDENTIDAD DIGITAL

El tema objeto de nuestro estudio es el robo de identidad, pero para poder estudiar el robo de identidad es necesario hacer una pequeña reflexión sobre qué entendemos por Derecho a la identidad.

A partir de la década de 1940 nos encontramos con los primeros estudios sobre el Derecho a la identidad. Antes de nada, conviene traer a colación la principal conclusión que nos ofrece Beltrán de Felipe en esta cuestión y es que "*el DI es uno de estos "nuevos" derechos que ofrece perfiles muy poco claros (y no sólo por estar basado esencialmente en textos de Derecho internacional) y que tiene contenidos y significados distintos en función de los países o del momento temporal. Pero ello no debe autorizar a ignorarlo sino, por el contrario, obliga a estar muy atentos a su desarrollo*" [5].

El concepto de identidad puede ser abordado desde diversas perspectivas que revisten importancia para el derecho, así nos encontramos con la identidad biológica o genética, la identidad individual o atributiva o la identidad cultural o colectiva, sin embargo, nos vamos a centrar en la identidad electrónica o digital, que en definitiva es la que afecta, en mayor medida, a nuestro estudio.

De manera muy sencilla podemos definir la identidad electrónica en palabras de Alamillo Domingo como "*el conjunto de los datos (a menudo denominados "atributos") que nos diferencia suficientemente del resto de personas o entidades, en un ámbito concreto, como por ejemplo, el nombre y apellidos, el nombre del padre y de la madre, los códigos de identificación que se nos asignan y otros; o en el caso de las máquinas la dirección IP o el nombre de dominio en Internet y otras redes*"[6].

---

[5] BELTRÁN DE FELIPE, M., *"¿Qué es el derecho a la identidad?"* en *"Robo de identidad y protección de datos"*. Aranzadi. Navarra, 2010, pág. 37.

[6] ALAMILLO DOMINGO, I.,*" Identidad Electrónica, Robo de Identidad y Protección de Datos Personales en la Red"* en *"Robo de identidad y protección de datos"*. Aranzadi. Navarra, 2010, pág.17.

Entre los tipos de identidad electrónica o digital más frecuentemente utilizados y siguiendo, de nuevo, la clasificación elaborada por Alamillo Domingo, podemos destacar:

- La identidad electrónica personal, que es la que nos identifica sin necesidad de estar conectados con ninguna organización, el ejemplo paradigmático es el Documento Nacional de Identidad (DNI). Está regulada por el Estado y es válida dentro de su territorio, aunque puede tener reconocimiento internacional como es el caso del Pasaporte.

- La identidad electrónica corporativa, que nos vincula con una organización pública o privada determinada y sirve para acreditar la pertenencia a la misma y es además la identificación personal dentro de la organización o corporación.

- La identificación electrónica de cliente, también nos vincula con una organización pública o privada, pero con la que se establece una relación de negocio que, en la mayoría de los casos, perdurara en el tiempo, aquí podemos encuadrar la identidad financiera.

La importancia de estas identidades es tal que las leyes llegan a admitir el derecho de los clientes de mantenerlas incluso una vez acabada la relación comercial cliente-empresa y el ejemplo más claro lo tenemos en el número de teléfono de móvil que se puede mantener de una compañía telefónica a otra, convirtiéndose en parte de nuestra identidad.

El denominador común de todas estas identidades es que son suministradas por terceras personas y por ello se les denomina de segunda o de tercera parte, según nos sirvan para relacionarnos con quien nos la suministró en cuyo caso serán de segunda o también para relacionarnos con terceras partes, que serán de tercera.

Por otra parte, nos encontramos con las llamadas identidades de primera parte, estas identidades se crean en el ámbito de la Web 2.0 por los propios usuarios, en plataformas como Facebook, Instagram o LinkedIn, en las que se divulgan datos personales gestionados por los propios usuarios, quienes también pueden controlar la privacidad de los datos que muestran.

En conclusión, podemos afirmar que la identidad electrónica es un mecanismo humano que presenta informaciones referidas a una persona y no de la persona en sí misma que en algunas ocasiones nace de la propia persona y en otras de terceros y que en cualquier caso está protegida por las leyes de protección de datos de carácter personal.

La mayoría de identidades de segunda y tercera parte son entendidas como un bien público por ejemplo el DNI o el Pasaporte o como una propiedad privada por ejemplo la Banca Electrónica lo que hace que estas identidades estén privatizadas y por ello no

puede existir un monopolio de ellas, por el contrario, las identidades de primera parte son de nuestra titularidad por lo que su gestión y privacidad corre a nuestra cuenta.

Las identidades de primera parte requieren una mayor diligencia en su uso, porque es frecuente que el hecho de que los datos que en ellas se publican o comparten no revistan la importancia de los que se muestran a través de las identidades de segunda y tercera parte hace que no prestemos tanta atención a la privacidad de estos y eso, a menudo, nos expone a importantes peligros.

3.2 LA PROTECCIÓN JURÍDICA DE LA IDENTIDAD

La identidad está íntimamente relacionada con la intimidad, no sólo conceptualmente si no también constitucionalmente. Por ello, donde exista derecho a la intimidad existe o debería existir derecho a la identidad, entendiendo este como el derecho de preservar la identidad frente al conocimiento ajeno o al uso indebido por los demás.

La doctrina española concluye que el derecho a la intimidad está vinculado a la construcción y evolución de los derechos de la persona[7]. Partiendo de que los derechos de la persona nacen de la especial consideración que tiene la persona en el ordenamiento jurídico y la intimidad como bien que define al individuo frente a los demás es por tanto objeto de protección jurídica.

El derecho a la identidad se encuentra reconocido en todos los países que han ratificado la Convención de Derechos del Niño aprobada por las NU en 1989 y es así porque su artículo 8 recoge el derecho de los niños de "*preservar su identidad":*

> *" 1. Los Estados Partes se comprometen a respetar el derecho del niño a preservar su identidad, incluidos la nacionalidad, el nombre y las relaciones familiares de conformidad con la ley sin injerencias ilícitas.*
> *2.Cuando un niño sea privado ilegalmente de algunos de los elementos de su identidad o de todos ellos, los Estados Partes deberán prestar la asistencia y protección apropiadas con miras a restablecer rápidamente su identidad ".*

Asimismo, algunas constituciones nacionales lo recogen expresamente. La CE de 1978 no recoge expresamente la protección de la identidad.

Por contra, el ordenamiento jurídico español sí reconoce a la identidad a nivel legislativo y concretamente lo hace a través de leyes autonómicas de manera implícita y explícitamente en la Ley de Navarra 15/2005, de 5 de diciembre, de promoción, atención y protección a la infancia y a la adolescencia, se define el derecho a la identidad en su artículo 18:

"A fin de garantizar adecuadamente el derecho a la identidad de los menores, la Administración de la Comunidad Foral de Navarra llevará a cabo las siguientes actuaciones:

---

7 CASTAN TOBEÑAS, J., *"Los derechos de la personalidad"*, RGLJ, 1952, pág.40.

a) En los Centros Sanitarios públicos o privados en que se produzcan nacimientos establecerá las garantías suficientes para la inequívoca identificación de los recién nacidos.

b) Asimismo, adoptará las medidas necesarias para la inscripción del nacimiento de un menor en el Registro Civil cuando quienes tienen la obligación legal de promover tal inscripción no lo hagan".

Recientemente, muchos países tienden a garantizar por ley la identidad sexual posibilitando los cambios de sexo con pleno reconocimiento.

De lo expuesto, podemos deducir que, aunque ciertas vertientes del derecho a la identidad encuentran reconocimiento en nuestro derecho, una importante vertiente y en concreto la que nos atañe, el derecho a la identidad electrónica o digital, no encuentra reconocimiento expreso alguno pero esto no obsta a que podamos sostener la existencia de la protección legal de la identidad, intimidad o privacidad en nuestro ordenamiento y prueba de ello es el castigo de los fenómenos de robo o suplantación de identidad.

Hoy en día la identidad de una persona puede ser suplantada empleando sus datos bancarios, su número de identificación o de seguridad social o sus claves y contraseñas secretas de acceso a diversos servicios, como ejemplo a la banca electrónica.

La noción de intimidad o privacidad ha ido adquiriendo un carácter abierto y extensivo incluyendo, entre otros, los datos económicos y en este sentido se pronuncia la STC 233/2005 *"En relación con la inclusión de los datos con trascendencia económica (y, por ende, tributaria) en el ámbito de intimidad constitucionalmente protegido es doctrina consolidada de este Tribunal la de que los datos económicos, en principio, se incluyen en el ámbito de la intimidad. Así lo han puesto de relieve, claramente, las SSTC* 45/1989*, de 20 de febrero, FJ 9;* 233/1999*, de 16 de diciembre, FJ 7; y* 47/2001*, de 15 de febrero, FJ 8. Señaladamente, en la citada STC* 233/1999*, este Tribunal afirmó que "la información cuya transmisión se prevé en el precepto cuestionado —esto es, aquélla que tiene trascendencia tributaria— puede incidir en la intimidad de los ciudadanos (SSTC* 110/1984, 45/1989, 142/1993*; ATC* 642/1986*). Concretamente, hemos dicho que "no hay dudas de que, en principio, los datos relativos a la situación económica de una persona ... entran dentro de la intimidad constitucionalmente protegida (ATC* 642/1986*)" (FJ 7). Por su parte la STC* 47/2001 *señaló que la resolución de la queja enjuiciada debía partir "necesariamente del reconocimiento de que en las declaraciones del IRPF se ponen de manifiesto datos que pertenecen a la intimidad constitucionalmente tutelada de los sujetos pasivos. Así lo hemos recordado en la reciente STC* 233/1999*, de 16 de diciembre, FJ 7, al señalar que la información con trascendencia tributaria 'puede incidir en la intimidad de los ciudadanos'" (FJ 8)*[8]*".*

Por tanto, hablamos de robo o suplantación de identidad cuando una persona utiliza datos de otra, esto es cuando una persona se hace pasar por otra que no es, privándole de algo a lo que tiene derecho, y esto es privándole de su identidad. Así podemos concluir

[8] STC (Sala Segunda) núm. 233/2005 de 26 de septiembre, en http://hj.tribunalconstitucional.es.

que en tanto se castigue este robo, estamos reconociendo el derecho a la identidad pues no se puede castigar el robo de algo a lo que no se tiene derecho.

4. EL ROBO DE IDENTIDAD

4.1 CONCEPTO

Una primera aproximación a esta nueva figura delictiva que se ha dado en llamar "*robo de identidad "* podemos obtenerla partiendo de la definición que nos ofrecen el profesor Mata y Martín y Galán Muñoz en su artículo "A workable definition for identity related crime"[9], "*Whosoever by any technological or conventional means obtains identifying information on another or other persons without the consent of the persons concerned and with such information, undertakes any relevant action in which they assume the identity they have appropiated will be punished by a sentence of…"*, que podríamos traducir por, "cualquiera que por medios tecnológicos o convencionales obtenga datos de la identidad de otra u otras personas sin su consentimiento y realice cualquier acción relevante en la que se apropie de la identidad suplantada, será castigado con la pena de …".

Partiendo de una definición como esta es frecuente que el robo de identidad se relacione, entre otros, con el tráfico internacional de viajeros y esto con de delitos referidos a la inmigración ilegal o al terrorismo en el seno de bandas de delincuencia organizada tal y como señala Villacampa Estiarte, C en su obra *"Tráfico de documentos falsificados y uso indebido de documentos auténticos en el proyecto de Ley Orgánica de modificación del CP del 2007[10]"*.

Pero no podemos pensar que el robo de identidad sólo se presenta con carácter internacional o en el seno de la delincuencia organizada pues el robo de identidad reviste las más variadas formas de aparición, en ocasiones los suplantadores tratan de menoscabar el honor de sus víctimas atribuyéndoles actos que nunca han cometido o simplemente utilizan otra identidad para conseguir artículos que con la suya no podrían conseguir, como por ejemplo utilizando la identidad de una persona que posea una licencia de armas para comprar un arma.

Es precisamente la gran variedad de formas en que puede presentarse este delito una de las principales dificultades con las que nuestro legislador se encuentra a la hora de crear un tipo penal que abarque todas estas posibles formas de aparición.

En nuestro ordenamiento jurídico el único delito al que se puede reconducir de una manera general el robo de identidad es la usurpación del estado civil en los términos que

---

[9] MATA Y MARTÍN, R., GALÁN MUÑOZ, A., *"A workable definition for identity related crime"*, en *Cahiers de defense sociale,*Numéro Extraordinarie à l'ocassion du Douzième Congress des Nations Unies pour la prévention du crime et la justice pénale Salvador, Brésil, 12-19 Avril 2010, pág. 67.

[10] VILLACAMPA ESTIARTE, C., *"La adecuación del Derecho penal español al ordenamiento de la Unión Europea. La política criminal europea"*. Tirant lo Blanch, Valencia, 2009, pág.668 y ss.

contempla el artículo 401 del CP, *"El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años"*. Si bien este delito goza de una eficacia muy limitada en relación con el robo de identidad y deja muchas de las formas de aparición del mismo fuera de su tipo, tal y como veremos en el apartado 3.4 de este trabajo, dedicado a los delitos a los que se reconducen las conductas de robo de identidad.

Todo esto ha llevado a afirmar a Quintero Olivares que "nuestro derecho positivo carece de una tutela general de la identidad", ya que "los actos que pueden realizarse utilizando el nombre de otro pueden ser muchos y sólo algunos son hoy delictivos"[11].

La postura del ordenamiento jurídico español en esta materia contrasta con la previsión que nos encontramos en el Código penal Federal de los Estados Unidos en la que el robo de identidad es aplicable a delitos tales como el robo, la falsa representación de la ciudadanía, la adquisición ilegal de armas o el fraude patrimonial, concretamente dicho Código afirma que "*Quien, durante la realización de cualquier violación delictiva enumerada en la subsección (c) conscientemente, transfiera posea o use sin autorización legal, un medio de identificación de otra persona deberá ser condenado, además con la pena correspondiente a dicho delito, a una pena de prisión de 2 años de duración"*[12].

Galán Muñoz propone en su ponencia "*El robo de identidad: aproximación a una y difusa conducta delictiva"*, la comprensión del robo de identidad desde un punto de vista más estricto, entendiendo que con robo de identidad se alude a "*aquellos fraudes de carácter económico que se efectúan mediante la utilización de los datos o documentos identificativos de otra persona"*[13]. Y es entendiendo el robo de identidad desde un concepto más restringido, como este, donde podemos encontrar referencias normativas en nuestro ordenamiento jurídico que analizaremos en otro epígrafe.

Y es en este sentido en el que Ravoet, Secretario General de la federación europea de bancos definió el robo de identidad como "*… la toma de la identidad de la víctima, para obtener créditos, tarjetas de crédito de bancos y minoristas, robar dinero de las cuentas existentes de la víctima, solicitar préstamos, establecer cuentas con compañías de servicios públicos, alquilar apartamentos, presentar bancarrotas u obtener un trabajo usando el nombre de la víctima"*[14].

Finalmente, para delimitar el alcance del concepto de robo de identidad es necesario mencionar otro concepto al que va íntimamente ligado, el *fraude de identidad*, UK Home Office Identity Fraud Steering Committee y CIFAS los definen en los siguientes términos:

---

[11] QUINTERO OLIVARES, G., *"La "clonación" de tarjetas y el uso de documentos ajenos"*, Boletín de Información del Ministerio de Justicia, 2006, pág.144.

[12] GALÁN MUÑOZ, A..; *"El robo de identidad: aproximación a una nueva y difusa conducta delictiva"* en *"Robo de identidad y protección de datos"*. Aranzadi. Navarra, 2010, nota al pie núm.286, pág.170.

[13] Ibidem, pág.171.

[14] Ravoet, G, *"The impact of fraud and identity theft on banking and financial systems"*, High Level Conference on maintaining the integrity of identity and payments, Bruselas 22 de noviembre de 2006, pág.9.

- "***Identity Theft*** *occurs when sufficient information about an identity is obtained to facilitate identity fraud, irrespective of whether, in the case of an individual, the victim is alive or dead*." *"El robo de identidad ocurre cuando se obtiene suficiente información sobre una identidad para facilitar el fraude de identidad, independientemente de si, en el caso de un individuo, la víctima está viva o muerta*".

- "***Identity Fraud*** *occurs when a false identity or someone else's identity details are used to support unlawful activity, or when someone avoids obligation/liability by falsely claiming that he/she was the victim of identity fraud. Examples include: using a false identity or someone else's identity details (name, address, date of birth etc) for commercial or monetary gain, to obtain goods or access to facilities or services e.g. opening a bank account, applying for a loan or credit card*"[15] "*El fraude de identidad ocurre cuando una identidad falsa o los datos de identidad de otra persona se utilizan para respaldar actividades ilegales, o cuando alguien evita la obligación / responsabilidad al afirmar falsamente que fue víctima de un fraude de identidad. Los ejemplos incluyen: usar una identidad falsa o los datos de identidad de otra persona (nombre, dirección, fecha de nacimiento, etc.) con fines comerciales o monetarios, para obtener bienes o acceder a instalaciones o servicios, p. abrir una cuenta bancaria, solicitar un préstamo o una tarjeta de crédito*".

- "***Identity Theft*** *- (also known as impersonation fraud) is the misappropriation of the identity (such as the name, date of birth, current address or previous addresses) of another person, without their knowledge or consent. These identity details are then used to obtain goods and services in that person's name." "El robo de identidad - (también conocido como fraude de suplantación) es la apropiación indebida de la identidad (como el nombre, fecha de nacimiento, dirección actual o direcciones anteriores) de otra persona, sin su conocimiento o consentimiento. Estos detalles de identidad se utilizan luego para obtener bienes y servicios en nombre de esa persona".*

- *"**Identity Fraud** - is the use of a misappropriated identity in criminal activity, to obtain goods or services by deception. This usually involves the use of stolen or forged identity documents such as a passport or driving licence.[16]" "Fraude de identidad: es el uso de una identidad indebida en una actividad delictiva para obtener bienes o servicios mediante el engaño. Esto generalmente implica el uso de documentos de identidad robados o falsificados, como un pasaporte o un permiso de conducir".*

De las definiciones expuestas podemos concluir que el robo de identidad se refiere a la conducta de mera apropiación de otra identidad y dentro del mismo podríamos

15 www.identitytheft.org.uk
16 www.cifas.org.uk

encuadrar conductas como el *dumpster diving*, el *skimming*, el *phishing*, el *pretexting*, o el *pharming*, que más adelante analizaremos prestando especial atención al phishing.

Por su parte el fraude de identidad va más allá refiriéndose también al uso de esa identidad o de esos datos robados.

Sin embargo, en mi opinión, y siguiendo las definiciones propuestas en esta materia por la doctrina que citábamos al principio de este apartado, la definición completa de robo de identidad abarcaría la obtención de datos o documentos de un tercero y su posterior utilización fraudulenta. Por ello, podemos concluir que para apreciar la conducta de robo de identidad deberían de concurrir estos dos elementos materiales, robo y fraude.

4.2 POSIBLES BIENES JURÍDICOS PROTEGIDOS

La creación de cualquier norma jurídica nace de la necesidad de sancionar las conductas que puedan lesionar determinados bienes que, con el nacimiento de esa norma, alcanzan la calificación de jurídicos.

El derecho penal se orienta a la protección de los bienes jurídicamente tutelados por el ordenamiento y es aquí donde cobra sentido el estudio que inicialmente hicimos del derecho a la identidad, pues es la identidad el principal bien jurídico que se pretende proteger con la tipificación del delito de robo de identidad. Asimismo, y como ya hemos adelantado cabe encuadrar la intimidad dentro de los bienes jurídicos que se pretenden proteger con la figura del robo de identidad pues está íntimamente relacionada con la identidad.

Muy relacionado con la intimidad, con la tipificación del robo de identidad, también, se trataría de proteger el derecho a la protección de datos que viene reconociendo la jurisprudencia constitucional, ligado al derecho a la intimidad pero con ciertas matizaciones dice el TC, "*La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, de 10 de abril, FJ 5; 115/2000, de 10 de mayo, FJ 4), es decir, el poder de resguardar su*

vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos"[17].

Podemos entender, tal y como viene haciéndolo el TC[18], que el derecho a la protección de los datos es un bien jurídico autónomo y suficientemente diferenciado del derecho a la intimidad como para necesitar de protección jurídica.

En la misma línea se pronuncia el TS al hacer una diferenciación entre el derecho a la intimidad como tal y la libertad informática, exponiendo *"Esta segunda dimensión de la intimidad conocida como libertad informática o habeas data, encuentra su apoyo en el art. 18.4 CE, en donde taxativamente se dispone que "la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". De esta proclamación se deriva su poder de acción del titular para exigir que determinados datos personales no sean conocidos, lo que supone reconocer un derecho a la autodeterminación informativa, entendido como libertad de decidir qué datos personales pueden ser obtenidos y tratados por otros. La llamada libertad informática significa, pues, el derecho a controlar el uso de los datos de carácter personal y familiar que pueden recogerse y tratarse informáticamente (habeas data); en particular -como señala la doctrina- entre otros aspectos, la capacidad del ciudadano para oponerse a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención (SSTC. 11/98 de 13.1, 45/99 de 22.3)"*[19].

Por otro lado, tal como expone el profesor Mata y Martín[20] el robo de identidad puede afectar a intereses colectivos como el propio tráfico económico y mercantil o la veracidad en las relaciones sociales y jurídicas.

Así, apuntan autores como Nieto Martín que entiende que el interés protegido o jurídicamente relevante que pretende tutelar el robo de identidad está en conexión con la necesidad de fortalecer la confianza de los usuarios en los medios de pago alternativos al dinero convencional[21].

Por último, conviene traer a colación que existe un sector doctrinal que apuesta por la creación del bien jurídico llamado seguridad informática, que abarcaría de una manera específica la integridad de los datos y de los programas informáticos[22], por lo

---

17 STC (Pleno) 292/2000 de 30 de Noviembre, FJ. 6º, en http://hj.tribunalconstitucional.es

18 STC (Pleno) 290/2000 de 30 de Noviembre, FJ. 7, en http://hj.tribunalconstitucional.es.

19 STS (Secc. 1ª) 8457/2009 de 30 de Diciembre, FJ. 6º, en (CENDOJ) ECLI: ES:TS:2009:8457.

20 MATA Y MARTÍN, R., *"Propuestas de política legislativa sobre el robo de identidad"*, en *Cahiers de defense sociale*,Numéro Extraordinarie à l'ocassion du Douzième Congress des Nations Unies pour la prévention du crime et la justice pénale Salvador, Brésil, 12-19 Avril 2010, pág.60.

21 NIETO MARTÍN, A, *"Robo de identidad: Del fraude económico a las migraciones clandestinas"*. Jornadas sobre Derechos humanos y armonización internacional del Derecho penal en el 60º Aniversario de la Declaración Universal de los Derechos humanos, Centro de Estudios Políticos y Constitucionales, Madrid, 19 y 20 de enero de 2009, pág.28.

22 RODRIGUEZ MOURULLO, G.; ALONSO GALLO, J.; LASCURAIN SÁNCHEZ, J.A.; *"Derecho penal e Internet"*, Régimen jurídico de Internet, J. Cremades/M. A Fernández-Ordoñez /R. Illescas (Coor.), 2002, pág.260 y ss.

que la seguridad informática se convertiría en un bien jurídico abstracto y supraindividual[23].

En síntesis, es claro que el robo de identidad puede afectar tanto a intereses individuales como son la identidad o la intimidad o incluso el patrimonio en tanto que a través de ese robo de identidad se obtienen datos que permiten generar una lesión en nuestro patrimonio como a intereses colectivos que perjudiquen el tráfico económico y mercantil pues supongan una pérdida de confianza en los avances tecnológicos e informáticos que tantos beneficios revisten para las sociedades actuales.

4.3 POLÍTICA CRIMINAL EN MATERIA DE ROBO DE IDENTIDAD EN LA UNIÓN EUROPEA

Europa no ha sido ajena a la necesidad de afrontar la problemática relativa al robo de identidad.

Así, a principios del año 2000 la UE empieza a tomar conciencia de la importancia de dar una respuesta penal a este fenómeno que en Estados Unidos se describía como "*uno de los delitos que más rápido aumenta*"[24].

Desde principios del año 2000 hasta el año 2006 se analiza el robo de identidad en las distintas instituciones de la UE, y es en los años 2003 y 2004 cuando la idea de suficiencia de las distintas legislaciones europeas para afrontar el robo de identidad reconduciéndolo a otras conductas ya tipificadas empieza a quebrarse y empezamos a ver informes que ponen de manifiesto la necesidad de una regulación autónoma de la conducta de robo de identidad.

Siguiendo la opinión de Muñoz de Morales Romero[25] es en la "High Level Conference on maintaining the integrity of identity and payments" celebrada en Bruselas el día 22 de noviembre de 2006 en marco del *Plan de Acción (2004-2007)* y organizada conjuntamente por la DG Libertad Seguridad y Justicia, cuando surge la idea de armonizar las legislaciones penales de los EEMM y de exigir una regulación autónoma del robo de identidad en cada uno.

Tras numerosos Discursos, tanto a favor como en contra de una regulación específica del robo de identidad y de la armonización penal europea de la misma, los estudios en materia de robo de identidad llevados a cabo por la UE concluyen a finales de 2007.

---

[23] PUENTE ABA, Mª. L., *"Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos: ¿Debe protegerse de forma autónoma la seguridad informática?"*, Nuevos retos del Derecho Penal en la era de la globalización, Tirant Lo Blanch, 2004, págs.398 y 405.

[24] MUÑOZ DE MORALES ROMERO. M. *"¿De la nada al todo?: la importación del robo de identidad por la UE"*, en *"Robo de identidad y protección de datos"*, Aranzadi. Navarra, 2010, nota al pie núm.7.

[25] Ibidem, pág.47.

La *Comunicación de Seguimiento del Plan de Acción 2004-2007* requería un estudio previo de las posibilidades de las legislaciones penales de los distintos EEMM para perseguir el robo de identidad, a partir del cual decidiría si era o no necesaria una regulación autónoma del mismo.

Así las cosas, en el año 2007 se publica un anuncio de licitación para la realización de un "Estudio comparativo (que evalúe) la necesidad de instrumentos con vistas a luchar contra las actividades de la delincuencia organizada relacionadas con la usurpación de identidad en los EEMM de la UE"[26], sin embargo, este proyecto nunca llego a adjudicarse ya que la Comisión anuncio la cancelación del mismo por razones administrativas al poco de publicarlo.

Por todo ello, no tenemos una regulación penal europea armonizada en materia de robo de identidad y siguen siendo numerosos los EEMM, entre los que se incluye España, que carecen de una regulación autónoma de robo de identidad.

Para terminar este apartado resta mencionar dentro de la actividad legislativa en materia de robo de identidad llevada a cabo por la UE sobre el robo de identidad, el Convenio de Cibercrimen de 23 de Noviembre de 2001 del Consejo de Europa que ha sido ejemplo para muchos EEMM, como Alemania, Austria, Italia, Bélgica, Francia o Rumania para establecer normas penales sobre criminalidad informática en sus ordenamientos jurídicos y en el mismo sentido es importante resaltar la Decisión Marco de la UE 2005/222/JAI sobre ataques a sistemas de la información[27].

4.4 DELITOS A LOS QUE SE RECONDUCEN LAS CONDUCTAS DE ROBO DE IDENTIDAD

El principal problema del que partimos en nuestro análisis es la ausencia de una regulación específica para las conductas de robo de identidad. Es por eso por lo que no podemos hablar de regulación del robo de identidad, por lo menos dentro de nuestras fronteras.

La solución que ofrece la jurisprudencia española, entre otras, es castigar las conductas que podrían encuadrarse en lo que hemos definido como robo de identidad a través de la aplicación de figuras afines ya tipificadas en el Código Penal pero que no ofrecen soluciones del todo satisfactorias.

A grandes rasgos son varios los delitos de nuestro Código Penal que pueden, de alguna manera, relacionarse con el robo de identidad, así podemos destacar, en sentido amplio, entre los delitos recogidos en el Título VI Delitos contra la libertad, los delitos

[26] Ibidem, nota al pie núm 69, pág. 52.

[27] SALVADORI, L..; *"La lucha contra el hurto de identidad: las diferentes perspectivas legales"* en *"Robo de identidad y protección de datos"*. Aranzadi. Navarra, 2010, pág.231.

de amenazas y coacciones, regulados en el Capítulo II (arts. 169 – 172) y en el Capítulo III (arts.172 – 172 ter).

Del Título VII De las torturas y otros delitos contra la integridad moral, especialmente el delito de humillación.

Del Título X Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, el delito de descubrimiento y revelación de secretos, regulado en el Capítulo I (art.197).

Del Título XI Delitos contra el honor, los delitos de calumnias e injurias, previstos en el Capítulo I (arts.205 – 207) y Capítulo II (arts.208 – 210).

Finalmente, del Título XIII Delitos contra el patrimonio y contra el orden socioeconómico, determinadas conductas de robo, que se encuentran en el Capítulo II (arts.237 - 242), el delito de estafa en sus diversas modalidades, Capítulo VI (arts.248 – 251 bis) y del Capítulo XI los delitos contra la propiedad intelectual (arts. 273 – 277).

Centrándonos, en los delitos con los que se castigan conductas concretas de robo de identidad es necesario hacer referencia a los siguientes delitos, usurpación del estado civil, estafa y descubrimiento y revelación de secretos.

4.4.1 Delito de usurpación del estado civil (art.401 CP)

En relación con este delito, ya advertíamos con anterioridad, que es al único al que se puede reconducir de una manera general la conducta de robo de identidad, aunque, no abarca, como veremos en nuestra exposición, de una manera completa la conducta de robo de identidad. El CP recoge los supuestos de usurpación del estado civil en su art. 401[28].

Según la doctrina y la jurisprudencia española la usurpación del estado civil requiere una falsedad personal[29], por lo que se puede concluir que lo que se pretende tutelar es la identidad o la personalidad más allá del estado civil.

En este sentido, se pronuncia la doctrinal penal mayoritaria, entendiendo que lo que pretende proteger este delito es un "bien jurídico colectivo constituido por la fe pública, que se puede concretar en la confianza de la comunidad en la correcta identificación de las personas"[30]. Por tanto, lo que se protege son los derechos inherentes al estado civil de una persona considerados como absolutos o intangibles[31].

---

[28] Art. 401 CP *"El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años".*

[29] SAP Lérida, Secc. 1ª, 325/2011 de 24 de Mayo en (CENDOJ) ECLI: ES:APL:2011:325, FJ. 5º. *"La actual tipificación y reubicación sistemática del delito de usurpación de estado civil, que en el vigente Código Penal ha pasado a conformar el capítulo IV del Título XIII, ha venido a dar carta de naturaleza a la antigua opinión doctrinal que lo configuraba como un delito de falsedad personal".*

[30] FARALDO CABANA, P.; "*De la usurpación del estado civil"*, en Gómez Tomillo (Dir.), *Comentarios al Código Penal,* 2ª ed, Ed. Lex Nova, 2010, págs.-1528-1530.

[31] QUINTERO OLIVARES, (Dir.), Comentarios a la Parte Especial del Derecho Penal, Aranzadi, 2005, págs. 1535 y ss.

La jurisprudencia, hace precisiones muy concretas de los requisitos necesarios para que nos encontremos ante una conducta de usurpación del estado civil, "*Trasladado esto al tema que nos ocupa, quiere decir que para usurpar no basta con usar un nombre y apellidos de otra persona, sino que es necesario hacer algo que solo puede hacer esa persona por las facultades, derechos u obligaciones que a ella solo corresponden; como puede ser el obrar como si uno fuera otro para cobrar un dinero que es de este, o actuar en una reclamación judicial haciéndose pasar por otra persona, o simular ser la viuda de alguien para ejercitar un derecho en tal condición, o por aproximarnos al caso presente, hacerse pasar por un determinado periodista para publicar algún artículo o intervenir en un medio de comunicación"*[32].

Esto es, nos encontramos ante un delito de mera actividad, a diferencia de los delitos de resultado como es la estafa, que analizaremos a renglón seguido, que requieren un resultado concreto para su consumación. Para estar ante un supuesto de usurpación del estado civil baste con la suplantación sin ser necesaria la producción de un perjuicio al "no exigir el tipo que la conducta tenga lugar en perjuicio de la persona suplantada o para perjudicarla"[33].

La jurisprudencia, hace dos precisiones más en cuanto a los requisitos exigidos para apreciar el tipo del art.401 CP, por un lado, requiere cierta permanencia en la identidad suplantada y, por otro lado, precisa que la usurpación no se límite a un uso concreto de otra identidad, sino que sea en sentido amplio y alcance a todas las facetas que integran la identidad humana[34].

La conducta de robo de identidad, tal y como la hemos entendido a lo largo de nuestro estudio, engloba la obtención de datos o documentos de un tercero y la utilización fraudulenta o relevante de los mismos, por tanto, es claro, que va más allá del delito de usurpación del estado civil del art.401 del CP.

A mayor abundamiento, y al hilo de las precisiones jurisprudenciales que hemos expuesto, nos reafirmamos en que el delito de robo de identidad no es reconducible al de usurpación del estado civil. Esto es, porque el robo de identidad puede afectar un dato concreto y aislado como puede ser la usurpación de un perfil de Facebook, que en principio supone el mero uso del nombre y apellidos de otra persona sin necesidad de

---

[32] SAP Madrid, Secc. 16ª, 17313/2011, de 21 de Noviembre en (CENDOJ) ECLI: ES:APM:2011:17313 , FJ. 1º.

[33] FARALDO CABANA, P.; *"De la usurpación del estado civil"*, en Gómez Tomillo (Dir.), *Comentarios al Código Penal,* 2ª ed, Ed. Lex Nova, 2010, pág.-86.

[34] SAP Tarragona, Secc. 2ª, 1403/2005, de 10 de octubre de 2005 en (CENDOJ) ECLI:ES:APT:2005:1403, FJ. 2º, *"ya que, como ha declarado la jurisprudencia, es condición precisa que la sustitución de persona se lleve a cabo para usar de sus derechos y acciones. Son, pues, atípicas y no punibles penalmente las conductas consistentes en utilizar de forma espuria un nombre o identidad ajena. De este modo, sólo en el caso de una verdadera "suplantación de identidad", que no se limite al nombre, sino a todas las características o datos que integran la identidad de una persona, nos hallaremos ante un delito de usurpación de estado civil, del art. 401 del Código Penal, en que el suplantador asume como propia y excluyente una identidad ajena. La permanencia es un presupuesto típico del delito de usurpación de estado civil, pero, aun siendo condición necesaria, no es suficiente, pues también el derogado delito de uso público de nombre supuesto, del derogado art. 322 del Código de 1973, requería tal permanencia, y un uso prolongado del nombre falso, diferenciándose por tal motivo de la falta del art. 571, que sólo precisaba un uso aislado o único".*

"*hacer algo que solo puede hacer esa persona por las facultades derechos u obligaciones que a ella solo corresponden*" como señala la SAP de Madrid de 21 de Noviembre de 2011 a la que aludimos en nuestra nota núm.26.

De igual manera, el robo de identidad no precisa ni permanencia ni uso en sentido amplio de la identidad suplantada, como sí precisa el art.401 del CP para entender que estamos ante un delito de usurpación del estado civil.

4.4.2 Delito de estafa (art. 248 CP)

El delito de estafa, según se regula en nuestro CP, presenta dos modalidades, la estafa convencional que se regula en el apartado 1º del art.248 y la estafa informática que se regula en su apartado 2º [35].

El delito de estafa, como ya hemos apuntado, un delito de resultado, pues en la mayoría de los casos requiere para su consumación que como consecuencia del engaño o de la manipulación informática se produzca un perjuicio patrimonial efectivo. Además, requiere la concurrencia de los siguientes elementos:

- ***Engaño*** precedente o concurrente, este debe de ser bastante para la consecución de los fines propuestos, y con suficiente entidad para provocar el traspaso patrimonial. Asimismo, debe de producir un error esencial en el sujeto pasivo (víctima), desconocedor de lo que constituía la realidad.
- ***Perjuicio para la víctima***, que se plasma en un riesgo para su patrimonio.
- ***Relación de causalidad*** entre el engaño del autor de la estafa y el perjuicio de la víctima, con lo que el dolo (intención de engañar) tiene que preceder a la acción defraudadora, no valorándose penalmente el dolo sobrevenido, esto es posterior a la acción engañosa.
- ***Ánimo de lucro***, que consisten en la intención de obtener un enriquecimiento de índole patrimonial.

Estos elementos que forman el delito de estafa vienen exigiéndose por la jurisprudencia, así, "*Tal como se ha expuesto en resoluciones precedentes de este Tribunal, los elementos que estructuran el delito de estafa , a tenor de las pautas que marcan la doctrina y la jurisprudencia (SSTS 220/2010, de 16-2 ; 752/2011, de 26-7 ; y 465/2012, de 1-6), son los siguientes: 1) La utilización de un engaño previo bastante , por parte del autor del delito, para generar un riesgo no permitido para el bien jurídico (primer juicio de imputación objetiva); esta suficiencia, idoneidad o adecuación del engaño ha de establecerse con arreglo a un baremo mixto objetivo-subjetivo, en el que*

[35] Art.248 CP *"Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.**2.** También se consideran reos de estafa: **a)** Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. **b)** Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo. **c)** Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero".*

se pondere tanto el nivel de perspicacia o intelección del ciudadano medio como las circunstancias específicas que individualizan la capacidad del sujeto pasivo en el caso concreto. 2) El engaño ha de desencadenar el error del sujeto pasivo de la acción. 3) Debe darse también un acto de disposición patrimonial del sujeto pasivo, debido precisamente al error, en beneficio del autor de la defraudación o de un tercero. 4) La conducta engañosa ha de ser ejecutada con dolo y ánimo de lucro. 5) De ella tiene que derivarse un perjuicio para la víctima, perjuicio que ha de aparecer vinculado causalmente a la acción engañosa (nexo causal o naturalístico) y materializarse en el mismo el riesgo ilícito que para el patrimonio de la víctima supone la acción engañosa del sujeto activo (relación de riesgo o segundo juicio de imputación objetiva)"[36].

Sin embargo, tras la reforma del CP operada por la LO 5/2010 de 22 de julio, la jurisprudencia considera que, en el seno de los delitos de estafa informática, estos es los del art.248.2 CP, la mera manipulación informática es suficiente para entender que se ha producido un engaño sin que sea necesario que se dé un engaño personal[37].

Las razones por las que entendemos que el robo de identidad no es subsumible al delito de estafa regulado en el art. 248 CP, están íntimamente relacionadas con los elementos necesarios para que concurra el mismo y que acabamos de analizar.

El robo o sustracción de datos, en lo que a nuestro modo de ver sería una conducta calificable como robo de identidad, no requiere un engaño, esto es, puede que esos datos se obtengan de una manera no engañosa, por ejemplo, cuando alguien deja abierta su cuenta de Banca Electrónica en el ordenador de su trabajo mientras se ausenta para comer dejando el ordenador encendido. Estos datos podrían incluso conseguirse de manera lícita por ejemplo en el supuesto de que alguien facilite sus datos personales, nombre, apellidos, número de DNI y de Pasaporte, fecha de nacimiento etc.… a un empleado de una agencia de viajes para que en su nombre realice una reserva y este empleado haga uso de ellos.

En el robo de identidad, el sujeto pasivo (víctima) no tiene por qué intervenir, por lo que el error que viene exigiendo la jurisprudencia que produzca el engaño en ella no tiene por qué concurrir, más aún cuando ni si quiera tiene porque darse ese engaño.

Finalmente, tal y como venimos planteando la definición de robo de identidad, si bien es cierto, que ésta requiere un uso fraudulento o al menos relevante de esos datos o documentos sustraídos no tiene por qué producir un perjuicio patrimonial en la víctima. El uso que el autor haga de los datos o documentos no tiene por qué perseguir la obtención de una ventaja patrimonial, en otras palabras, el sujeto activo no tiene por qué

---

[36] STS, Secc. 2ª, 5573/2014, de 26 de Diciembre de 2014, FJ 3º, en(CENDOJ) ECLI: ES:TS:2014:5573.

[37] SAP de Cádiz, Secc. 8ª, 1500/2017, de 23 de Octubre de 2017, FJ. 2º *"Con la reforma operada por LO. 5/2010 de 22 de julio, el apartado 2 del artículo 248 del CP determina que también se consideran reos de estafa 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 de otra. Como indica la Juzgadora a quo no es preciso la concurrencia del engaño propio de la estafa básica por parte del estafador porque la asechanza a patrimonios ajenos realizada mediante manipulaciones informáticas actúa con automatismo en perjuicio de tercero, precisamente porque existe la manipulación informática y por ello no se exige el engaño personal en la forma referida (STS 533/07, 12-6)".*

tener una finalidad lucrativa. En las conductas de robo de identidad podemos encuadrar por ejemplo el supuesto en el que una persona que desea alquilar un coche para lo que necesita tener una antigüedad de 2 años en su permiso de conducir y que no tiene, utiliza el permiso de conducir de otra que si tiene esa antigüedad y que previamente ha sustraído con la finalidad de alquilar ese coche. Esta conducta, a priori, no produce un perjuicio en el patrimonio del sujeto pasivo ni tampoco enriquece al actor que lo que persigue es poder alquilar ese coche que con su permiso de conducir no puede.

En conclusión, aunque ciertas conductas de robo de identidad pueden encontrar acomodo en la regulación del delito de estafa en el CP español, entendemos que las diferencias expuestas son suficientes para justificar las carencias que la regulación del delito de estafa presente ante una conducta de robo de identidad, pues no todas las conductas de éste podrían reconducirse fácilmente al delito previsto en el art. 248 del CP.

4.4.3 Delitos contra la intimidad (art. 197 CP y art.197 Bis del CP)

Los delitos contra la intimidad se encuentran regulados dentro del Título X del CP cuya rúbrica es "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio". En este epígrafe vamos a analizar el Capítulo Primero "Del descubrimiento y revelación de secretos" y concretamente el art.197 apartado 1 y 2 y el art.197 bis:

Art.197 CP: "*1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, 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.* ***2.*** *Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero*".

Art.197 Bis CP*: "****1.*** *El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.****2.*** *El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones*

electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses".

El art.197 Bis fue introducido por el número ciento siete del artículo único de la LO 1/2015, de 30 de marzo, por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal.

En nuestro análisis de los delitos contra la intimidad, comenzaremos por el estudio del art.197 apartados 1 y 2 del CP.

La primera de las conductas que tenemos que resaltar en la redacción de este artículo es el apoderamiento, para la consumación de este delito es necesaria la aprehensión material, es decir que no es suficiente el simple acceso a datos a través de sistemas informáticos.

Sin embargo, sí parece suficiente la acción de apoderamiento indicativa del ánimo del sujeto de conocer la intimidad de otro sin llegar realmente a descubrir el contenido del documento, en este sentido parece admitirse por la jurisprudencia las formas imperfectas de ejecución del delito[38].

Los correos electrónicos contienen información perteneciente a la esfera íntima de su titular no accesibles a terceras personas de manera indiscriminada por lo que el mero intento de descubrir su contenido es suficiente para consumar el delito previsto en el art.197.1 del CP sin que sea necesaria la posterior divulgación del contenido de los mismos[39].

El apartado 2 del art.197 hace referencia a datos reservados, lo cual nos hace plantearnos que datos se engloban en este concepto. Romeo Casabona entiende que son aquellos "cuyo conocimiento o acceso está limitado a terceros ajenos al fichero en el que se hallan registrados y archivados, aunque no sean íntimos en sentido estricto"[40]. Este apartado exige que quien realice la conducta lo haga en perjuicio de un tercero o en perjuicio del titular de los datos.

En la conducta subsumible al robo de identidad no es suficiente con apoderarse de los datos de otra persona, es decir, no es suficiente con apoderarse del correo electrónico de un tercero, sino que es necesario suplantar la identidad de ese tercero, tampoco es necesario el apoderamiento material de los datos o documentos que se quiere sustraer. Por lo que si reconducimos una conducta de robo de identidad al art.197 CP estaríamos

---

38 STS 6858/2011, de 14 de Octubre de 2011, FJ 9º *"Respecto al " iter criminis ", es una figura delictiva que se integra en la categoría de los delitos de intención, y en la modalidad de delito mutilado de dos actos, uno de apoderamiento, interceptación o utilización de artificios técnicos, unido a un elemento subjetivo adicional al dolo, consistente en el ánimo de realizar un acto posterior, descubrir el secreto, o vulnerar la intimidad de otro, sin necesidad de que éste llegue a producirse. Por ello, la conducta típica del artículo 197.1 , se consuma con el apoderamiento, interceptación, etc, sin necesidad que se produzca el efectivo descubrimiento de los secretos, o vulneración de la intimidad, siendo posibles las formas imperfectas de ejecución, tentativa acabada o inacabada. El elemento subjetivo del delito, constituido por la conducta típica que ha de ser dolosa, pues no se recoge expresamente la incriminación imprudente, exigida conforme al artículo 12 del texto legal, que ha de llevarse a cabo con la finalidad de descubrir secretos o vulnerar la intimidad, ya que la dicción literal del precepto emplea la preposicionn " para* "".

39 ROMEO CASABONA, C. M.ª, *"Los delitos de descubrimiento y revelación de secretos: Especial consideración a su comisión en conexión con las nuevas tecnologías de la información y de la comunicación"*, Tirant Lo Blanch, Valencia, 2004, pág. 83 y ss.

40 Ibidem pág. 110.

dejando impune una parte esencial de lo que denominamos robo de identidad, el uso relevante o fraudulento de la información o documentos sustraídos.

El robo de identidad tampoco podría encuadrarse en el tipo previsto en el art.197.2 del CP puesto que no es necesario que los datos o documentos que conforman el objeto material del robo de identidad tengan la calificación de datos reservados.

En cuanto a lo que refiere al art.197 Bis, que regula lo que se ha dado en llamar "*intrusismo informático"*, recoge el acceso al conjunto o a una parte del sistema informático. Lo que llama la atención en la redacción de este artículo es que prevé también como sujeto activo del delito la conducta del que facilite el acceso, siendo castigado con la misma pena que él lo haga por sí mismo.

La pretensión del legislador parece ser, una ampliación del ámbito de lo punible, castigando la conducta del sujeto que facilita el acceso al conjunto o a una parte del sistema informático de igual manera que el que realiza la acción como autor.

La nueva redacción del art.197 Bis refiere al conjunto o a una parte del sistema informático, mientras que en la anterior redacción del art.197 ter se aludía a "datos o programas informáticos contenidos en un sistema informático en parte del mismo"[41]. Esta conducta se limita a castigar el acceso al sistema informático vulnerando las medidas de seguridad establecidas, pero no abarca las conductas que se realicen una vez se haya conseguido el acceso.

El art.197 Bis limita la conducta típica a quien acceda, o facilite el acceso sin estar debidamente autorizado y vulnerando las medidas de seguridad. En el robo de identidad, como ya expusimos anteriormente, en el estudio del delito de estafa, nos encontramos con situaciones en las que el autor del delito obtiene los datos a través del titular, quien por ejemplo se los entrega voluntariamente por que recibe un mail fraudulento de su compañía telefónica diciendo que necesitan ciertos datos para hacer un estudio en un cambio de su tarifa. Por otra parte, como ya advertíamos anteriormente, reconduciendo una conducta de robo de identidad al art.197 Bis estaríamos dejando impune aquellos actos que se realicen con la información obtenida o la cuestión se tendrá que resolver por la teoría del concurso, lo que evidenciaría que este tipo no es suficiente para sancionar esta conducta en su conjunto.

Finalmente, cabe destacar que quien es autor del delito del art.197 Bis no está suplantando la identidad de nadie, sino que está burlando las medidas de seguridad para acceder o facilitar el acceso a un sistema o a parte de un sistema informático.

Nuevamente nos encontramos con que los delitos contra la intimidad no son suficientes para abarcar el conjunto de conductas que se pretende proteger con el supuesto de tipo que se ha dado en llamar robo de identidad.

[41] MORALES PRATS, F., (Coor.) *"Comentarios a la Parte Especial del Derecho Penal"*, Cizur Menor (Navarra), Aranzadi, 2016, págs. 479-480.

5. LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

El derecho a la protección de datos es un derecho fundamental garantizado por el artículo 18 de la CE., que *"persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado"*.

En el ámbito europeo, la primera norma que hace referencia a la existencia de una autoridad de control que vele por este derecho es el Convenio 108, concretamente en la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos. Esta directiva no solo establece la necesidad de crear autoridades de control, sino que también prevé la regulación y configuración jurídica de estas instituciones. Así, en su Considerando 62, establece que *"la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los estados miembros constituye un elemento esencial en la protección de las personas en lo que respecta al tratamiento de sus datos personales."*

La AEPD se creó en 1992 y comenzó a funcionar en 1994. Cuenta con un presupuesto propio y plena autonomía funcional. Se crearon tres agencias autonómicas: en Madrid en el año 2001, en Cataluña en el año 2003 y en el País Vasco en el año 2004. La agencia de Madrid fue suprimida en 2013 y sus funciones fueron asumidas por la AEPD.

La AEPD está encargada de vigilar el cumplimiento de la legislación sobre protección de datos, en especial lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

Tiene potestad normativa en el ámbito de sus competencias. Pudiendo dictar instrucciones y recomendaciones precisas para adecuar los tratamientos automatizados a los principios de la LOPD.

Asimismo, realiza una función represiva, a través de su potestad sancionadora que sea visto favorecida por el artículo 197.2 del Código Penal, que, como ya hemos analizado, tipifica las conductas consistentes en apropiarse, utilizar o modificar en perjuicio de terceros datos reservados que se hallen registrados en ficheros o soportes informáticos.

Por último, la Agencia tiene la función de representar a España en los foros internacionales en la materia y cooperar con diversos organismos internacionales y con los órganos de la Unión Europea en materia de protección de datos[42].

[42] www.agpd.es

5.1 CASOS TRAMITADOS POR LA AEPD

El jefe del área de Inspección de Datos de la AEPD, en su artículo "Casos de suplantación de identidad detectados en denuncias tramitadas en la Agencia Española de Protección de Datos"[43], resalta los casos tipo de robo de identidad con los que suele dar la AEPD y cómo el robo de identidad sale a la luz.

Así, destaca los siguientes:

- ***Financiación empleando carnet de identidad robado:***

En estos casos el suplantador necesita hacerse con el DNI de un tercero, lo cual no reviste excesiva complejidad y además necesita tener un conocimiento de los procedimientos de venta o contratación de servicios de la compañía para así poder emplear esa información de la forma adecuada.

La forma en la que la mayoría de los casos llegan a la AEPD es a través de los ficheros de morosos porque adquieren el bien con identidad falsa y luego no se hacen cargo del pago de las cuotas, lo cual supone un problema para el suplantado.

Este fenómeno es común en el ámbito de la venta de vehículos automóviles, así como en el ámbito de los servicios de contratación de telefonía móvil, que solamente requieren para contratar datos personales como el número de cuenta corriente y el documento nacional de identidad.

- ***Créditos con DNI y nóminas manipuladas***:

El suplantador también actúa manipulando las nóminas de sus víctimas y un caso concreto presentado ante la AEPD, supuso que el suplantador consiguió financiación para sus compras informáticas presentando una nómina falseada. El método de manipulación de nóminas es sencillo, utilizan el nombre de una empresa en la que el suplantado nunca estuvo empleado y en ella incluyen el número de cuenta corriente abierta por el suplantador, pero con los datos personales del suplantado. Nuevamente se llega al conocimiento del robo de identidad, a través de las listas de morosidad.

- ***Acceso a las áreas del cliente de un servicio contratado:***

Otra de las formas de aparición del robo de identidad las encontramos a través del acceso al portal de las empresas en Internet, muy frecuentemente a la banca electrónica.

Estos accesos están protegidos por el nombre de usuario y su contraseña, pero en la mayoría de los casos ese nombre de usuario es simplemente el DNI y la contraseña es la que es configurada por el usuario.

---

[43] DE SALVADOR CARRASCO, L.; *"Casos de suplantación de identidad detectados en denuncias tramitadas en la Agencia Española de Protección de Datos"* en "*Robo de identidad y protección de datos"*. Aranzadi. Navarra, 2010, págs 65- 75.

No son pocas las ocasiones en las que los usurpadores tratan de hacerse con las contraseñas a través de los procedimientos de recuperación de contraseña, y es gracias al envío de mensajes de texto por parte de la empresa al titular en la verificación durante los procedimientos de recuperación como se ha tenido cuenta de que se producen este tipo de robos de identidad.

- ***Contratación a empresas de servicios:***

Finalmente, conviene referirse a los robos de identidad llevados a cabo por empresas, fruto de las presiones del mercado.

En los años de la liberación de los servicios de energía, las empresas suministradoras realizaban los contratos por medio de centros de venta o de empresas representantes cuyo objetivo principal era la captación de clientes y la contratación de productos y servicios, pues con el fin de aumentar los objetivos marcados por las empresas suministradoras se produjeron casos de suplantación por parte de alguno de estos centros de venta.

En el seno de las empresas también tenemos que destacar los robos de identidad que se producen consecuencia del acceso a los ficheros de información personal.

6. ESTUDIO DEL PHISHING BANCARIO

6.1 CONCEPTO

El término "phishing" se acuñó por primera vez en enero de 1996 en las noticias del grupo de hackers 2600.*alt*, y podría traducirse por "pesca de datos informáticos"[44].

La conducta de phishing consiste en la suplantación de la página web de una entidad de crédito, fundamentalmente, aunque también puede ser de cualquier otra empresa de la que se pueda obtener un beneficio socioeconómico, haciendo creer al usuario que esta ante la página oficial de la misma.

El término phishing no ofrece una definición estática, sino que es un término que se encuentra en constantes evolución. Quizá, una de las definiciones más utilizadas nos la proporciona el APWG, precisamente porque prevé las constantes actualizaciones del mismo.

"Los ataques de phishing recurren a formas de ingeniería social y subterfugios técnicos para robar los datos de identificación personal de consumidores y las credenciales de cuentas financieras. Los ardides de ingeniería social se basan en correos electrónicos engañosos que conducen a los consumidores a sitios web falsos diseñados para estafar a los destinatarios para que divulguen datos financieros tales como números de tarjetas de crédito, nombres de usuario de cuentas, contraseñas y números de la seguridad social. Apropiándose de nombres comerciales de bancos,

[44] VELASCO NUÑEZ, E.; *"Fraudes informáticos en red: del phishing al pharming"*. La Ley nº 37 (2007), pág.1.

distribuidores y compañías de tarjetas de crédito, los phishers, a menudo convencen a los destinatarios para que respondan. Los subterfugios técnicos implican la instalación de crimeware en ordenadores personales para robar las credenciales directamente, habitualmente utilizando troyanos, que captan las pulsaciones del teclado"[45].

Las características que hacen al phishing una figura específica dentro de los delitos de fraude informático podemos resumirlas en:

- ***Ingeniería social***: El phishing es una conducta que se realiza a personas concretas, manipulándolas para que faciliten datos o claves personales que permitan al phisher llevar a cabo la conducta delictiva.

- ***Tecnología:*** Esta conducta se lleva a cabo a través de las tecnologías de la información y en particular a través de correos electrónicos.

- ***Suplantación:*** Es necesario que los atacantes consigan la apariencia real de una entidad bancaria oficial o de una agencia gubernamental.

6.2 PRIMERAS APARICIONES DEL PHISHING EN ESPAÑA Y SU EVOLUCIÓN

La primera aparición del phishing en España fue en mayo del año 2003 y viene de la mano de una investigación llevada a cabo por la Brigada de Investigación Tecnológica, que se había creado dentro de la Comisaría General de Policía Judicial en el año 2001.

Un joven con conocimientos informáticos suficientes "clonó" la página de una de las entidades de crédito más importantes de nuestro país, con el propósito de obtener números de tarjetas bancarias de los clientes y con esos datos recargar los teléfonos móviles de sus amigos. La página se consiguió cerrar en apenas 72 horas y el joven paso a disposición judicial gracias a los rastros que había dejado el joven como consecuencia de su inexperiencia[46]. Sin embargo, el phishing ha ido evolucionando, hasta el punto de que esta conducta hoy en día no tendría encaje en lo que se entiende por phishing, ya que le faltan dos elementos fundamentales, esto es la ingeniería social, pues aquí no ha habido engaño y la suplantación, en este caso de la entidad financiera.

Asimismo, se han ido dejando atrás los casos en los que simplemente se suplantaba la identidad de una entidad conocida y se solicitaba vía correo electrónico datos personales al usuario, con pretextos como fallos en el sistema o motivos de seguridad y se ha dado paso a la creación de enlaces a la "página original de la entidad" en la que se capturan los datos de la víctima. También, nos empezamos a encontrar con variantes del

[45] www.antiphishing.org

[46] VELASCO NUÑEZ, E.(Dir); (2006) *"Delitos contra y a través de las nuevas tecnologías ¿cómo reducir su impunidad?"*, Cuadernos de Derecho Judicial, pág.135.

phishing como el "*smishing*" que supone la misma conducta a través de mensajes de texto o incluso a través de voz IP, simulando ser un trabajador del banco.

No sólo han evolucionado los métodos con los que se lleva a cabo esta conducta, también los objetivos y la victimología. Pasando de buscar obtener datos bancarios atacando a grandes grupos financieros, los cuales han ido mejorando su seguridad informática, a entidades más pequeñas y vulnerables y finalmente a cualquier proveedor que ofrezca datos personales de interés.

Todo ello ha hecho que cada vez sean más y más sofisticadas las variantes de phishing con que nos podemos encontrar, lejos, de los meros engaños a través de un correo electrónico falso.

6.3 CALIFICACIÓN JURÍDICO PENAL DEL PHISHING: EL PHISHER Y EL CYBER-MULER

En la mayoría de conductas de phishing concurren dos sujetos, el phisher y cyber-mula o mulero informático.

El phisher es la persona que realiza lo que podríamos llamar la conducta preparatoria y la consumación del delito, esto es, es la persona que piensa el engaño que va a realizar y s uplantar a la entidad u organización a partir de la cual engañará a su víctima.

Por su parte, el mulero informático, es una especie de intermediario que retiene las cantidades económicas que se obtienen gracias a la conducta engañosa llevada a cabo por el phisher. La razón de que se cree esta figura radica en la disminución de probabilidades de identificación y posterior enjuiciamiento. El mulero, se encarga de mover el dinero a cuentas, en muchas ocasiones del extranjero, a través de empresas de paquetería postal, normalmente Moneygram o Western Union. Lógicamente, el mulero obtiene un porcentaje de la transferencia de la víctima.

No es extraño que este intermediario actúe como consecuencia de un contrato de teletrabajo que se pacta a través de internet o de falsas empresas pero que operan bajo apariencia de empresa real en la web[47].

Hay dos problemas con los que nos topamos a la hora de calificar jurídicamente el phishing, la competencia y la ignorancia deliberada.

6.3.1 Problemas de competencia territorial en el phishing

La conducta de phishing se realiza en internet, lo cual ya supone un primer inconveniente para poder situarlo en un ámbito territorial concreto. Asimismo, y como anticipábamos anteriormente, normalmente se opera desde diferentes países, por un

[47] SANCHIS CRESPO, C (Coor), *"Conductas típicas y prueba electrónica en los fraudes electrónicos"*, Civitas, Madrid, 2013, pág. 244.

lado, el lugar donde se ubica el phisher, por otro lado, el lugar donde se encuentran las víctimas sobre las que desplegará su conducta engañosa y por último nos encontramos con la localización del mulero, que es el que se encarga de la gestión de las transferencias, en otras palabras, quien mueve el dinero para disminuir las posibilidades de identificación.

En este sentido y dada la relación existente entre el phishing, como modalidad de robo de identidad, y el delito de estafa que previamente hemos analizado, podemos entender que le es aplicable la Teoría de la Ubicuidad a la que se refiere el Acuerdo del Pleno no jurisdiccional de la sala de lo Penal del Tribunal Supremo de fecha 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*."[48]. Al que hace referencia la STS 341/2005 "*Así, los dos primeros motivos denuncian, por vía del artículo 5.4 de la Ley Orgánica del Poder Judicial en relación con el 24 de la Constitución Española , la infracción del derecho al Juez legalmente predeterminado, ya que se afirma la competencia territorial de los Juzgados de Madrid, en vez de los de Málaga que fueron los que investigaron y enjuiciaron los hechos (motivo Primero), y la funcional del Juzgado de lo Penal en vez de la Audiencia, órgano que, en definitiva, conoció del procedimiento y dictó la Sentencia correspondiente (motivo Segundo). Respecto de la primera de tales alegaciones, que ya obtuvo en tres ocasiones respuesta de coincidente de parte de los órganos que intervinieron en la causa, sólo cabe insistir en que, aun tratándose en todo caso de una materia de mera legalidad ordinaria y, por ende, nunca susceptible de alegación en forma de denuncia de quebranto de un derecho fundamental, sucede que, la tramitación del procedimiento no adolece de defecto alguno por esta causa, toda vez que no sólo la competencia territorial ha de corresponder a los Tribunales del lugar en que se cometió el delito más grave, en este caso la Estafa y, por tanto, a los órganos de Málaga que es donde se produjo el desplazamiento patrimonial consumativo del ilícito, sino que, además, con la aplicación del criterio de la ubicuidad como principio para la atribución de competencia, aceptado por esta Sala según Acuerdo de su Pleno no jurisdiccional de fecha 3 de febrero de 2005, la cuestión queda ya libre de toda polémica*"[49].

Sin embargo, la Sala II del Tribunal Supremo no ha tomado siempre la misma postura en materia de competencia en la resolución de los recursos de casación frente a las sentencias dictadas contra los "muleros". La postura del Supremo varía en función de si lo encuadra dentro de la estafa informática, entendiendo que el elemento distintivo del delito es el aspecto subjetivo de la participación del mulero según que actúe conscientemente o no.

---

[48] "Acuerdos de Pleno no jurisdiccional, sala de lo Penal Tribunal Supremo años 2000 - 2016", Gabinete Técnico Sala de lo Penal, 2016, pág.49.

[49] STS (Secc. 1ª) 1702/2005, de 17 de marzo en (CENDOJ) ECLI: ES:TS:2005:1702, FJ 1º.

6.3.2 La ignorancia deliberada del mulero informático

El TS entiende el principio de ignorancia deliberada en los siguientes términos *"se trata de una alegación irrelevante y sólo exterioriza el principio de ignorancia deliberada. Quien no quiere saber, aquello que puede y debe conocer, y sin embargo trata de beneficiarse de dicha situación, si es descubierto, no puede alegar ignorancia alguna, y debe responder de las consecuencias de su ilícito actuar -- SSTS nº 1637/99 de 10 de Enero de 2000 y 1583/2000 de 16 de octubre"*[50].

En relación con el principio de ignorancia deliberada son numerosos los argumentos a favor de la aplicación de la teoría de la ignorancia deliberada a la conducta del mulero, bien para imputar autoría o cooperación necesaria en la estafa informática e incluso para estimar la presencia de dolo eventual o de imprudencia grave en el marco del delito de blanqueo de capitales. A sensu contrario destaca la STS de 3 de diciembre de 012, que rechaza la aplicación de esta doctrina entendiendo, que la utilización de la misma puede servir para eludir la prueba de conocimiento necesaria para poder aplicar la figura de dolo eventual[51]. En el mismo sentido se pronuncia el Supremo en su sentencia de 20 de marzo de 2013.[52]

En definitiva, hay un sector doctrinal que aboga por la aplicación del principio de ignorancia deliberada, en el sentido de que el cyber-muler podía haber conocido la finalidad última de sus actuaciones mientras que otros entienden que no es aplicable el principio de ignorancia deliberada porque su aplicación supone una inversión de la carga de la prueba para el sujeto acusado que se ve en la necesidad de probar la diligencia debida en su actuación.

En nuestra opinión, y sin perjuicio de que debemos estar a la situación de cada caso, en la mayoría de ocasiones entendemos que es aplicable el principio de ignorancia deliberada a los autores de estas conductas, especialmente porque parece lógico deducir que si tienen una capacidad intelectual suficiente como para conseguir el desvió de cuentas bancarias la tienen para indagar el objeto de su conducta.

7. GLOSARIO

- ***CRIMEWARE***: Es un tipo de software diseñado con la finalidad específica de cometer delitos financieros. El término crimeware fue acuñado por el secretario general del Anti-Phishing Working Group, Peter Cassidy, para distinguirlo de

[50] STS (Secc. 1ª) 3615/2002, de 22 de mayo en (CENDOJ) ECLI: ES:TS:2002:3615, FJ 1º.

[51] STS 8316/2012, (Secc. 1ª) de 3 de diciembre en (CENDOJ) ECLI: ES:TS:2012:8316, FJ 4º, *"Este punto de vista ha sido fuertemente criticado en la doctrina porque se lo entendió como una transposición del "willful blindness" del derecho norteamericano y porque se considera que no resulta adecuado a las exigencias del principio de culpabilidad, cuyo rango constitucional ha puesto de manifiesto el Tribunal Constitucional. Asimismo, se ha llamado la atención sobre el riesgo de que la fórmula de la "ignorancia deliberada" -cuya incorrección idiomática ya fue señalada en la STS de 20-7- 2006 - pueda ser utilizada para eludir "la prueba del conocimiento en el que se basa la aplicación de la figura del doloeventual ", o, para invertir la carga de la prueba sobre este extremo".*

[52] STS 227/2013, (Secc. 1ª) de 20 de marzo en(CENDOJ) ECLI: ES:TS:2013:1134
.

otros tipos de software malicioso como malwares, spywares o adwares. Los crimeware pueden instalarse en el ordenador del usuario o emplearse para manipular los servidores DNS y redirigir a los usuarios a páginas fraudulentas. El objetivo es robar la información necesaria para acceder a los servicios financieros online del usuario. En ocasiones el uso de estos programas se combina con la utilización de técnicas de ingeniería social que aprovechan la ingenuidad del usuario para obtener información.

- ***PHARMING:*** Para entender que es el pharming, es conveniente recordar cómo funcionan los sistemas de navegación por internet. Cuando tecleamos en el ordenador el nombre de un sitio web, este lo envía a un servidor DNS (Domain Name System) que transforma este nombre en una dirección IP que nos conecta con la página solicitada. El ciberatacante puede actuar sobre el DNS haciendo que este nos redirija a un sitio falso preparado por el estafador para hacerse con nuestras claves o cualquier tipo de información confidencial, o bien puede introducir un virus en nuestro propio equipo que desvíe el tráfico de la red a un sitio web falso. Si el infectado es nuestro equipo, podemos detectar el virus y tratar de eliminarlo, sin embargo, si el ataque se efectúa sobre el DNS nuestro equipo no detectará ningún tipo de malware y será muy difícil protegernos.

- ***PRETEXTING***: Es una forma de ingeniería social utilizada por los delincuentes informáticos para obtener información personal y documentos de una compañía, sin permiso del cliente, simulando ser otra persona. El estafador recopila suficiente información sobre la víctima para hacer creer al teleoperador que es el mismo y obtener así aquello que desea. El éxito de estas estafas está en la capacidad de los delincuentes para recopilar suficiente información personal de la víctima para poder hacerse pasar por ella. En el año 2005 la compañía HP se vio envuelta en un escándalo cuando contrato a unos detectives privados, que por medio del pretexting demostraron que varios consejeros estaban filtrando información confidencial a periodistas.

- ***SCAMS***: El scam es un fraude a través del correo electrónico. Consiste en una mezcla de phishing y fraude piramidal. Los estafadores obtienen los datos bancarios de su primera víctima por medio del phishing. A continuación, captan una segunda víctima a través de un correo electrónico con una jugosa oferta de trabajo, esta hará de “mulero” para los estafadores. Los estafadores ingresan, desde la cuenta de la primera víctima, en la cuenta del “mulero” una cantidad como pago por su trabajo de la que podrá retener su comisión, enviando el resto a los estafadores a por medio de una entidad de envío de dinero. De esta forma, no queda rastro alguno de los estafadores y si de la víctima que ha hecho de “mulero”.

- ***SKIMMING***: El skimming o clonado de tarjetas de crédito es una de las actividades fraudulentas más extendidas. Los delincuentes utilizan un pequeño aparato llamado skimmer para copiar las bandas magnéticas de las tarjetas, el mismo que utilizan los cajeros automáticos para leerlas. Una vez copiada pueden transferir los datos a una tarjeta en blanco o utilizarlos para transacciones on-line. El sistema es tan sencillo que cualquier puede ser víctima de esta estafa. Por ejemplo, cuando pagamos en un comercio con nuestra tarjeta, el dependiente la pasa por un datafono y nos dice amablemente que ese datafono no funciona y que va a pasarla por otro. El primero lo ha utilizado para clonar nuestra tarjeta y con el segundo ha efectuado el cobro. Manipulando los cajeros automáticos e instalando en ellos micro cámaras, además de clonar la tarjeta, pueden conseguir nuestro PIN de acceso.

- ***SMISHING***: Es una variante del phishing que tiene como víctimas a los usuarios de telefonía móvil. A través de un mensaje de texto se invita al usuario a conectar con una página web fraudulenta en la que el estafador se hace con información personal, roba datos bancarios o introduce algún troyano en el dispositivo. En otras ocasiones estos mensajes tratan de convencer al usuario para qué llame a un numero de tarificación especial pretextando la para que reclame un premio supuestamente obtenido o se beneficie de una falsa oferta.

- ***SNIFFERS:*** Son aquellos cibedelincuentes que utilizan el sniffing (sniff: olfatear) para robar información, su nombre deriva del dispositivo informático que emplean para ello. Es muy común que varios dispositivos conectados en red utilicen el mismo medio de transmisión de datos; los sniffers son programas informáticos que permiten al usuario controlar y analizar el tráfico de dicha red. Proporcionan al usuario información sobre todo el tráfico de la red: capturan, interpretan y analizan toda la información (mensajes, contraseñas, etc.) de la red. Aunque en principio los sniffers no fueron diseñados con una finalidad maliciosa, es evidente que no es muy difícil darles un uso fraudulento

- ***TROYANOS***: Son programas maliciosos que llegan al equipo del usuario a través de programas inofensivos que al ser ejecutados instalan un segundo programa, el troyano. La finalidad de estos programas es permitir al intruso controlar remotamente el equipo infectado. Pueden eliminar, modificar, copiar o bloquear datos. También pueden copiar los datos introducidos mediante el teclado, tales como las contraseñas. Existen muchos tipos de troyanos, pero, a diferencia de los gusanos y los virus, estos no pueden multiplicarse.

- ***WISHING O WHALE PHISHING***: Es un tipo de phishing que tiene como objetivos específicos a ejecutivos de nivel C en adelante de las grandes compañías, “los peces gordos”. Al igual que en el phishing el procedimiento consiste en el envío de correos electrónicos falsos que contienen enlaces a sitios

web fraudulentos. Al tratarse de objetivos muy concretos los correos deben ser más elaborados: deben contener referencias personales (que los estafadores pueden obtener de las redes sociales), la dirección del remitente debe resultar familiar a la víctima, los falsos enlaces deben contener logos corporativos que resulten creíbles, etc., es decir requiere más ingeniería social.

8. CONCLUSIONES

I. En el presente trabajo hemos comprobado que la evolución tecnológica a pesar de las muchas ventajas que presenta y de las mejoras que ha supuesto en nuestras vidas también presenta peligros que se manifiestan a través de los delitos informáticos y que cada vez, en mayor medida tenemos que afrontar.

II. Abordando esta problemática desde lo que, a nuestro modo de ver, debería de calificarse como delito de robo de identidad hemos podido comprobar las carencias que presenta nuestro ordenamiento jurídico para castigar estas conductas.

III. No podemos aceptar, que nuestro Código Penal se convierta en un parche para las nuevas conductas que surgen como consecuencia de la evolución de la sociedad y concretamente de la evolución tecnológica. Consideramos que la conducta de robo de identidad está suficientemente consolidada como para que la necesidad de una regulación sea una realidad que nuestro legislador no puede ignorar.

IV. Si bien es cierto, y así lo hemos comprobado a lo largo de nuestro estudio, que en nuestro ordenamiento jurídico existen figuras afines a esta conducta, pero ninguna de ellas es suficiente para abarcar todo lo que la conducta de robo de identidad conlleva y es por eso por lo que está más que justificada la necesaria intervención legislativa. No podemos perder de vista la importancia de la suplantación en esta conducta, porque, aunque se tiene que producir un engaño, la razón de ser de la conducta y del engaño que la misma genera tiene su origen en la suplantación de una identidad ajena. Hoy en día, no tenemos ninguna figura en nuestro ordenamiento que tenga la capacidad de desplegar una intervención eficaz contra esta conducta en su conjunto.

V. Asimismo, nos hemos referido a un subtipo de robo de identidad que es el phishing bancario. El hecho de existan subtipos de robo de identidad no hace más que evidenciar la realidad ante la que nos encontramos, pues la existencia de esta figura está más que reconocida por la doctrina hasta el punto de que existen distintas tipologías de la misma, como por ejemplo el phishing bancario.

VI. La conducta de phishing afecta cada día a más usuarios de internet, siendo España el país de la UE donde se producen más robos de identidad, ya que un 7% de los

internautas españoles han sido víctimas del delito de phishing[53]. En este sentido conviene destacar que la Policía Nacional Española ha creado un portal específico para que los ciudadanos puedan poner en su conocimiento este tipo de conductas. Adjuntamos el formulario que está a disposición de los ciudadanos como apéndice en nuestro trabajo Estas conductas, de phishing, no quedan impunes, pero en su mayoría se castigan por la vía del art. 248 CP que prevé el delito de estafa, lo cual hace que la esencia de esta conducta, es decir, la suplantación de la identidad que ha facilitado el engaño para que la víctima sufriera un perjuicio, habitualmente económico, queda fuera del tipo que prevé el art.248 CP.

VII. Por todo esto creemos que es fundamental el esclarecimiento de este nuevo tipo delictivo que se ha convertido en habitual en nuestras fronteras y que además se manifiesta de muy diversas maneras.

VIII. Finalmente, resta mencionar que dada la necesaria y justificada necesidad de un nuevo tipo penal. Podemos afirmar que estamos completamente de acuerdo con las propuestas legislativas que se vienen haciendo por parte de la doctrina, entre otras Mata y Martín y Galán Muñoz en los siguientes términos: "El que por cualquier medio tecnológico o convencional obtenga sin consentimiento del titular los datos identificativos de otra u otras personas y con ellos realice cualquier tipo de acción relevante haciéndose pasar por la persona suplantada, será castigada con la pena de.."[54]

9. REFERENCIAS BIBLIOGRAFICAS

ALAMILLO DOMINGO, I. (2010): "Identidad Electrónica, Robo de Identidad y Protección de Datos Personales en la Red" en "Robo de identidad y protección de datos"

BELTRÁN DE FELIPE, M.(2010): "¿Qué es el derecho a la identidad?" en "Robo de identidad y protección de datos"

BENIGNO PENDÁS /PILAR BASELGA (1995): "El derecho a la Intimidad"

CASTAN TOBEÑAS, J. (1952): "Los derechos de la personalidad"

DE SALVADOR CARRASCO, L.(2010): "Casos de suplantación de identidad detectados en denuncias tramitadas en la Agencia Española de Protección de Datos" en Robo de identidad y protección de datos".

Especial Delegada para la Criminalidad informática".

[53] http://www.abc.es/tecnologia/redes/abci-espana-pais-donde-producen-mas-robos-identidad-internet-201801021152_noticia.html.

[54] MATA Y MARTÍN, R., GALÁN MUÑOZ, A.., *"Propuestas de política legislativa sobre el robo de identidad",* en *Cahiers de defense sociale*,Numéro Extraordinarie à l'ocassion du Douzième Congress des Nations Unies pour la prévention du crime et la justice pénale Salvador, Brésil, 12-19 Avril 2010, pág. 66.

FARALDO CABANA, P. ; “De la usurpación del estado civil”, en Gómez Tomillo (Dir.), Comentarios al Código Penal.

FARALDO CABANA, P.: “De la usurpación del estado civil”, en Gómez Tomillo (Dir.), Comentarios al Código Penal.

GABINETE TÉCNICO SALA DE LO PENAL (2016): “Acuerdos de Pleno no jurisdiccional, sala de lo Penal Tribunal Supremo años 2000 – 2016”.
GALÁN MUÑOZ, A. (2010); “El robo de identidad: aproximación a una nueva y difusa conducta delictiva” en “Robo de identidad y protección de datos”.

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN (2007): “Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing”, Observatorio de la seguridad de la información

MATA Y MARTÍN, R.(2010): “Propuestas de política legislativa sobre el robo de identidad”. en Cahiers de defense sociale.

MATA Y MARTÍN, R./ GALÁN MUÑOZ, A.(2010): “A workable definition for identity related crime”, en Cahiers de defense sociale.

MEMORIA FISCALÍA GENERAL DEL ESTADO (2015): “Fiscales especialistas y delegados para materias específicas, en el apartado relativo a la actividad de la Fiscalía
MILLER, A.R (1969): “Personal privacy in the computer age: the challenge of a new technology and information oriented society”

MORALES PRATS, F., (Coor.) (2016) “Comentarios a la Parte Especial del Derecho Penal”.

NIETO MARTÍN, A (2009): “Robo de identidad: Del fraude económico a las migraciones clandestinas”. Jornadas sobre Derechos Humanos y Armonización Internacional del Derecho Penal en el 60º Aniversario de la Declaración Universal de los Derechos Humanos.

PUENTE ABA, Mª. L.(2004): “Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos: ¿Debe protegerse de forma autónoma la seguridad informática?”, Nuevos retos del Derecho Penal en la era de la globalización

QUINTERO OLIVARES, (Dir.) (2005): Comentarios a la Parte Especial del Derecho Penal.

QUINTERO OLIVARES, G.(2006), “La “clonación” de tarjetas y el uso de documentos ajenos”, Boletín de Información del Ministerio de Justicia.

RAVOET, G, (2006): “The impact of fraud and identity theft on banking and financial systems”. High Level Conference on maintaining the integrity of identity and payments.

REBOLLO DELGADO, L. / SERRANO PÉREZ, M. (2008): "Introducción a la protección de datos"

RODRIGUEZ MOURULLU, G./ ALONSO GALLO, J./LASCURAIN SÁNCHEZ, J.A.(2002): "Derecho penal e Internet"

ROMEO CASABONA, C. M.ª (2004): "Los delitos de descubrimiento y revelación de secretos: Especial consideración a su comisión en conexión con las nuevas tecnologías de la información y de la comunicación".

SALVADORI, I. (2010): "La lucha contra el hurto de identidad: las diferentes perspectivas legales" en "Robo de identidad y protección de datos".

SANCHIS CRESPO, C (Coor) (2013): "Conductas típicas y prueba electrónica en los fraudes electrónicos".

VELASCO NUÑEZ, E. (2007): "Fraudes informáticos en red: del phishing al pharming". La Ley Pena nº 37.

VELASCO NUÑEZ, E.(Dir); (2006) "Delitos contra y a través de las nuevas tecnologías ¿cómo reducir su impunidad? Cuadernos de Derecho Judicial.

VILLACAMPA ESTIARTE, C.(2009): "La adecuación del Derecho penal español al ordenamiento de la Unión Europea. La política criminal europea"

WARREN,S./ BRANDEIS,L.D. (1980): "The right to privacity"

PÁGINAS WEB

www.agpd.es

www.antiphishing.org

http://www.abc.es/tecnologia/redes/abci-espana-pais-donde-producen-mas-robos-identidad-internet-201801021152_noticia.html.

www.cifas.org.uk

www.identitytheft.org.uk

10. LEGISLACIÓN Y JURISPRUDENCIA

LEGISLACIÓN ESPAÑOLA

Constitución Española de 1978

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

Ley Orgánica 5/2010 de 22 de julio por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre del Código Penal.

Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ley de Navarra 15/2005, de 5 de diciembre de Promoción, Atención y Protección a la Infancia y a la Adolescencia de Navarra

LEGISLACION EXTRANJERA

Convenio de Cibercrimen de 23 de Noviembre de 2001 del Consejo de Europa

Datenschutz, de 7 de octubre de 1970 (Alemania)

Data Lag de 1973 en Suecia

Decisión Marco de la UE 2005/222/JAI sobre Ataques a Sistemas de la Información

Código penal Federal de los Estados Unidos

Privacy Security Act 1974

Resolución 509 de 1968 de la Asamblea del Consejo de Europaç

Resolución del Comité de Ministros del Consejo de Europa nº 73 de 26 de Septiembre de 1973

Resolución del Comité de Ministros del Consejo de Europa nº 74 de 20 de septiembre de 1974

Social Security Act de 1935

Convención de Derechos del Niño aprobada por las NU en 1989

JURISPRUDENCIA

TRIBUNAL CONSTITUCIONAL

STC (Sala Primera) 110/1984, de 26 de noviembre.

STC (Pleno) 45/1989, de 20 de febrero.

STC (Pleno) 142/1993, de 22 de abril.

STC (Sala Segunda) 144/1999, de 22 de julio.

STC (Sala Primera) 134/1999, de 15 de julio.

STC (Pleno) 233/1999, de 16 de diciembre

STC (Sala Primera) 98/2000, de 10 de abril

STC (Sala Segunda) 115/2000, de 10 de mayo

STC (Pleno) 292/2000 de 30 de noviembre.

STC 290/2000 (Pleno)de 30 de noviembre.

STC (Pleno) 47/2001, de 15 de febrero

STC (Sala Segunda) 233/2005, de 26 de septiembre.

ATC 642/1986

TRIBUNAL SUPREMO

STS (Secc. 1ª) 16/2000, de 10 de enero.

STS (Secc. 1ª) 7366/2000, de 16 de octubre.

STS (Secc. 1ª) 3615/2002, de 22 de mayo

STS (Secc. 1ª) 1702/2005, de 17 de marzo

STS 8457/2009 de 30 de diciembre.

STS (Secc. 1ª) 5339/2011, de 26 de julio

STS (Secc. 1ª) 3813/2012, de 1 de junio

STS (Secc.1ª) 8316/2012, de 3 de diciembre

STS (Secc.1ª) 227/2013, de 20 de marzo

STS, (Secc. 2ª), 5573/2014, de 26 de diciembre

AUDIENCIAS PROVINCIALES

SAP Tarragona, Secc. 2ª, 1403/2005, de 10 de octubre.

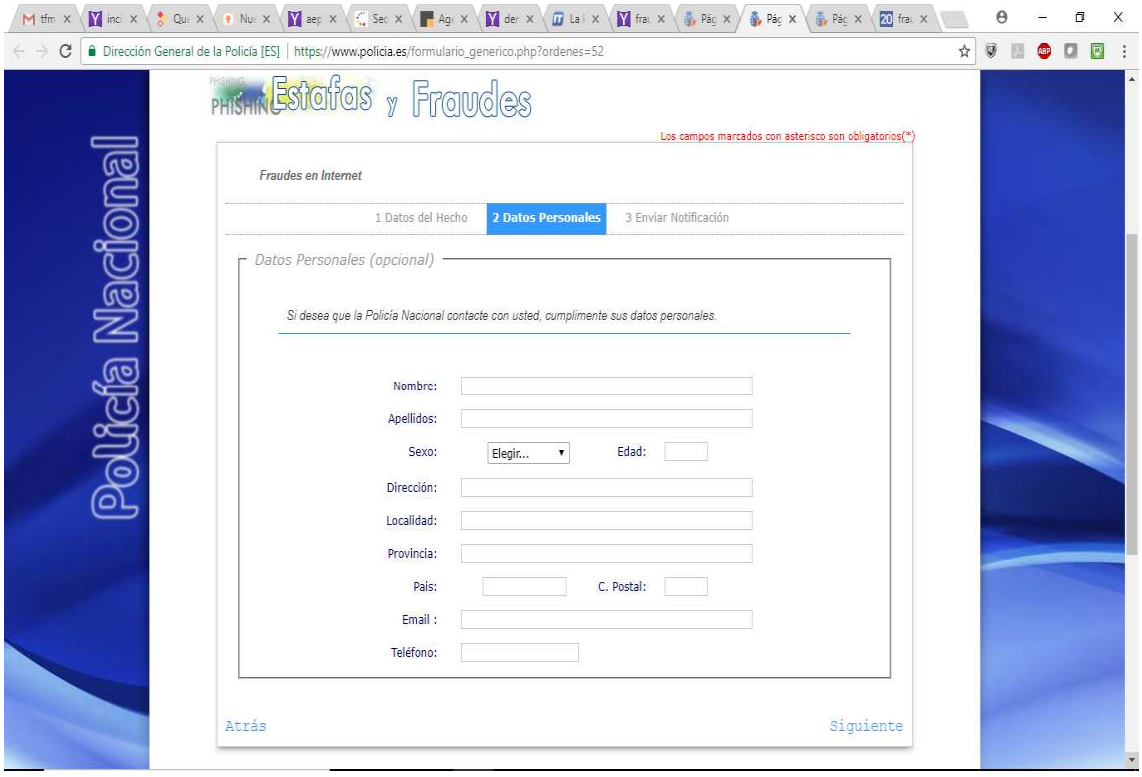
SAP Lérida, Secc. 1ª, 325/2011 de 24 de mayo.

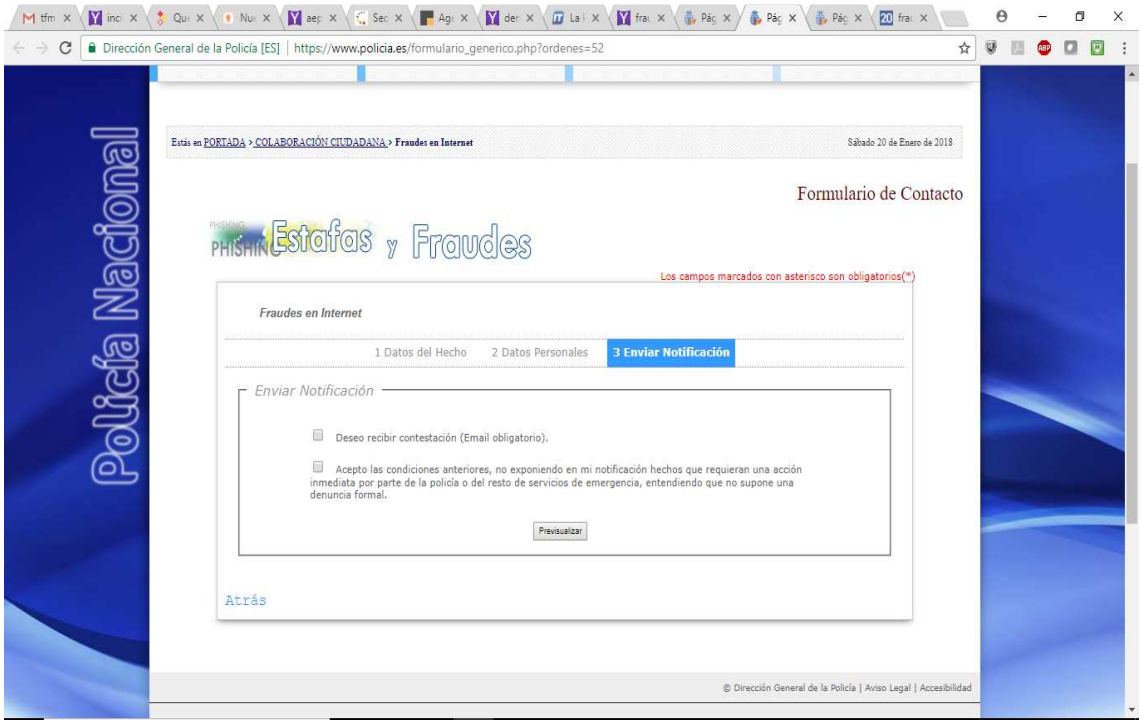
SAP Madrid, Secc. 16ª, 17313/2011, de 21 de noviembre.

SAP de Cádiz, Secc. 8ª, 1500/2017, de 23 de octubre de 2017.

11. APÉNDICE


Dirección General de la Policía [ES] | https://www.policia.es/formulario_generico.php?ordenes=52
Policía Nacional
Estás en PORTADA > COLABORACIÓN CIUDADANA > Fraudes en Internet
Sábado 20 de Enero de 2018
Formulario de Contacto
PHISHING Estafas y Fraudes
Los campos marcados con asterisco son obligatorios(*)
Fraudes en Internet
1 Datos del Hecho
2 Datos Personales
3 Enviar Notificación
Datos del Hecho
No utilice este cuadro para referirse a otro hecho ilícito al mismo tiempo. Solo se puede notificar un hecho por incidencia. Si desea informar sobre otro hecho debe hacerlo en una nueva comunicación
Información necesaria o complementaria sobre el hecho.
Comentario(*):
Importante: ¿Ha notificado esta incidencia a otro organismo oficial? (Oficina de antención al consumidor, Agencia Española de Protección de Datos, etc...)
Otras notificaciones:
Atrás
Siguiente


Dirección General de la Policía [ES] | https://www.policia.es/formulario_generico.php?ordenes=52
Policía Nacional
PHISHING Estafas y Fraudes
Los campos marcados con asterisco son obligatorios(*)
Fraudes en Internet
1 Datos del Hecho
2 Datos Personales
3 Enviar Notificación
Datos Personales (opcional)
Si desea que la Policía Nacional contacte con usted, cumplimente sus datos personales.
Nombre:
Apellidos:
Sexo:
Elegir...
Edad:
Dirección:
Localidad:
Provincia:
País:
C. Postal:
Email :
Teléfono:
Atrás
Siguiente


Dirección General de la Policía [ES] | https://www.policia.es/formulario_generico.php?ordenes=52
Policía Nacional
Estás en PORTADA > COLABORACIÓN CIUDADANA > Fraudes en Internet
Sábado 20 de Enero de 2018
Formulario de Contacto
PHISHING Estafas y Fraudes
Los campos marcados con asterisco son obligatorios(*)
Fraudes en Internet
1 Datos del Hecho
2 Datos Personales
3 Enviar Notificación
Enviar Notificación
Deseo recibir contestación (Email obligatorio).
Acepto las condiciones anteriores, no exponiendo en mi notificación hechos que requieran una acción inmediata por parte de la policía o del resto de servicios de emergencia, entendiendo que no supone una denuncia formal.
Previsualizar
Atrás
© Dirección General de la Policía | Aviso Legal | Accesibilidad