Universitat de les Illes Balears

Facultad de Derecho

Memoria del Trabajo Fin de Grado

La falta de regulación frente a la suplantación y usurpación de identidad en Internet

Elionor Vidal Torres

Grado en Derecho

Año académico 2017-18

DNI del alumno: 43220843W

Trabajo tutelado por Gabriel Garcías Planas
Departamento de Derecho Penal

Se autoriza a la Universidad a incluir este trabajo en el Repositorio Institucional para su consulta en acceso abierto y su difusión en línea, con finalidades exclusivamente académicas y de investigación.	Autor		Tutor	
	Sí	No	Sí	No
	X			

Resumen

El aumento de los *ciberdelitos* contrasta con su falta de regulación específica en nuestro Ordenamiento Jurídico.

Más allá de la suplantación de identidad en la red, que no constituye *per se* un delito, se encuentra el delito de usurpación de identidad en internet, que puede llevarse a cabo juntamente con otros delitos como el delito de descubrimiento y revelación de secretos, el Phishing, el Hacking o el Cracking.

Palabras clave del trabajo: Ciberseguridad, ciberdelitos, suplantación de identidad, usurpación de identidad en internet, usurpación de estado civil, concurso de delitos, usurpación de identidad en redes sociales, Phishing, Cracking, Hacking.

ÍNDICE

1. Introducción y marco histórico ... 3
2. Concepto y diferencia entre usurpación y suplantación de identidad en internet ... 4
Concepto ... 3
Diferencia ... 6
Evolución de la suplantación ... 7
3. Marco legal y novedades tras la reforma ... 8
4. Tipo penal. ... 10
Conducta típica ... 11
Tipo subjetivo ... 11
Pena ... 12
5. Tipologías y relaciones concursales ... 12
Usurpación y suplantación en redes sociales ... 12
Phishing y estafa informática ... 13
Delito de descubrimiento y revelación de secretos ... 15
Hacking ... 15
Cracking ... 16
6.6. El Ilícito civil ... 17
6. Conclusiones ... 17
BIBLIOGRAFÍA ... 19

1. Introducción y marco histórico

El actual panorama sociocultural y el incremento exponencial de las Tecnologías de la Comunicación y de la Información (TIC) ha tenido su repercusión en la aparición de nuevas formas delictivas o adaptaciones a las ya existentes. La facilidad de uso y rapidez que caracterizan la comisión de delitos en la red, así como el anonimato capaz de existir en tales delitos, ha dado lugar al traslado de los delitos a Internet.

En los últimos años, ha habido un incremento de la actividad delictiva en Internet, lo que ha dado lugar a la aparición de los denominados delitos informáticos o ciberdelitos, que son aquellas conductas típicas, antijurídicas, culpables y punibles realizadas a través de vías informática o con el objetivo de dañar ordenadores, medios electrónicos y redes de Internet.

Este tipo de delitos actualmente están presentes en cualquier parte del mundo en la que se tenga acceso a un medio electrónico y virtual debido a que el uso de los dispositivos electrónicos es una actividad cada vez más normalizada en todo el mundo.

Debido al ritmo al que avanzan los ciberdelitos y las tipologías de comisión de los mismos, las legislaciones de todos los países han tenido que hacer frente a esta relativamente nueva tipología delictiva, llevando a cabo un seguido de regulaciones tanto a nivel interno como a nivel internacional para que dichos delitos no queden impunes.

Una de las primeras regulaciones de los ciberdelitos fue Estados Unidos a través de la aprobación de la Crime Control Act en 1984, lo que dio paso a las primeras causas en materia de ciberdelitos, tales como el caso "United States vs Robert Morris"[1], en que se juzgaba al primer hacker acusado por propagar un virus.

Seguidamente, la regulación de los delitos informáticos se extendió a Europa, pero en España no fue hasta 1995, con la entrada en vigor del Código Penal, cuando encontramos legislación que hace referencia a esta materia, aunque no existe una ley específica que regule tales delitos, sino que se trata de una regulación dentro del propio Código Penal.

[1] UNITED STATES of America, Appellee, v. Robert Tappan MORRIS, Defendant–Appellant. No. 774, Docket 90–1336. | Argued Dec. 4, 1990. | Decided March 7, 1991.

En la actualidad, la creciente preocupación por la ciberseguridad[2] por parte de los Gobiernos a nivel mundial, ha generado multitud de legislación[3] y jurisprudencia con el objetivo de punir la comisión de estos hechos delictivos, aunque en el Ordenamiento Jurídico Español, no existe una regulación específica de los ciberdelitos sino que debemos acudir a la regulación que establece el Código Penal para encajarlos con los tipos penales regulados en el código.

En cuánto a la usurpación de identidad se refiere, no existe una regulación concreta que tipifique tal conducta, sino que se ha tratado de reconducir dicha conducta al delito de usurpación de estado civil tipificado en el artículo 401 del Código Penal, aunque es preciso hacer referencia a que en muchas ocasiones tal reconducción no puede llevarse a cabo ya que no puede ajustarse a los requisitos de este tipo y, por lo tanto, en muchas ocasiones podrían verse impunes dichas conductas.

Por todo ello, una gran parte de la doctrina critica este vacío legal[4] y la ausencia de regulación específica frente a los delitos informáticos, siendo muchos sectores los partidarios de una normativa específica y conjunta que regule los ciberdelitos como las existentes en otros países

2. Concepto y diferencia entre suplantación y usurpación de identidad en Internet

Concepto

La usurpación de estado civil tipificada en el Código Penal, ha evolucionado a lo largo de los años y ha dado lugar a la suplantación y usurpación de identidad en Internet, dos conceptos análogos aunque con una repercusión jurídica distinta.

Suplantación y usurpación son dos conceptos muy relacionados, que vienen definidos por la Real Academia Española definiendo, en primer lugar, la suplantación haciendo referencia a la acción de suplantar como " ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba" y, en segundo lugar, la usurpación de estado civil como "delito que comete quien utiliza de forma estable el estado civil, nombre y apellidos de otra persona, suplantando su personalidad."

[2] El último informe de McAfee, "McAfee Labs Threats Report: March 2018", demuestra que las muestras nuevas de malware crecieron un 32% durante el último trimestre de 2017.
[3] El Convenio sobre la ciberdelincuencia fue elaborado por el Consejo de Europa en Estrasburgo, con la participación activa de los estados observadores de Canadá, Estados Unidos, Japón, Chile, Costa Rica y Filipinas.
[4] ÁLVARO ÉCIJA BERNAL ("El ciberespacio, un mundo sin ley").

Se entiende por suplantación de identidad en internet[5], aquella acción mediante la cual una persona se hace pasar por otra en Internet. Se trata de la mera apropiación de derechos y facultades propias de la persona suplantada como podría ser la apropiación de redes sociales ajenas (Facebook, Instagram, Twitter…)[6].

En este aspecto, debemos diferenciar entre el suplantador y el suplantado, siendo el primero la persona física o jurídica que realiza el acto de apropiarse de cuentas u elementos identificativos de otra persona, el suplantado.

Por otro lado, la usurpación de identidad en Internet, tiene lugar desde que el suplantador empieza a realizar actos desde el perfil del suplantado haciendo entender que actúa siendo el suplantado, propietario de los derechos y facultades.

En este sentido y de conformidad con la Sentencia 14 de octubre de 2011: "el delito por tanto, se perfecciona con la realización de la actividad usurpadora y cesa cuando concluye la implantación. La conducta del agente exige una cierta permanencia y es insito al propósito de usurpación plena de la personalidad global del afectado".[7]

Es entonces, cuando la suplantación de identidad se convierte en usurpación de identidad y, en consecuencia, el suplantador pasa a denominarse usurpador y el suplantado pasa a ser el usurpado.

En la usurpación de identidad en redes sociales, el usurpado es la persona física o jurídica cuya identidad ha sido apropiada por un tercero que tiene abierta una cuenta en una red social (Facebook, Tuenti, Twitter…), y que la usa habitualmente ya sea para fines personales o profesionales mientras que el usurpador es la persona física o jurídica que se apropia de la identidad de un tercero haciéndose pasar por él y realizando acciones como si de él se tratase, como podrían ser la publicación de contenidos inapropiados o el envio de mensajes a terceros.

Según la jurisprudencia del Tribunal Supremo, la sentencia de 23 de mayo de 1986 establece que "El que usurpe el estado civil de una persona es fingirse ella misma para usar de sus derechos, es suplantar su filiación, su paternidad, sus derechos conyugales, es la falsedad, aplicada a la persona y con el ánimo de sustituirse por otra real y verdadera".[8]

---

[5] El Instituto Nacional de Tecnologías de la Información (adscrito al Ministerio de Industria español) definió la identidad digital como *el conjunto de la información sobre un individuo o una organización expuesta en Internet (datos personales, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha persona en el plano digital.*

[6] En España, el Instituto Nacional de Ciberseguridad trabaja concienciando, para evitar que estas situaciones ocurran y saber cómo identificarlas, al tiempo que da soporte técnico para reportarlas.

[7] STS (2ª) de 14 de Octubre de 2011, F. 7º (RJ 1045)

[8] STS (2ª) de 23 de Mayo de 1986, F. 1º(RJ 756)

Diferencia

La diferencia entre suplantación y usurpación de identidad radica en que mientras en la primera únicamente se lleva a cabo la apropiación de derechos y facultades de un perfil que pertenece e identifica a un tercero, en la segunda, además de dicha ocupación y apropiación, también se utilizan los datos del suplantado para actuar en su nombre.

Es imprescindible llevar a cabo esta diferenciación ya que en función de los hechos que tengan lugar, se incurrirá en una suplantación o usurpación de identidad; dos conductas subsumibles en diferentes tipos penales.

En el caso de que hablemos de una suplantación de identidad, debemos tener en cuenta que en la práctica y, de lege data, no existe una regulación específica en esta materia, ni un tipo penal concreto con el que pueda encajarse la mera suplantación de identidad en internet, aunque si se lleva a cabo tal suplantación con otros fines aunque no se pueda encuadrar con el delito del art.401 del Código Penal, sí que podrá encajar con otros tipos si se cumplen los requisitos, tales como los del art.197 y siguientes del Código Penal, en el caso de que se incurra en un delito de descubrimiento y revelación de secretos.

No obstante,debemos hacer un inciso en el hecho de que la mera ocupación de un perfil ajeno por lo que se refiere a las redes sociales, no supondrá delito si simplemente se limita a un nombre[9], sino que debe haber también una apropiación de los datos y características que integran la identidad de la persona suplantada. Ello viene establecido en la jurisprudencia del Tribunal Supremo; Así lo señala en su sentencia de 15 de junio de 2009 [10], en la que se establece que no basta con una sola acción o conducta de “hacerse pasar por otro”, sino que para que exista delito, el usurpador debe apropiarse de los derechos y obligaciones del usurpado.

Si, por el contrario, hablamos de usurpación de identidad, se trata del delito de usurpación de estado civil, tipificado en el art.401 del Código Penal, siendo un hecho indispensable para la comisión de éste delito, que el suplantador lleve a cabo acciones usando derechos y facultades del suplantado. Así lo establece el Tribunal Supremo en su Sentencia 331/2012 de 4 de Mayo[11], en la que define usurpar como “arrogarse la dignidad, empleo u oficio e otro, y usarlos como si fueran propios"

En el caso de las redes sociales, se estaría cometiendo un delito de usurpación de identidad cuando el suplantador actuase como si fuese el verdadero titular de la cuenta. Un ejemplo de ello, sería cuando el suplantador subiese fotografías o escribiese comentarios a otros perfiles actuando desde el perfil del suplantado y como si del mismo se tratase.

Tal y como se ha señalado anteriormente, es imprescindible llevar a cabo un análisis exhaustivo de la conducta del suplantador y llevar a cabo una correcta distinción entre

[9]La mera creación de un perfil con un nombre falso en una red social no supone delito.
[10] STS (2ª) de 15 de Junio de 2009, (RJ 635).
[11] STS (2ª) de 4 de Mayo de 2009, (RJ 331).

suplantación y usurpación de identidad, puesto que en función de si se trate de suplantación o usurpación de identidad, será delito o no. En el caso de que estemos ante la comisión de un delito, según se trate del primer o el segundo tipo penal, estaremos ante un delito del art. 197 y ss o del art.401 del Código Penal, y ello, tiene como consecuencia, la aplicación de diferentes penas.

Análisis histórico y evolución de la usurpación de estado civil

Aunque podamos pensar que la suplantación de identidad es un fenómeno que solo ha tenido cabida en los últimos años, este suceso viene existiendo históricamente.

Ya en la mitología griega, podemos encontrar multitud de relatos mitológicos en los que la suplantación de identidad es la protagonista. Así lo cuenta Plauto en su obra "Anfitrión", en que Zeus se hizo pasar por Anfitrión adoptando su misma forma y aspecto para ordenar al Sol que no saliese durante tres días para permanecer una larga noche de amor junto a Alcmena (prometida de Anfitrión).

A lo largo de la historia, ha habido una evolución de la suplantación de identidad y son muchas las historias relacionadas con este ilícito. En la Edad Contemporánea, si nos centramos en el panorama español, podemos destacar la suplantación de identidad que protagonizó Gabriel de Espinosa en Ávila en el siglo XVI, un pastelero que se hizo pasar por el rey Sebastián I de Portugal, quien había desaparecido, aunque fue descubierto y juzgado y condenado ser "arrastrado y a muerte natural de horca y descuartizado, su cabeza puesta en un palo en el puesto más público de aquel lugar, siendo llevado con pregoneros por todas las calles públicas".

Pero el fenómeno de la suplantación de identidad, también se vio reflejado en muchas otras historias a nivel internacional, ya que tuvieron lugar todo un seguido de casos relacionados con este ilícito. Un buen ejemplo de ello, es el caso de Mary Baker (1791-1864), quien llegó en 1817 a Bristol, haciéndose pasar por una exótica princesa de Caraboo; o el caso de Anna Anderson (1896-1984, nacida Franziska Schanzkowska) que entre los años 1920 y 1923, se hizo pasar por la famosa Anastasia, hija menor del último zar del Imperio Ruso, Nicolás II, asesinada junto a su familia en julio de 1918, cuando fue objeto de muchos intentos de suplantación de identidad.

En los últimos años la usurpación de identidad también ha sido un ilícito presente en casos de gran polémica. Desde el caso de Marcos Castagno, un estudiante de ingeniería electrónica de Argentina, que en el año 2000 se hizo pasar por ganador de un premio de la Fundación Motorola y consiguió hacerse famoso y obtener una beca para irse a Japón, al caso del "pequeño Nicolás" o Francisco Nicolás Gómez Iglesias, quien fue acusado, de entre otros cargos, de usurpación de identidad tras haber fingido ser otra persona para infiltrarse en las altas esferas del poder político y económico español, llegando incluso a afirmar que trabajaba para el Cuerpo Nacional de Inteligencia (CNI).

Todos estos casos, son solo algunos de los acontecidos a lo largo de la historia, pero lo cierto, es que existe una gran multitud de casos en los que se juzga por haber cometido usurpación de identidad.

Aunque en el pasado la suplantación y usurpación de identidad se cometían sin la utilización de medios electrónicos, con el creciente desarrollo de las nuevas tecnologías y el acceso a Internet, la usurpación de estado civil tipificada en el Código Penal, ha ido evolucionando y cada vez es más común la comisión de este delito a través de la red, es decir, la usurpación de identidad en Internet.

Puesto que en Internet se encuentran datos de los usuarios como la cuenta bancaria, gustos, datos de usuarios conocidos… La usurpación de identidad sirve como instrumento para conseguir otro tipo de delitos como la estafa, el robo o la calumnia.

Acceder al perfil o cuenta de otro usuario usurpando su personalidad, puede conllevar graves consecuencias jurídicas ya que dicho acceso puede producirse de varias formas, cabiendo así la posibilidad de concurso con otros delitos como el delito de lesión de privacidad, considerado una forma de descubrimiento y revelación de secretos y viene contemplado en el art.197 del Código Penal; o también como el delito denominado hacking, que tras la reforma de 2015, está tipificado en el art.197 bis 1 del Código Penal, así como el delito de daños a redes, soportes o sistemas informáticos, también denominado cracking, que viene tipificado en el art.164 del Código Penal.

Por lo tanto, la combinación de delitos que pueden cometerse junto al delito de usurpación de identidad varían en función del tipo de acceso a las cuentas o perfiles del usurpado, así como de los datos a los que se acceda y el uso que se haga respecto de ellos, es decir, en función de la conducta típica del sujeto activo, el delito podrá subsumirse en uno u otro tipo penal.

3. Marco legal y novedades tras la reforma del Código Penal

Tal y como se venía explicando anteriormente, no existe una norma específica que regule la usurpación de identidad en internet, sino que esta conducta se encuadra a al delito de usurpación de estado civil regulado en el art.401 del Código Penal.

Debido al vacío legal frente a los ciberdelitos, la Fiscalía General del Estado, ha propuesto la tipificación del delito de usurpación de identidad en medios electrónicos para evitar que las conductas referentes a este delito queden impunes.

Desde la perspectiva internacional, debemos tener en cuenta que el alcance de los ciberdelitos preocupa a los gobiernos de todo el mundo y se han llevado a cabo una serie de convenios y acuerdos para velar por la seguridad en las redes.

De este modo, es importante destacar el Convenio de Cibercriminalidad de Budapest[12] de 2001, ratificado por España en 2010, que persigue castigar los ilícitos a sistemas informáticos, la

[12] Fue el primer tratado internacional que hizo frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales.

interceptación y propagación de virus, la producción y distribución de pornografía infantil así como los ataques contra la propiedad intelectual entre otros delitos informáticos.

También debemos destacar la Estrategia de Ciberseguridad Nacional[13] que aprobó el Gobierno en 2013 para dar respuesta al "desafío que supone la preservación del ciberespacio de los riesgos y amenazas que se ciernen sobre él".

El Código Penal de 1995 aunque no contiene expresamente una regulación de los ciberdelitos, sí que contiene tipos penales relacionados con la ciberdelincuencia que pueden dividirse en tres grandes grupos en relación con la usurpación de identidad en internet:

- Delito de usurpación de identidad para la comisión de delitos contra los propios sistemas informáticos:

Debemos encuadrar aquí el delito de daños y sabotaje informático del artículo 264 del Código Penal y el delito de descubrimiento y revelación de secretos del artículo 197 del Código Penal así como el Hacking, que viene regulado en el art.401 bis 1 del Código.

- Delito de usurpación de identidad en internet como medio para la comisión de otros delitos que atentan contra el patrimonio y el honor de las personas:

En este grupo encontramos todo tipo de ciberdelito servido como instrumento para la comisión de otro tipo penal como podría ser el delito de estafa informática regulada en el artículo 248 del Código Penal, delitos de abusos sexuales a menores recogidos en el artículo 183 ter del Código Penal y los delitos contra la propiedad industrial e intelectual regulados en el artículo 273 a 277 del Código Penal.

- Delito de usurpación de identidad en internet como medio para cometer delitos que requieren investigaciones complejas y conocimientos específicos

Dentro de este grupo encajan delitos como falsificaciones documentales en internet, que viene regulado en el artículo 390 y siguientes del Código Penal o el ciberbullying que aunque tampoco viene regulado específicamente en el Código Penal si que puede relacionarse con otros tipos penales.

Después de la reforma del Código Penal en 2015 debemos destacar una serie de aspectos en relación a los ciberdelitos, ya que aunque como se ha explicado anteriormente no existe una regulación específica del delito de usurpación de identidad en internet, si que se han endurecido las penas relacionadas con una serie de materias que están muy relacionados con este delito.

[13] La Estrategia de Ciberseguridad Nacional se divide en cinco capítulos : "El ciberespacio y su seguridad"; "Propósito y principios rectores de la ciberseguridad en España"; "Objetivos de la ciberseguridad"; "Líneas de acción de la ciberseguridad Nacional"; "La ciberseguridad en el Sistema de Seguridad Nacional".

En primer lugar, la reforma ha endurecido las penas por delitos contra la libertad sexual y la protección de menores. La Directiva 2011/93/UE[14] obliga a los estados miembros a endurecer las sanciones en esta materia, castigándose así, la producción, difusión o asistencia a espectáculos pornográficos en los que participen menores de edad, y se amplía la tipificación del child grooming (acciones emprendidas por adultos con el fin de abusar sexualmente de las víctimas), considerándose delito agravado la participación de menores de dieciséis años en este tipo de actos.

En segundo lugar, tras la reforma, se tipifica la revelación de secretos si se han conseguido imágenes con la aquiescencia de una persona, pero luego se divulgan contra su voluntad, lesionando gravemente la intimidad de la víctima[15].

Terceramente, se introdujo como delito la supresión o alteración de medidas de seguridad tecnológicas para proteger programas de software o ejecución de los mismos, sin autorización de los titulares de los derechos de propiedad intelectual.

Todo ello ha dado paso a una nueva regulación de los ciberdelitos, dando paso así a una mayor ciberseguridad. No obstante, es importante hacer referencia al hecho de que existen una serie de vacíos legales entorno a este tipo de delitos y ello se ve reflejado en la falta de regulación de muchos ellos como son la usurpación de identidad en internet.

4. Tipo penal

El art.401 del Código Penal establece que "El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años."

De este modo, encontramos el tipo penal en el que debemos encajar la usurpación de identidad en internet, en el delito de usurpación de estado civil, que tal y como establece el Código Penal, se castiga a aquellos sujetos que usurpen el estado civil de otros con una pena de prisión de seis meses a tres años.

Conducta típica

En el delito de usurpación de estado civil, el bien jurídico protegido es la fe pública, que se concreta en la confianza de la sociedad en una correcta identificación de las personas. Por lo tanto, la conducta que se sanciona en este tipo penal es la utilización de un falso nombre y la filiación a ese nombre de otra persona que existe realmente, independientemente de que esté viva o haya fallecido y no la mera utilización de un nombre ajeno.

[14] Esta Directiva lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y sustituye la Decisión marco 2004/68/JAI del Consejo.

[15] El art.197.7 CP tipifica este delito estableciendo una pena de prisión de tres meses a un año o multa de seis a doce meses en su tipo básico, que se impondrá en su mitad superior en cuanto concurran las circunstancias del tipo agravado.

Tal y como indica FARALDO CABANA, lo que se castiga es la suplantación de identidad de otra persona; si la persona cuyo estado civil se usurpa vive, puede constituirse en perjudicado por el delito a efectos de la responsabilidad civil, en su caso.

Ha sido motivo de debate el hecho de si es necesario que la conducta del sujeto activo tenga lugar en perjuicio del sujeto pasivo o para perjudicarle, a lo que la jurisprudencia ha dado su respuesta ya que la Sentencia de la Audiencia Provincial de Sevilla de 23 de mayo de 2000[16] absuelve en un supuesto en que el usurpador actúa con conocimiento y en beneficio del usurpado, por lo que podemos afirmar que la jurisprudencia ha fijado que la conducta típica del sujeto activo debe contener el elemento de actuar en perjuicio del usurpado.

Visto lo anterior, podemos concluir que para que tenga lugar la usurpación de identidad en internet debe existir una conducta del sujeto activo consistente en hacerse pasar por otra persona en internet, no siendo suficiente la utilización de un nombre o una fotografía[17], sino que debe ser suficiente el engaño para que pueda pensarse que el usurpador es el usurpado, y actuar en su perjuicio usando sus derechos y facultades, habiendo por lo tanto dolo directo en tales acciones.

Tipo subjetivo

El delito de usurpación de identidad requiere el dolo directo del sujeto activo, es decir, se trata de un tipo que requiere de la voluntad y conocimiento del usurpador. No cabe modalidad imprudente en para la concurrencia del tipo.

Aunque debemos hacer un pequeño inciso en el hecho de que en la jurisprudencia se ha aludido a un elemento subjetivo que no aparece expresamente en el tipo penal, esto es «el propósito de ejercitar derechos y acciones de la persona suplantada» tal y como viene diciendo el Tribunal Supremo en su sentencia de 26 de marzo de 1991[18], que absuelve a quien suplantó la identidad de su hermano para escapar de la justicia o en su sentencia de 20 de enero de 1993, por entender que hacerse pasar por otro en un negocio de compraventa no supone ejercer derechos y acciones de la persona suplantada.

Pena

La pena que establece el Código Penal para castigar la usurpación de estado civil es de seis meses a tres años de prisión.

Asímismo, el Código Penal prevé un tipo especial de usurpación, que castiga de manera más dura la comisión de este tipo penal y viene regulado en el art.402 del Código Penal, que señala que “El que ilegítimamente ejerciere actos propios de una autoridad o funcionario público

[16] STS (2ª) de 23 de Mayo de 2000, (RJ 945).
[17] La jurisprudencia considera que para que tenga lugar una verdadera usurpación de identidad, debe haber una usurpación de identidad digital, siendo insuficiente el mero uso de datos ajenos tales como el nombre de la víctima.
[18] STS (2ª) de 22 de Marzo de 1991, (RJ 1751).

atribuyéndose carácter oficial, será castigado con la pena de prisión de uno a tres años." Y otro castigado únicamente con pena de multa, como es el del artículo 403 del código, que señala que "El que sin estar autorizado usare pública e indebidamente uniforme, traje o insignia que le atribuyan carácter oficial será castigado con la pena de multa de uno a tres meses."

Visto lo anterior, podemos concluir que para que tenga lugar la usurpación de identidad en internet debe existir una conducta del sujeto activo consistente en hacerse pasar por otra persona en internet, no siendo suficiente la utilización de un nombre o una fotografía, sino que debe ser suficiente el engaño para que pueda pensarse que el usurpador es el usurpado, y actuar en su perjuicio usando sus derechos y facultades, habiendo por lo tanto dolo directo en tales acciones.

5. Tipologías y relaciones concursales

La usurpación de identidad en internet, tal y como se ha señalado, puede servir como instrumento para llevar a cabo otros delitos pero también puede ser un fin. A continuación se explican los ciberdelitos más relevantes relacionados con la usurpación de identidad, tanto aquellos que pueden considerarse una tipología de este delito como aquellos que van estrechamente unidos a éste, aunque no se trate del mismo y con los que puede castigarse conjuntamente mediante concurso de delitos.

Usurpación y suplantación en redes sociales

Uno de las tipologías más comunes de usurpación de identidad en Internet, tiene lugar en las redes sociales. Con el auge de las redes sociales tales como Instagram, Facebook o Twitter[19], que están al alcance de todos los usuarios que tienen acceso a dispositivos electrónicos, se ha incrementado gravemente el número de delitos de usurpación de identidad cometidos a través de estas redes sociales.

En concreto, la usurpación de identidad en las redes sociales supone hacerse pasar por otra persona en el perfil abierto de ésta en una red social, accediendo de forma ilícita al servicio del usuario en dicha red social.

La Sentencia de la Audiencia Provincial de Baleares de 12 de marzo de 2013[20] trata una denuncia de suplantación de identidad en Facebook y Badoo "utilizando los datos de la denunciante, vulnerando el derecho a la propia imagen del art. 18 CE, siendo dicha suplantación utilizada en la red como una actividad maliciosa."

Phishing y estafa informática

[19] El 98% de las personas que disponen de una conexión a Internet utilizan de forma regular una o más redes sociales.
[20] STS (2ª) de 12 de Marzo de 2013, (RJ 94).

Un delito relacionado con la usurpación de identidad en Internet es el phishing[21], que se considera una forma de suplantación consistente en el uso de un tipo de ingeniería social[22], caracterizado por adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o bien información privada sobre tarjetas de crédito o cualquier otro tipo de información bancaria detallada.

El origen de este delito, tiene lugar en los años noventa, y su operativa se centraba en el envío masivo de correos electrónicos fraudulentos a los clientes de entidades financieras (conocido como *smishing*, o incluso a través de llamadas telefónicas, el denominado *vishing*), para la obtención de datos y claves de usuario que les permitían acceder fraudulentamente a la cuenta de la víctima.

Se trata de un método utilizado, en la mayor parte de los casos, para cometer un delito de estafa u obtener información confidencial de forma fraudulenta a través de la obtención de contraseñas e información privilegiada. La técnica del *phishing* ha evolucionado hacia otras formas de comunicación online como las redes sociales, mediante la colocación de *posts* en Facebook o Twitter, entre otros, con promociones y beneficios a los que se accede a través de información personal y bancaria en las correspondientes webs clonadas.

Por otra parte, también existe una modalidad de obtención de datos y contraseñas del usuario a través de *malware*[23], la implantación de programas maliciosos con virus en el sistema informático desde el que la víctima maneja sus cuentas bancarias.

El *modus operandi* más común para la consecución de las claves de la cuenta bancaria en la práctica judicial es el denominado *pharming,* en que se simula la entidad bancaria copiando una página web de un banco y en los correos anzuelo[24] incluyen una URL en la que la víctima debe hacer click, y automáticamente, le dirige a la página web simulada en la que introduce sus datos y contraseñas, valiéndose de una excusa lo más verosímil posible.

El sujeto activo, esto es, el usurpador, recibe también el nombre de *pisher* y su conducta consiste en hacerse pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

Según RODRÍGUEZ CARO, todo comienza, por lo general, cuando un usuario de la banca on line recibe un correo que supuestamente procede de su banco, que tiene la finalidad de inducir al cliente para que clique en un enlace que le redirige a una web maliciosa mediante la que se

[21] El término phishing proviene de la unión de los siguientes vocablos en inglés: password, harvesting y fishing, con lo que se viene a hacer alusión a “cosecha y pesca de contraseñas”.
[22] Se trata de la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos.
[23] También denominado "malicious software”
[24] Correos electrónicos que aparentan ser de fuentes fiables, y cuyo objetivo es pescar los datos confidenciales de los usuarios.

suplanta la identidad del banco para obtener las claves de acceso del usuario engañado, sus datos bancarios, etc.

La Sentencia 834/2012 del Tribunal Supremo de 25 de octubre de 2012[25] trata un caso de phishing en el que "se reclama contra la sentencia que condenó a la acusada como autora de un delito de blanqueo de capitales cometido por imprudencia. Se trata una actuación fraudulenta que toma como punto de partida el envío masivo de mensajes de correo electrónico desde diversos sitios en la web, que tiene como destinatarios a usuarios de la banca informática -banca on line- a quienes se les redirecciona a una página web que es una réplica casi perfecta del original y en la que se les requiere, normalmente con el aviso amenazante de perder el depósito y la disponibilidad de las tarjetas de crédito, a que entreguen sus claves personales de acceso con el fin de verificar su operatividad. De forma gráfica se dice que el autor " pesca los datos protegidos" -de ahí la denominación phishing-, que permiten el libre acceso a las cuentas del particulares y, a partir de ahí, el desapoderamiento. No hay razón que justifique que la acusada sólo deba responder de la parte del lucro propio. Es cierto que en los delitos de receptación, la responsabilidad civil se señala en función del lucro experimentado por el receptador. Pero en este caso, no estamos ante una receptación, en la cual la intervención del reo es independiente del alcance del tipo principal. Aquí la acusada interviene en el blanqueo de todo el dinero que es sustraído a la víctima. Por ello debe responder civilmente del total sustraído."

El phishing o estafa informática[26] puede considerarse un delito estrechamente relacionado con la usurpación de identidad en la red, el cual viene regulado por el art. 248.2 del Código Penal, que castiga 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” con una pena de seis meses a tres años de prisión. Este delito puede ser castigado conjuntamente con el delito de usurpación de identidad a través de concurso medial.

Algunos autores[27] afirman que el *phishing* no encaja dentro del delito común de estafa ya que en ocasiones el engaño no es idóneo para causar error, o directamente no hay engaño al producirse una manipulación informática de la cual el usuario no es consciente[28]. A mi juicio, el *phishing* existe un engaño idóneo ya que hay una manipulación informática que induce claramente a error. Por ello, a mi parecer, existe una línia muy fina entre el delito denominado *phishing* y el delito de usurpación de identidad, puesto que aunque están estrechamente relacionados, en el *phishing* el engañado se limita a proporcionar los datos que dan acceso a su patrimonio, pero no realiza disposición patrimonial alguna, siendo necesario un acto de apoderamiento por parte del delincuente, materializado en el uso de los mencionados datos.

Delito de descubrimiento y revelación de secretos

[25] STS (2ª) de 25 de Octubre de 2012, (RJ 834).
[26] La postura clásica en torno al delito de estafa negaba que se pudiera engañar a una máquina. Vid. por todos ANTÓN ONECA, J., Las estafas y otros engaños, Seix, Barcelona, 1957, p. 10.
[27] QUINTERO OLIVARES, G., «Fraudes», cit., p. 99.
[28] FERNÁNDEZ TERUELO, J. G., Cibercrimen, cit., p. 43; del mismo autor, «Respuesta penal», cit., p. 233.

Otro tipo penal que va estrechamente ligado con la usurpación de identidad en la red, es el delito de descubrimiento y revelación de secretos contemplado en el art.197 del Código Penal, que establece que " 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" y en su apartado segundo hace referencia al uso de soportes informáticos estableciendo que "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".

En este sentido, debemos hacer referencia a que la comisión de un delito de usurpación de identidad, puede llevar aparejada la comisión de un delito de descubrimiento y revelación de secretos y, por ello, tiene cabida el concurso medial de estos delitos.

Haking

El *hacking* es el conjunto de técnicas a través de las que se accede a un sistema informático vulnerando las medidas de seguridad establecidas originariamente. Para que tenga lugar el *hacking,* deben existir una serie de elementos:

- **Acceso**: debe existir una intrusión, penetración o allanamiento.
- **Ilícito**: existe una carencia de autorización o justificación para ese acceso y ya fuere una carencia absoluta como si se excediere la que se posea.
- **Sistema informático**: debe entenderse en sentido amplio, es decir, comprensivo de equipo, elemento componente o redes de comunicación.

El *hacking* como tal, hace referencia a un conjunto de técnicas para introducirse en un sistema informático vulnerando las medidas de seguridad con independencia de la finalidad con la que se realice. Por ello, aunque la sociedad generalmente se refiere a esta técnica aludiendo al ilícito o "Black Hat Hacking"(*hacking* malo o dañino), también existe el "White Hat Hacking", que es aquel considerado "*hacking* bueno", que se utiliza para luchar contra el primero.

Esta conducta tiene como víctima a cualquier cibernauta que tenga información almacenada en la red o sistemas informáticos[29].

[29] STS (2ª) de 27 de Abril de 2015, (RJ 329).

El *hacking* que se tipifica en el Código Penal es el malo o dañino, que en 2010 se introdujo en el art. 197.3 del Código Penal y, tras la reforma de 2015, pasó a estar regulado en el art.197 bis 1 del Código, que castiga a quien cometa este delito con una pena de prisión de seis meses a dos años.

Igualmente, se trata de un delito estrechamente vinculado con el delito de usurpación de identidad, y aunque no se trate del mismo tipo penal, ambos pueden llevarse a cabo para la consecución de un mismo fin, por lo que cabe la posibilidad de que sean castigados mediante concurso medial de delitos.

Cracking

En el caso de que para la comisión del delito de usurpación de identidad, el usurpador haya dañado algún sistema informático o robado contraseñas, estará cometiendo además un delito de daños a redes, soportes o sistemas informáticos, recogido en el artículo 264.2 del Código Penal[30], que también se denomina *cracking*.

Podemos definir el *cracking* como la modificación del *software* con la intención de eliminar los métodos de protección de los que este disponga, ya sean protección de copias, versiones de prueba, números de serie, claves de *hardware*, verificación de fechas, verificación de CD o publicidad y *adware*.

Son muchas las causas enjuiciadas por la comisión del *cracking* de *software* aunque la mayoría han tenido que ver con la distribución de copias duplicadas en vez de con el proceso de quebrantar la protección. Los métodos más conocidos para producir la destrucción de los elementos lógicos son los virus[31], caballos de Troya[32], sniffers[33]...

Se trata de un delito contra el que se lucha a nivel mundial, de este modo, Estados Unidos, aprobó la Digital Millennium Copyright Act (DMCA) declaró a la modificación de *software*, así como a la distribución de información que habilita el *cracking* de software, ilegal. Aunque debemos hacer un inciso en que la ley ha sido apenas probada en el poder judicial de EE. UU. en casos de ingeniería inversa para único uso personal.

---

[30] Como refiere CREMADES GARCÍA, en la aplicación de este art. 264.2 CP, es necesario tener en cuenta para calificar la acción como delito, la utilidad de esos datos y el reflejo de ese menoscabo en la actividad de su titular, además del valor de esos propios datos.

[31] Se trata de programas informáticos diseñados para realizar dos funciones: replicarse de un sistema informático a otro y situarse en los ordenadores de forma que pueda destruir o modificar programas y ficheros de datos, interfiriendo los procesos normales del sistema operativo (vid. SNEYERS, Alfredo, El fraude y otros delitos informáticos, Tecnologías de Gerencia y Producción, S.A., Madrid, 1990, 101-105).

[32] Se denomina caballo de Troya (o troyano), a un programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, para de recabar información o controlar remotamente a la máquina anfitriona. Un troyano no es en sí un virus, aún cuando teóricamente pueda ser distribuido y funcionar como tal. La diferencia fundamental entre un troyano y un virus consiste en su finalidad.

[33] Programas rastreadores usados para penetrar en el disco duro de los ordenadores conectados a la red buscando cierto tipo de información.

A nivel europeo, la Unión Europea aprobó la Directiva de la Unión Europea sobre derecho de autor en mayo de 2001, haciendo la infracción de los derechos de autor de *software* ilegal en los estados miembros, una vez que la legislación nacional fuera promulgada en favor de la directiva.

Tal y como afirma MATA Y MARTÍN[34], lo principal de este tipo de comportamientos es que van dirigidos a atacar los elementos lógicos del sistema, es decir, al software en general y a los ficheros o archivos informáticos en los que se recogen datos, información o documentos electrónicos, cualquiera que sea su contenido concreto.

Por otra parte, la doctrina[35] reseña que el modus operandi concreto (borrado, formateado, virus) es indiferente.

En definitiva, el bien jurídico protegido con esta tipificación, es sin embargo es más amplio que el patrimonio ya que también se atenta contra la ciberseguridad o la seguridad jurídica en el ciberespacio. A mi parecer, estamos ante la comisión de un tipo delictivo pluriofensivo puesto que son varios los bienes jurídicos protegidos contra los que se atenta.

6.5. Ilícito civil

En aquellos casos en los que se crea un perfil falso y se utiliza información personal de la persona suplantada, como puede ser una fotografía, se está cometiendo un es un ilícito civil, de vulneración del derecho a la propia imagen de la Ley Orgánica 1/1982[36].

Por lo que aunque no se trate de un tipo penal tipificado en el Código Penal, estamos ante un ilícito civil.

8.Conclusiones

Tal y como se ha expuesto a lo largo del trabajo, los ciberdelitos o delitos cometidos en la red, son cada día más frecuentes en la actual realidad sociocultural, y ello supone un peligro frente a la ciberseguridad, ya que los delitos en la red evolucionan a un ritmo constante y mucho más rápido que la legislación en este ámbito.

Más concretamente, la usurpación de identidad en internet en sus diversas modalidades y los delitos que se derivan de ésta suponen un peligro para el bien jurídico protegido de la fe pública en la identidad de los ciudadanos, además de otros bienes jurídicos protegidos como el derecho al honor, a la intimidad personal y familiar o a la propia imagen, así como el patrimonio entre otroe, por lo que su tipificación en el Código Penal es de vital importancia.

---

[34] MATA Y MARTÍN, Ricardo, Delincuencia informática y Derecho penal, Edisofer, Madrid, 2001, p. 59.
[35] PIÑOL RODRÍGUEZ, José Ramón, Manual de Derecho Penal. Parte. Especial, 4ª Ed, Thomson Civitas, 2006, p. 293.
[36] Regula la protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

La comisión de los ciberdelitos suele concretarse en la comisión de tipos pluriofensivos puesto que se atenta contra varios bienes jurídicos protegidos, por lo que la lucha contra estos delitos es de vital importancia. Debido a la dificultad y sofisticación de estos delitos, que hacen que sea mucho más difícil su persecución, a mi juicio, es insuficiente la regulación existente en la actualidad sobre los mismos, puesto que a pesar de la última reforma del Código Penal, y de la normativa expuesta a lo largo del trabajo existente en referencia a estos tipos, no resulta adecuada puesto que no existe una ley específica que regule tales delitos.

Aunque si bien es cierto que la reforma del Código Penal de 2015 supuso un gran avance en cuanto a los ciberdelitos se refiere, en el ámbito de la usurpación de identidad en la red, todavía es necesario que exista una regulación específica puesto que actualmente la desprotección de la víctima frente a ciberataques es una realidad.

El hecho de que la jurisprudencia encaje el ciberdelito de la usurpación de identidad en el delito de usurpación de estado civil del art.401 del Código Penal, es sin duda, una manera de punir el crimen, aunque a mi parecer resultaría mucho más efectiva una regulación precisa del delito de usurpación de identidad en internet así como del resto de ciberdelitos en el Código Penal, expuestos a lo largo del trabajo, tales como el *phishing, hacking o cracking*, puesto que muchos de ellos quedan hoy en día impunes por no poder encajarse en un tipo penal concreto o no cumplir los requisitos para su concurrencia, quedando en muchos casos absueltos los delincuentes, tal y como sucede en otros países.

Aunque tal y como apunta SERRANO GÓMEZ[37], para la correcta comprensión de los delitos informáticos, hay que tener presente que el Código Penal da por sobreentendidos ciertos conceptos jurídicos que operan como elementos normativos, y que tienden a ser integrados por las definiciones previamente configuradas por la LOPDAT 15/1999, de 13 de diciembre, de protección de datos de carácter personal y su reglamento de desarrollo (aprobado por el RD 1720/2007, de 21 de diciembre) y dichos elementos funcionan como un puente entre la protección penal y la administrativa, es necesario recalcar que aunque existe una variedad de normativa en relación con este tipo delictivo, como ya se venía diciendo, no existe ninguna norma concreta que los regule.

En definitiva, aunque la actual normativa castiga la comisión de los ciberdelitos en su gran mayoría, todavía queda un largo camino por recorrer para la regulación de los mismos puesto que la actual legislación en este ámbito da lugar a una inseguridad jurídica constante incapaz de solventar el problema en su totalidad.

[37] SERRANO GÓMEZ, Alfonso, Derecho penal. Parte especial, 8ª Ed, Dykinson, Madrid, 2003, p. 267.

Bibliografía

UNITED STATES of America, Appellee, v. Robert Tappan MORRIS, Defendant–Appellant. No. 774, Docket 90–1336. | Argued Dec. 4, 1990. | Decided March 7, 1991.

ANTÓN ONECA, J., Las estafas y otros engaños, Seix, Barcelona, 1957, p. 10.

QUINTERO OLIVARES, G., «Fraudes», cit., p. 99.

FERNÁNDEZ TERUELO, J. G., Cibercrimen, cit., p. 43; del mismo autor, «Respuesta penal», cit., p. 233.

MATA Y MARTÍN, Ricardo, Delincuencia informática y Derecho penal, Edisofer, Madrid, 2001, p. 59.

PIÑOL RODRÍGUEZ, José Ramón, Manual de Derecho Penal. Parte. Especial, 4ª Ed, Thomson Civitas, 2006, p. 293.

SERRANO GÓMEZ, Alfonso, Derecho penal. Parte especial, 8ª Ed, Dykinson, Madrid, 2003, p. 267.

GÓMEZ TOMILLO, Manuel, Comentarios prácticos al Código Penal, 1º Ed, Aranzadi, 2015, p.155.

GÓNZALEZ CUSSAC, José, Comentarios a la reforma del Código Penal de 2015, 2ª Ed, Tirant lo Blanch, 2015.

QUINTERO OLIVARES, Gonzalo, La reforma del Código penal de 2015, 1ª Ed, Aranzadi, 2016.