Suplantación de identidad en internet: necesidad de reforma del Código Penal

[Phishing in internet]

■ ■ ■

MERCEDES DE PRADA RODRÍGUEZ

Profa. Dra. Derecho Procesal del CUV y de la EPJ (UCM)
Directora del Área de Derecho y Empresa del CUV
mprada@villanueva.edu

JESÚS SANTOS ALONSO

Ex Fiscal de la Audiencia Nacional
Director del Departamento de Penal de Baker & McKenzie
Prof. de Derecho Penal del CUV (UCM)
jsantos@villanueva.edu

Fecha de recepción: 5 junio de 2013.
Fecha de aceptación: 1 de julio de 2013.

Resumen

La mayor incidencia de las manifestaciones criminales cometidas directamente contra los sistemas informáticos o que se sirven de ellos para atentar contra los más variados bienes jurídicos, deben tener una adecuada protección penal. Si bien la última redacción ofrecida por la Ley Orgánica 5/2010, de 22 de junio, supuso un avance al objeto de tipificar conductas relacionadas con este tipo de delitos, nuestro Código Penal

sigue sin ofrecer una penalización clara y directa. En este trabajo, se propone la inclusión de un nuevo tipo penal sobre la suplantación de identidad, real o ficticia, en internet.

Palabras clave

Delitos informáticos, nuevas formas de criminalidad, internet, nuevas tecnologías, identidad digital, suplantación de identidad.

Abstract

The increased number of criminal acts committed directly in relation to information systems or that use such systems to commit an offence against a wide range of legal rights and assets must be adequately punished by criminal legislation. Although the recent wording of Constitutional Act 5/2010, dated 22 June, represents a step forward in defining the conduct related to this type of offence, our Criminal Code still fails to provide for clear and direct punishment. This paper proposes the definition of a new type of criminal offence for phishing on the Internet.

Keywords

Computer crime, new forms of criminality, the Internet, new technologies, digital identity, phishing.

I. INTRODUCCIÓN

El progresivo aumento de las investigaciones criminales vinculadas a la utilización de las nuevas tecnologías, especialmente, internet y la generalización del uso de estos nuevos instrumentos, ha determinado la aparición de nuevas formas de criminalidad y favorecido también dinámicas y mecanismos, hasta ahora no conocidos, en la comisión de conductas ilícitas de carácter más tradicional. La mayor incidencia de las manifestaciones criminales cometidas directamente contra los sistemas informáticos o que se sirven de ellos para atentar contra los más variados bienes jurídicos, –algunos de carácter personalísimo, como el honor y la intimidad, otros de carácter patrimonial e incluso algunos de naturaleza supraindividual, como la propia seguridad de Estado–, deben establecer una decidida actuación del legislador para dar una adecuada protección penal a estas nuevas realidades delictivas.

La Fiscalía especial en materia de delitos informáticos ha puesto de manifiesto en las últimas tres Memorias publicadas, relativas a los años 2010, 2011 y 2012, la falta de datos estadísticos fiables en relación con el número de delitos que se cometen a través de Internet. Y es que, normalmente, no se trata de un delito propio *per se* cuyos procedimientos sean cuantificables, sino que se tratan de numerosos delitos cometidos mediante la utilización de internet como instrumento.

Podemos clasificar los delitos informáticos en dos grupos: a) «stricto sensu», como la intrusión en equipos ajenos «hacking»; la revelación de contenidos albergados en programas y archivos informáticos, los fraudes «phising» y «pharming»[1]; la falsificación informática y los daños a los elementos lógicos del sistema «cracking» y b) delitos clásicos que encuentran en la red su medio comisivo, así, las amenazas, las vejaciones, el ciberterrorismo, los delitos contra la libertad sexual, etc[2]. Con la peculiaridad de que la utilización de la red los convierte en más dañinos y de muy difícil persecución penal, tanto en lo que se refiere a la facilidad para cometerlos, a la ocultación de la autoría, a su difusión y a la dificultad de determinación de la competencia desde el punto de vista territorial[3].

A nuestro juicio, más que de delitos informáticos, a día de hoy y según está redactado el Código Penal, debería hablarse de *delitos cometidos por medios informáticos*[4].

Y una posible clasificación de los «delitos cometidos por medios informáticos» sería:

a) Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TICs.
b) Delitos en los que la actividad criminal se beneficia de las ventajas que ofrecen las TICs para la ejecución del delito.
c) Delitos en los que la actividad criminal, además de beneficiarse para su ejecución de las ventajas que ofrecen las TICs, entraña especial complejidad en su investigación que demanda conocimientos específicos en la materia.

En todo caso, es manifiesta la falta de regulación de los delitos cometidos a través de la red, destacando la incapacidad del Código Penal actual y de la regulación española para adaptarse a la realidad social de nuestro tiempo. Prácticamente cualquier conducta delictiva puede ejecutarse mediante estos medios, si bien, podemos destacar aquéllos que por su propia naturaleza se adaptan de forma inmediata al perfil de delitos informáticos como, por ejemplo: los delitos de amenazas, coacciones, delitos contra la intimidad, contra la libertad, injurias y calumnias, el acceso inconsentido a un sistema informático, la interceptación ilícita de comunicaciones, las interferencias en el sistema, el abuso de dispositivos, el fraude informático, exhibicionismo y provocación sexual, delitos relativos a la prostitución, y corrupción de menores, descubrimiento y revelación de secretos, estafa, defraudaciones de fluido

1. Nos ha parecido muy interesante el artículo de Rey Huidobro, L. F., «La estafa informática: relevancia penal del phising y el pharming», *La Ley Penal*, nº 101, Sección Estudios, *La Ley* 1851/2013.
2. Urbano Castrillo, E. de., «Los delitos informáticos tras la reforma del CP de 2001», *Revista Aranzadi Doctrinal* núm. 9/2011, Aranzadi, Pamplona, 2011.
3. En este sentido, *vid*., Velasco San Martín, C., *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet,* Tirant lo Blanch, Valencia, 2012.
4. En algunos países se habla de ciberdelitos o cibercrimen (computer crime). El Consejo de Europa utilizó el término «delitos relacionados con las Tecnologías de la Información» y se definen como «delitos que contemplan cualquier conducta penal en una investigación en la cual las autoridades investigadoras tienen que obtener acceso a la información que es procesada o transmitida en sistemas de cómputo o sistemas electrónicos de procesamiento de datos».

eléctrico y análogas, daños, delitos relativos a la propiedad intelectual e industrial, delitos relativos al mercado y los consumidores, receptación, conductas afines, falsedades documentales y apología del racismo, terrorismo y xenofobia, entre otros.

El escenario actual nos muestra que, junto a las conductas para las que el legislador ha previsto una precisa tipificación y protegido específicamente, como son la seguridad de los datos, programas y/o sistemas informáticos, existen otras conductas ilícitas que, afectando a los más diversos bienes jurídicos, se planifican y ejecutan aprovechando las ventajas que ofrecen las nuevas tecnologías de la sociedad de la información y que presentan, por tanto, numerosas singularidades y dificultades a los efectos de investigación, enjuiciamiento y calificación jurídica[5]. Si bien la última redacción ofrecida por la Ley Orgánica 5/2010, de 22 de junio, *por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Pena,* supuso un avance al objeto de tipificar conductas relacionadas con este tipo de delitos, nuestro Código Penal sigue sin ofrecer una penalización clara y directa de aquellos delitos cuyo encaje, por su naturaleza, resulta altamente complicado[6].

Por otra parte, es muy amplio el espectro de los agentes implicados en el ámbito de las redes sociales: el proveedor de servicios, los usuarios, los creadores de aplicaciones, los anunciantes, etc. Si, además, tenemos en cuenta la cantidad de personas en España con acceso a Internet (alrededor de 21 millones) y el aumento de la comisión de estas modalidades delictivas, podemos concluir que es evidente la necesidad de dar protección legal a las víctimas de estos delitos y a su privacidad. Por ello, las dificultades surgen no sólo en la tipificación sino también en la determinación de la participación en este tipo de delitos y, especialmente, en la adopción de medidas cautelares claras y contundentes, como pueda ser: el cierre de páginas webs o la responsabilidad civil de aquellos portales a través de los cuales se cometan delitos de este tipo[7].

II. LA SUPLANTACIÓN DE IDENTIDAD, REAL O FICTICIA

De entre todas las conductas señaladas que pueden cometerse a través de la red y que no tienen el debido reproche penal, queremos centrar nuestro trabajo en la *suplantación de identidad, real o ficticia*.

---

5. Como afirma Velasco San Martín, C., *La jurisdicción y competencia…, op. cit.,* pág. 37, por la gran importancia «del tema a nivel mundial y en vista de la necesidad de poder construir y fomentar una Sociedad de la Información integradora con la participación, asociación y cooperación entre los gobiernos, el sector privado, la sociedad civil y las organizaciones internacionales, el 21 de diciembre de 2001, la Asamblea General de Naciones Unidas adoptó la Resolución (A/RES/56/183) que refrenda la organización de la Cumbre Mundial sobre la Sociedad de la Información (WSIS)».

6. Flores Prada, I., *Criminalidad informática, (Aspectos sustantivos y procesales),* Tirant lo Blanch, Valencia, 2012, pág. 37, afirma que el concepto de «criminalidad o delincuencia informática» es un «concepto dogmático amplio que contiene al de delitos informáticos y éste, a su vez, engloba al de delitos en internet. Los delitos informáticos definen la criminalidad informática tipificada en el CP, mientras que los delitos en internet señalan aquéllos delitos informáticos cometidos a través de la red». Por ello «no todo lo que se suele denominar criminalidad informática encuentra encaje en un tipo penal, como tampoco los llamados delitos informáticos que se cometan a través de internet».

7. Flores Prada, I., *Criminalidad informática…, op. cit.,* pp. 299 y ss.

Como es sabido, la suplantación de identidad genera un perjuicio, en muchas ocasiones, irreparable para aquellos que lo sufren y no tiene encaje por analogía en ninguno de los tipos penales que contempla el actual Código Penal. Por ello, debe acudirse, no sin problemas de fundamentación, a la analogía con el delito de la usurpación del estado civil, de revelación de datos personales o el delito de coacciones, en su modalidad agravada por afectar al derecho al empleo de medios de comunicación.

Las redes sociales hoy ofrecen la posibilidad de comunicarse con diferentes partes del mundo, investigar sobre diversos hechos que suceden e incluso hacerse eco a tiempo real de la actualidad informativa; pero también permiten hacer juicios de valor, opinar y desacreditar a otras personas, con el agravante añadido de que la inmediatez que caracteriza a internet hace que las consecuencias de dichas opiniones se magnifiquen y desplieguen sus efectos a mayor escala de lo que lo harían a través de otros medios tradicionales de comunicación[8].

La capacidad de movilización social que permite internet es innegable y, de hecho, es uno de los mayores beneficios que ofrecen las redes sociales, pero es cierto que el anonimato que permiten los perfiles de las redes sociales genera que numerosas opiniones vulneradoras de los derechos al honor y a la propia imagen queden impunes. Y, a mayor abundamiento, permite que un gran número de personas se unan a dichas manifestaciones sin posibilidad de represaliar dichos actos en aquellos casos en los que sea legalmente justificable[9]. Por todo ello, se impone la necesidad de adaptación flexible a este entorno en constante evolución, creando elementos de control de la información junto a políticas legislativas transparentes de información y el respeto absoluto a la normativa sobre protección de datos[10].

Son claras las cifras que revelan que gran número de los perfiles creados en las redes sociales son falsos y no se corresponden con una persona real. Así, aproximadamente 83 millones de los perfiles creados en la red social Facebook son falsos o duplicados, dividiéndose dichos perfiles en (i) perfiles duplicados –una cuenta secundaria que un usuario utiliza conjuntamente con su cuenta principal– y que responde al 4,8% de los perfiles creados en Facebook, (ii) perfiles mal clasificados –que corresponde con aquellos perfiles que han sido creados por usuarios ya existentes con un fin laboral, promocional o cuentas creadas a mascotas y otras entidades que no corresponden a seres humanos– y que responde al 2,4% del total de los perfiles y (iii) perfiles indeseados –cuentas que se han creado con el propósito de violar los términos del contrato con Facebook, como spam– y que se corresponden con el 1,5% del total de las cuentas de Facebook[11].

---

8. Ortiz López, P., «Redes sociales: Funcionamiento y tratamiento personal», *Derecho y redes sociales* (Coord. Rallo Lombarte y Martínez Martínez), Civitas, Pamplona, 2010, pág. 23 y ss., plantea cuáles son los desafíos que, desde un punto de vista jurídico, se establecen en el tratamiento de la información personal. Diferenciando en tres grandes grupos de redes sociales de comunicación, especializadas y profesionales.

9. *Vid*., *Estudio sobre la privacidad de datos personales, Instituto Nacional de Tecnologías de la Comunicación y la Agencia Española de Protección de Datos*, pp. 45-51. *http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/est_inteco_redesso_022009.pdf.*

10. Ortiz López, P., «Redes sociales: Funcionamiento y…, *op. cit*., pág. 35.

11. Información recogida el 22 de abril de 2013 de *http://www.nydailynews.com/news/national/fake-book-facebook-reveals-83-million-fake-users-site-article-1.1127486.*

Estos datos revelan la posibilidad que existe de que un usuario, con varias cuentas de correo electrónico, pueda crear varios perfiles falsos en diferentes redes sociales, empleando todos ellos al mismo tiempo. Esta multiplicidad de perfiles en internet tiene como principal consecuencia la ausencia de control sobre quién es quién en la red, y puede tener consecuencias muy negativas para los intereses de los ciudadanos. A modo de ejemplo, podemos citar aquellos supuestos en los que se crean perfiles falsos correspondientes a personas reales que no quieren aparecer en las redes sociales. Esto permite a sus creadores hacer manifestaciones de opiniones que no son reales, que no corresponden a la persona cuya identidad se ha visto suplantada y que pueden acarrear nefastas consecuencias para la víctima.

Del mismo modo, debemos hacer referencia a aquellos casos en los que una persona ve continuamente vulnerados su derecho al honor en internet porque se le acosa en la red por otro usuario. Si bien esta conducta ya es penalmente sancionable y, por supuesto, moralmente reprochable, el efecto multiplicador que tendría la misma en el caso de que la persona que acosa en la red a otro lo haga mediante la utilización de varios perfiles a la vez sería infinitamente superior y mucho más dañino[12].

La capacidad que ofrece la red para magnificar las opiniones mostradas en las redes sociales debe poder controlarse de algún modo, ya que si no podría darse el supuesto de que mediante la creación ilimitada de cuentas de correo electrónico y sus correspondientes perfiles en las redes sociales, una persona podría verter opiniones injuriosas en la red sobre otra, multiplicando los efectos de su opinión individual creando un supuesto clamor popular contra algo o alguien que no es tal sino, exclusivamente, la opinión de un único usuario.

Podemos concluir indicando que la suplantación de identidad, real o falsa, en internet es un comportamiento que debe tener su correspondiente sanción penal y ello debido a los efectos multiplicadores que tiene la red, que puede convertir un simple comentario, con o sin efectos penales, en una avalancha de opiniones que pueden causar grandes perjuicios a la víctima de esos comentarios.

III. LA REGULACIÓN DE LOS DELITOS COMETIDOS POR MEDIOS INFORMÁTICOS EN DERECHO COMPARADO

Nos parece necesario, en este punto, detenernos en la normativa existente en otros países por su importancia y actualidad; pueden ser un punto de referencia para una posible reforma de nuestro ordenamiento.

Así, en la regulación penal de la creciente criminalidad en internet llevada a cabo por los diferentes Estados que nos rodean, podemos observar tres técnicas legislativas diferenciadas: «a) el recurso a Leyes penales especiales; b) la tipificación de nuevas figuras delictivas en el Código Penal, y c) la elaboración de normas internacionales»[13].

12. Ley 25/2007, de 18 de octubre, *de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*.

13. Seguimos en este punto a BARRIO ANDRÉS, M., «Los delitos cometidos en internet. Marco comparado, internacional y derecho español tras la reforma penal de 2010», *La Ley Penal,* nº 86, octubre de 2011, *La Ley* 16989/2011.

En función de esta clasificación, podemos destacar las diferentes opciones legislativas que han sido adoptadas por diversos países:

a) *Leyes penales especiales*.

Los ordenamientos de países como Francia, Gran Bretaña, Alemania, Holanda, Estados Unidos, Chile o Venezuela, han optado por elaborar leyes penales especiales para abordar este fenómeno. En Europa, destacan: Alemania con su «Ley contra la Criminalidad Económica» de 1986 pero cuenta también con artículos en su código punitivo que contienen delitos informáticos; Francia que cuenta con una «Ley relativa al fraude informático» de 1988 y Reino Unido que promulgó, en 1991, la *Computer Misuse Act* a raíz de un grave caso de hacking. Este Acta sobre el mal uso de los sistemas de cómputo es la legislación aplicable a los delitos cometidos a través de sistemas de cómputo e internet y que afecta a ciudadanos e instituciones ubicados en Inglaterra, Gales; Escocia y el Norte de Irlanda[14]. En América, Estados Unidos adoptó, en 1994, el Acta Federal de Abuso Computacional, Computer Fraud and Abuse Act, (18 USC Sec. 1030), que modificó el Acta de Fraude y Abuso Computacional de 1986 y que ha sufrido una serie de reformas, destacando la más reciente de 2001 con la entrada en vigor de la controvertida legislación conocida como US Patriot Act[15]. En Iberoamérica, debemos destacar la Ley chilena contra los delitos informáticos de 1993, es pionera en los países de ese entorno.

b) *La tipificación de nuevas figuras delictivas en el Código Penal.*

En segundo lugar, la tipificación de nuevos delitos en el Código Penal ha sido la otra técnica empleada para hacer frente a este desafío. Han optado por esta regulación: Portugal, Austria, Italia, España, Argentina y México, como principales exponentes.

c) *La elaboración de normas internacionales.*

En tercer y último lugar, la dimensión transnacional también ha obligado a adoptar soluciones a nivel internacional.

- En el ámbito de las Naciones Unidas, debemos citar el *Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos*, de 1977.
- En el ámbito del Consejo de Europa, destaca el Convenio sobre Cibercrimen, aprobado en Budapest en 2001 y vigente desde julio de 2004.
- Y, por último, a nivel comunitario, el objetivo de armonización del Derecho Penal en la Unión Europea ha realizado un giro más decidido a partir de la firma del Tratado de Lisboa en 2007, que opta por la Directiva en vez de por la Decisión Marco para conseguir una mayor armonización de disposiciones relativas a las infracciones con dimensión transfronteriza de especial gravedad, entre las que se encuentra la delincuencia informática.

14. *Vid*., *http://www.legislation.gov.uk/ukpga.*
15. *Vid*., *http://wwwepic.org/privacy/terrorism/hr3162.html*.

Analizando las diferentes jurisdicciones y normas promulgadas al efecto, debemos destacar que el *Convenio sobre la Ciberdelincuencia* del Consejo de Europa, de 23 de noviembre de 2001, en Budapest, ya puso de manifiesto la creciente «necesidad de aplicar, con carácter prioritario, una política penal común con el objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular, mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional»; así como la necesidad de «prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal y como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable»[16].

España ratificó el citado Convenio en 2010, pero aún no se han llevado a cabo todas las reformas necesarias para la adecuación de nuestro Código Penal a su contenido para defender los derechos de los ciudadanos frente a las injerencias de relevancia penal que puedan cometerse contra sus derechos mediante el uso de la Red.

Esta necesidad sí ha sido abordada por otros países, que han tipificado específicamente la comisión del delito de suplantación de identidad por internet. En concreto y, a modo de ejemplo, citaremos brevemente los siguientes países:

A) En Reino Unido: tanto la «Malicious Communications Act» de 1998, como el artículo 127 de la «Communications Act» de 2003, sancionan penalmente las conductas relativas a las comunicaciones electrónicas indecentes, ofensivas, obscenas o falsas, así como aquellas que pueden ser amenazantes, realizadas con el objetivo de causar perjuicio o ansiedad a otra persona. Esto es, se sanciona la utilización de las redes sociales con el fin de perjudicar a otros ciudadanos, tipificando aquellos supuestos que no tendrían cabida en cualquier otro precepto del Código Penal. Además, también se regula mediante otros preceptos de su ordenamiento penal aquellas conductas que pueden ser consideradas como amenazas de lesiones o daños, acoso o coacción a otra persona y aquellas que suponen la ruptura de una orden de alejamiento.

B) En Francia se ha incluido en el Código Penal, por la LOI, nº 2011-267 de 14 de marzo de 2011, el artículo 226-4-1, que tipifica la suplantación de identidad en la red. Según su tenor literal: «El hecho de usurpar la identidad de un tercero o de hacer uso de uno o varios datos de cualquier naturaleza que permitan ser identificado con vistas a perturbar su tranquilidad o la de otros; o que suponga un atentado a su honor o a su reputación, está castigado con la pena de un año de prisión y multa de 15.000 €. Esta infracción se castiga con las mismas penas en caso de ser cometida en una red de comunicación al público en línea». Asimismo se establecen las medidas cautelares que serán de aplicación en caso de comisión del citado delito.

16. *http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf.*

C) En Canadá se ha incluido en el contenido del artículo 403 del Código Penal la suplantación de identidad. En él se dispone que: «Comete un delito aquel que fraudulentamente suplante a otra persona, viva o fallecida (a) con la intención de obtener algún beneficio para sí o para otro, (b) con la intención de obtener la propiedad de algo o un interés en alguna propiedad, (c) con el interés de causar un perjuicio a la persona suplantada u otra persona o (d) para evitar la detención, la imputación en un procedimiento o con la intención obstruir el curso de la Justicia. Para los intereses del artículo anterior, suplantación de una persona incluye pretender ser esa persona o utilizar la información y los datos identitarios de la persona –ya sea por sí mismo, ya sea mediante la utilización de información en posesión de otra persona– como si fuesen suyos».

Como podemos observar la amplitud de la redacción ofrecida en este precepto y que no haga mención a la suplantación *online*, permite que pueda ser empleado tanto para sancionar aquellos casos de suplantación física como cualquier posible suplantación en la red.

D) En Estados Unidos, son varios los Estados que ya han introducido el delito de suplantación en Internet del tipo penal de suplantación de identidad online. A modo de ejemplo, debemos hacer mención a los ordenamientos de California y de Texas.

Así, el artículo 528.5 del Código Penal de California dispone que: «(a) No obstante cualquier otra disposición de esta ley, cualquier persona que a sabiendas y sin su consentimiento suplante de un modo creíble a otra persona real en la red, en un sitio web o cualquier otro medio electrónico con la intención causar un perjuicio, intimidar, amenazar o defraudar a otra persona, es culpable de un delito castigado de acuerdo con el apartado «d» del presente artículo. (b) Para los intereses de esta sección, una suplantación será creíble si la otra persona puede creer razonablemente, o creyó razonablemente, que el acusado era o es la persona cuya identidad suplanta.

(c) Para los intereses de esta sección, «medios electrónicos» incluye la apertura de una cuenta de e-mail o una cuenta o perfil en una red social online en nombre de otra persona. (d) La violación de lo dispuesto en el apartado (a) se castigará con una multa no superior a mil dólares (1.000 $) o mediante pena de prisión en una cárcel del condado no superior a un año, o ambas penas».

Del mismo modo, el Estado de Texas ha incluido el artículo 33.07 en su Código Penal sancionando la suplantación en internet como sigue: «Suplantación online: (a) Una persona comete este delito cuando, sin consentimiento y con la intención de causar un perjuicio, defraudar, intimidar o amenazar a cualquier persona, utiliza el nombre o identidad de otra persona para: (1) Crear una página web en una red social comercial o cualquier otro sitio web, o (2) Enviar uno o más mensajes a través de una red social comercial o cualquier otro sitio web, correo electrónico o programa de mensajería online. (b) Una persona comete este delito si la persona envía un e-mail, mensaje emergente, mensaje de texto o comunicación similar que haga referencia a un nombre, dominio, teléfono o cualquier otro dato identificando información que pertenezca a otra persona: (1) Sin su consentimiento; (2) Con la intención de hacer creer razonablemente al receptor de la comunicación que la persona suplantada autorizó o realizó la transmisión, y (3) Con la intención de causar un daño o defraudar a cualquier persona.

(c) El delito cometido en el apartado (a) es un delito de tercer grado. El delito del apartado (b) es una falta de tipo A, pero será un delito de tercer grado si el autor lo comete con la intención de solicitar una respuesta por parte del personal de emergencias».

E) En **América Latina** son varios los países que bien han introducido nuevos tipos penales en sus Códigos Penales para luchar contra la suplantación de identidad cometida a través de Internet, bien han promulgado Leyes penales especiales que ofrecen una respuesta a las necesidades de la sociedad en relación con la creciente inseguridad jurídica derivada de internet.

En una rápida aproximación a la Memoria de 2012 de la Fiscalía General del Estado podemos apuntar que: en Perú, existe un proyecto legislativo para incluir en la norma penal sustantiva un nuevo tipo penal que sancione el delito de robo de identidad virtual tal y como sigue: «El que se apropie indebidamente, cree, utilice, adopte una identidad ajena obtenida a través del internet, será reprimido como mínimo de cuatro años de pena privativa de libertad hasta un máximo de seis años de privación de la libertad».

Por otra parte, en Argentina, se ha desarrollado el proyecto para incorporar como artículo 139 TER de su Código Penal la suplantación de identidad. La reforma dispone que «Será reprimido con pena de prisión de 6 meses a 3 años el que adoptare, creare, apropiare o utilizare, a través de Internet, cualquier sistema informático, o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca. La pena será de 2 a 6 años de prisión cuando el autor asumiera la identidad de un menor de edad o tuviese contacto con una persona menor de dieciséis años, aunque mediare su consentimiento o sea funcionario público en ejercicio de sus funciones».

Como podemos observar, son ya bastantes países de nuestro entorno los que han modificado sus legislaciones penales para dar respuesta al problema creciente de la suplantación de identidad en internet.

IV. ESTADO DE LA CUESTIÓN EN EL ORDENAMIENTO ESPAÑOL

Centrados ya en nuestro ordenamiento, la última Memoria de la Fiscalía General del Estado da cuenta del progresivo y llamativo incremento de las investigaciones relacionadas con delitos contra la libertad, intimidad y el honor de las personas y, concretamente, amenazas, coacciones o injurias cometidas a través de la red. La generalización del uso de internet por parte de los ciudadanos y la utilización cada vez más frecuente de las redes sociales está íntimamente vinculada a ese incremento[17]. Para el agresor, servirse de la red de redes con esta finalidad no sólo facilita la

17. En España los distintos delitos informáticos, se encuentran en una estela de artículos ubicados en distintos capítulos en función de los bienes jurídicos protegidos pero sin relación ni sistemática, así: arts. 186-189 CP, pornografía infantil; art. 197.2 CP, espionaje informático; art. 211 CP, Injurias y calumnias a través de la red; art. 238.5 CP, Robo inutilizando sistemas de guarda criptográfica; art. 248.2, estafa informática; art. 256, ubicación abusiva de equipos terminales de telecomunicación; art. 264.2 CP, sabotaje o daños informáticos; art. 270 CP propiedad intelectual; arts. 273-275 CP, contra la propiedad industrial; art .278.1 CP, secretos de empresa; art.28 CP, uso ilegal de equipos, programas y servicios informáticos; art.

ejecución del delito, que puede llevarse a efecto desde el propio domicilio, sino que, también, cuando lo que se pretende es perjudicar la fama o el honor y la reputación tanto de personas físicas como de personas jurídicas, le garantiza ese efecto al potenciar la difusión del mensaje ofensivo e intimidatorio.

En el momento actual, la cuenta de correo electrónico que nos permite operar en internet, el perfil que editamos en las redes sociales, chats, foros o mensajería instantánea, etc., integran nuestra *identidad digital*, entendida como el conjunto de datos que nos permiten comunicarnos en internet, intervenir en redes sociales y operar en páginas web[18]. En definitiva, son los datos que identifican o hacen identificable a una persona en sus intervenciones *online*. Las actuaciones consistentes en la creación de perfiles en redes sociales que deliberadamente simulen pertenecer a otras personas, normalmente de proyección pública y la posterior utilización del indicado perfil para realizar manifestaciones o expresiones de variada índole, dan lugar a diversas valoraciones jurídicas en atención al bien jurídico lesionado y al alcance y contenido de la actividad desarrollada por el suplantador pero, a excepción de aquellos supuestos en los que esta suplantación genera un perjuicio al honor o la consideración pública del suplantado, generalmente no tienen encaje en los tipos penales que ofrece nuestra regulación, por lo que la conducta resulta, en muchas ocasiones, atípica[19].

El problema fundamental se encuentra en el encaje de la suplantación electrónica de identidad en los tipos penales que prevé el Código Penal Español[20].

Son varias las opiniones vertidas al respecto. Por una parte se ha tratado de encajarlo en el *delito de usurpación de estado civil*, tipificado en el artículo 401 del Código Penal[21]. Sin embargo, y a tenor de la definición generalizada que ofrece la jurisprudencia de «estado civil», las dificultades se agravan: así no se consideraría estado civil, por ejemplo, la utilización del nombre y fotografía *online* de otra persona[22].

---

402 CP, usurpación de funciones públicas por e-correo; arts. 417-418 CP y 423 CP, infidelidad en la custodia de documentos y violación de secretos); art. 560.1 CP, ataques a líneas o instalaciones de telecomunicación o correspondencia postal y arts. 598 y 603 CP, descubrimiento y revelación de secretos relativos a la Defensa Nacional.

18. Cfr. Alamillo Domingo, I., «La identidad electrónica en la red» en *Derecho y redes sociales* (Coord. Rallo Lombarte y Martínez Martínez), Civitas, Pamplona, pp. 37 y ss.

19. La European Network and Information Security Agency (ENISA) publicó «*Security issues and Recommendations for on line social networks*», 2007.

20. La LO 5/2010, de 22 de junio *por la que se reforma la LO 10/1995, que aprobó el vigente Código Penal*, señala en su Preámbulo: a) la necesidad de cumplir con previas obligaciones internacionales contraídas por España –lo cual es visible en la introducción de la responsabilidad penal directa de las personas jurídicas, en el reforzamiento de la lucha contra la corrupción y en el tratamiento de la criminalidad organizada, como temas más relevantes–; y b) lo que llama «el surgimiento de nuevas cuestiones que han de ser abordadas», fruto de «la cambiante realidad social».

21. Cfr. Díaz López, A., *El delito de usurpación del estado civil, op. cit*., pp. 221 y ss. El autor realiza un análisis sobre la adapatbilidad del art. 401 CP con las nuevas formas de criminalidad contemporáneas.

22. Por su parte, la jurisprudencia, ha declarado en la SAP de Segovia de 25 de marzo de 2010 (JUR 2010, 76707) lo que sigue: «en las sentencias de 5 de mayo de 1887, 7 de octubre de 1882, 21 de diciembre de 1893 y 16 de abril de 1901, se dice que es condición precisa, para la concurrencia de la infracción, que la suplantación se lleve a cabo para usar de los derechos y acciones de la persona sustituida; la de 23 de febrero de 1935, indica que se ha de suplantar la personalidad de otro, arrogándosela así como su profesión; la de 8 de marzo de 1947, estimó que, comete usurpación, quien, sin necesidad de una suplantación total, ejerce los actos propios de otra persona con una cierta continuidad y trascendencia, sin que dichos

Por otra parte, también se entiende que el estado civil no está legalmente definido, sino que se compone de una serie de hechos, actos y relaciones importantes y trascendentes en la vida de las personas, que forma su historia jurídica[23]. Y, por lo tanto, que la información que se recopila en nuestro ordenador de manera constante, rigurosa y ordenada sin contar con nuestro consentimiento pero que expresa gran parte de nuestra personalidad y, por ello, nuestro estado civil. En consecuencia, la suplantación en internet de nuestro perfil *online* estaría cubierta por el delito de usurpación de estado civil. Sin embargo, se puede llegar a considerar que lo anterior supondría una interpretación extensiva del Derecho penal, que afectaría a lo dispuesto en el artículo 4 CC, por lo que no tendría encaje la conducta cometida en el artículo 401 del Código Penal por faltarle el presupuesto fáctico del delito.

El segundo de los delitos en los que se ha tratado de encajar la suplantación de personalidad, real o ficticia, en internet, ha sido el *delito de falsedad en documento privado*, considerando que la creación de un perfil falso en una red social cumpliría lo dispuesto en el artículo 390.1.1º del Código Penal –falsificación de documento mercantil en sus elementos esenciales–, primer requisito legalmente exigido; no obstante, para que pudieran considerarse las manifestaciones realizadas con dicho perfil como falsificación en documento privado, debería existir un dolo específico de perjudicar a la persona a la que se suplanta, lo cual en muchas ocasiones es muy complicado y difícil de acreditar.

Otro de los delitos a través de los que se puede configurar la suplantación de identidad *online* son los *delitos de revelación de datos personales*, así como el *delito de coacciones* pero, en ambos casos, no ha sido acogido con éxito entre la mayor parte de nuestros autores.

En cualquier caso, las anteriores construcciones parecen, a nuestro juicio excesivamente teóricas y, en ningún caso, darían respuesta a la creciente necesidad de crear un nuevo tipo penal que ponga coto a la conducta de suplantación de identidad, real o ficticia, en la red.

La Fiscalía General del Estado, por medio de las Memorias Anuales que publica al final de cada año judicial[24], ya ha hecho patente esta necesidad. Así, en la Memoria

---

actos le correspondan; la de 27 de septiembre de 1958, después de subrayar que, usurpación, gramaticalmente, equivale a «arrogarse la dignidad, empleo u oficio de otros y usar de ellos como si fueran propios», añade que, la mentada infracción, equivale a sustituir la personalidad ajena suficientemente conocida a fin de aprovecharse de sus derechos con el natural perjuicio que, esa suplantación, implica; la de 4 de abril de 1960, entiende que no hubo usurpación del estado civil de un hermano cuando se asumió e invocó el nombre de éste tan sólo para la obtención de un pasaporte, y ello porque no se trató de privación total de la personalidad de otro ni de sustitución del mismo en todos sus derechos; por último, la sentencia de 3 de junio de 1966 se ocupó de un problema de coautoría».

Asimismo, ya dejó claro nuestro Alto Tribunal en su STS de 15 de junio de 2009 (JUR 2009, 6642) que «usurpar el estado civil de otro lleva siempre consigo el uso del nombre y apellidos de ese otro, pero evidentemente requiere algo más, sin que sea bastante la continuidad o la repetición en el tiempo de ese uso indebido para integrar la mencionada usurpación».

23. *Vid.*, RODRÍGUEZ FERNÁNDEZ, P., «Suplantación electrónica de identidad. Posible respuesta jurídica penal», *Diario La Ley*, nº 7906, de 20 de julio de 2012, *La Ley* 7719/2012.

24. *http://www.fiscal.es/cs/Satellite?c=Page&cid=1242052134611&pagename=PFiscal%2FPage%2FFGE_memorias&selAnio=2012.*

del año 2010, la Fiscal de Sala Delegada en materia de Delitos Informáticos recogió la preocupación por la falta de un tipo penal que ofrezca una solución al problema planteado. En la citada Memoria se afirma que: «Además de las dificultades mencionadas, ha de tenerse en consideración –especialmente en el delito de usurpación o robo de identidad– el hecho de la ausencia de una figura penal concreta donde radicar la tipificación del hecho. Cabría considerarlo como una modalidad del delito de usurpación del estado civil, de poder acreditarse un uso continuado en el tiempo, lo que no aparece en la realidad criminal informática; o como un delito contra la intimidad en cuanto a captación, acceso y utilización de datos personales que se hallen en cualquier tipo de soporte y registro; si bien esta solución se enfrenta al problema del bien jurídico protegido y al especial propósito de revelación de secretos de otro, así como a la aprehensión del verdadero objeto del delito –el apoderamiento de datos que, por sí, definen o identifican a una persona–, que no llega a coincidir con el de dato reservado de carácter personal. […] Por ello, y así se han dictado instrucciones a las unidades policiales, se considera más práctico y viable la consideración de los supuestos de usurpación o robo de identidad como actos delitos de falsedades documentales, cuando tienen su reflejo en el empleo de las identidades usurpadas en relaciones contractuales».

En cualquier caso y pese al «parche» que supone la utilización de dichos tipos penales, concluyó la Fiscalía afirmando que «cabe analizar que este tipo de delitos ha aumentado de manera significativa y conviene ir adaptando la legislación con la finalidad de ir atajando las diferentes modalidades delictivas»[25].

En la Memoria del año 2011 se afirma que, en el contexto actual, es necesario sumar a los delitos contra la intimidad y contra la libertad, los delitos de usurpación de identidad. Y señala que «Esta figura, muy cercana en significación antijurídica a la usurpación de estado civil, carece de *nomen* jurídico propio, debiendo ser reconducida –por vía de análisis de la prueba– a los delitos cercanos de revelación de datos personales (art. 197.1º o 2º) y al de coacciones (art. 172.2), en su modalidad agravada por afectar al derecho al empleo de medios de comunicación, de los que el perjudicado muchas veces se ve privado por la usurpación de su identidad digital por el atacante […]».

Además se pone de manifiesto que revisten una importancia preocupante los fenómenos de coacciones y amenazas, asociados a la revelación de secretos personales porque «estas modalidades afectan igualmente a diversos bienes jurídicos personales (intimidad, libertad, honor, integridad moral); y son frecuentemente cometidos por ex parejas y menores, en sus ámbitos de relaciones personales».

V. CONCLUSIONES

El progreso tecnológico posee aspectos positivos y negativos. Es indudable que las comunicaciones, la seguridad y el acceso a la información han experimentado

25. Velasco Núñez, E., *Delitos cometidos a través de Internet: cuestiones procesales*, La Ley, Madrid, 2010, pp. 325 y ss., sostiene la necesidad de adecuar la protección jurídica con nuevas cautelas e instrumentos procesales. Las nuevas tecnologías aplicadas a la delincuencia determinan cuatro características fundamentales en estos delitos: la masividad, la perdurabilidad, la mutabilidad y la necesidad de traducción. Características «impensables en la delincuencia convencional clásica».

avances positivos gracias a la mejora tecnológica. Sin embargo, también ha traído consigo nuevas amenazas para la sociedad. Una de ellas es el aumento de la delincuencia cometida a través de la red. El Derecho debe dar respuesta a los nuevos comportamientos de la sociedad[26]. Se ha hecho patente la necesidad de un tipo penal concreto que persiga una nueva conducta que debe considerarse como típica: la usurpación de identidad de personas en la red. La legislación penal existente no ofrece una respuesta lo suficientemente clara para este comportamiento.

Es opinión generalizada por parte de los Fiscales que existe, en la actualidad, la necesidad de tipificar esta conducta[27]. A este respecto, se ha puesto de manifiesto una sugerencia para introducir un tipo sobre la suplantación de identidad en internet realizada por el Fiscal Jefe de Albacete, Delegado de Criminalidad Informática en la provincia. Esta propuesta considera que debe tipificarse el que una persona se haga pasar por otra de forma creíble con el fin de intimidar, amenazar o defraudar. Hasta ahora, se castigaba por el contenido injurioso o amenazante de la información que se vertía en la red. La conducta que se pretende que se persiga es diferente a la del delito de amenazas o acceso ilícito a información reservada. Lo que se propone es castigar el hecho de tomar la identidad en la red de otra persona para cometer un delito, que de manera independiente ya tiene cobertura típica[28].

La jurisprudencia se ha pronunciado poco al respecto, por lo que no existe mecanismo alguno que esclarezca cómo obrar en actos de suplantación de identidad y el daño de imagen y reputación que puede causar en los afectados a través de Internet. Aisladamente, la Audiencia Provincial de Segovia, en la SAP de 25 de marzo de 2010 (JUR 2010, 76707), ha castigado a dos jóvenes por crear un perfil falso de una compañera de instituto, de manera muy real, con datos verdaderos y fotos, con el fin de humillarla y aislarla del resto. El tipo en el que incardina esta conducta la Audiencia es en el de usurpación de estado civil (art. 401 Código Penal). Literalmente dice la sentencia que se trata de *«un ilícito cometido mediante el uso de Internet. Es evidente que se trata de un* ***ámbito en constante evolución y en el que en ocasiones***

26. Afirma Barrio Andrés, M, «Los delitos cometidos en internet…», *op. cit.*, p. 3, «(y no a la inversa), lo cual conlleva como una de sus funciones la de canalizar, por cauces adecuados, la nueva realidad social, económica y cultural en que se traducen los avances de Internet».

27. La Fiscal de Sala, Coordinadora en materia de Criminalidad Informática, incluyó entre las «Sugerencias, Propuestas y Reflexiones» de la Memoria correspondiente al año 2012, la necesidad de incluir un tipo penal concreto para este supuesto de hecho. Afirmando que: «Como ya se ha indicado, son diversos los Fiscales que hacen patente su preocupación ante los comportamientos consistentes en la usurpación de identidad de otra persona en la red y, en general, a través de los medios electrónicos y la falta de tipificación penal específica de estas conductas, al margen de la que puedan atraer, en atención a su contendido (sic.) infamante o injurioso o, en su caso, como consecuencia del acceso ilícito a secretos o informaciones de carácter reservado».

28. En tal sentido, se sugiere como posible redacción del tipo penal la siguiente: «De la suplantación de identidad en internet». «El que sin consentimiento y de forma creíble se haga pasar por otra persona real o ficticia a través de un sitio Web o por otros medios electrónicos con el fin de ofender, intimidar, amenazar o defraudar al mismo o a un tercero». «A los efectos del párrafo anterior, una suplantación es creíble si cualquiera podría creer razonablemente, o creyó, que el sujeto podía ser o es la persona que aparentaba». «La expresión «medios electrónicos» comprende la creación de sitios web, la apertura de cuentas de correo electrónico, y la apertura de una cuenta o perfil en redes sociales a nombre de otra persona, real o ficticia. Las penas señaladas se impondrán sin perjuicio de las procedentes por los hechos en que consista la ofensa, amenaza, intimidación o fraude».

puede ser difícil para la legislación penal seguir el acelerado avance tecnológico, lo que puede dar idea de una cierta desprotección de los derechos*, sobre todo aquellos relacionados con la intimidad, con la propia imagen o con los derechos de propiedad intelectual, cuando se atenta contra los mismos por medio de los instrumentos tecnológicos de la red».*

Por tanto, siguiendo tanto el criterio de los tribunales como de miembros del Ministerio Fiscal que están en continuo contacto con los problemas y demandas de la sociedad, deben comenzarse los trámites legislativos para amoldar nuestro ordenamiento jurídico a la nueva realidad social, económica y cultural, así como a los ordenamientos jurídicos de los países de nuestro entorno.