Estudios de Deusto

Revista de Derecho Público

Vol. 72/1 enero-junio 2024

DOI: https://doi.org/10.18543/ed7212024

ESTUDIOS

SUPLANTACIÓN DE IDENTIDAD DIGITAL: HACIA UNA NECESARIA TUTELA PENAL

Digital identity theft: towards a necessary criminal protection

Gemma Martínez Galindo

Prof. Contratada Doctora Derecho Penal

Universidad Internacional de La Rioja (UNIR), España

https://orcid.org/0000-0003-1679-7299

https://doi.org/10.18543/ed.3105

Fecha de recepción:25.07.2023

Fecha de aprobación: 03.03.2024

Fecha de publicación en línea: junio 2024

SUPLANTACIÓN DE IDENTIDAD DIGITAL: HACIA UNA NECESARIA TUTELA PENAL

Digital identity theft: towards a necessary criminal protection

Gemma Martínez Galindo
Prof. Contratada Doctora Derecho Penal
Universidad Internacional de La Rioja (UNIR), España
https://orcid.org/0000-0003-1679-7299

https://doi.org/10.18543/ed.3105

Fecha de recepción:25.07.2023
Fecha de aprobación: 03.03.2024
Fecha de publicación en línea: junio 2024

Resumen

La identidad digital es una parte de nuestra intimidad que está continuamente en riesgo ante los avances comunicativos que se producen en el entorno de las nuevas tecnologías, ya que puede ser fácilmente aprovechada por los ciberdelincuentes para llevar a cabo conductas delictivas (y, así, procurarse el anonimato) con finalidades de todo tipo, ya sean económicas, sexuales, vengativas o, simplemente, por diversión. El Código penal español no sanciona el mero hecho de suplantar la identidad de alguien, sino los comportamientos que se llevan a cabo a posteriori. Resulta, por ello, prioritario que se conciba un nuevo tipo penal para castigar este ataque tan grave a lo más personal e íntimo que tenemos: quiénes somos frente a los demás.

Palabras clave

Identidad digital; suplantación online; intimidad; usurpación de estado civil; reforma legislativa.

Abstract

Digital identity is a part of our privacy that is continuously at risk due to the communicative advances that occur in the environment of new technologies, since it can be easily used by cybercriminals to carry out criminal behavior (and, thus, procure anonymity) or for all kinds of purposes, be they financial, sexual, revenge or simply for fun. The Spanish Penal Code does not penalize the mere fact of supplanting someone's identity, but behaviors that are carried out after the fact. It is, therefore, a priority that a new criminal offense be conceived to penalize this serious attack on what is most personal and intimate that we have: who we are in front of others.

Keywords

Digital identity; online impersonation; privacy; usurpation of civil status; legislative reform.

Sumario: I. Introducción. II. La mera suplantación de identidad como conducta punible. III. El bien jurídico de nueva generación: la identidad digital como extensión del derecho a la intimidad. IV. Estado actual de la cuestión: la imposibilidad de sanción penal. V. Necesidad de homogeneidad de la tutela penal. VI. Lentitud del legislador versus criterios de política criminal. VII. Conclusiones. VIII. Referencias Bibliográficas.

I. INTRODUCCIÓN

Desde hace años, con la explosión de internet y esencialmente de los medios de comunicación y socialización cibernéticos, el empleo de las redes sociales (en España, casi 30 millones de personas poseen perfil en redes sociales, en el que incluyen datos como su nombre, fotografías y otro tipo de información personal) y en general con el uso de los sistemas de información y de la comunicación, se ha incrementado el riesgo de que se causen daños en bienes personalísimos, como son la reputación online, el honor, la intimidad o libertad de las personas, o incluso, su patrimonio cibernético, entre otros derechos. En muchas ocasiones, los ataques producidos constituyen una mera victimización, y los más dañinos (aunque no los más numerosos) son los que afectan a los bienes jurídicos más íntimos y personales, que constituye la denominada ciberdelincuencia social. En este ámbito, los avances tecnológicos facilitan que se desarrollen nuevas conductas que, en ocasiones, tienen difícil encaje dentro de los tipos penales previstos en la legislación, lo que –por mera aplicación del principio de legalidad– deja importantes lagunas de impunidad.

Se producen, así, continuamente, con el avance de las nuevas tecnologías y el empleo de redes sociales por parte de la ciudadanía nuevos escenarios a los que la legislación debe enfrentarse. Prueba de ello han sido las numerosas modificaciones que ha sufrido el Código Penal en materia cibernética desde la ratificación por España el 20 de mayo de 2010 del Convenio sobre Ciberdelincuencia de Budapest del Consejo de Europa de 23 de noviembre de 2001[1], y por las nuevas necesidades que se iban detectando, que han motivado la incorporación de tipos penales específicos[2]. Y más adelante –por qué

[1] Instrumento de Ratificación del Convenio publicado en el BOE de 17 de septiembre de 2010.

[2] Entre las diferentes reformas que se han ido aprobando para incorporar delitos informáticos, debemos destacar la operada por la Ley Orgánica 5/2010, de 22 de junio, que vino a cumplimentar la Decisión Marco 2005/222 sobre ataques contra sistemas de información, incorporando las siguientes conductas: el delito de daños, en que se introdujo el

art. 264 del CP, que sancionaba las conductas que se refieren a hacer inaccesibles o deteriorar datos o programas informáticos y que tienen objeto obstaculizar el funcionamiento de un sistema informático; los delitos contra la intimidad (197 del CP): se sancionó como novedad el acceso sin autorización a un sistema informático o a datos o programas informáticos, en el apartado 3, el denominado hacking blanco, el acceso a sistemas de información sin autorización y con independencia de que se produzca algún tipo de daño; y en la estafa se introdujo en el art. 248.2 del CP el apartado c) para incorporar la utilización de tarjetas ajenas causando un perjuicio a su titular. La reforma operada por la Ley Orgánica 1/2015, de 30 de marzo introdujo, entre otras, las siguientes conductas: en los delitos contra la intimidad, se solventaron algunos problemas por falta de tipicidad de conductas, suponiendo la reforma la transposición de la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información y la interceptación de datos electrónicos cuando no se trata de una comunicación personal (arts. 197 a 201), produciéndose una separación nítida entre los supuestos de revelación de datos que afectan directamente a la intimidad personal, y el acceso a otros datos o informaciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal, sancionándose muchas conductas nuevas; se tipificó la interceptación de transmisiones entre sistemas (es decir, automáticas, no personales) y la facilitación o la producción de programas informáticos o equipos específicamente diseñados o adaptados para la comisión de estos delitos; en el delito de daños se modificó el precepto 2 del art. 264 que reflejaba los daños por la obstaculización o interrupción del funcionamiento de un sistema informático ajeno, y se introdujeron nuevas conductas a través de las que pudieran cometerse los daños informáticos (art. 264 bis, ter, quáter del CP); en los delitos contra la libertad e indemnidad sexual, se introdujeron nuevas formas de comisión de delitos para proteger a los menores frente a los abusos cometidos a través de Internet u otros medios de telecomunicación, debido a la facilidad de acceso y el anonimato que proporcionan, con los arts. 183 ter y quáter del Código Penal, y se añadió un apartado al art. 189.5 para sancionar a quien acceda, a sabiendas, a pornografía infantil por medio de las tecnologías de la información y la comunicación, en la conciencia de que las nuevas tecnologías constituyen una vía principal de acceso a los soportes de la pornografía; en el ámbito de los delitos contra la propiedad intelectual se plantearon mejoras en cuanto a la regulación para lograr un cierto equilibrio entre esa protección de la propiedad intelectual y la que también deriva del legítimo uso de las nuevas tecnologías de la información y comunicación, lo que supuso una modificación del art. 270 introduciendo el castigo a quien facilite el acceso a través de los sistemas de información de obras protegidas por estos derechos con ánimo de obtener un beneficio económico; y en el ámbito de los delitos contra los derechos fundamentales y libertades públicas, se añadió el art. 510 para incorporar el denominado el delito de odio que puede cometerse a través de cualquier medio, incluso tecnológico, incluyendo, en ese caso, como pena, la retirada de contenidos de la red. A su vez, la Ley Orgánica 2/2015, de 30 de marzo, introdujo conductas relacionadas con el terrorismo online, como el autoadoctrinamiento a través de internet, en el art. 575, o el enaltecimiento del terrorismo en el art. 578. También la Ley Orgánica 1/2019, de 20 de febrero, trasponiendo Directivas de la Unión Europea en el ámbito económico, modificó el art. 284 relativo al mercado y los consumidores para sancionar la conducta por la que se comunican *fake news* de una empresa que puedan modificar su cotización y alterar el mercado. La Ley Orgánica 8/2021, de 4 de junio introdujo conductas para proteger a los menores en internet (arts. 143 bis, 156 ter, 189 bis ó 361 bis). A su vez, la Ley Orgánica 14/2022, de 22 de diciembre, de transposición de directivas europeas y otras disposiciones para la adaptación de la legisla-

no– podrán surgir nuevos tipos penales para sancionar las conductas del programador, incluso, que está detrás de una inteligencia artificial para responder del comportamiento de la máquina contra otras personas[3], o para sancionar de alguna manera los delitos cometidos en el metaverso o realidad virtual o paralela, sobre lo que ya se está debatiendo[4].

Existen nuevas formas de delinquir y el Derecho Penal ha tenido que adaptarse a estas transformaciones para hacer frente al crimen y dar respuestas efectivas, a la altura de los retos que plantea esta era hiperconectada. Podríamos decir que se ha producido una celeridad en los avances tecnológicos versus lentitud del Legislador.

Un ejemplo de esta lentitud legislativa es en materia de suplantación de identidad digital: hacerse pasar por otra persona en cualquier sistema de la información, robarle su identidad, para utilizarla como si le perteneciera[5]. Este comportamiento lleva produciéndose más de diez años en nuestra

---

ción penal al ordenamiento de la Unión Europea, y reforma de los delitos contra la integridad moral, desórdenes públicos y contrabando de armas de doble uso, que modificó de forma amplia, el delito de estafa por medios electrónicos para incorporar, conforme la Directiva 2019/713, de 17 de abril, el fraude y de la falsificación de los medios de pago distintos del efectivo, alejándose de la sistemática clásica de nuestro Código Penal, que atiende prioritariamente a los diferentes bienes jurídicos tutelados o puestos en peligro, tales como el patrimonio, la seguridad del tráfico o la fe pública, y no al concreto modo de comisión. Y, finalmente, la Ley Orgánica 10/2022, de 7 de septiembre, modificó también algunos artículos relativos a la intimidad (art. 197.7) y menores (art.183).

[3] A este respecto debemos diferenciar el *machine learning*, que consiste en que un programador dota a los ordenadores, mediante distintos algoritmos, de la capacidad de identificar patrones en datos masivos para elaborar predicciones, y en cuyo caso es mucho más sencillo atribuir al programador las correspondientes responsabilidades a modo de autor mediato; del *deep learning*, que es el sistema al que estamos asistiendo este último año, consiste en inteligencia artificial, en la que el tecnólogo entrena a la computadora para que aprenda por cuenta propia reconociendo pautas mediante el uso de muchas capas de procesamiento y permitiendo rectificar la programación errónea, en cuyo caso, es más complicado pensar en que el hombre de atrás tenga responsabilidad penal por las acciones llevadas a cabo por una computadora que ha sido autosuficiente para crear una conducta. De interés, vid. Elisa Simó Soler, "Retos jurídicos derivados de la Inteligencia Artificial Generativa", *Indret: Revista para el Análisis del Derecho*, n.º 2 (2023).

[4] Javier López Gutiérrez, "Delitos en el metaverso: hacia un nuevo horizonte legislativo", *Economist & Jurist*, vol. 30, n.º 262 (2022): 16-23; Alfonso Trallero Masó/Eva Tomás Román, "Metaverso y Derecho Penal", *La ley penal: revista de derecho penal, procesal y penitenciario*, n.º 158 (2022): en línea; y Antonio Serrano Acitores, "Metaverso y derecho" (Madrid: Tecnos, 2023, 2 ed.).

[5] Claudio Cilli, "Identity Theft: A New Frontier for Hackers and Cybercrime". *Information Systems Control Journal*, vol. 6, (2005): 1, lo define como "el uso de información sobre una persona obtenida desde internet con el propósito de identificarse a uno mismo como tal persona para llevar a cabo acciones ilegales".

sociedad, esencialmente desde el gran avance comunicativo que supusieron las redes sociales y el smartphone y con un incremento alarmante[6], siendo España uno de los países europeos con mayor tasa de suplantación de identidad online. Sobre él ha llamado la atención, por la falta de punición concreta en nuestro país, tanto la Fiscalía especial de Criminalidad Informática, que desde 2012[7] viene reclamando un tipo penal concreto, como la doctrina penal[8]. Es el denominado *spoofing* desde un punto de vista criminológico, consistente en una técnica habitualmente utilizada por los cibercriminales, que supone la suplantación de la identidad de una persona física o jurídica

[6] Según los datos que figuran en el Sistema Estadístico de Criminalidad del Ministerio de interior (https://estadisticasdecriminalidad.ses.mir.es), el total de hechos conocidos como suplantaciones de identidad en 2022 (último año que consta publicado a la fecha de este trabajo), identificados como usurpación de identidad, fue de 12.509 frente a las 1.850 de 2011.

[7] En la Memoria de la Fiscalía General del Estado del año 2020, pp. 1291 a 1293, se dedica un capítulo íntegro a motivar la necesidad de la incorporación de un artículo específico de suplantación de identidad digital. En él se recoge la que hizo este órgano propuesta al Congreso de los Diputados como capítulo independiente en el Título XVIII dedicado a las Falsedades, con la siguiente redacción: "El que, en perjuicio de otro, suplantare la identidad de una persona física realmente existente, utilizando sus datos identificativos a través de Internet, medio electrónico o sistema informático en línea de tal modo que genere error sobre la intervención en esos medios de la persona suplantada, será castigado con la pena de seis meses a dos años de prisión. A los efectos de este artículo se entenderá por datos identificativos tanto los correspondientes a la identidad personal oficial como cualesquiera otros que el afectado utilice habitualmente y por los que sea públicamente conocido". Esto se vuelve a reiterar en la última Memoria de la Fiscalía General de Estado, de 2022 publicada hasta la fecha de este trabajo, que establece en su página 1.073 que, dentro de los delitos de falsedad, "tanto por número de incoaciones, que ascienden a 5650, como por su incremento porcentual respecto del año anterior, de un 35%, debe resaltarse el delito de usurpación de estado civil, el cual tiene relación con el incremento de conductas de suplantación de identidad con datos obtenidos de forma ilegítima mediante la utilización de medios relacionados con las nuevas tecnologías, sobre todo como medio para la comisión de otros ilícitos penales, generalmente de carácter patrimonial", insistiendo en la página 1147 en la necesidad de "su incorporación como delito en el código penal español".

[8] Ricardo Mata y Martín. "El robo de identidad: ¿una figura necesaria?". VV.AA. *Robo de identidad y protección de datos* (Madrid: Aranzadi, 2010): 199-220; María Pilar Rodríguez Fernández, "Suplantación electrónica de identidad: posible respuesta jurídica penal", *Diario La Ley*, n.º 7906, (2012): en línea; Mercedes De Prada Rodríguez/Jesús Santos Alonso, "Suplantación de identidad en internet: necesidad de reforma del Código Penal", *Anu*ario jurídico Villanueva, n.º 7, (2013): 215-230; Vicente Magro Servet, "La tipificación penal de la suplantación de identidad en el uso de las redes sociales", *Diario La Ley*, n.º 9005 (2017): en línea; y Mariana N. Solari Merlo, "Suplantación de identidad digital: ¿necesidad de criminalización?", *Cuadernos de política criminal*, n.º 136, (2022): 125-164.

Estudios de Deusto
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 72/1, enero-junio 2024, págs. 199-228
https://doi.org/10.18543/ed.3105 • http://www.revista-estudios.deusto.es/

con distintas finalidades y para la realización de infracciones de muy diverso tipo. Como ya mantenía Fernando Miró Llinares en 2012 es la "expresión concreta y tecnológicamente avanzada del género de conductas que tratan de configurar el *identity theft* o robo de identidad", aunque este autor lo diferencia en el sentido de que se habla de *identity theft* cuando el uso de la identificación personal de otro ya tiene desde el inicio una finalidad que se presupone delictiva[9], lo que no siempre es así.

A pesar de que todas estas conductas son reales y se producen diariamente en el ciberespacio, y cada vez con más intensidad, en España existe un vacío legal porque al no estar tipificado en el Código Penal de manera autónoma este comportamiento, cuando se produce la mera conducta de suplantar la identidad de otro con cualquier finalidad posterior –delictiva o no–, los Tribunales deben tratar de encajarla en otras figuras ya existentes en función del comportamiento que lleve a cabo el ciberdelincuente con esa identidad suplantada, es decir, a posteriori, pero no por el mero hecho de la suplantación[10].

Se plantea así una cuestión: ¿es necesaria realmente una modificación legislativa del artículo 401 del Código Penal a fin de que se incluya, expresamente, la conducta de suplantación de identidad como un comportamiento punible con carácter independiente a la sanción que se puede producir por la comisión de otros delitos con el uso de esa identidad suplantada, ajenos al mero hecho de su mero empleo? Y si la respuesta de la tutela penal es positiva, ¿por qué el legislador no la ha introducido en ninguna de las 22 reformas del Código penal que se han dictado en nuestro país desde la ratificación del mencionado Convenio sobre Ciberdelincuencia de Budapest a pesar de haber sido reclamada desde hace años la introducción de un concreto precepto sancionador?

Este es el estado de la cuestión que voy a exponer en las siguientes páginas, en las que analizaré cuáles son las motivaciones más habituales de los ciberdelincuentes para suplantar la identidad de una persona y afectar a este bien jurídico que es la privacidad digital, y cómo sancionan los Tribunales los hechos cometidos con la identidad suplantada a través de los tipos penales existentes, determinando si se condena en la actualidad por el delito de usurpación de identidad del art. 401 del Código Penal o si la conducta aparece integrada dentro de otros delitos ajenos al hecho de suplantar la identidad de alguien. Por último, trataré de identificar los motivos por los que el Legislador no le está dando la debida importancia a esta situación y haré una

[9] Fernando Miró Llinares, *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio* (Madrid: Marcial Pons, 2012): 79.

[10] La Sentencia de la Audiencia Provincial de Madrid 260/2020, de 9 de junio entendió que la creación falsa de una cuenta en una red social en Internet a nombre de otra persona real era atípica por apenas haber estado en funcionamiento unas horas.

propuesta de *lege ferenda*, sumándome al criterio de Fiscalía, que ha vuelto a reiterar en la Memoria de 2022 su propuesta de modificar el Código Penal para introducir un tipo delictivo específico para sancionar esta conducta.

II. LA MERA SUPLANTACIÓN DE IDENTIDAD COMO CONDUCTA PUNIBLE

Cada vez es más frecuente en España y a nivel internacional la compraventa de datos personales en plataformas ocultas y la *dark web*, cuya obtención se lleva a cabo a través de diversas técnicas de ataques informáticos a servidores de organismos públicos y privados que, aparentemente no parecen tener consecuencias graves pero que, en el fondo, suponen una filtración de información confidencial de los ciudadanos, cuyos efectos pueden ser gravísimos no solo por su afección a la intimidad de las personas sino también por sus consecuencias económicas e incluso por el riesgo que pueden generar para la seguridad de instituciones públicas o del propio Estado. Tanto la Policía Nacional en España, como Europol e Interpol desarticula de forma cada vez más habitual organizaciones criminales y perfectamente organizadas que tienen como negocio la oferta y venta online de esos datos obtenidos ilícitamente: desde credenciales de acceso a sistemas online, fotocopias y datos del DNI, dirección, domicilio, número de la Seguridad Social, correos electrónicos, hasta números de tarjetas y cuentas bancarias.

Es obvio que, con este comportamiento, se producen ya varias conductas punibles, pues existe un delito de acceso ilícito y otro de descubrimiento y revelación de secretos de los arts. 197 bis y 197.1, respectivamente, del Código Penal. Pero el que adquiere esos datos, ya sea un particular, ya una organización criminal, está llevando a cabo actos preparatorios de futuras actividades que pueden derivar en la suplantación de la identidad de la persona a la que pertenecen esos datos para cometer otras acciones que podrían tener, también, un carácter delictivo, aunque la obtención de información de los ciudadanos no siempre se produce mediante procedimientos ilícitos, sino a través de técnicas de ingeniería social, cediendo la información los propios ciudadanos.

De una forma u otra, la finalidad más habitual de esas suplantaciones de identidad que se producen con esta información previamente obtenida está relacionada con motivos económicos[11]. El autor persigue, así, causar un daño patrimonial u obtener un beneficio económico cuando, por ejemplo, se

[11] Javier Gustavo Fernández Teruelo, "Fraudes online: transferencias ilegítimas, doble factor de autenticación, muleros y subsunción típica", en VV.AA. *Estudios político-criminales, jurídico-penales y criminológicos. Libro Homenaje al Profesor José Luis Díez Ripollés* (Valencia: Tirant lo Blanch, 2023): 1391-1404. Patricia Faraldo Cabana,

suplanta la identidad de una empresa de la competencia llevando a cabo determinados comportamientos para afectar a su reputación y favorecer que los consumidores dejen de adquirir sus productos; cuando alguien se hace pasar por un famoso para, simplemente, estafar a los seguidores solicitándoles dinero con base en la confianza generada; cuando se utiliza el nombre de un familiar para realizar solicitudes de dinero[12] o se configura una web valiéndose de la identidad de otra empresa para conseguir clientes[13] o se realizan contrataciones telemáticas de servicios a nombre de otra persona para que le lleguen a la víctima los cargos[14]; cuando se bloquea la cuenta real de una persona para exigir dinero a cambio de su desbloqueo; cuando se suplanta la identidad de un directivo de una compañía (o de una empresa proveedora) en un correo electrónico para que otro empleado realice una transferencia a una cuenta que no corresponde al verdadero deudor; o si se utilizan las cuentas de otras personas para realizar apuestas online, cargando a éstas las consecuencias económicas negativas.

De hecho, el primer comportamiento ilícito cuya posible responsabilidad penal debiera analizarse en relación con el *phishing* o *smishing* (variante a través de sms), como una de las conductas que más habitualmente implican la comisión de un delito de fraude cibernético, es precisamente este robo o suplantación de la identidad con intención maliciosa, y ello porque, mediante el *spoofing*, el atacante crea un contexto engañoso para así hacer caer en un error a la víctima de forma que tome una decisión relacionada con la seguridad inapropiada. El ciberdelincuente crea un escenario falso, falaz, pero convincente alrededor de la víctima, actuando ésta de forma que pasa inadvertida su situación de peligro y a través de diferentes técnicas como *holograph attack* (utilización de caracteres de otro idioma), IDN *spoofing* (cambio de servidor de dominios), IP *spoofing* (empleo de programas para sustituir la IP original), etc. que permiten llevar a cabo el *spoofing* con cierto éxito. La captura de claves puede realizarse a través de programas que interceptan la información en el momento que se introducen en la banca online real, o también se llevan a cabo técnicas como la denominada *man in the middle* (introducirse en medio del correo enviado por una persona y recibido por la otra para

"Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico", *Revista de Derecho Penal y Criminología*, n.º 3 (2010): 73-134.

[12] Sentencia de la Audiencia Provincial de Pontevedra 23/2015, de 5 de mayo, en que fue absuelto el padre que se hace pasar por su hijo para tener conversaciones por Messenger con una mujer a fin de solicitarle varias sumas de dinero.

[13] Sentencia de la Audiencia Provincial de Barcelona 198/2012, de 8 de marzo.

[14] Sentencias 414/2008, de 27 de junio de la Audiencia Provincial de Granada, 2/2014, de 7 de enero de la Audiencia Provincial de Islas Baleares, 59/2018, de 21 de marzo de la Audiencia Provincial de La Rioja, 247/2019, de 20 de junio de la Audiencia Provincial de Las Palmas.

sustituir y suplantar la identidad[15]), el uso de *keyloggers* (programas que capturan las pulsaciones del teclado) o el uso de programas de control remoto.

Pero no solo es un paso previo al phishing sino también al *pharming*, a través del *web spoofing*, que implica que mediante una suplantación de una página web, que se imita y está albergada en otro servidor, la víctima accede a la página falsa a la que le remite un código introducido en su ordenador, por un *malware*, que genera una confianza en la víctima, para que el sujeto pasivo acceda sin darse cuenta de la suplantación y, al acceder a la que cree real, revela sus datos.

Aparte de esta finalidad, que quizás es la que motiva más supuestos delictivos en la práctica, es muy habitual que encontremos suplantaciones de identidad digital por mera venganza cuando, por ejemplo, alguien accede a la cuenta, perfil o usuario original que tiene su expareja porque conoce sus claves, para cambiarlas y bloquearle el acceso o realizar comentarios ofensivos a sus seguidores para que sea objeto de críticas y causarle un daño reputacional, en el contexto de violencia de género que puede derivar en un acoso o provocación al odio (cuando se realizan comentarios desagradables en un chat o foro), con mensajes obscenos e indecentes, amenazantes, o que contengan información falsa del suplantado y le genere una situación de ansiedad con daños psicológicos[16]; o cuando un empleado despedido pone en un periódico escrito o en páginas de internet de contactos sexuales el correo electrónico y teléfono de la persona que le despidió[17].

---

[15] Relevante es el estudio realizado por Margarita Robles Carrillo, "Email Spoofing: un enfoque técnico-jurídico", *Revista Científica de Sistemas e Informática*, vol. XVI (2021): 139-144, sobre la técnica para llevar a cabo este tipo de suplantación de identidad y algunas herramientas técnicas para prevenirla.

[16] La Sentencia de la Audiencia Provincial de Málaga 4/2015, de 15 de enero, condena por delito contra la intimidad a un sujeto que aprovechando una relación de amistad con la víctima, y teniendo acceso a sus fotografías personales, acabada la relación, abrió en Facebook un perfil con el mismo nombre de la víctima, haciendo creer a otros usuarios de la red que tras él estaba el verdadero usuario, perfil al que exportó las fotos de que disponía, con el fin de perjudicarle incorporando comentarios personales relativos a su vida privada de pareja. Y el Auto de la Audiencia Provincial de Segovia 46/2010, de 25 marzo, se refiere a un supuesto de uso falso de la personalidad de la denunciante en la red social Tuenti para ridiculizarla.

[17] Supuesto examinado en la STS 344/2020, de 25 de junio. Sobre este tema, José Miguel Sánchez Tomás, "Anuncios de solicitud sexual con usurpación de identidad: entre el acoso, la injuria y la infracción de protección de datos", *La ley penal: revista de derecho penal, procesal y penitenciario*, n.º 147 (2020): en línea, en el que analiza la difícil calificación jurídico penal de estos hechos y su subsunción posible en los delitos de acoso (art. 172 *ter.*1.3ª CP), de injurias (art. 208 CP) y de usurpación de estado civil (art. 401 CP); concluyendo que lo más adecuado es su consideración de infracción del art. 72.1.b) de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garan-

O con una finalidad sexual, cuando, por ejemplo, el ciberdelincuente se hace pasar por un famoso cantante para obtener seguidores –normalmente adolescentes– a las que, después, les manda mensajes directos aprovechándose del engaño reclamándoles fotografías o videos sexuales. En este ámbito de los menores es especialmente preocupante la suplantación de identidad en el contexto del ciberbullying, pues asistimos a multitud de comportamientos que normalmente no llegan, siquiera, a los Juzgados de menores, pero implican conductas delictivas en sí mismas, como cuando un adolescente por ejemplo, utiliza la imagen de una compañera de clase para realizar un montaje fotográfico de connotaciones sexuales y hacerse pasar por ella en una red social para ridiculizarla o molestarla, o simplemente hacerse pasar por un compañero/a popular tener mayor aceptación social arrogándose su identidad[18].

Y también se puede llevar a cabo la suplantación de identidad, incluso, para encubrir una actuación delictiva, de forma que alguien se hace pasar por otra persona para cometer hechos delictivos y que se dirija la investigación contra el tercero que, en realidad, es una víctima[19], siendo habitual los casos de suplantación de identidad en la apertura fraudulenta de las cuentas bancarias online, como consecuencia en ocasiones, de una inadecuada aplicación o supervisión de la normativa sobre la prevención del blanqueo de capitales por parte de los responsables de las entidades bancarias y por lo que, éstas deberían responder civilmente. De hecho, la STS 300/2015, de 19 de mayo, advertía de la relativa facilidad para suplantar la identidad de otra persona a través de estos medios de comunicación y, en consecuencia, la necesidad de que exista una pericial informática para acreditar la autoría del delito[20]. Sobre

tía de los derechos digitales, es decir, ajeno a la sanción penal por falta de tipificación. Téngase en cuenta que, precisamente con la reforma operada en el artículo 172 ter por la Ley Orgánica 10/2022, de 6 de septiembre, se ha introducido un nuevo apartado 5 consistente en "El que, sin consentimiento de su titular, utilice la imagen de una persona para realizar anuncios o abrir perfiles falsos en redes sociales, páginas de contacto o cualquier medio de difusión pública, ocasionándole a la misma situación de acoso, hostigamiento o humillación", pero esta conducta no englobaría la mera utilización, como ocurrió en la citada resolución del Tribunal Supremo, del correo electrónico y el número de teléfono, no de la imagen.

[18] Ese supuesto, en adultos, fue el examinado en la STS 635/2009, de 15 de junio, en el que una persona se hizo pasar por un famoso periodista para mejorar sus relaciones sociales para firmar un precontrato de compraventa, cheques, formalizar ante un notario tres escrituras públicas e inscribirse en un hotel, siendo absuelto por no integrarse en la conducta de usurpación de estado civil del art. 401 CP.

[19] Supuesto que, aunque no en el ámbito digital, fue objeto de condena en la Sentencia de la Audiencia Provincial de Asturias 206/2013, de 19 de diciembre.

[20] Esta Sentencia indicaba, en su Fundamento Jurídico Cuarto, que "la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería

esta circunstancia preocupa, como informa la Fiscalía General del Estado, que los efectos perversos de esta práctica se incrementan año tras año, pues "los delincuentes se sirven de datos personales ajenos, sustraídos u obtenidos con ocasión de contactos online, para utilizarlos en posteriores acciones criminales en la red, generando a los legítimos titulares de la identidad suplantada graves perjuicios y en muchas ocasiones múltiples reclamaciones judiciales como presuntos autores de actos ilícitos" y, a este respecto, indica que se están intentando ofrecer soluciones efectivas ante estas situaciones, a través de mecanismos que permitan interrelacionar de forma automática la información derivada de los distintos expedientes[21].

Por otro lado, hay ocasiones en que, simplemente, la suplantación se lleva a cabo con una finalidad aparentemente más nimia, pero que puede llegar a provocar graves daños personales, como obtener más *likes* en una red social, para conseguir más seguidores, actuar en redes como si fuera esa otra persona haciendo comentarios fingiendo que es la real la que los publica, atribuyendo al suplantado expresiones, pensamientos, opiniones o planteamientos que no le son propios y que le desprestigian o desmerecen en su consideración pública[22], o le provocan enfrentamientos con su círculo de amigos o familiares o con su ámbito de contactos de carácter profesional como compañeros de trabajo, clientes, proveedores, o para realizar *fake news* o desestabilizar la opinión pública (los denominados *troles*), sin ninguna trascendencia penal.

Asimismo, como indicaba al principio, existen diversas modalidades de comisión, desde las formas más sencillas que puede llegar a cometer cualquier persona mediante técnicas de ingeniería social o engaño, hasta las más complejas en las que se utiliza la ingeniería informática solo al alcance de unos pocos. Y por un lado, se puede llevar a cabo mediante la suplantación de la identidad real en la cuenta, perfil o usuario de una red social o sistema de la información (accediendo sin autorización con las claves reales o habiendo obtenido las credenciales a través de cualquier técnica), o creando nuevas cuentas o perfiles que simulen ser la persona real (utilizando el mismo nombre, la imagen, el *nick*, el avatar, el usuario y de cualquier forma que implique

instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo".

[21] Memoria de la Fiscalía General del Estado de 2022, pp. 857 y 858.

[22] Un supuesto similar fue objeto de absolución por la Sentencia de la Audiencia Provincial de Madrid 96/2012, de 26 de marzo, pues a pesar de que se usurpó la identidad de una persona para perjudicarla en su imagen y publicar, en su nombre, expresiones soeces y de mal gusto entre sus amistades, se consideró que no colmaba las exigencias del tipo penal de injurias.

Estudios de Deusto
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 72/1, enero-junio 2024, págs. 199-228
https://doi.org/10.18543/ed.3105 • http://www.revista-estudios.deusto.es/

una confusión con el real, es decir, para que el perfil parezca auténtico, actuando como tal en chats, foros o plataformas similares de contacto interpersonal) y, de esta forma, inducir a error a los demás usuarios. Pero tanto en uno como en otro caso, existe una apariencia de que realmente se trata de una persona cuando, en realidad, es otra la que actúa faltando a la verdad.

III. EL BIEN JURÍDICO PROTEGIDO DE NUEVA GENERACIÓN: LA IDENTIDAD DIGITAL COMO EXTENSIÓN DEL DERECHO A LA INTIMIDAD

El Título X de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, regula los derechos en la era digital al referirse al derecho al olvido, a la desconexión digital, a la neutralidad de Internet, a la seguridad y educación digital o a la protección de los menores en Internet, pero no define como tal la identidad digital, que con mayor frecuencia es uno de los aspectos que más afectación tienen. Este concepto ha sido definido por INTECO (Instituto Nacional de Tecnologías de la Información, adscrito al Ministerio de Industria) 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"[23] o por la doctrina como "la herramienta que permite singularizar, asociar información e interconectar a las personas físicas, entidades y objetos en un contexto digital"[24]. Se trata, pues, del equivalente a la identidad de una persona o entidad, pero en un entorno digital y se utiliza para la identificación de la persona en las conexiones o las transacciones entre ordenadores, teléfonos móviles u otros dispositivos personales, de forma que no solo se trata de emplear la información offline de la persona, sino la imagen que proyecta la huella y sombra digital del usuario, así como por su reputación online.

Esta identidad, por tanto, al integrar todo lo que una persona es en relación con las nuevas tecnologías (ya sea con su nombre y apellidos, dirección física, datos fiscales, correo electrónico, su whatsapp, su perfil o usuario en cualquier página o red social o, incluso, su número de teléfono o su imagen, fotografías, historiales de navegación y comportamiento en línea), forma parte del contenido más íntimo de la persona, con implicaciones sobre la

[23] INTECO, Guía para usuarios: Identidad digital y reputación online. España: Instituto Nacional de Tecnologías de la Comunicación, Ministerio de Industria, Energía y Turismo, (2012): 5.

[24] José Antonio Hurtado Martos, "La identidad digital, una herramienta para el desarrollo sostenible", *RA & DEM: Revista de Administración y Dirección de empresas*, n.º 4 (2020): 115-130.

intimidad y libertad individual y, por ello, se engloba dentro del derecho fundamental a la intimidad y a la privacidad informática[25], siendo necesario extender su protección al entorno en línea con el advenimiento de la era digital y por los abusos que se están produciendo.

Por eso, se trata de un bien jurídico de nueva generación, o 5.0, que ya fue visionado por nuestra Constitución de 1978 que, en un momento en que era un futurible conocer el desarrollo que tendrían las nuevas tecnologías, reflejó en el apartado 4 del artículo 18, que "la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos", previendo que en un futuro, como es el presente actual, 45 años después, las aplicaciones de la informática han supuesto un elemento transgresor de nuestra intimidad, con la posibilidad de que suplanten nuestra identidad con una gran facilidad.

En definitiva, la identidad, como conjunto de los signos o rasgos de una persona que la caracterizan e individualizan en la vida social, constituye un derecho de la personalidad como bien jurídico autónomo y muy relevante para la configuración de la dignidad personal, y como presupuesto del ejercicio de muchas facultades reconocidas y amparadas por el ordenamiento jurídico. Así figura en los artículos 8 de la Convención sobre los Derechos del Niño ("derecho del niño a preservar su identidad"), 33.1 de la Constitución portuguesa (que regula los derechos a la identidad, la buena fama y la intimidad), y 4, 5, 15 y 29 de la Ley española 20/2011, de 21 de julio, del Registro Civil (que se refieren de forma expresa al derecho a la identidad de la persona). Y, de manera coincidente, la jurisprudencia del Tribunal Europeo de Derechos (esencialmente sus Sentencias de 26 de junio de 2014 –n.º 65192/11, caso Mennesson c. Francia, y 65941/11, caso Labasseé v. Francia–) ha valorado de manera autónoma el derecho a la identidad en el haz de los propios de la personalidad.

Este derecho está íntimamente conectado con la fe pública desde un punto de vista de la autenticidad digital como bien jurídico protegido de las falsedades documentales, pues se concreta en la confianza de la comunidad en la correcta identificación de las personas, a su vez instrumento esencial de la vida social y del tráfico jurídico[26], incluso del económico[27] –uno de los

[25] Ya la STC 126/1998, de 15 junio, mencionaba este derecho a la intimidad informática en relación con un supuesto de incorporación a un registro informático de determinados datos personales que propiciaban la discriminación.

[26] Emiliano Borja Jiménez, "Capítulo IV. De la usurpación del estado civil", en VV.AA. *Comentarios al Código penal* (Valencia: Tirant lo Blanch, 2023): 2536, afirma que, en esta figura delictiva, junto a la usurpación de funciones públicas y al intrusismo, "la mutación de la verdad y su incidencia en la seguridad del tráfico jurídico no se proyecta sobre concretos objetos materiales, sino sobre determinados comportamientos del sujeto".

[27] Patricia Faraldo Cabana (2010): 74.

aspectos que, como antes he indicado, están más en riesgo cuando se producen estas suplantaciones de identidad–. Este nuevo concepto de bien jurídico es de carácter colectivo, puede considerarse una extensión de la integridad y seguridad informática, que cumple una función preventivo-positiva y viene a dar una protección anticipada a otros bienes jurídicos de naturaleza personal. De hecho, iría destinado a garantizar la autenticidad de las comunicaciones personales y de todos los datos que figuran en cualquier soporte informático de una persona.

Como afirman Avelina Alonso de Escamilla y Esteban Mestre Delgado, "una falsedad es una mentira, una alteración de la verdad, pero, a efectos penales"[28]. Por ello, es necesario hablar de un bien jurídico penal más específico, de nueva generación, que supone la verificación de la autenticidad de la persona en sí misma considerada.

Pero debe diferenciarse, precisamente porque no tiene implicación en este derecho a la intimidad, lo que supone la suplantación de esa identidad real de la mera creación de perfiles o identidades falsas en el ciberespacio, que no pueden tener la misma consideración jurídica. 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, buscando la desinformación y manipulación, propagar noticias falsas, generar polarización, influir en elecciones o promover agendas políticas o comerciales ocultas, o bien para cometer otros delitos, tratando así de ampararse en el anonimato.

Ello, sin embargo, es decir, cuando se produce una mera creación de un perfil falso sin suplantación de una persona real, debe atajarse desde la legislación administrativa. Es decir, esta conducta de crear perfiles falsos, de carácter ficticio, que no afecta a otra persona, en el que no se utilizan fotografías ni datos ajenos, debe quedar extramuros al Derecho penal porque, con ello, no se afectaría a ningún bien jurídico objeto de tutela penal y por mera intervención del principio de intervención mínima[29], pues desde un punto de vista político-criminal debe limitarse la aplicación penal para que accedan al campo de lo punible solo hechos gravemente

[28] Avelina Alonso de Escamilla y Esteban Mestre Delgado, "Tema 21. Falsedades". En *Delitos. La parte especial del Derecho penal,* coordinadora Carmen Lamarca Pérez, 6ª edición, (Madrid: Dykinson, 2021): 848.

[29] Como afirman las SSTC 229/2003, de 18 de diciembre, 26/2018, de 5 de marzo, y del Pleno 25/2022, de 23 de febrero "en materia penal rige el denominado principio de intervención mínima, conforme al cual la intromisión del Derecho Penal debe quedar reducida al mínimo indispensable para el control social. De modo tal que la sanción punitiva, como mecanismo de satisfacción o respuesta, se presenta como *ultima ratio*, reservada para aquellos casos de mayor gravedad y siempre sometida a las exigencias de los principios de legalidad y tipicidad".

atentatorios contra, en este caso, el derecho a la intimidad de una persona cierta y real[30].

Llevo afirmando tiempo en distintos foros que, a mi juicio, debería exigirse a las plataformas online que implementen medidas de seguridad y verificación de identidad más rigurosas que las que existen en la actualidad, para que pueda facilitarse la identificación real de la persona que crea un perfil o una cuenta, similar a la que utiliza la Administración Pública española ante cualquier trámite online, que para asegurar la identidad en un trámite captan una fotografía del interesado con el DNI, asegurando, así que los datos que se indican son ciertos y reales, y se puede comprobar la identidad. Si ello se hiciera así, los ciberdelincuentes no podrían ampararse en el anonimato para cometer muchas de sus conductas delictivas. Asimismo, sería necesario mejorar los mecanismos de denuncia y eliminación de contenido falso en esas plataformas.

Pero una cuestión es solicitar, desde un punto de vista legal que las entidades requieran la garantía de esta identidad para poder usar esos servicios o, incluso, sancionar la creación de perfiles falsos en redes sociales y otra muy distinta que esto deba ser objeto de tutela penal.

Finalmente, aunque el principal efecto que genera para el suplantado es, evidentemente, la afectación a su intimidad, ello no implica que se generen daños en otros bienes penalmente protegidos como en el patrimonio, en el honor o, incluso, en la integridad cuando se producen daños de tipo psicológico ante la incomprensión de los hechos por la víctima, el estrés emocional y el trauma que le puede generar el hecho de que alguien le haya usurpado su identidad.

IV. ESTADO ACTUAL DE LA CUESTIÓN: LA IMPOSIBILIDAD DE SANCIÓN PENAL

Como se ha indicado, tanto la Fiscalía especial de Criminalidad Informática como la doctrina han debatido sobre el encaje penal que podría tener la mera suplantación de identidad digital, y se llega siempre a la misma conclusión: no tiene ninguno.

Ya he dicho que lo que se puede sancionar es la conducta que se lleva a cabo a posteriori con esa identidad suplantada. Así, si se simula ser la persona real y se llevan a cabo injurias o calumnias o amenazas sobre los seguidores de una cuenta u otras personas, se sancionaría como un delito contra el

[30] De hecho, en el supuesto examinado en la Sentencia de la Audiencia Provincial de Madrid 695/2011, de 21 de noviembre, como no puedo comprobarse si las identidades tarjetas de residencia que utilizaban los acusados pertenecían a una persona real y cierta, tuvo que absolverse del delito de usurpación de estado civil del art. 401 del CP.

Estudios de Deusto
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 72/1, enero-junio 2024, págs. 199-228
https://doi.org/10.18543/ed.3105 • http://www.revista-estudios.deusto.es/

honor (arts. 205 y ss.) o de amenazas (arts. 169 y ss.). Así fue, por ejemplo, en el supuesto examinado en la Sentencia de la Audiencia Provincial de Valladolid 58/2011, de 9 de marzo, en que un adolescente de 15 años accede al perfil de una compañera del colegio en «Tuenti» para insultar y amenazar a otros alumnos, o en la Sentencia de la Audiencia Provincial de Segovia 32/2011, de 24 de mayo (que en una situación similar se condenó por una antigua falta de vejaciones injustas).

Si con esa suplantación se están revelando datos personales de otro, como un delito contra la intimidad (arts. 197 y ss.), como en el supuesto examinado en la Sentencia de la Audiencia Provincial de Badajoz 117/2020, de 17 de noviembre, en que se hace pasar por otra persona en una conversación telefónica para obtener secretos de la víctima y luego compartir la grabación en redes sociales.

Si se utiliza la identidad de otro para obtener videos sexuales de menores se sancionaría como delito contra la libertad sexual o de pornografía infantil. Este caso fue, por ejemplo, el examinado en la Sentencia de la Audiencia Provincial de Madrid 772/2013, de 23 de octubre, que entre otras conductas, el acusado simulando ser un amigo de la joven y con el pretexto de ayudarla por el acoso que estaba recibiendo de él mismo la convenció para que cambiara la contraseña de su cuenta de correo en la red social Tuenti, consiguiendo de esta manera el acceso a dicha cuenta y tomar conocimiento de su contenido y de las direcciones electrónicas de su familia y amigos, con la finalidad de presionarla y conminarla para que volviera con él y le remitiera videos de contenido pornográfico.

También se sancionaría como daños informáticos (arts. 267 y ss.) si se borra contenido previamente reflejado por la persona real (fotografías, comentarios o videos). Si se ejercitan derechos o se contratan servicios en su nombre se sancionaría como una usurpación del estado civil (art. 401), o si de lo que se trata es de utilizar esa identidad para engañar patrimonialmente a otros, se sancionaría como estafa (art. 248).

Pero no existe ningún delito específico que sancione el mero hecho de suplantar esa identidad sin hacer nada más, es decir, hacerse pasar alguien por otra persona, lo que indudablemente afecta a lo más íntimo que tiene aquélla, como se ha indicado: su identidad real.

Aunque un sector doctrinal ha solicitado el encaje en el art. 401 de las meras conductas de creación de perfiles suplantados de otra persona en las redes sociales o páginas web de Internet[31], ello no es correcto, y los Tribunales no están castigando por este precepto, ya que este tipo delictivo, como ha

[31] Juan Alberto Díaz López, *El delito de usurpación del estado civil* (Madrid: Dykinson, 2010): 221 y ss. Paz Lloria García, "Delitos y redes sociales: los nuevos atentados a la intimidad, el honor y la integridad moral. Especial referencia al 'sexting'", *La Ley Pe-*

exigido la jurisprudencia (SSTS 710/2017, de 27 de octubre, 371/2019, de 23 de julio) exige no solo arrogarse la condición de otra persona, sino actuar en el tráfico jurídico como ella, en todas sus facetas de la vida, es decir, el uso de los derechos y acciones de la personalidad sustituida en todas –o, al menos, variadas-[32], que no se cumple con el mero hecho de hacerse pasar por otra persona frente a los demás, motivo por el que está tratándose de condenar, en los casos en que no se colman las exigencias de este tipo penal, por un delito de falsedad documental cuando implica la suscripción de documentos de los arts. 390 y siguientes[33]. Silvia Mendoza Calderón pone el acento en que este precepto "incide sobre los nombres que por filiación pertenecen a otra persona y consiste lógicamente en usarlos como propios, de manera tal que las restantes personas puedan creer que son los nombres y apellidos pertenecientes realmente al usurpador"[34].

nal, n.º 105 (2010): en línea. Y Álvaro Écija Bernal, "Principales conductas antisociales de Internet (y III)", *Diario La Ley*, n.º 4, sección Ciberderecho (2017): en línea.

[32] En la Sentencia de la Audiencia Provincial de Jaén 251/2020, de 23 de octubre se condena a una mujer extranjera que había sido expulsada de España y, para regresar utilizó un pasaporte a nombre de otra persona, amiga suya, utilizando su documentación identificativa como propia de forma plena y continuada, suplantándola en todos los actos de la vida civil, como abrir cuentas bancarias, llegando, incluso, a contraer matrimonio que le permitió obtener el permiso de residencia como familiar comunitario y, posteriormente, adquirir la nacionalidad española, haciendo uso de dicho documento de manera continuada, siendo condenada por delito de falsedad documental en concurso medial con el delito de usurpación de estado civil.

[33] Auto de la Audiencia Provincial de Valencia 1166/2016, de 17 de noviembre. De hecho, en la Memoria de la Fiscalía del año 2010 ya se reflejaba la preocupación por la comisión de delitos a través de las nuevas tecnologías, indicando 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".

[34] Silvia Mendoza Calderón, *Criminalidad juvenil en la era digital* (Valencia: Tirant lo Blanch, 2022): 174.

De este modo, podríamos encontrarnos en estos supuestos, simplemente sancionados por el art. 401 cuando la usurpación de la identidad digital implica el ejercicio de acciones concretas, pero si la jurisprudencia ni siquiera sanciona como delictivos todos los casos en que una persona se hace pasar por otra asumiendo su personalidad, cuando no se usurpan todos sus derechos[35] o cuando no es de forma continuada[36], menos aún en los supuestos en que no se utiliza ninguno, sino únicamente el nombre y la identidad de alguien.

Hay casos en que lo que se está llevando a cabo es una manipulación informática previa para suplantar la identidad digital en un documento haciendo creer al sistema que un documento está suscrito por la persona auténtica y luego se lleva a cabo una actuación en su nombre ejerciendo derechos. Pensemos, por ejemplo, en el empleo de la técnica de phishing para instalar un malware en el ordenador de un empleado de una multinacional y a continuación, sin que el usuario se percate, el cibercriminal utiliza su firma digital y el sello de la persona jurídica o la del Director Financiero o, incluso, del representante, para plasmarla en un documento con cualquier finalidad, ya sea defraudatoria o declaratoria de voluntad. O cuando esto mismo ocurra en el ordenador de un funcionario de cualquier Administración Pública para lograr la firma y sello electrónico de un documento público (quien ha solicitado, por ejemplo, una subvención, o quien en un Ayuntamiento está esperando una licencia de construcción o de actividad o cualquier acto público o quien modifica la consideración de una finca, de rústica a urbana)[37]. O hacer

[35] Por ejemplo, las Sentencias de la Audiencia Provincial de Madrid 22/2021, de 21 de enero y Lleida 298/2012, de 20 de septiembre absuelven cuando la suplantación se refiere a un acto concreto. En la primera, el acusado haciéndose pasar por su ex mujer procedió a firmar unos recibos y se le absolvió considerándose que al no suponer la asunción total de la personalidad de su ex mujer, ni de sustitución de la misma en todos sus derechos, aunque ello pudiera causar un perjuicio, no es susceptible de ser calificado como un delito de usurpación del estado civil, dado que la verdadera suplantación de identidad "no se limita al nombre, sino a todas las características o datos que integran la identidad de una persona, único supuesto en el que nos hallaremos ante un delito de usurpación de estado civil, del art. 401 del Código Penal".

[36] Sentencia de la Audiencia Provincial de Madrid 111/2006, de 6 de noviembre, o la de la Audiencia Provincial de Barcelona 385/2016, que absolvió de este delito porque "para la comisión del delito de usurpación de estado civil no basta con una suplantación momentánea y parcial, sino que es preciso continuidad y persistencia, y asunción de la total personalidad ajena con ejercicio de sus derechos y acciones dentro de su status familiar y social. Y de lo que se acusa en autos es de que en momentos y situaciones puntuales, el acusado habría utilizado el nombre de otra persona para imputarle la comisión de unas infracciones administrativas".

[37] De conformidad con lo previsto en la disposición adicional segunda de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios elec-

lo mismo en un usuario particular y utilizar, después, la firma electrónica desde su ordenador para solicitar un préstamo digitalmente o para abrir una cuenta corriente e ingresar en ella dinero proveniente de actividades ilícitas, para evitar ser descubierto el verdadero autor. De hecho, por haberse detectado estas brechas de seguridad en el empleo de la firma digital, se están implementado programas más avanzados para exigir un doble *check* a la firma digital, como el Viafirma, la autenticación multifactorial (MFA), las opciones móviles como el escaneo de huellas dactilares y el reconocimiento facial, o las contraseñas de un solo uso entregadas a través de una aplicación de autenticación móvil o un mensaje SMS, aunque evidentemente, con el uso de la inteligencia artificial también es posible la suplantación de la identidad a través de sistemas de reproducciones de huellas o el uso de máscaras faciales (*facial recognition technology*) y las propiciadas por brechas de seguridad.

Pues bien, como afirma la STS 635/2009, de 15 de junio, "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. Usurpar equivale a atribuirse algo ajeno. En la segunda acepción de nuestro diccionario oficial se dice que es arrogarse la dignidad, empleo u oficio de otro y usarlos como si fueran propios… Quiere decir(se) que para usurpar no basta con usar un nombre y un apellido de otra persona, sino que es necesario hacer algo que solo puede hacer esa persona por las facultades, derechos y obligaciones que solo a ella corresponden".

Por tanto, llevar a cabo la suplantación de la identidad, incluso utilizando su nombre y apellidos o su firma electrónica sin llevar a cabo un acto negocial concreto o declarativo o una atribución de facultades, no podrían sancionarse dentro del art. 401 del Código Penal, pero tampoco como falsedad documental (art. 392) porque al plasmar la firma electrónica con los datos correctos del titular, realmente no se estaría cometiendo una falsedad clásica, ya que no se está imitando o suplantando la firma, ni falsedad en documento privado (art. 395), como ha sido desestimado por los Tribunales[38], porque la concurrencia de este tipo implica cometer en documento privado alguna de

trónicos de confianza, "todos los sistemas de identificación, firma y sello electrónico previstos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, tendrán plenos efectos jurídicos. Además de ello, es relevante el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

[38] Autos de la Audiencia Provincial de Madrid 356/2017, de 29 de mayo y de la Audiencia Provincial de La Rioja 137/2022, de 25 de abril.

las falsedades previstas en los tres primeros números del apartado 1 del art. 390 CP para perjudicar a otro, conducta en la que esa suplantación no encaja directamente.

Esa conducta, por tanto, en la que se usurpa la identidad de alguien mediante manipulaciones informáticas se podría castigar por un delito contra la intimidad de acceso ilícito (art. 197 bis), pero la suplantación quedaría sin sanción penal, igual que ocurría en los años 80 con las manipulaciones informáticas que se produjeron para cometer fraudes, que al no estar expresamente previstas, se absolvía cuando se efectuaban transferencias de fondos en la banca online, porque no entraban dentro del concepto clásico de estafa, al no llevarse a cabo ningún engaño (pues se utilizaban las contraseñas correctas del titular de la cuenta haciendo creer a la máquina que quien estaba realizando esa transferencia era el verdadero titular).

En este caso, por tanto, ni la manipulación informática para suplantar la firma de alguien si no está, con ella, atribuyéndose derechos o funciones es delito del suplantado reales y concretas causándole un perjuicio es delito[39], ni menos aún lo es, que el ciberdelincuente simplemente se haga pasar por otra persona.

Pero es que, recientemente se ha querido suplir esta laguna, sin éxito, porque la suplantación de identidad digital tampoco tiene cabida en el nuevo tipo penal incluido en la Ley Orgánica 10/2022, en el apartado 5 del artículo 172 ter, que se refiere, exclusivamente, al empleo de la imagen "para realizar anuncios o abrir perfiles falsos en redes sociales, páginas de contacto o cualquier medio de difusión pública, ocasionándole a la misma situación de acoso, hostigamiento o humillación". Con este precepto se ha realizado un parche, pues se sanciona la suplantación de la imagen de una persona pero con una exclusiva finalidad de acoso pero cuando no se emplea la imagen ni se causa esa situación, la conducta sigue siendo atípica.

Como refiere ese Auto de la Audiencia Provincial de Madrid 356/2017, de 29 de mayo: "crear un perfil falso en cualquier red social, simulando ser la víctima y utilizando su imagen sin su consentimiento, naturalmente con intención de difamar, humillar, acosar etc. (no por ejemplo para parodiar): ¿Puede ser un hecho constitutivo de delito? y la respuesta es afirmativa: desde un delito de usurpación o suplantación de identidad, un delito contra la intimidad y el derecho a la propia imagen, un delito de injurias y/o calumnias, hasta un delito de acoso propiamente dicho, en el caso: ciberbullying, lo

[39] Como tampoco lo es en el mundo real: la ya citada en notas anteriores STS 635/2009, de 15 de junio, que solo condena por la falsedad documental en la firma de un cheque nominativo, pero no por hacerse pasar por una persona famosa y firmar operaciones en su nombre como un precontrato de compraventa o escrituras públicas o se inscribe en un hotel.

que en países anglosajones también es conocido como *stalking*, ex art. 172 ter del Código Penal, bien entendido que esta última conducta tiene que ser insistente y reiterada, y tiene que alterarse gravemente el desarrollo de la vida cotidiana de la víctima, pero desde luego, no de un delito de falsedad documental". Y es que estamos en el ámbito de las falsedades, aunque no documentales, sino personales, pero tampoco tienen cabida en ellas.

Previamente, el Auto de la Audiencia Provincial de Segovia 46/2010, de 25 de marzo, afirmó que aun admitiendo que el uso del perfil propio en una red social sea un derecho exclusivo de la persona que vaya más allá del derecho al uso del propio nombre, se trataba de una actividad aislada dentro de la actividad usurpadora. Nótese que, como se decía, el tipo penal exige atribuirse concretos derechos, de forma que, si con esa creación de un perfil suplantador no se realizó ninguna otra conducta atributiva de la personalidad ajena, ni tuvo otra trascendencia que la limitada al foro de contactos en que se actuaba, se consideraba que no existió la completa asunción de la personalidad de la víctima y, por ello, se absolvió, aunque esa asunción pudiera ser total en el marco limitado de Tuenti.

Por otro lado, algún autor[40] ha considerado que puede encontrarse sanción en el art. 197.2 del Código penal, que castiga (con ese carácter tan amplio y con deficiente técnica legislativa como hace todos los apartados reflejados en este precepto), entre otras conductas, al que "utilice (…), 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", y vuelve a repetir el precepto al final del párrafo, que con iguales penas se castigará a quien utilice los datos en perjuicio del titular. Así se ha entendido por robar la cuenta profesional de Instagram y realizar publicaciones sin consentimiento de la legítima usuaria[41], o crear un perfil en una red social utilizando el nombre, usuario, fotografías y datos personales de la víctima para perjudicarla[42] y otra jurisprudencia[43]. Sin embargo, a mi juicio no se cumplen todos los presupuestos típicos para poder condenar en estos casos, ya que lo primero que exige el precepto es que se trate de datos reservados y, por ejemplo, el mero hecho de utilizar el nombre, apellidos o usuario de una red social no puede considerarse un dato reservado, pues son datos públicos que figuran en

[40] Miguel Marcos Ayjón, *La protección de datos de carácter personal en la justicia penal* (Barcelona: JM Bosch, 2020): 569.

[41] Sentencia de la Audiencia Provincial de Soria 30/2022, de 4 de abril.

[42] Sentencia de la Audiencia provincial de Badajoz 67/2012, de 11 de mayo.

[43] Sentencias de la Audiencia Provincial de Málaga 409/2017, 31 octubre, Pontevedra 320/2017, 12 diciembre, Sevilla 328/2016, 8 agosto y del Juzgado de lo Penal n.º 1 de Badajoz 350/2019, de 30 de diciembre.

el perfil, y lo que se hace es suplantar el mismo, que es público, así como las fotografías. Y tampoco se podría sancionar cuando los datos que se utilizan para suplantar la identidad no provienen de un fichero o soporte informático, aunque también puedan encontrarse en él, como el número de DNI o el nombre y apellidos, que están en soporte físico. En este sentido, Mata y Martín[44] entiende que este precepto no puede sancionar la mera suplantación de identidad cuando los datos los facilita el titular, ya sea voluntariamente como ocurriría en este caso en que son públicos, ya cuando los facilita previa petición fraudulenta, de forma que solo podría sancionarse cuando el acceso es ilegítimo, supuesto en el que ya se habrían colmado las exigencias de este precepto[45], pues se habría producido un apoderamiento previo sin el consentimiento del titular. Por tanto, este tipo penal tampoco engloba toda la conducta de suplantación completamente.

En consecuencia, la mera suplantación, sin implicar ningún otro bien jurídico protegido, sin realizar ninguna otra acción, cuando no existe apoderamiento previo ilícito de datos, solo puede ser sancionada, a lo sumo, como mera infracción civil en materia de intimidad o de protección de datos, y motivar el bloqueo de la cuenta a través de la red social, pero no una sanción penal.

De hecho, estas conductas en muchos casos no llegan a ser, siquiera, denunciadas. Y, si lo hacen, a través de un procedimiento específicamente previsto para ello, ponen los hechos en conocimiento de los prestadores de servicios y solicitan la retirada de los perfiles creados de forma fraudulenta o, en casos que se afecta su reputación online, contratan a empresas específicas para revertir el proceso y recuperar esa reputación. Y en ocasiones, la única solución es acudir a la Agencia Española de Protección de Datos a denunciar la suplantación, lo que constituye una vía muy útil para conseguir que los proveedores de servicios en Internet retiren la información y colaboren judicialmente en la identificación de los suplantadores[46].

Pero ello, como antes decía respecto a la previsión que hace nuestra Constitución en el art. 18.4, no debería ser así, pues un ataque grave a la intimidad que merece tutela penal.

---

[44] Roberto Mata y Martín, *ob. cit.,* 214 y 215.

[45] En el mismo sentido, Eloy Velasco Núñez, "Fraudes informáticos en red: del phishing al pharming", *La Ley Penal, n.º 37* (2007).

[46] En el procedimiento sancionador PS/00137/2011, en el que una persona suplantó la identidad de otra en una red social, y habiendo identificado al suplantador mediante la información facilitada sobre la IP del ordenador desde la que ésta se produjo, en el que la Agencia Española de Protección de Datos consideró que existía un tratamiento de datos personales y se vulneraba el principio del consentimiento del artículo 6.1 Ley Orgánica de Protección de Datos.

Mientras tanto, en otros países de nuestro entorno, la política criminal sí que ha decidido singularizar este comportamiento delictivo y tipificarlo expresamente. Es el caso de Francia, Gran Bretaña y, fuera de nuestras fronteras europeas, en Canadá, Costa Rica, México, Argentina y varios Estados de Estados Unidos como California o Texas.

V. NECESIDAD DE HOMOGENEIDAD DE LA TUTELA PENAL: PROPUESTA DE SANCIÓN

Todo lo anterior lleva a la conclusión de que existe una disfunción de nuestro Derecho penal en la relación con lo ocurrido en la sociedad. La identidad ya está reconocida en nuestro ordenamiento jurídico como un bien jurídico protegido, que justifica la aplicación, en los casos que he reseñado en páginas previas, y otros muchos semejantes, de los delitos contra el honor, de amenazas, contra la intimidad, contra la libertad o la indemnidad sexual, falsedad documental o usurpación de estado civil. Téngase así en cuenta, como ejemplo significativo, que el delito de falsificación del Documento Nacional de Identidad protege la función probatoria del documento[47], pero esencialmente (aunque el Código Penal todavía no lo reconozca expresamente) el derecho a la identidad personal del acreditado por él. Por esta razón, utilizar esos datos personales e identificación personal u otro tipo de información de la persona implica una necesidad de tutela penal porque, además, aunque estos robos o suplantaciones de identidad también se producen en el mundo offline (pensemos, por ejemplo, de una mujer que hurta una cartera y, después, enseña el DNI en una entidad financiera, tiñéndose el pelo del mismo color y utilizando accesorios para evitar el reconocimiento fotográfico), lo cierto es que en el ciberespacio la suplantación de identidad no solo resulta más sencilla de ejecutar sino que potencialmente es mucho más peligrosa porque se elimina la inmediatez física y, por tanto, las posibilidades de ser descubierto.

En este sentido, la Exposición de Motivos de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal hacía referencia a "la antinomia existente entre el principio de intervención mínima y las crecientes necesidades de tutela en una sociedad cada vez más compleja, dando prudente acogida a nuevas formas de delincuencia", por lo que la esencia de nuestro Derecho penal contemporáneo hace inexcusable que deba homogeneizarse la respuesta penal en estos supuestos, lo que conlleva una modificación necesaria del Capítulo IV del Título XVIII del Libro II CP, para diferenciar el delito de usurpación de estado civil del artículo 401 del Código Penal español

[47] Sentencia de la Audiencia Provincial de Madrid 254/2021, de 2 de junio, que castiga por un delito de falsedad como medio para una suplantación de identidad.

Estudios de Deusto
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 72/1, enero-junio 2024, págs. 199-228
https://doi.org/10.18543/ed.3105 • http://www.revista-estudios.deusto.es/

actualmente vigente de un nuevo delito que castigue de forma específica la usurpación o suplantación de identidad digital en cualquier medio informático, sistema de la información o plataforma, y sin habitualidad, pues se está produciendo cada vez con mayor frecuencia y afecta, como se indica, a un bien jurídico como la propia esencia de la persona, siendo la ubicación sistemática más ajustada incluir un nuevo artículo 401 bis, al tratarse, también, de una falsedad personal, es decir, de una falsedad que rompe la correlación entre una concreta persona y la manifestación pública de sus rasgos o caracteres más propios. De hecho, el rótulo del Capítulo IV debería pasar a denominarse "De la suplantación de identidad".

La descripción del comportamiento delictivo debe efectuarse como un delito común (pues no hay ningún elemento significativo de autoría que permita restringir el ámbito de los responsables), es decir, que pueda cometer cualquier persona que actúe a través de cualquier medio tecnológico, lo que resulta consustancial a la mecánica comisiva que debe desarrollarse para suplantar la identidad. El sujeto pasivo, como titular de la identidad, puede ser una persona física o jurídica (pues como tiene reconocido el Tribunal Constitucional, éstas son titulares también del derecho a la intimidad y, por ende, son titulares de su identidad como una prolongación del mismo). Y la conducta típica debe ser un comportamiento descrito en términos omnicomprensivos (suplantar la identidad de otro, de manera suficiente para provocar error en un tercero[48]), y por tanto sin necesidad de concretar las múltiples modalidades de realización y limitándose a la mera suplantación como infracción de mera actividad, pues, como se ha indicado, los resultados más habituales que se cometen, posteriormente, con esa identidad suplantada ya está prevista por otros preceptos del Código Penal, pudiendo ser sancionados mediante la concurrencia de otros tipos delictivos, que entrarían en régimen concursal con este nuevo tipo penal, sin que se resulte necesario que en este artículo se pronuncie el Legislador sobre la resolución de esos problemas concursales que la eventual aplicación combinada del delito de actividad y el de resultado puede generar.

Sin embargo, tampoco pueden dejarse sin punición las conductas que, aunque en menor medida, pueden producirse, de suplantación de identidad ajenas a ese medio digital, por lo que se debe añadir un inciso de la

[48] En este sentido, como afirman Sergio Cámara Arroyo/Alfredo Abadías Selma, "El delito de usurpación del estado civil y su compleja aplicación en el ámbito cibernético". En Enrique Sanz Delgado/Daniel Fernández Bermejo (coord.). *Tratado de Delincuencia Cibernética* (Cizur Menor: Aranzadi, 2021): 604, es condición sine qua non que en la usurpación exista una verosimilitud de la conducta, siendo atípica "cuando no resulte absolutamente creíble que la persona que comete la usurpación diga quien dice ser", es decir, "el factor de la credibilidad es fundamental".

posibilidad de comisión por cualquier otro medio, mediante una categoría diferenciada por la entidad de la pena a imponer.

Por otro lado, como requisito de atipicidad (a los efectos de evitar la tramitación de procedimientos judiciales por hechos de nula lesividad) debe añadirse que la suplantación se realice sin estar debidamente autorizado, pues es sabido que, en muchas ocasiones, por motivos profesionales, el verdadero titular de la identidad no es quien publica ni utiliza los perfiles para realizar publicaciones, sino que las delega en un equipo de marketing o publicidad, lo que, como es obvio, no puede sancionarse penalmente. Asimismo, debido al carácter íntimo de esta identidad digital, debe incluirse, como requisito de perseguibilidad, la denuncia previa de la persona agraviada o de su representante legal, al igual que se prevé para los delitos de descubrimiento y revelación de secretos, salvo en el caso de menores, que puede denunciar el Ministerio Fiscal.

Por ello, propongo una modificación del rótulo del Capítulo IV del Título XVIII del Libro II del Código Penal, que debe pasar a denominarse "De la suplantación de identidad", con la incorporación de un nuevo artículo 401 bis, con el siguiente contenido:

> "1. El que, sin estar debidamente autorizado, suplantare la identidad de otra persona física o jurídica en una red social, servicio de la sociedad de la información, sistema o plataforma informática o en cualquier otro medio, será castigado con la pena de tres meses a un año de prisión o multa de seis a doce meses.
>
> 2. Para proceder por este delito será necesaria denuncia de la persona agraviada o de su representante legal, salvo que la víctima sea menor de edad o una persona con discapacidad necesitada de especial protección, en que bastará la denuncia del Ministerio Fiscal".

Considero más apropiado que se incluya un artículo específico sobre la suplantación de identidad digital que una modificación del artículo 401 ya existente, para diferenciar ambas conductas punibles (la que se produce con el ejercicio de derechos civiles en nombre del suplantado y la que consiste en la mera suplantación de la identidad en el ámbito digital), sin perjuicio de que también podría incorporarse en un apartado de este precepto ya existente.

VI. LENTITUD DEL LEGISLADOR VERSUS CRITERIOS DE POLÍTICA CRIMINAL

Después de indicar por qué considero que este comportamiento debe sancionarse de forma específica en nuestro Código Penal, como también lo llevan haciendo Fiscalía y la doctrina que ha investigado sobre este tema desde hace años, la segunda cuestión que debe plantearse es si el hecho de que, hasta la fecha, no se haya introducido un artículo específico en el Código

Estudios de Deusto
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 72/1, enero-junio 2024, págs. 199-228
https://doi.org/10.18543/ed.3105 • http://www.revista-estudios.deusto.es/

penal, a pesar de las múltiples ocasiones que ha tenido el Legislador para hacerlo (en concreto, 22 veces desde que comenzó a reformarse el Código penal en materia cibernética tras la ratificación por España del Convenio de Budapest) es una cuestión de mera dejadez y lentitud en la adaptación de la Ley a la realidad cibernética o tiene una motivación específica porque no interesa, por motivos de política criminal, la punición anticipada de este comportamiento, ya que se considera suficiente sanción con el comportamiento que se efectúa a posteriori.

Pues bien, tras analizar el nulo interés que ha tenido el Legislador en incorporar esta conducta en el Código penal, a pesar de que ha tenido, como indico, multitud de oportunidades, me planteo si no es porque ya existe un excesivo rigor en la norma y la punición de esta conducta supondría sancionar una mera conducta preparatoria, anticipando la barrera de protección penal de forma excesiva (a pesar de que lo estamos haciendo en otros tipos), ya que, como he referido anteriormente, los actos de arrogación ilegítima de la identidad de otro persiguen una finalidad concreta, por lo que dicha actividad quedaría consumida (por el principio de consunción) en el propio delito final cometido. Y ello es especialmente relevante en la suplantación de la identidad en el delito de estafa, pues ésta formaría parte del desarrollo del engaño, como se interpretó en las Sentencias de la Audiencia Provincial de Las Palmas 247/2019, de 20 de junio y Huesca 48/2019, de 12 de abril y así lo indica Javier Gustavo Fernández Teruelo[49], no ejerciendo los Tribunales la posibilidad de solicitar al Legislador la modificación del Código penal, pues no han visto su necesidad.

Sin embargo, no puede equipararse esa consunción en el delito de estafa, que tiene una clara finalidad dirigida a un enriquecimiento patrimonial con otros tipos delictivos, que afectan a bienes personalísimos y en los que esta suplantación crea un grave daño personal, como son, por ejemplo, los adolescentes, que tienen una especial vulnerabilidad, donde su autoimagen o autoconcepto se crea a partir del grupo, valorándose cualquier contenido que no sea controlado por ellos, o la utilización de una imagen o nombre en la red social, como una situación de gran ansiedad y que puede condicionar su equilibrio psicológico. O las mujeres, a las que se está protegiendo en el ámbito de la violencia de género y sexual y, sin embargo, se las deja desprovistas de tutela ante una conducta de una expareja que, por mera venganza, la quiera hacer daño arrogándose su cualidad y manipulando la información que ofrece en su red social.

Por otro lado, quizás el Legislador se ha planteado si debe anticiparse la barrera de protección penal cuando en realidad estamos hablando de suplantación de identidad digital sobre datos que se encuentran públicamente en la

[49] Javier Gustavo Fernández Teruelo (2023): 1398.

red y que son de conocimiento general, sin que para su obtención se haya precisado el acceso a ningún archivo reservado, pero no es razonable pensar que los ciudadanos, en la actualidad, tengan que negarse a tener datos en lugares públicos por el miedo a ser suplantados en su identidad.

Me inclino, por tanto, más bien por la opción de que se trata de una enorme lentitud legislativa y de falta de interés[50]. Y lo peor es que no es previsible, a medio plazo, un interés normativo sobre la cuestión. A pesar de la gravedad del problema, no se trata de una prioridad en la agenda política. Pero, en cualquier caso, el mantenimiento del statu quo, atendiendo a los datos existentes y a la importante cifra de conductas cometidas, es una irresponsabilidad, pues con el uso de la inteligencia artificial, la suplantación de la identidad de una persona será mucho más peligrosa y el Derecho penal debe proteger anticipadamente a la sociedad y no cuando exista una estadística muy elevada de sobreseimientos y archivos de causas en los Juzgados o absoluciones en Sentencias por ser una conducta penalmente atípica.

VII. CONCLUSIONES

La identidad como aquella parte de lo más íntimo de la persona que la diferencia de otra y el empleo digital de todos los datos que nos identifican a todos como únicos en un entorno tecnológico no se encuentra en la actualidad suficientemente protegida por la norma penal, pues carecemos en la legislación de un delito concreto que sancione a modo de prevención general negativa, las conductas que se están desarrollando cada vez con más asiduidad en nuestra sociedad, consistentes en el robo de identidad de otra persona (física o jurídica) con distintas finalidades. Así se ha considerado por las distintas resoluciones judiciales que sancionan únicamente los delitos cometidos con esa usurpación de la identidad digital (amenazas, estafas, extorsiones, calumnias e injurias, etc.) y no por el mero empleo de esa identidad suplantada, pues el actual artículo 401 del Código Penal solamente sanciona la actuación en el tráfico jurídico como si se tratase de la persona suplantada, exigiendo actos concretos en el uso de derechos y acciones de la personalidad sustituida, que no se cumplen por el mero hecho de hacerse pasar por otra persona frente a los demás.

Sin embargo, la situación actual de las nuevas tecnologías, el desarrollo de la inteligencia artificial, los hechos que nos alarman como sociedad reflejados en las noticias, cuando cualquiera, incluso jóvenes menores de edad, con una aplicación, son capaces de generar una imagen y crear un contenido falso haciendo pasar por verdadero lo que no lo es a los ojos de los demás,

[50] El delito del art. 401 tiene exactamente la misma redacción que el art. 483 del CP 1870, del art. 464 del CP 1932 y del art. 470 del CP 1973.

incluso de los más allegados, hace necesario que el Legislador no demore más la propuesta legislativa que desde hace diez años lleva haciendo tanto la Fiscalía de Criminalidad Informática como la doctrina para introducir en la legislación penal esta conducta específica.

Es urgente, por ello, una reforma del Código Penal para introducir, dentro de las falsedades personales, como delito autónomo, y con la exigencia de denuncia previa, un artículo 401 bis, que castigue como delito común y de mera actividad, la suplantación de la identidad de otro, de manera suficiente para provocar error en un tercero a través de cualquier medio tecnológico y con cualquier finalidad y sin estar debidamente autorizado por el titular de esa identidad. Solo de este modo protegeremos la intimidad y privacidad digital, nuestro "ser tecnológico" que cada vez se encuentra más en riesgo en la sociedad en la que vivimos.

VIII. REFERENCIAS BIBLIOGRÁFICAS

Alonso De Escamilla, Avelina/Mestre Delgado, Esteban. "Tema 21. Falsedades". En Lamarca Pérez, Carmen (coord.). *Delitos. La parte especial del Derecho penal*. 6ª edición, 837 a 871, Madrid: Dykinson, 2021.

Borja Jiménez, Emiliano. "Capítulo IV. De la usurpación del estado civil". VV.AA. *Comentarios al Código penal*, 2536 a 2538. Valencia: Tirant lo Blanch, 2023.

Cámara Arroyo, Sergio/Abadías Selma, Alfredo. "El delito de usurpación del estado civil y su compleja aplicación en el ámbito cibernético". En Sanz Delgado, Enrique/Fernández Bermejo, Daniel (coord.). *Tratado de Delincuencia Cibernética*, 599-634. Cizur Menor: Aranzadi, 2021.

Cilli, Claudio. "Identity Theft: A New Frontier for Hackers and Cybercrime". *Information Systems Control Journal*, vol. 6 (2005).

De Prada Rodríguez, Mercedes/Santos Alonso, Jesús. "Suplantación de identidad en internet: necesidad de reforma del Código Penal". *Anuario jurídico Villanueva*, n.º 7 (2013): 215-230.

Díaz López, Juan Alberto. *El delito de usurpación del estado civil*. Madrid: Dykinson, 2010.

Écija Bernal, Álvaro. "Principales conductas antisociales de Internet (y III)". *Diario La Ley*. n.º 4, sección Ciberderecho, 2017.

Faraldo Cabana, Faraldo. "Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico". *Revista de Derecho Penal y Criminología*, n.º 3, (2010): 73-134.

Fernández Teruelo, Javier Gustavo. "Fraudes online: transferencias ilegítimas, doble factor de autenticación, muleros y subsunción típica". En VV.AA. *Estudios político-criminales, jurídico-penales y criminológicos. Libro Homenaje al Profesor José Luis Díez Ripollés,* 1391-1404. Valencia: Tirant lo Blanch, 2023.

Hurtado Martos, José Antonio. "La identidad digital, una herramienta para el desarrollo sostenible". *RA & DEM: Revista de Administración y Dirección de empresas*, n.º 4, (2020): 115-130.

INTECO. Guía para usuarios: Identidad digital y reputación online. España: Instituto Nacional de Tecnologías de la Comunicación, Ministerio de Industria, Energía y Turismo (2012).

Lloria García, Paz. "Delitos y redes sociales: los nuevos atentados a la intimidad, el honor y la integridad moral. Especial referencia al 'sexting'". *La Ley Penal*, n.º 105, (2013).

López Gutiérrez, Javier. "Delitos en el metaverso: hacia un nuevo horizonte legislativo". *Economist & Jurist*, Vol. 30, n.º 262. (2022): 16-23.

Magro Servet, Vicente. "La tipificación penal de la suplantación de identidad en el uso de las redes sociales". *Diario La Ley*, n.º 9005, (2017).

Marcos Ayjón, Miguel. *La protección de datos de carácter personal en la justicia penal.* Barcelona: JM Bosch, 2020.

Mata y Martín, Ricardo. "El robo de identidad: ¿una figura necesaria?". VV.AA. *Robo de identidad y protección de datos* (Madrid: Aranzadi, 2010): 199-220.

Mendoza Calderón, Silvia. *Criminalidad juvenil en la era digital*. Valencia: Tirant lo Blanch, 2022.

Miró Llinares, Fernando. *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons, 2012.

Tallero Masó, Alfonso/Tomás Román, Eva. "Metaverso y Derecho Penal". *La ley penal: revista de derecho penal, procesal y penitenciario*, n.º 158 (2022).

Robles Carrillo, Margarita. "Email Spoofing: un enfoque técnico-jurídico". *Revista Científica de Sistemas e Informática*, vol. XVI (2021): 139-144.

Rodríguez Fernández, María Pilar. "Suplantación electrónica de identidad: posible respuesta jurídica penal". *Diario La Ley*, n.º 7906 (2012).

Sánchez Tomás, José Miguel. "Anuncios de solicitud sexual con usurpación de identidad: entre el acoso, la injuria y la infracción de protección de datos". *La ley penal: revista de derecho penal, procesal y penitenciario*, n.º 147 (2020).

Serrano Acitores, Antonio. "Metaverso y derecho". Madrid: Tecnos, 2023, 2 ed.

Solari Merlo, Mariana N. "Suplantación de identidad digital: ¿necesidad de criminalización?". *Cuadernos de política criminal*, n.º 136 (2022): 125-164.

Velasco Núñez, Eloy, "Fraudes informáticos en red: del phishing al pharming", *La Ley Penal, n.º 37* (2007).