



COMILLAS
UNIVERSIDAD PONTIFICIA

ICAI

ICADE

CIHS

Facultad de Derecho
Departamento de Derecho Público

LA TUTELA PENAL DE LA IDENTIDAD DIGITAL
Relevancia penal de las suplantaciones en redes sociales

Autor: José Lorenzo Otero
Tutor: F. Javier Gómez Lanz
Derecho Penal – 5.º E-3 C

Madrid
Junio de 2020

RESUMEN

En el presente trabajo, se examina la protección que recibe la identidad de una persona en el ámbito virtual bajo la legislación penal vigente en España, concretamente en los casos de suplantación en redes sociales. Para ello, se comienza proponiendo una definición de *identidad digital* con base en nuestro ordenamiento jurídico, estudiando su contenido y sus caracteres. Este concepto será puesto en relación con otros bienes jurídicos protegidos en el Derecho penal, determinando en qué grado la tutela de éstos abarca, desde una perspectiva teórica, las lesiones a la identidad digital. Con este marco analítico, se abordarán los principales problemas de tipicidad y concursales que se pueden dar en los supuestos de suplantación de identidad en redes sociales. Esta tarea se hará a partir de dos casos prácticos de referencia, que ayudarán a reflejar la relevancia penal que tienen o debieran tener estas conductas. Asimismo, se hará alusión a las diferentes alternativas que se han propuesto desde la doctrina y la jurisprudencia. Como corolario de lo expuesto, se discutirá, en clave político-criminal, si el texto penal adolece de una falta de adaptación a esta nueva forma de ciberdelincuencia. Respondiendo afirmativamente a este extremo, se termina con una propuesta de reforma penal dirigida a salvar apropiadamente las lagunas apreciadas.

Palabras clave: *ciberdelitos, identidad digital, suplantación de identidad en redes sociales, política criminal.*

ABSTRACT

In this paper, we examine the protection that the Spanish criminal legislation in force grants to a person's identity in the virtual realm, particularly in the event of identity thefts on social media. For this purpose, we start proposing a definition of *digital identity* based on our legal system, studying its content and nature. The concept will be put together with other legally protected interests in order to clarify to which degree the penalisation of these interests encompasses the assault of identity theft from a theoretical viewpoint. Given this analytic framework, we will analyse the issues that identity thefts face as punishable acts. This task will be accomplished through two case studies, which will help to reflect the criminal relevance that this behaviours (should) have. Additionally, a reference to the different conclusions reached by the academic literature and the jurisprudence in this regard will be made. As a corollary to the above, we will discuss, in terms of criminal policy, whether the criminal legislation suffers from a lack of adjustment to this new new cybercrime phenomenon. With an affirmative answer, we conclude with a criminal-law reform proposal so as to properly bridge the legal loopholes found.

Keywords: *cybercrimes, digital identity, identity theft on social media, criminal policy.*

ÍNDICE DE CONTENIDOS

I. INTRODUCCIÓN	1
1. ESTRUCTURA	1
2. CONTEXTO: CIBERDELITOS EN LA ERA DIGITAL	1
3. ESTADO DE LA CUESTIÓN	2
II. DELIMITACIÓN CONCEPTUAL DE LA IDENTIDAD DIGITAL	6
1. PRIMERA APROXIMACIÓN: SIGNIFICADO COMÚN Y CONCEPCIÓN FILOSÓFICA	6
2. EL CONCEPTO DE IDENTIDAD EN NUESTRO DERECHO	8
A) Menciones a la identidad en las legislaciones internacional e interna	8
B) Caracterización de la identidad en cuanto objeto	9
C) El estado civil como correlato de la identidad	10
3. DELIMITACIÓN DE LA IDENTIDAD DIGITAL	12
A) Nuevos elementos de la identidad digital	13
B) Conclusión. Otros usos del concepto	14
III. TUTELA PENAL DE LA IDENTIDAD DIGITAL	16
1. ACLARACIONES PREVIAS	16
2. LA USURPACIÓN DE ESTADO CIVIL EN EL PLANO DIGITAL	17
3. LA SUPLANTACIÓN DE LA IDENTIDAD DIGITAL COMO FALSEDAD DOCUMENTAL	19
4. CONEXIÓN DE LA IDENTIDAD DIGITAL CON OTROS BIENES JURÍDICOS	21
A) El honor. Calumnia e injuria por medios digitales	22
B) La privacidad. Descubrimiento y revelación de secretos en el ciberespacio	23
daños informáticos	26
D) La libertad de obrar. Acoso moral por medios digitales	28
IV. RELEVANCIA PENAL DE LAS SUPLANTACIONES EN REDES SOCIALES	30
1. EXAMEN DE TIPICIDAD A TRAVÉS DE DOS SUPUESTOS PRÁCTICOS	30
A) Suplantación a través de creación de cuenta falsa	31
a) Tipicidad ad supplantationem	31
b) Tipicidad in supplantatione	32
B) Suplantación a través de intrusismo informático	33
a) Tipicidad ad supplantationem	34
b) Tipicidad in supplantatione	35
C) Conclusiones. Otros problemas de tipicidad y concursales	36
2. DISCUSIÓN DE POLÍTICA CRIMINAL SOBRE LA SUPLANTACIÓN DE IDENTIDAD DIGITAL	37
A) Consideraciones previas	37
B) Propuesta de reforma penal	39

V. CONCLUSIONES	41
BIBLIOGRAFÍA.....	43
1. DOCTRINA CIENTÍFICA.....	43
2. DOCTRINA JURISPRUDENCIAL Y ADMINISTRATIVA	46
3. LEGISLACIÓN	46
4. BASES DE DATOS.....	47

ÍNDICE DE ABREVIATURAS

AAP	Auto de la Audiencia Provincial
AECE	Asociación Profesional de Expertos Contables y Tributarios de España
AEPD	Agencia Española de Protección de Datos
art.	artículo
ATSJ	Auto del Tribunal Superior de Justicia
BOE	Boletín Oficial del Estado
CC	Código Civil
CE	Constitución Española
Cendoj	Centro de Documentación Judicial del CGPJ
CEDH	Comisión Europea de Derechos Humanos
CIEC	Comisión Internacional del Estado Civil
CGPJ	Consejo General del Poder Judicial
CP	Código Penal
dir.	director
DOUE	Diario Oficial de la Unión Europea
FGE	Fiscalía General del Estado
FJ	fundamento jurídico
Incibe	Instituto Nacional de Ciberseguridad
Inteco	Instituto Nacional de Tecnologías de la Comunicación
LOPD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos
LRC	Ley 20/2011, de 21 de julio, del Registro Civil
OCDE	Organización para la Cooperación y el Desarrollo Económicos
<i>(op.) cit.</i>	(obra) citada
p(p).	página(s)
pg(s).	parágrafo(s)
RAE	Real Academia Española
SAN	Sentencia de la Audiencia Nacional
SAP	Sentencia de la Audiencia Provincial
SJP	Sentencia del Juzgado de lo Penal
STC	Sentencia del Tribunal Constitucional
STEDH	Sentencia del TEDH
STS	Sentencia del Tribunal Supremo
TC	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
trad(s).	traductor(es)
TS	Tribunal Supremo
§	sección o epígrafe

I. INTRODUCCIÓN

El presente trabajo pretende abordar la delimitación de la identidad digital como concepto jurídico, para examinar después en qué medida los ataques contra la misma son objeto de tutela penal bajo la legislación vigente, y concluir discutiendo la relevancia penal de las suplantaciones de identidad en redes sociales.

1. ESTRUCTURA

Este contenido será desarrollado en un total de cuatro capítulos, cada uno de los cuales constará de varios epígrafes y, en su caso, secciones y subsecciones:

a) Primero, se delimitará el concepto técnico-jurídico de identidad digital, lo que nos obligará a buscar, con carácter previo, una definición de identidad en el Derecho español (capítulo II).

b) A continuación, se estudiará, desde una perspectiva teórica, el modo en que nuestro Derecho penal tutela la identidad digital: más propiamente, cómo adapta la protección de la identidad al plano digital (capítulo III).

c) En tercer lugar, con base en el marco teórico anterior, se hará un examen de dos supuestos prácticos de referencia, incidiendo en los problemas de tipicidad y concursales encontrados, tras el que se hará una discusión político-criminal sobre cómo solucionar los problemas observados (capítulo IV).

d) Por último, se expondrán las principales conclusiones del trabajo (capítulo V).

2. CONTEXTO: CIBERDELITOS EN LA ERA DIGITAL

El progreso socioeconómico producido por la innovación tecnológica en el planeta es indudable, pero igual de indudables son los riesgos que ese producto lleva aparejados. A mediados de la década de 1990, las amenazas que internet comportaba desde la perspectiva de la delincuencia eran causa de preocupación para la doctrina jurídica y los poderes públicos. El primer estudio exhaustivo que se realizó al respecto fue el preparado por Sieber para la Comisión Europea en 1998¹, donde figura la expresión *computer-related crimes* (“delitos relacionados con ordenadores”) en alusión a estos nuevos fenómenos criminales.

¹ SIEBER, U.: *Legal aspects of Computer-Related Crime in the Information Society. COMCRIME study*, Universidad de Würzburg, 1998.

En un principio, las características de estas conductas ilícitas impedían hablar en puridad de una categoría autónoma de delitos². No obstante, el tiempo ha evidenciado la existencia de una auténtica *ciberdelincuencia*, en la que internet es utilizado tanto para facilitar la comisión de delitos antes tipificados, aprovechando las potenciales dificultades de persecución que se derivan de este medio (principalmente, la ubicuidad y el anonimato), como para infligir daño sobre los propios dispositivos y sistemas electrónicos³. El principal reflejo legislativo de esta realidad es, en el plano internacional, el Convenio de Budapest de 2001, en donde se establecen cuatro grupos de medidas a adoptar a nivel nacional por los Estados firmantes, y que es ratificado por España en 2010⁴.

Así pues, la interacción en el ciberespacio⁵ como resultado de la entrada de nuestra civilización en la era digital⁶ en absoluto escapa de la ciencia jurídica ni, dentro de ésta, del Derecho penal. En concordancia con esta realidad, tanto las Fuerzas y Cuerpos de Seguridad como el Ministerio Fiscal han adaptado progresivamente su estructura organizativa para dar una respuesta más eficaz a la ciberdelincuencia⁷.

3. ESTADO DE LA CUESTIÓN

La utilización masiva de páginas de internet y aplicaciones informáticas que permiten interactuar virtualmente con terceros es una de las notas definitorias de la era digital. A propósito de esta realidad, varios autores del ámbito de la ciberseguridad y el Derecho han comenzado a emplear expresiones como *identidad digital* para referir la extensión de nuestra persona en el mundo virtual.

En concreto, el Instituto Nacional de Ciberseguridad (Incibe) publicó en 2012 —cuando aún operaba como Instituto Nacional de Tecnologías de la Comunicación (Inteco)— una guía informativa con recomendaciones político-criminales orientadas a proteger la identidad digital, expresión que definía 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”⁸. Como

² BARRIO ANDRÉS, M.: *Ciberdelitos: amenazas criminales del ciberespacio*, Reus, Madrid, 2017, pp. 23-25.

³ BARRIO ANDRÉS, M.: *Ciberdelitos...*, *op. cit.*, pp. 27-30.

⁴ *Cfr.* Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 (BOE, 17-09-2010). En el Capítulo II del citado Instrumento se recogen los cuatro grupos de ciberdelitos.

⁵ Definido por la RAE como “ámbito artificial creado por medios informáticos”. RAE: *Diccionario de la Lengua Española*, 2020.

⁶ El uso de este término en el contexto jurídico se encuentra, de manera destacada, en el Preámbulo (§ IV) de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales (BOE 06-12-2018).

⁷ *Cfr.* MENDO ESTRELLA, Á.: “Delitos y redes sociales: Mecanismos formalizados de lucha y delitos más habituales. El caso de la suplantación de identidad”, *Revista General de Derecho Penal*, 22, 2014, pp. 3-11.

⁸ INTECO: *Guía para usuarios: identidad digital y reputación online*, Ministerio de Industria, Energía y Turismo, Gobierno de España, Madrid, 2012, p. 5.

se observa, el término se utiliza en alusión a un bien que pertenece no sólo a las personas físicas, sino también a las personas jurídicas. En una línea similar, un reciente análisis publicado por el Real Instituto Elcano⁹, dirigido principalmente a empresas, estudia el marco regulatorio de la identidad digital en España y en la Unión Europea, distinguiendo otra vez entre identidad digital (“quiénes somos en [internet]”) y reputación *online* (“qué dicen de nosotros en la [red]”).

Las definiciones anteriores, si bien contribuyen a delimitar una nueva realidad con trascendencia jurídica, adolecen, a nuestro juicio, de una cierta ausencia de rigor e imprecisión. El primer objetivo de este trabajo será proponer un concepto de *identidad digital* que corrija esas carencias.

Puesto que nuestro campo de estudio es el Derecho penal, el siguiente paso será analizar la tutela que recibe la identidad digital bajo la legislación penal vigente. Esta labor queremos llevarla a cabo, primero, desde una perspectiva amplia y teórica: el alcance (directo o indirecto) de la tutela, los bienes jurídicos vinculados a la identidad digital y, en fin, el modo en que la protección de la identidad se traslada al ámbito digital.

La literatura no se ha ocupado todavía de esta cuestión en términos generales. Empero, sí existen revisiones doctrinales de la normativa penal en torno al hecho delictivo específico en el que se manifiesta la mayor agresión a la identidad digital: las suplantaciones de identidad en redes sociales. Este grupo de conductas no está contemplado en el citado Convenio de Budapest, ni ha encontrado recepción expresa en el Código Penal español a raíz de las reformas de 2010 y 2015. El motivo, quizá, es que se consideró que estas acciones ya encontraban acogida en el tipo de usurpación de estado civil (art. 401 CP), castigado en nuestro ordenamiento desde el siglo XIII. Sin embargo, es discutible que el citado tipo, en su redacción original, pueda adaptarse perfectamente al plano virtual. Así, en relación con el encaje que ha de darse a la suplantación de la identidad digital en nuestro ordenamiento, encontramos posturas diversas:

a) Un sector de la doctrina, encabezado por Díaz López¹⁰, argumenta que el tipo de usurpación de estado civil es aplicable, sin necesidad de modificación alguna, a la totalidad de comportamientos de suplantación de identidad ajena que merecen reproche penal. Así, los actos que quedan impunes serían las mismas “bromas u ostentaciones” que ya carecen de tipificación en el mundo físico¹¹. Esta visión es compartida por De la Mata Barranco, para

⁹ ALONSO LECUIT, J.: *Identidad digital y seguridad online*, Real Instituto Elcano, Madrid, 2020.

¹⁰ DÍAZ LÓPEZ, J. A.: *El delito de usurpación del estado civil*, Dykinson, Madrid, 2010.

¹¹ De negar la subsumción de estos supuestos en el art. 401 CP, “se estaría creando una laguna de punibilidad que afectaría a la correcta protección de un derecho fundamental, cuando realmente es posible *de lege lata* interpretar el precepto de forma que excluya dicha laguna”. DÍAZ LÓPEZ, J. A.: *El delito...*, *op. cit.*, pp. 135-138.

quien todo desvalor de resultado *relevante* derivado de estas conductas es subsumible en el art. 401¹², y por Bicarregui Garay¹³, entre otros.

Los restantes grupos de opinión cuestionan que la suplantación de identidad en internet pueda ser objeto de punición a través del citado precepto, y sugieren hasta un total de cinco alternativas.

b) La fiscal Rodríguez Fernández propone reconducir estos supuestos a la falsedad documental, haciendo una interpretación extensiva del concepto de *documento* a efectos jurídico-penales¹⁴. De esta interpretación se hace eco, principalmente, Magro Servet¹⁵. Cabe notar que determinados actos de suplantación de identidad en el espacio físico han sido castigados por este grupo de delitos¹⁶.

c) Por su parte, Barrio Andrés apunta que la reforma penal de 2015 incluyó este fenómeno a través del art. 197 y, en particular, de la circunstancia agravante del art. 197.4.b), que impone una pena superior a la prevista para el tipo genérico de descubrimiento y revelación de secretos cuando los actos se llevan a cabo mediante la utilización no autorizada de datos personales de la víctima¹⁷. Esta tesis está en línea con la exposición de Tomás-Valiente Lanuza, que apunta adicionalmente al art. 197 bis como posible vía de sanción penal¹⁸. Esta visión parte de la (correcta) consideración de que las lesiones a la intimidad son habituales en estas suplantaciones.

d) Al analizar este asunto, Davara Rodríguez hizo referencia también, junto con las propuestas anteriores, al tipo de daños informáticos del art. 264 CP, que castiga a quienes deterioren, alteren o hagan inaccesibles datos informáticos, entre otras conductas¹⁹.

e) La Fiscalía General del Estado (FGE) comenta la posible subsunción de los actos mencionados en el tipo de acoso moral (art. 172 ter CP), que se acabaría introduciendo en nuestro ordenamiento penal a través de la reforma de 2015. No obstante, la FGE acusa que sólo en algunos supuestos podría apreciarse tipicidad (de forma que “no [se recogen] las acciones que consistan en utilizar aspectos de la identidad de otra persona hasta el punto de originar frente a terceros un error sobre la verdadera identidad del suplantador”), haciendo

¹² En GONZÁLEZ RUS, J. J., y otros: “Delito e informática: algunos aspectos”, *Cuadernos penales José María Lidón*, 4, 2007, pp. 71-72.

¹³ BICARREGUI GARAY, J.: “El fraude on-line: Nuevo escenario, vieja picaresca”, *Boletín de Estudios Económicos*, 194, 311-332, 2008, p. 318.

¹⁴ Cfr. RODRÍGUEZ FERNÁNDEZ, M. P.: “Suplantación electrónica de identidad. Posible respuesta jurídica penal”, *Diario La Ley*, 7906, 2012.

¹⁵ MAGRO SERVET, V.: “La tipificación penal de la suplantación de identidad en el uso de las redes sociales”, *Diario La Ley*, 9005, 2017, pp. 7-10.

¹⁶ STS 02-03-2016 (Cendoj, ECLI:ES:TS:2016:923).

¹⁷ BARRIO ANDRÉS, M.: *Ciberdelitos...*, op. cit., p. 81.

¹⁸ Cfr. TOMÁS-VALIENTE LANUZA, C.: “Delitos contra la intimidad y redes sociales (en especial, en la jurisprudencia más reciente)”, *Revista de Internet, Derecho y Política*, 30, 30-41, 2020.

¹⁹ Cfr. DAVARA RODRÍGUEZ, M. A.: “Suplantación de identidad en la Red”, *El consultor de los ayuntamientos*, 20, 2012.

acto seguido una propuesta de delito autónomo de suplantación de identidad en internet²⁰. Antes de que el citado art. 172 ter estuviera vigente, la Asociación Profesional de Expertos Contables y Tributarios de España (AECE) ubicaba el tipo de coacciones (art. 172) como alternativa junto con algunas de las opciones ya mencionadas²¹.

f) En último lugar, extramuros del Derecho penal, algunas conductas consistentes en la creación de perfiles falsos en internet han sido castigadas como ilícitos civiles por la Agencia Española de Protección de Datos (AEPD)²². Lo subrayan, entre otros, Magro Servet²³.

Esta diversidad de líneas doctrinales no es sino reflejo de la necesidad de una revisión profunda de estas conductas delictivas. Dice acertadamente Gordon Benito: “Lo que es seguro es que, a día de hoy, la figura de la suplantación de identidad *online* es inexistente. Es un punto muerto irrazonable a la espera de una intervención político-criminal que no acaba de llegar”²⁴. Por ende, tras el análisis general sobre la protección penal de la identidad general, trataremos de dilucidar esta problemática concreta.

Interesa señalar que la importancia de este grupo de conductas no es menor: el número de casos de usurpación de estado civil en el ámbito digital conocidos anualmente por las Fuerzas y Cuerpos de Seguridad del Estado, bien por medio de denuncia interpuesta, o bien por labores preventivas o actuaciones en el marco de una investigación policial, aumentaron casi el triple entre 2012 (1.617 hechos conocidos) y 2019 (un total de 4.244)²⁵.

Sin ánimo de ser exhaustivos, cabe mencionar que esta discusión no es exclusiva de nuestro ordenamiento. Díaz López²⁶ se hace eco de algunas de las iniciativas legislativas promovidas en otros países de nuestro entorno, como Argentina y, especialmente, Chile²⁷. Por su parte, algunos estados de Estados Unidos han llegado a contemplar la figura penal de *identity theft* (“robo de identidad”) en reformas recientes²⁸. Finalmente, cabe mencionar el estudio de la OCDE —hoy desclasificado— acerca de la identidad digital (*digital identity*)²⁹.

²⁰ FGE: *Memoria elevada al Gobierno de S.M. presentada al inicio del año judicial por el Fiscal General del Estado*, Ministerio de Justicia, Gobierno de España, Madrid, 2014, p. 742-749. La *Memoria* alerta sobre la falta de tipificación específica de “los comportamientos consistentes en la usurpación de identidad de otra persona en la red y, en general, a través de los medios electrónicos, [con independencia de la tutela prevista] en atención al contenido infamante o injurioso [o] como consecuencia del acceso ilícito a secretos o informaciones de carácter reservado”. Este tipo de conductas, prosigue, pueden provocar un perjuicio “en el normal desarrollo de la vida y actividad personal y profesional”, y, sin embargo, carecen de “una respuesta [penal] adecuada”.

²¹ AECE: “La suplantación de una identidad digital”, *Cont4bl3*, 45, 38, 2013.

²² Cfr. EDITORIAL LA LEY: “Primera sanción de la AEPD al responsable de crear un perfil falso en una red social”, *Diario La Ley*, 7720, 2011.

²³ MAGRO SERVET, V.: “La tipificación...”, *op. cit.*, pp. 8-11.

²⁴ GORDON BENITO, I.: “Suplantaciones...”, *op. cit.*, p. 8.

²⁵ Datos del Sistema Estadístico de Criminalidad, Ministerio del Interior, Gobierno de España, 2020.

²⁶ Cfr. DÍAZ LÓPEZ, J. A.: *El delito...*, *op. cit.*, pp. 77-116.

²⁷ Cfr. MATUS ACUÑA, J. P. y HERNÁNDEZ BASUALTO, H.: “Anteproyecto de Código Penal Chileno de 2005, elaborado por la Comisión Foro Penal”, *Política Criminal*, 1(1), 1-92, 2005.

²⁸ Cfr. STEPHAN, M. J., y otros: “Identity burglary”, *Texas Review of Law & Politics*, 13(2), 401-418, 2009.

²⁹ RUNDLE, M., y otros: *At a crossroads: “personhood” and digital identity in the information society*. Dirección de Ciencia, Tecnología e Industria de la OCDE, 2008, p. 22.

II. DELIMITACIÓN CONCEPTUAL DE LA IDENTIDAD DIGITAL

Para examinar la tutela que nuestro Derecho penal extiende a la identidad digital, es conveniente proponer antes una definición técnico-jurídica de ese concepto. Esta tarea, a su vez, debe comenzar por lo general: la *identidad* a secas.

Como soporte teórico, nos serviremos de la Real Academia Española y haremos un breve repaso del tratamiento que ha recibido la identidad en la literatura filosófica. A continuación, estudiaremos si puede extraerse un concepto jurídico de identidad de nuestro Derecho, atendiendo principalmente a normas supranacionales y a la Constitución. Llegado este punto, se trasladará el concepto al plano de lo digital, discutiendo la inclusión de nuevos componentes puramente virtuales.

1. PRIMERA APROXIMACIÓN: SIGNIFICADO COMÚN Y CONCEPCIÓN FILOSÓFICA

Procedente del latín *idem* ‘el mismo’, la voz *identidad* se utiliza en el ámbito cotidiano con varias acepciones, de las cuales nos interesa mencionar dos:

- (i) “conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás”, y
- (ii) “conciencia que una persona o colectividad tiene de ser ella misma y distinta a las demás”³⁰.

Ambos significados comparten un aspecto: la caracterización o distinción de la persona o el colectivo con identidad, frente al resto de personas o colectivos. Mientras que la primera acepción parece referirse a este aspecto desde una perspectiva externa —pues habla de los *rasgos* del sujeto, de forma más bien descriptiva-objetiva—, la segunda presenta una vertiente interna de la identidad —alude a su *conciencia*—. Se infiere, por tanto, una doble cara de la identidad. Por otra parte, se pone de manifiesto el carácter referencial de la identidad; dicho en otras palabras: “La identidad no es una persona; es sólo una referencia a una persona”³¹.

Hecha esta aclaración inicial, interesa exponer la visión filosófica de diferentes autores sobre el concepto que estamos abordando, siempre desde el punto de vista del individuo (la identidad *colectiva* no es relevante a nuestro análisis).

Aunque más superficialmente, los pensadores griegos habían realizado algunas postulaciones a este respecto. Aristóteles planteó la noción de que cada ser humano es capaz de juzgar una situación y entender qué comportamiento debe adoptar para lograr el “bien

³⁰ REAL ACADEMIA ESPAÑOLA: *Diccionario de la Lengua Española*, 2020.

³¹ RUNDLE, M., y otros: *At a crossroads...*, *op. cit.*, p. 26.

verdadero”. Su conducta será virtuosa —y, de este modo, *buena*— si se adecúa a esta deliberación; en cambio, su conducta estará guiada por el “vicio” —lo cual no es deseable— si obedece a motivos diferentes de lo que dicta la razón³². Observamos aquí una reflexión sobre la conciencia del sujeto como ser dotado de autonomía que puede verse afectado por elementos externos³³. Siglos más tarde, Agustín de Hipona mantiene el esquema anterior, añadiendo la presencia de “Dios” como fuerza capaz de imponer un castigo a aquella persona que no actúa rectamente³⁴.

Cuando irrumpe Descartes en el panorama filosófico, crece la atención hacia el individuo, que es definido como el ser que, por garantía divina, piensa (*res cogitans*) y se presenta al mundo exterior (*res extensa*) con una serie de cualidades primarias que se pueden medir y cuantificar objetivamente —la extensión, tamaño, figura y movimiento— y con otras cualidades secundarias —el olor, el color, el gusto, entre otras— que dependen más bien de la interpretación subjetiva³⁵. En una línea similar a los autores anteriores, Kant profundiza sobre la autonomía humana, y defiende la existencia de un principio moral universal que debemos obedecer a fin de obrar bien³⁶.

Rechazando la tradición filosófica anterior, Nietzsche considera que el ser humano no está encaminado a ningún fin³⁷, y habla la propia personalidad como un proceso sujeto a una mutabilidad constante y dirigido a obtener la versión “ideal” de uno mismo³⁸. Este primer contacto con el psicoanálisis es continuado por autores como Freud, quien distingue el *yo* como la instancia psíquica encargada de equilibrar, de un lado, los deseos y estímulos externos (el *ello*), y, del otro, las restricciones que nos imponemos (el *superyó*)³⁹. Kierkegaard, por su parte, introduce la idea de que los seres humanos tendemos a compararnos constantemente con los demás, sintiéndonos *abrumados*, lo que nos impide reflexionar sobre quiénes somos en realidad⁴⁰. Como última idea a mentar, la fenomenología de Husserl subraya el papel de las relaciones intersubjetivas en la determinación de nuestra identidad: ésta no sólo será el resultado de indagar en las convicciones propias, sino también de interactuar con el exterior⁴¹.

Pese a la presencia de posturas contradictorias, pueden extraerse algunas conclusiones:

³² Cfr. ARISTÓTELES: *Ética a Nicómaco*, Alianza Editorial, Madrid, 2005.

³³ ESTRADA DÍAZ, J. A.: “Del primado del cosmos al descubrimiento de la subjetividad interior”; en P. Gómez García (coord.): *Las ilusiones de la identidad*, Universitat de València, Valencia, 2001, p. 204.

³⁴ DE HIPONA, A.: *Del libre albedrío*, trad. E. Seijas, Federación Agustiniana Española, 2005.

³⁵ DESCARTES, R.: *Discurso del método*, trad. M. García Morente, Austral-Espasa Calpe, Madrid (versión en línea), 2010.

³⁶ KANT, I.: *Fundamentación de la metafísica de las costumbres*, trad. M. García Morente, Biblioteca Virtual Miguel de Cervantes, 1999.

³⁷ NIETZSCHE, F.: *Crepúsculo de los ídolos o cómo se filosofa con el martillo*, trad. A. Sánchez Pascual, Alianza Editorial, Madrid, 2013, pp. 60-70.

³⁸ BRAGG, M., y otros: “Authenticity”, *In Our Time*, BBC Radio, 2019.

³⁹ FREUD, S.: *El yo y el ello y otros escritos de metapsicología*, trads. R. Rey Ardid y L. López-Ballesteros y de Torres, Alianza Editorial, Madrid, 2012.

⁴⁰ KIERKEGAARD, S.: *Edifying discourses: A selection*, trads. D. F. Swenson y L. M. Swenson, Harper & Brothers, Nueva York (versión en línea), 1958, pp. 237-242.

⁴¹ HUSSERL, E.: *Meditaciones cartesianas*, trads. J. Gaos y M. García-Baro, Foro de Cultura Económica, México (versión en línea), 1996, pp. 185-194.

a) En línea con las primeras acepciones de identidad que se indicaron, se aprecia una dicotomía entre la conciencia del individuo —su pensamiento— y su aspecto y comportamiento externos —la *res extensa*—. Cuando se habla de personalidad, se está haciendo referencia a la segunda vertiente.

b) Respecto de esa parte exterior, en un individuo pueden distinguirse una serie de caracteres que se pueden medir objetivamente (p. ej., el tamaño), mientras que el valor de otros caracteres depende del sujeto que las observa (el gusto).

c) Además, la personalidad está sujeta a cambios constantes, que se derivan tanto de la reflexión interna del sujeto —quien obedece a estímulos y restricciones— como de su relación con otros.

d) El sujeto tiende a compararse con otros, así como a buscar formas de diferenciarse.

e) Existe una evidente relación entre la identidad del sujeto y su autonomía o libre albedrío.

En suma, puede afirmarse que la identidad presenta una dimensión interna y otra externa, esta última comprendida, a su vez, por unos atributos ciertos o estables —objetivamente mensurables—, y otros más bien subjetivos. Este conjunto de rasgos, que puede variar con el tiempo, nos definen e individualizan con respecto a las demás personas. Por último, la identidad tiene gran importancia por ser consustancial a la autonomía del individuo: se es diferente de los demás por manifestar a terceros —en nuestra libertad— esos atributos.

2. EL CONCEPTO DE IDENTIDAD EN NUESTRO DERECHO

En vista de que la identidad individualiza a la persona y se origina de su libre albedrío, no sería extraño que el Derecho se preocupara por dotarla de alguna clase de relevancia. Comprobaremos a continuación que esta preocupación sí existe, aunque no se traduce en una regulación precisa de la identidad.

A) Menciones a la identidad en las legislaciones internacional e interna⁴²

La mención más explícita de la identidad como concepto con connotación jurídica se hace en una norma del Derecho internacional. Se trata del artículo 8 de la Convención sobre los Derechos del Niño (CDN)⁴³, cuyo primer párrafo establece: “Los Estados Partes se

⁴² Nos basamos en la exposición que se encuentra en GÓMEZ BENGOCHEA, B.: *Derecho a la identidad y filiación*, Dykinson, Madrid, 2007, pp. 49-74.

⁴³ Instrumento de Ratificación de la Convención sobre los Derechos del Niño, adoptada por la Asamblea General de las Naciones Unidas el 20 de noviembre de 1989 (BOE, 31-12-1990).

comprometen a respetar el derecho del niño a preservar su identidad, incluidos la nacionalidad, el nombre y las relaciones familiares [*sic*] de conformidad con la ley sin injerencias ilícitas”. Por su parte, el art. 7 CDN exige la inscripción del nacimiento y reconoce los derechos de todo niño al nombre, a la nacionalidad y, “en la medida de lo posible, a conocer a sus padres y a ser cuidado por ellos”.

Si acudimos a la jurisprudencia internacional, debe destacarse el caso *Gaskin contra Reino Unido*, sustanciado en el Tribunal Europeo de Derechos Humanos (TEDH). El objeto de este asunto era determinar si las autoridades británicas podían denegar el acceso del demandante a un expediente en el que figuraba información sobre los años de su infancia en que estuvo bajo la tutela de varias familias. Mientras que Reino Unido invocaba la vulneración del interés público para restringir la difusión del expediente, el TEDH afirmó lo siguiente: “El respeto de la vida privada exige que cualquier persona esté en condiciones de asentar con detalle su identidad [...] y que, en principio, la Administración no le impida, sin motivo justificado, conseguir estas informaciones fundamentales”⁴⁴.

A diferencia de lo que sucede en el Derecho internacional, nuestra Constitución no se refiere a la identidad (personal) de manera expresa⁴⁵. Este silencio no es exclusivo de España: con excepción de una minoría de ordenamientos jurídicos⁴⁶, puede apreciarse una cierta reticencia a proteger la identidad en un sentido literal. Con todo, comoquiera que los tratados internacionales válidamente celebrados por España se insertan en el ordenamiento interno (art. 96.1 CE), cabe trasladar las consideraciones antes expuestas a nuestro Derecho.

Si descendemos en la pirámide normativa, observamos que las leyes y las normas reglamentarias nacionales tienden a utilizar la voz *identidad* de manera más restrictiva, en alusión a los datos que permiten la identificación de alguien de manera más inmediata, es decir, el nombre y los apellidos. Este parece ser el significado que se le da a lo largo de la LRC⁴⁷ (arts. 4, 6, 11, 15 y 44, entre otros).

B) Caracterización de la identidad en cuanto objeto

A nuestro juicio, las fuentes anteriores permiten distinguir dos vertientes de la identidad: por un lado, el *objeto* compuesto por el nombre, la nacionalidad y las relaciones familiares (o,

⁴⁴ STEDH 07-07-1989 (HUDOC, ECLI:CE:ECHR:1989:0707JUD001045483), anexo. Realmente, aquí el TEDH está citando a la Comisión Europea de Derechos Humanos, órgano que se encargaba de revisar *ex ante* las demandas que se dirigían al TEDH. Ese órgano se suprimió en 1998 a través del Protocolo n.º 11 al CEDH, relativo a la reestructuración del mecanismo de control establecido por el Convenio, el cual convirtió al TEDH en órgano único y le dotó de carácter permanente.

⁴⁵ La única mención literal a la identidad se hace en el art. 147.2 CE, que dispone como contenido obligatorio de los Estatutos de autonomía “la denominación de la Comunidad que mejor corresponda a su identidad *histórica*”.

⁴⁶ GÓMEZ BENGOCHEA, B.: *Derecho...*, *op. cit.*, p. 61.

⁴⁷ Ley 20/2011, de 21 de julio, del Registro Civil (BOE 22-07-2011). Si bien esta ley no se encuentra en pleno vigor a día de hoy (en principio, lo hará el 30 de abril de 2021), su contenido apenas difiere del texto de 1957.

en sentido más restringido, sólo el nombre y los apellidos); por el otro, el *derecho*⁴⁸ a indagar en la historia personal del sujeto, incluyendo sus orígenes biológicos⁴⁹ y la tutela recibida durante la infancia. Por ser la que más se adecúa a los propósitos de este trabajo, en adelante se empleará *identidad* para referirse a la primera de las dos vertientes, en sentido amplio.

Partiendo de esta concepción de la identidad en cuanto objeto, podemos distinguir una serie de rasgos comunes a sus tres elementos. En efecto, todos ellos son aspectos (i) exteriorizados, de forma que la conciencia queda excluida del concepto jurídico de identidad; (ii) con relevancia social, al ser susceptibles de ser conocidos y compartidos en las relaciones cotidianas —frente a, por ejemplo, el domicilio, de carácter más reservado, o el número de identificación fiscal, cuya relevancia se reduce a determinadas relaciones jurídicas—; (iii) esencialmente estables, aunque sea posible su alteración (cambiando de nombre, perdiendo la nacionalidad o contrayendo matrimonio, entre otras formas), y (iv) objetivos u objetivo-normativos⁵⁰, en la medida en que se pueden constatar empíricamente con independencia del sujeto observador.

C) *El estado civil como correlato de la identidad*

Tras haber alcanzado una definición jurídica de identidad, puede observarse su gran parecido con otra figura nacida en el Derecho romano⁵¹ y presente en la mayoría de ordenamientos comparables: el estado civil. De hecho, Díaz López sugiere que si la identidad personal es la condición necesaria para su autonomía en el ámbito cotidiano, el estado civil cumple esa misma función en el ámbito jurídico⁵². Similarmente, Boix Reig afirma: “Puede decirse que el estado civil delimita atributos jurídicos de la personalidad. Permite su identificación”⁵³.

⁴⁸ Gómez Bengoechea resalta la “tradicional falta de positivación [de la identidad] como un derecho autónomo con sustantividad propia, tanto en el plano internacional como en el Derecho interno», en GÓMEZ BENGOCHEA, B.: *Derecho...*, *op. cit.*, p. 49. Por su parte, la identidad se califica de derecho de la personalidad en ENCABO VERA, M. A.: *Derechos de la personalidad*, Marcial Pons, Madrid, 2012, p. 101.

⁴⁹ Esta cuestión, que escapa del ámbito de nuestro trabajo, se analiza en relación con el marco regulatorio actual en DE MONTALVO JÄÄSKELÄINEN, F. y otros: *Informe de Comité de Bioética de España sobre el derecho de los hijos nacidos de las técnicas de reproducción humana asistida a conocer sus orígenes biológicos*, Comité de Bioética de España, Madrid, 2020.

⁵⁰ La nacionalidad, el nombre y las relaciones familiares de una persona son, *prima facie*, objetivas, aunque hay algunos conceptos —como *patria potestad*— cuyo significado requiere de una valoración a través de normas jurídicas. La distinción entre descriptivo y normativo es propia del ámbito penal —que es, al cabo, nuestra área de investigación—. Cfr. OBREGÓN GARCÍA, A. y GÓMEZ LANZ, J.: *Derecho Penal. Parte General: Elementos básicos de teoría del delito*, Tecnos, Madrid, 2015, pp. 72-73.

⁵¹ En concreto, procede de la suma de tres *stati*: el *status civitatis* o posición del individuo en la comunidad política (ciudadano, latino o peregrino), el *status familiae* o situación en el ámbito familiar (titular de la patria potestad o sujeto a ella) y el *status libertatis* o condición social (libre o esclavo). Véase MANTILLA MOLINA, R. L.: “Sobre el concepto de *status*”, *Revista de la Facultad de Derecho de México*, 29, 1958.

⁵² DÍAZ LÓPEZ, J. A.: *El delito...*, *op. cit.*, p. 29.

⁵³ BOIX REIG, J.: *El delito de usurpación de estado civil*, Universidad de Valencia, Valencia, 1980, p. 28.

Ello nos obliga a abordar el contenido del estado civil. Desafortunadamente, estamos ante una cuestión controvertida, puesto que este concepto “es empleado por diversos agentes jurídicos y sociales con cierta ligereza, difuminando aún más la distinción entre estado civil e identidad”⁵⁴. Para adoptar una postura en torno a esta discusión, comenzamos acudiendo a tres fuentes:

a) La Ley 20/2011, de 21 de julio, del Registro Civil (LRC)⁵⁵ hace una referencia clave a esta figura en su art. 2.2, al disponer que “el Registro Civil tiene por objeto hacer constar oficialmente los hechos y actos que se refieren al estado civil de las personas y aquellos otros que determine la presente Ley”. Por su parte, el art. 4 LRC enumera una lista cerrada de 15 categorías de hechos inscribibles. Inferimos entonces que todos los datos relativos al estado civil se inscriben en el Registro —por tanto, se encuentran en la citada lista—, si bien no todos los hechos inscribibles son elementos del estado civil.

b) El Diccionario del Español Jurídico define *estado civil* como “condición de una persona en relación con su nacimiento, nacionalidad, filiación o patrimonio, que se hacen constar en el Registro Civil y que delimitan el ámbito propio de poder y responsabilidad que el [Derecho] reconoce a las personas naturales”⁵⁶.

c) Un informe de 2018 de la Comisión Internacional del Estado Civil (CIEC), organismo intergubernamental del que España es miembro, lo expresa como “la situación (*status*) de la persona en Derecho privado, entre su nacimiento y su muerte”, que está comprendida por filiación, nacionalidad, apellidos, nombre, domicilio, edad, sexo y capacidad jurídica. Estos elementos “diferencian a cada persona de los demás”⁵⁷.

El denominador común de estos textos está en dos grandes elementos: las *relaciones familiares* (donde se incluyen aspectos como la filiación, los apellidos, el nacimiento, la edad, el sexo⁵⁸ y la capacidad jurídica⁵⁹) y la *nacionalidad* (la cual abarca también la vecindad civil). Surgen dudas, no obstante, respecto de otros dos componentes:

a) Primero, el *nombre*, rasgo nuclear de la identidad. Dada la estrecha relación entre éste y los apellidos (que sí son parte del estado civil) y que la propia inscripción del nacimiento en el Registro debe ir acompañada del nombre, estimamos razonable incluirlo en el concepto⁶⁰.

⁵⁴ DÍAZ LÓPEZ, J. A.: *El delito...*, *op. cit.*, p. 119.

⁵⁵ Si bien esta ley no se encuentra en pleno vigor a día de hoy (en principio, lo hará el 30 de abril de 2021), su contenido apenas difiere del texto de 1957.

⁵⁶ RAE y CGPJ: *Diccionario del español jurídico*, 2020.

⁵⁷ MASSIP, J., y otros: *Commission Internationale de l'Etat Civil (CIEC)*, Kluwer Law Online, 2018, p. 8.

⁵⁸ Sin significar un traslado a “épocas sombrías” en donde ser hombre o mujer tenía repercusión en la capacidad jurídica del individuo, aceptamos que el sexo forma parte del estado civil. *Cfr.* DÍAZ LÓPEZ, J. A.: *El delito...*, *op. cit.*, p. 125.

⁵⁹ La capacidad jurídica de un individuo se ve limitada fundamentalmente por razón de su minoría de edad, que le hace estar sujeto a la patria potestad de sus padres o, en su defecto, a tutela.

⁶⁰ *Cfr.*, por ejemplo, QUINTERO OLIVARES, G., y otros: *Comentarios al Código Penal Español*, Aranzadi, Madrid, 1995, t. 2, pp. 1252-1253.

b) Segundo, el *domicilio*, que debemos rechazar, por cuanto no figura en la lista cerrada del art. 4 LRC. La exclusión es coherente con la posibilidad de tener múltiples domicilios en función de distintos factores (art. 40 CC).

El Derecho privado es la rama jurídica donde más trascendencia tiene el estado civil, pero no la única: el Código Penal hace mención de esta expresión en el art. 401, al tipificar la usurpación de estado civil. Esta dualidad ha llevado a autores como Rodríguez Devesa a distinguir entre el estado civil iuscivilista de aquél en el plano jurídico-penal, buscando simplificar así las dificultades que existen sobre su exacto contenido⁶¹. En nuestra opinión, desde el momento en que existe una lista cerrada y en absoluto extensa del contenido del estado civil en el art. 4 LRC, el estado civil deja de ser un concepto jurídico *tan* indeterminado como para justificar esta separación ficticia. Es de rigor afirmar, en línea con Boix Reig⁶², que estamos ante un único concepto.

Esto último no obsta a que el mencionado término sea utilizado en ocasiones con un sentido más estricto refiriendo la situación de soltero, casado o viudo de alguien (el estado civil *familiar*). Ésta es la acepción que adopta en el lenguaje vulgar⁶³, así como en determinadas normas jurídicas.

En suma, observamos que el estado civil consta del mismo contenido que la identidad en cuanto *objeto*: nombre, nacionalidad y relaciones familiares. Además, los caracteres del estado civil, según los describen Díez-Picazo y Gullón⁶⁴, son coherentes con los caracteres que se señalaron respecto de la identidad. Estos autores hablan de cuatro notas: la personalidad, pues toda persona tiene su propio estado civil como haz de cualidades propias; el orden público, en tanto que el estado civil de un sujeto tiene relevancia no sólo individual, sino social; la eficacia *erga omnes*, “al [extenderse] la autoridad de cosa juzgada de las sentencias sobre el estado civil a todos los terceros” *ex* art. 1252 CC, y el carácter imperativo de las normas que lo regulan.

3. DELIMITACIÓN DE LA IDENTIDAD DIGITAL

Dado que *identidad* es un término con escasa presencia en nuestro Derecho, no sorprende que la legislación vigente no se refiera a una identidad *digital*. Con todo, según indicábamos en el capítulo I de este trabajo, sí se ha empleado el término en el ámbito académico.

Es posible hablar de una identidad digital porque, a día de hoy, el libre desarrollo de nuestra personalidad ya no se circunscribe al espacio físico. Acaso la manifestación más

⁶¹ RODRÍGUEZ DEVESA, J. M. y SERRANO GÓMEZ, A.: *Derecho...*, *op. cit.*, p. 260.

⁶² BOIX REIG, J.: *El delito...*, *op. cit.*, p. 26.

⁶³ La segunda acepción de *estado civil* que proporcionaba el Diccionario de la Lengua Española de la RAE de 2001 era “condición de soltería, matrimonio, viudez, etc., de un individuo”.

⁶⁴ Díez-PICAZO, L. y GULLÓN, A.: *Sistema de Derecho civil. Vol. I*, Tecnos, Madrid, 1989, pp. 248-249.

evidente de ello se encuentra en la facilidad que tenemos para crear, libre y voluntariamente, perfiles personales en redes sociales, blogs, foros y otras aplicaciones comparables. Así pues, partiendo del concepto de identidad postulado, la identidad digital sería el resultado de la *digitalización* de la identidad, es decir, la manifestación o utilización de nuestra identidad (analógica⁶⁵) en el ciberespacio.

A) *Nuevos elementos de la identidad digital*

Ahora bien: en la medida en que la era digital ha redefinido las relaciones sociales y jurídicas, consideramos que es necesario revisar si el contenido de la identidad digital se ha visto alterado o, mejor dicho, ampliado. En este sentido, nuestra tesis es la siguiente: mientras que la era digital no ha dotado de nuevo contenido a las relaciones familiares —no existe, por ejemplo, una institución equiparable al matrimonio que tenga naturaleza puramente digital— ni a la nacionalidad, sí podría decirse que el papel que cumple el *nombre* de una persona se complementa con nuevas formas de identificarla en el ciberespacio. Si éstas reúnen los caracteres propios de la identidad —exteriorización, relevancia social, estabilidad esencial y objetivo-normatividad— no parece atrevido afirmar que la identidad digital abarca *nuevos* elementos.

Dicho lo anterior, se justifica a continuación la inclusión de otros tres (micro)elementos en el contenido de la identidad digital que ampliarían el alcance del nombre:

a) Número de teléfono. En términos generales, el teléfono móvil es el medio de comunicación no presencial más inmediato en nuestra sociedad. Sea vía llamada, sea mediante un mensaje en una plataforma de mensajería descargada en el dispositivo (ligada, normalmente, a ese número), permite a un usuario contactar directamente con otro. Nuestra postura se ve reforzada por el hecho de que el número telefónico ha sido considerado por la jurisprudencia como un dato personal⁶⁶.

b) Dirección de correo electrónico. Aunque el correo electrónico pertenece más bien a la esfera profesional, no puede obviarse que su dirección funciona como credencial para acceder a perfiles de numerosos sitios de internet de carácter social (*v. gr.*, redes sociales o blogs). La relevancia que tiene este dato a efectos identificativos reside, como ha reiterado la AEPD, en que “se forma por un conjunto de signos o palabras libremente elegidos generalmente por su titular, con la única limitación de que dicha dirección no coincida con la correspondiente a otra persona”⁶⁷. Por si fuera poco, cuando la combinación elegida carece de significado,

⁶⁵ Este término es utilizado en INTECO: *Guía...*, *op. cit.*, p. 7.

⁶⁶ “Es claro que un número telefónico asociado a un nombre y apellidos es un dato de carácter personal [...]. Es más, [...] sin aparecer directamente asociado a una persona, puede tener la consideración de dato personal si a través de él se puede identificar a su titular”. SAN 17-09-2008 (Cendoj, ECLI:ES:AN:2008:3250), FJ 4.º.

⁶⁷ Informe AEPD 16-02-2011 (AEPD, 0437/2010), p. 1.

todavía es posible rastrear a su usuario a partir de su dirección IP. Por ello, el citado Informe de la AEPD entiende que la dirección de correo electrónico es un dato personal en todo caso⁶⁸. A efectos de nuestro trabajo, sólo lo será si se puede identificar a su titular *directamente* (no a través, por ejemplo, del citado rastreo).

c) Nombre de usuario de red social. Esta inclusión es acaso más conflictiva, pues no existen pronunciamientos doctrinales ni jurisprudenciales acerca de su categorización como dato personal. El principal problema reside en la discutible relevancia social en este elemento: en muchos casos, el nombre de usuario no sirve más que para iniciar sesión en la red; en otros, éste coincide con el número de teléfono (el caso de WhatsApp), con la dirección de correo o con ambos datos alternativamente (LinkedIn). Dicho esto, hay dos redes sociales en concreto en las que sí cabría configurar el nombre de usuario como elemento de la identidad digital. Se trata de Instagram y Twitter, cuyo uso en España no es menor: respectivamente, el 65 y el 53 % de la población están familiarizada con ellas⁶⁹. En ambos casos, el nombre de usuario figura como encabezado en cada publicación realizada por ese perfil: en Instagram aparece sólo este dato y la imagen de perfil, mientras que Twitter muestra, junto a estos dos datos, el “nombre de la cuenta”, que podrá coincidir o no con el nombre de quien está detrás de ese perfil. Además, el nombre de usuario se utiliza para mencionar o etiquetar a terceros —de forma que éstos sean notificados— en una publicación.

En la medida en que los datos propuestos sean utilizados por una única persona identificable por sus interlocutores y con ánimo de permanencia, formarán parte del concepto de identidad digital. Por supuesto, habrá supuestos en que surjan dudas, cuales son la tenencia de múltiples números de teléfono, direcciones de correo electrónico o cuentas en una red social. Abarcar toda la casuística excede de los fines de este trabajo; con todo, sí indicaremos que no debería existir, propiamente, un límite teórico. Así, el número del teléfono vinculado a una empresa, por ejemplo, podría ser perfectamente considerado parte de la identidad digital de su titular en adición a su número particular.

B) *Conclusión. Otros usos del concepto*

A modo de resumen, el concepto de identidad digital que se manejará en este trabajo comprende tres macroelementos:

a) El *nombre*, en donde se integrarían, junto con el nombre en sentido estricto —el hecho inscribible en el estado civil—, los datos identificativos de origen digital de análoga naturaleza, concretamente: el número de teléfono, el correo electrónico y el nombre de

⁶⁸ Informe AEPD 16-02-2011 (*cit.*), p. 2.

⁶⁹ Los datos proceden de HOOTSUITE y WE ARE SOCIAL: *Digital 2020: Spain*, 2020, p. 43.

usuario de una red social. Igualmente, no habría problema en incorporar el apodo de una persona, siempre que (nuevamente) cumpla con los requisitos de la identidad⁷⁰.

b) La *nacionalidad*, que abarca también la vecindad civil.

c) Las *relaciones familiares*: el nacimiento —y, relacionado con éste, la edad y el sexo—; la sujeción a la patria potestad de los progenitores o a la tutela de un tercero; la situación de soltero, casado o viudo, y los efectos que las condiciones anteriores presenten en la capacidad jurídica.

Si bien el vínculo entre estado civil e identidad es estrecho, su contenido no es —valga la redundancia— idéntico. Por otra parte, conviene diferenciar entre el significado que estamos dando a este concepto y otros sentidos que le ha dado la doctrina jurídica, más concretamente:

a) La acepción más amplia que utilizan organismos como el Incibe o el Real Instituto Elcano (*cfr.* introducción a este trabajo), que se extiende a *todo* dato que pueda identificar a un individuo en internet, y se propone también para personas jurídicas⁷¹. Nosotros, además de restringir el contenido de la identidad digital, sólo la concebimos para personas físicas.

b) En el contexto de la tecnología de cadena de bloques (*blockchain*) —con la que operan, por ejemplo, el bitc in o los contratos inteligentes—, se habla de la *infraestructura de identidad digital* para designar el registro masivo de datos creado a ra z del uso continuado de dicha tecnolog a⁷². Estos datos no son, ni aspiran a ser, un medio de identificaci n m s all  de esa infraestructura.

⁷⁰ En este sentido, D az L pez defiende interpretar de manera laxa el *nombre* en el  mbito de la usurpaci n de estado civil, considerando que, si puede deducirse en el contexto social concreto qui n est  detr s de un apodo, la acci n ser  t pica. *Cfr.* D AZ L PEZ, J. A.: *El delito...*, *op. cit.*, p. 172.

⁷¹ Adem s de las referencias anteriores, *cfr.* INCIBE: *Ciberseguridad en la identidad digital y la reputaci n online*, Ministerio de Asuntos Tecnol gicos y Transformaci n Digital, Gobierno de Espa a, 2016.

⁷² MART N SIERRA,  .: *Concepto y l mites del 'legal smart contract'*, Universidad Pontificia Comillas, Madrid, 2020, p. 18. En este trabajo se ofrece, adem s, una explicaci n did ctica del funcionamiento de la *blockchain*.

III. TUTELA PENAL DE LA IDENTIDAD DIGITAL

Toda vez que contamos con una definición precisa de *identidad digital*, estamos en disposición de analizar cómo se protege ésta en el Derecho penal español. Como punto de partida, observamos que la identidad, en términos generales, no está tutelada de manera *directa* o explícita por ningún tipo penal, lo que no impide que si a través de un menoscabo de la identidad se lesiona un bien jurídico que sí está penalmente protegido, pueda hablarse de una tutela *indirecta* o implícita de ésta.

El método que utilizaremos en nuestra exposición consistirá en estudiar en qué grado las normas penales que tutelan (implícitamente) la identidad pueden adaptarse al ámbito virtual.

1. ACLARACIONES PREVIAS

Como preámbulo, es menester distinguir dos componentes del tipo penal: el objeto *material* y el objeto jurídico⁷³. El primero es, simplemente, “la persona o cosa sobre la que recae la acción [típica]”; en el tipo de homicidio, el objeto material sería la *víctima*. En cambio, al hablar de objeto *jurídico*, nos referimos al bien jurídico protegido, es decir, el “interés vital para el desarrollo de los individuos de una sociedad determinada, que adquiere reconocimiento jurídico [a través de su tipificación penal]”, siguiendo la definición de Kierszenbaum⁷⁴; en el caso anterior, el objeto jurídico del tipo es la *vida* de la víctima. Esta distinción es importante por lo que hemos anticipado arriba: el propósito de la norma penal es tutelar los objetos *jurídicos* de los tipos: es el menoscabo de éstos lo que determina la realización del tipo (y, en buena parte, la delimitación de la pena), y no el daño sufrido por el objeto *material*, aunque este se produzca indirectamente.

Por otra parte, en nuestra exposición omitiremos el hecho de que la persecución de ciberdelitos en general se ve obstaculizada considerablemente a raíz del potencial anonimato que internet concede a los usuarios, que explica, al menos en parte, el “extraordinario éxito [...] como canal de ejecución delictiva”⁷⁵, así como de su ubicuidad. Esta cuestión procesal, a la que ya nos referimos en la introducción a este trabajo, queda allende nuestro objetivo.

⁷³ Cfr. OBREGÓN GARCÍA, A. y GÓMEZ LANZ, J.: *Derecho Penal...*, *op. cit.*, p. 75.

⁷⁴ KIERSZENBAUM, M.: “El bien jurídico en el Derecho penal. Algunas nociones básicas desde la óptica de la discusión actual”, *Lecciones y Ensayos*, 86, 187-211, Universidad de Buenos Aires, 2009, p. 188.

⁷⁵ BARRIO ANDRÉS, M.: *Ciberdelitos...*, *op. cit.*, p. 37. En las pp. 33-50, el autor aborda en detalle este asunto.

2. LA USURPACIÓN DE ESTADO CIVIL EN EL PLANO DIGITAL

Puesto que, como se ha argumentado previamente, el estado civil guarda una estrecha relación con la identidad, tiene sentido comenzar por el delito de usurpación de estado civil, tipificado en el art. 401 CP. Dispone este precepto: “El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años”.

Nos hallamos ante un delito cuyos orígenes se remontan, por lo menos, al *Liber Iudiciorum*, promulgado por el rey visigodo Recesvinto (siglo VII) y traducido a nuestra lengua en 1241 como *Fuero Juzgo*⁷⁶. Precisamente por las escasas modificaciones que ha sufrido la redacción de este tipo a lo largo de la historia, algunos autores se cuestionan su idoneidad para recoger *nuevas* conductas de supuesta usurpación de estado civil (lo apuntábamos en la introducción).

Con todo, la discusión más relevante acerca de este delito radica en la determinación del bien jurídico protegido. Diferenciamos tres sectores de opinión al respecto:

a) El primero, minoritario, que identifica el estado civil⁷⁷ o, más ampliamente, la “personalidad”⁷⁸ como único interés tutelado basándose en la apariencia de la propia descripción típica y en la ubicación sistemática histórica del delito.

b) El segundo, mayoritario, integrado por autores que consideran el estado civil no como objeto *jurídico*, sino como objeto *material*, siendo el bien jurídico tutelado la seguridad del tráfico jurídico o la fe pública (en este sector, se manejan distintas propuestas)⁷⁹. Basan su postura en la ubicación sistemática del precepto penal (dentro del Título XVII, dedicado a las “falsedades”), en la existencia de tipicidad en supuestos de usurpación del estado civil de una persona fallecida y en la ausencia de una delimitación precisa del concepto de estado civil.

c) Un tercer sector de corte ecléctico que postula la protección conjunta de ambos bienes a través de un tipo *pluriofensivo*⁸⁰. Se reconoce la fe pública como bien jurídico principal, y el estado civil como bien secundario. Aun cuando la jurisprudencia no ha sido consistente sobre el asunto, ésta es la postura con mayor acogida actual: el Supremo ha reiterado “la doble naturaleza [del art. 401]: su aspecto falsario y constituir un atentado contra un bien de carácter personal, el estado civil”⁸¹.

⁷⁶ Un recorrido histórico detallado de la materia se encuentra en DÍAZ LÓPEZ, J. A.: *El delito...*, *op. cit.*, pp. 51-75.

⁷⁷ Así se clasifica en RODRÍGUEZ DEVESA, J. M. y SERRANO GÓMEZ, A.: *Derecho Penal...*, *op. cit.*, p. 266.

⁷⁸ GORDON BENITO, I.: “Suplantaciones...”, *op. cit.*, p. 5.

⁷⁹ Destacadamente, DÍAZ LÓPEZ, J. A.: *El delito...*, *op. cit.*, pp. 156-164 y BOIX REIG, J.: *El delito...*, *op. cit.*, pp. 29-33. También Morillas Cueva en COBO DEL ROSAL, M. (dir.): *Compendio de Derecho penal español*, Marcial Pons, Madrid, 2000, p. 758.

⁸⁰ Así lo considera F. de la Fuente Honrubia, citado en DÍAZ LÓPEZ, J. A.: *El delito...*, *op. cit.*, p. 181.

⁸¹ Por todas, STS 15-06-2009 (Cendoj, ECLI:ES:TS:2009:3931), FJ 2.º.

Consideramos que el quid de este debate reside en delimitar claramente qué es *usurpación*. La jurisprudencia, con relativa uniformidad, ha sentado que usurpar implica suplantar a otra persona apropiándose de sus derechos y obligaciones (ha de “usarlos como si fueran propios”), lo que exige la concurrencia de dolo. No es necesaria una suplantación total, aunque esta sí debe comprender, al menos, el nombre y los apellidos del suplantado⁸². Además, es precisa una cierta “continuidad y persistencia”, factor que debe ser analizado en el caso concreto⁸³. Sin perjuicio de esto último, una sola acción o conducta de “hacerse pasar por otro” no bastará, a juicio de la doctrina mayoritaria, para la realización del tipo⁸⁴.

En vista de esta calificación, parece que, con independencia de que el estado civil del suplantado pueda lesionarse a resultas de la usurpación, la posición que aquél ocupa en el tipo no es otra que la de objeto material; el bien jurídico protegido es, en cambio, la fe pública o la seguridad del tráfico, según defiende la mayoría de autores. Es importante subrayar que la identidad ocupará *siempre* la citada posición, siendo el art. 401 CP el único tipo penal en el que se da este hecho.

El grupo de autores que se inclina por esta postura suele apoyarse en que el art. 401 CP no exige que la persona cuyo estado civil se ha usurpado esté viva. Este argumento presenta sus problemas: pese a que la jurisprudencia tiende a aceptar suplantaciones de personas fallecidas⁸⁵, no faltan casos en los que este extremo se ha rechazado⁸⁶. A nuestro juicio, optar por una decisión u otra no es relevante a los efectos del debate sobre el bien jurídico protegido: puede esgrimirse que cuando la identidad suplantada pertenece a una persona finada, la lesión a la fe pública penalmente punible se ha cometido no tanto mediante una falsedad *personal* cuanto por una falsedad de carácter *documental* del art. 395 (tipo que enseguida trataremos)⁸⁷. En cualquier caso, nos adherimos a la línea de opinión de que la muerte del suplantado no obsta a la tipicidad de la conducta.

No cabe duda de que la realización del tipo en el plano *digital* también afectará, en todo caso, a la identidad digital como objeto material. El problema radica, sin embargo, en dos aspectos principales: primero, en la exigencia de que nombre y apellidos sean usurpados en todo caso —que autores como Díaz López, según comentamos, interpretan relajadamente—; segundo, en determinar la continuidad de la usurpación, cuestión que ya era problemática en el mundo físico, pero que plantea nuevas incógnitas en el ciberespacio.

Para finalizar, conviene hacer referencia a la posibilidad, frecuente en la práctica, de que una usurpación de estado civil concorra con una estafa (art. 248 CP), tipo penal que, por

⁸² El razonamiento de la exigencia del nombre y los apellidos reside en que el tipo consiste en usurpar el estado civil *de otro*, lo que implica que ese *otro* debe ser identificable. Para la jurisprudencia, esta identificación pasa necesariamente por el nombre y apellidos, aunque Díaz López lo interpreta de forma más laxa. *Cfr.* DÍAZ LÓPEZ, J. A.: *El delito...*, *op. cit.*, pp. 138-156.

⁸³ GORDON BENITO, I.: “Suplantaciones...”, *op. cit.*, p. 5.

⁸⁴ Citas de la STS 15-06-2009 (*cit.*), FJ 2.º y de la STS 01-06-2009 (Cendoj, ECLI:ES:TS:2009:3961), FJ 2.º.

⁸⁵ STS 04-05-2012 (Cendoj, ECLI:ES:TS:2012:3030), FJ 12.º.

⁸⁶ *Cfr.* SAP Zaragoza 13-04-2011 (Cendoj, ECLI:ES:APZ:2011:1002), FJ 1.º, resolución que es confirmada más tarde —aunque sin referencia expresa a esta cuestión— en STS 12-06-2012 (Cendoj, ECLI:ES:TS:2012:3999).

⁸⁷ De hecho, en la STS 12-06-2012 (*cit.*), el acusado es castigado por un delito de falsedad documental.

cierto, incluye expresamente la actuación a través de una manipulación informática. Cuando así suceda, estaremos ante un concurso medial de delitos, según parece entender la jurisprudencia⁸⁸. Con todo, no debemos confundir este concurso medial con una estafa cuyo *engaño* —elemento nuclear del tipo— consista en suplantar la identidad de otro, sin que pueda apreciarse que esta suplantación reúne los requisitos de toda usurpación de estado civil⁸⁹. En este último supuesto, difícilmente podrá hablarse de una agresión a la identidad.

3. LA SUPLANTACIÓN DE LA IDENTIDAD DIGITAL COMO FALSEDAD DOCUMENTAL

En el capítulo introductor de este trabajo anticipábamos que, con respecto a las suplantaciones de identidad en redes sociales, algunos autores plantean la subsunción en los tipos de falsedad documental. En la medida en que la identidad se tutela indirectamente como resultado de la protección a la fe pública en el tipo del art. 401, correspondería analizar si esta relación conceptual se puede dar también en el otro grupo de delitos contra la fe pública: las falsedades documentales (Capítulo II del Título XVIII de la Parte Especial).

Como nota previa, cabe señalar que, desde el Código Penal de 1848, la doctrina ha discutido la distinción entre las voces *falsedad* y *falsificación*⁹⁰. A día de hoy, puede afirmarse que la cuestión carece de trascendencia, pues, como apunta Morillas Cueva, el legislador emplea ambos términos indistintamente, sin que ello afecte en modo alguno al contenido de cada uno de los tipos⁹¹.

Procedemos a mencionar las conductas típicas de ese Capítulo que estimamos relevantes:

a) El art. 390.1 CP, que describe las diferentes falsedades de documento *público* que se pueden cometer, incluye (i) alterar el documento en alguno de sus elementos o requisitos de carácter esencial; (ii) simular el documento en todo o en parte, en un grado suficiente para inducir a error sobre su autenticidad; (iii) suponer la intervención de personas en un acto cuando éstas no han intervenido en realidad, y (iv) atribuir a quienes sí han intervenido en un acto declaraciones o manifestaciones distintas de las que hayan realizado. Si un particular⁹² comete —dolosamente— uno de estos actos de falsificación, estará incurriendo en delito *ex* art. 392.1 CP.

⁸⁸ ATSJ Andalucía 17-11-2003 (Cendoj, ECLI:ES:TSJAND:2003:270A), FJ 4.º.

⁸⁹ Por ejemplo, si la suplantación consiste en una burda (inidónea) imitación de un famoso, o si la persona suplantada, directamente, no existe. *Cfr.* DÍAZ LÓPEZ, J. A.: *El delito...*, *op. cit.*, p. 204.

⁹⁰ RODRÍGUEZ DEVESA, J. M. y SERRANO GÓMEZ, A.: *Derecho Penal...*, *op. cit.*, p. 946.

⁹¹ *Cfr.* COBO DEL ROSAL, M. (dir.): *Compendio...*, *op. cit.*, p. 729.

⁹² Se distingue la falsedad cometida por *funcionario público* en el ejercicio de sus funciones (tipificada en el art. 390 CP) de aquella ejecutada por un *particular* que no reúne esa condición —o un funcionario que no actúa en el ejercicio de sus funciones— (arts. 392 y siguientes).

b) Después, el art. 395 CP establece una pena algo inferior al particular que realiza una de las conductas arriba descritas respecto de un documento *privado*, con un requisito adicional de carácter subjetivo: la falsificación debe efectuarse “para perjudicar a otro”.

Si bien la discusión sobre el bien jurídico protegido en estos tipos ha sido prolífica, y ello tanto en España como en otros ordenamientos de nuestro entorno⁹³, en lo que coincide la mayoría de la doctrina es en su carácter abstracto: partiendo de un bien jurídico más amplio cual es la fe pública, el delito castigaría, más precisamente, ofensas a aspectos de la fe pública como el valor probatorio que se reconoce al contenido del documento (en esta línea, Morillas Cueva⁹⁴ y, con mayor detalle, Villacampa Estiarte⁹⁵). Entretanto, parece evidente que el objeto *material* del delito es el documento y, en términos más concretos, su contenido. Por lo tanto, en la medida en que el contenido de un documento falsificado se refiera a la *identidad* de una persona, esa identidad funcionaría, una vez más, como objeto material del tipo. Y ello no será algo poco frecuente: de las cuatro conductas de falsificación que se han definido, las dos últimas exigen fingir la *intervención* de una persona, que debe ser identificada o identificable; asimismo, la identidad de una persona es un elemento *esencial* de un contrato (por cuanto de ella se deriva su personalidad), el documento por excelencia.

La cuestión es hasta qué punto la falsificación de la identidad *digital* de alguien resulta punible. Rodríguez Fernández⁹⁶ advierte aquí que el art. 26 CP define *documento* como “todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica”. Dada la amplitud del concepto, no parece problemático integrar en su ámbito objetivo tanto los documentos escritos e impresos como cintas de vídeo, disquetes informáticos⁹⁷ y hasta archivos electrónicos a los que quepa atribuir relevancia jurídica⁹⁸.

En relación con el carácter —público o privado— que ha de otorgarse a esos archivos electrónicos, Rodríguez Fernández razona de este modo⁹⁹:

Los servicios prestados por [internet] suelen estar soportados por un contrato mercantil, y la página web no deja de ser un documento, aunque sea electrónico, por lo que el falseamiento de los datos implica que se ha falsificado un documento mercantil.

Una vez que el suplantador ya ha accedido a la [red social] tras la formalización del mencionado contrato mercantil y crea su perfil, emite entonces opiniones, deseos o cualquier otra manifestación de voluntad, poniéndolas en boca —o por mejor decir, en el supuesto *twit* [*sic*]— del suplantado. Esta información también se expresa en un soporte informático, ya que el *twit* constituye un archivo electrónico [...]. Pero en este caso no nos encontramos ya ante el documento mercantil que

⁹³ Un examen de esta cuestión, enfocada a la falsedad documental, se lleva a cabo en VILLACAMPA ESTIARTE, C.: *La falsedad documental: Análisis jurídico-penal*, Universitat de Lleida, Lleida, 1998, pp. 6-49.

⁹⁴ En COBO DEL ROSAL, M. (dir.): *Compendio...*, *op. cit.*, pp. 729-730 y 749.

⁹⁵ VILLACAMPA ESTIARTE, C.: *La falsedad...*, *op. cit.*, pp. 49-59.

⁹⁶ RODRÍGUEZ FERNÁNDEZ, M. P.: “Suplantación...”, *op. cit.*

⁹⁷ En esta línea, *cfr.* también COBO DEL ROSAL, M. (dir.): *Compendio...*, *op. cit.*, p. 740.

⁹⁸ RODRÍGUEZ FERNÁNDEZ, M. P.: “Suplantación...”, *op. cit.*, párr. 17.

⁹⁹ RODRÍGUEZ FERNÁNDEZ, M. P.: “Suplantación...”, *op. cit.*, pgs. 18-19.

se encuentra en el fundamento de la prestación de los servicios de Internet, sino que se trata de un documento por el que se establece una relación o comunicación entre el suplantador y los demás usuarios [...]. Nos encontramos entonces ante un documento privado entre particulares.

La autora distingue dos situaciones diferentes, aunque no incompatibles: primero, la creación de un perfil de internet falso con la identidad de un tercero, subsumible en el tipo de falsificación de documento público del art. 392.1 CP, y segundo, la publicación de contenidos en nombre de otro (previo apoderamiento de su cuenta, sea mediante la creación del perfil falso, sea de una forma distinta) para perjudicarlo, que sería típica por el art. 395. Esta solución suena coherente, aunque no termina de ser una construcción interpretativa que, además, involucra dos tipos penales autónomos, arrojando penas acaso excesivas en supuestos de concurso: de tres a cuatro años y medio si calificamos el concurso como ideal, y de seis meses hasta cinco años en el supuesto de concurso medial.

En definitiva, siendo el contenido específico de un documento el objeto material concreto de los delitos de falsedad documental, y dando por buena la consideración de los archivos en línea como documento, la identidad digital podría jugar, haciendo una interpretación generosa de la ley penal, un importante papel en los supuestos de falsificación: serían punibles falsificaciones, por ejemplo, de mensajes de correo electrónico, de datos contenidos en una red social o de una conversación telefónica. La Audiencia Provincial de Madrid, en un caso del que aún no ha recaído sentencia firme, ha aceptado esta interpretación¹⁰⁰.

De forma similar a lo que sucede con la usurpación de estado civil, son habituales las falsedades documentales utilizadas para cometer estafa; trasladamos aquí, *mutatis mutandis*, las anteriores consideraciones realizadas al respecto. Además, se puede plantear el problema concursal, de resolución todavía más complicada, entre este tipo y la propia usurpación de estado civil; en el capítulo IV volveremos sobre esta cuestión.

4. CONEXIÓN DE LA IDENTIDAD DIGITAL CON OTROS BIENES JURÍDICOS

A lo largo de este trabajo, se ha hecho referencia en varias ocasiones al vínculo entre identidad y autonomía. Concretando este vínculo, no es conflictivo afirmar que tanto la dignidad humana como el libre desarrollo de la personalidad (consagrados en el art. 10.1 CE) constituyen *presupuestos* de la identidad: de no concebirse el ser humano como digno y libre, su identidad sería irrelevante. Al mismo tiempo, ambos principios son una *expresión* de la identidad personal: en merced de nuestra identidad, podemos ejercer nuestra personalidad.

En el ámbito jurídico-penal, la dignidad y el libre desarrollo de la personalidad se articulan a través de distintos bienes jurídicos, de entre los cuales nos interesa examinar el honor, la

¹⁰⁰ AAP Madrid 25-05-2017 (Cendoj, ECLI:ES:APM:2017:1634A), FJ 1.º. *Cfr.* también el artículo de Magro Servet, juez de esa Sección de la Audiencia Provincial: MAGRO SERVET, V: “La tipificación...”, *op. cit.*

privacidad. Junto con éstos, trataremos la seguridad de los sistemas informáticos como bien jurídico colectivo de reciente incorporación. Por último, se hablará de la libertad de obrar.

A) *El honor. Calumnia e injuria por medios digitales*

Reconocido *ex art.* 18.1 CE junto con la intimidad y propia imagen¹⁰¹, el derecho fundamental al honor se traslada a la esfera penal a través de los delitos de calumnia e injuria (arts. 205 a 210 CP). Si bien estamos ante un concepto jurídico indeterminado¹⁰², autores como Carmona Salgado¹⁰³ opinan que el honor, derivado del principio de dignidad, se concreta en dos nociones complementarias: una es la autoestima (o la “propia estimación”, dice el art. 208 CP), de carácter interno, entendida como la dignidad que posee toda persona en cuanto ser racional; la otra, externa, es la reputación (“fama”), esto es, el “juicio que la comunidad proyecta sobre el individuo”¹⁰⁴. Los pronunciamientos del TC más reiterados son coherentes con esta exposición¹⁰⁵.

Interesa comentar varios extremos acerca de los tipos penales mencionados:

a) Es calumniosa la imputación —a otra persona— de un delito con conocimiento de la falsedad de esa imputación o con “temerario desprecio hacia la verdad” (art. 205 CP). En tanto que el hecho delictivo imputado pueda probarse (alegando la *exceptio veritatis*), la conducta deviene atípica o, si se prefiere, no punible¹⁰⁶.

b) En lo tocante a la injuria, definida como “acción o expresión que lesiona la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación” (pg. 1.º del art. 208 CP), únicamente se castigan aquellas que “sean tenidas en el concepto público por graves” (pg. 2.º), lo que exige analizar la naturaleza, los efectos y las circunstancias en que se realiza. Quedan excluidas (i) las imputaciones de hechos realizadas sin conocimiento de su

¹⁰¹ El art. 18.1 CE reconoce, *stricto sensu*, un único derecho: “al honor, a la intimidad personal y familiar y a la propia imagen”. No obstante, actualmente existe consenso en que “nos encontramos ante tres derechos distintos y autónomos”; *cf.* ESCRIBANO TORTAJADA, P.: “Algunas cuestiones sobre la problemática jurídica del derecho a la intimidad, al honor y a la propia imagen en internet y las redes sociales”, en A. Fayos Gardó (dir.): *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Dykinson, Madrid, 2015, p. 63.

¹⁰² *Cfr.* STC 03-07-2006 (HJ, ECLI:ES:TC:2006:216), FJ 7.º.

¹⁰³ Carmona Salgado se refiere a esta dualidad en COBO DEL ROSAL, M. (dir.): *Compendio...*, *op. cit.*, pp. 326-327.

¹⁰⁴ COBO DEL ROSAL, M. (dir.): *Compendio...*, *op. cit.*, pp. 327.

¹⁰⁵ Son daños al honor aquellas “expresiones o mensajes insultantes, insidias infamantes o vejaciones que provoquen objetivamente el descrédito de la persona a quien se refieran”. STC 26-02-2001 (HJ, ECLI:ES:TC:2001:49), FJ 5.º.

¹⁰⁶ La opción por una u otra expresión (“atipicidad” o “falta de punibilidad”) depende del modelo de delito por el que se opte. En nuestro caso, siguiendo a Obregón García y Gómez Lanz, consideramos que, en términos generales, concurre delito cuando hay, por un lado, acción y tipicidad, sin que concurren faltas de justificación —conjunto al que los citados autores denominan *injusto penal*, de carácter fundamentalmente objetivo—; y, por el otro, imputabilidad y dolo, más ausencia de exigibilidad de una conducta distinta —elementos que conforman la *culpabilidad*, subjetiva—. No se postula un elemento de punibilidad, que es perfectamente reconducible a la atipicidad en algunos casos (como éste), y al ámbito de lo procesal en otros. *Cfr.* OBREGÓN GARCÍA, A. y GÓMEZ LANZ, J.: *Derecho Penal...*, *op. cit.*, pp. 189-194.

falsedad o sin temerario desprecio hacia la verdad (pg. 3.º), y (ii) determinadas injurias dirigidas contra cargos públicos (art. 210).

c) La injuria leve se protege civilmente en la Ley Orgánica 1/1982¹⁰⁷ (*cf.* art. 7.7), y penalmente sólo en los supuestos acotados en el art. 173.4 CP.

d) Tanto la calumnia como la injuria son delitos perseguibles solamente en virtud de querrela de la persona ofendida o de su representante legal (art. 215 CP).

Es evidente que, toda vez que el honor de una persona ha de ser atacado de manera *directa* para que concurra alguno de estos tipos, la identidad se ubica nuevamente como objeto material, si no de todos, de la inmensa mayoría de conductas calumniosas o injuriosas. En el plano digital, este hecho se hace todavía más evidente, por cuanto plataformas como las redes sociales facilitan (i) que el mensaje lesivo del honor pueda enviarse al destinatario directamente, sin importar el momento o el lugar desde el que se envía, y (ii) la difusión y publicidad de los juicios proferidos, elementos que acentúan potencialmente el desvalor de resultado —esto es, el menoscabo del bien jurídico—.

B) *La privacidad. Descubrimiento y revelación de secretos en el ciberespacio*

Profundamente reformado en 2015, el art. 197 CP encabeza el catálogo de delitos “contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio” (Título X, Parte Especial del Código Penal), siendo éstos los bienes que, al menos en apariencia, se ven protegidos. El citado precepto se articula en una serie de *tipos mixtos alternativos* (su realización puede darse a través de distintas acciones, todas ellas “unificadas externamente por la asignación de una pena única”¹⁰⁸) que hemos de revisar. Sin embargo, antes conviene delimitar los bienes jurídicos implicados:

a) La intimidad (“personal y familiar”, dice el art. 18.1 CE) tampoco presenta un contenido claro. La doctrina del TC ha reiterado que implica “la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario —según las pautas de nuestra cultura— para mantener una calidad mínima de la vida humana”¹⁰⁹.

b) Respecto de la propia imagen, se trata de un bien jurídico de discutible autonomía, por cuanto su lesión suele venir acompañada de lesiones a la intimidad y, en su caso, al honor. De acuerdo con el Supremo, “atribuye a su titular un derecho a determinar la información gráfica generada por sus rasgos físicos personales que pueden tener difusión pública y a impedir la

¹⁰⁷ Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (BOE).

¹⁰⁸ OBREGÓN GARCÍA, A. y GÓMEZ LANZ, J.: *Derecho Penal...*, *op. cit.*, p. 94.

¹⁰⁹ STC 02-12-1998 (HJ, ECLI:ES:TC:1988:231), FJ 3.º.

obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado”¹¹⁰.

c) Por último, numerosos autores se han referido a la privacidad en las últimas décadas como un bien de ámbito expansivo y más amplio que la intimidad¹¹¹. De esta suerte, la intimidad, la propia imagen y la inviolabilidad del domicilio serían sólo algunas de las manifestaciones de la privacidad, todas ellas de contenido negativo. En virtud de la fuerza expansiva de la privacidad, se han ido desarrollando en nuestro Derecho una serie de derechos *positivos*, es decir, que permiten a su titular hacer o exigir algo. Este desarrollo lo inauguró la STC 30-11-2000, en la que se consolida la *libertad informática* como derivado de la privacidad: “La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad [...]. La ‘libertad informática’ es así derecho a controlar el uso de los mismos datos insertos en un programa informático”¹¹². Más tarde, este concepto se trasladó al Derecho positivo en la forma de derecho fundamental a la protección de datos, por medio del Reglamento (UE) 2016/679¹¹³ y de la LOPD.

Procedemos ahora a describir las principales conductas típicas establecidas en el art. 197 —precepto que emplea una técnica criticada ampliamente por la doctrina¹¹⁴—:

a) Art. 197.1: el apoderamiento de cualesquiera documentos o efectos personales de un tercero, donde se incluyen expresamente sus mensajes de correo electrónico; la interceptación de sus telecomunicaciones, o la utilización de artificios técnicos de reproducción de la imagen. Estas acciones deben realizarse con la finalidad de “descubrir los secretos o vulnerar la intimidad” de ese tercero y “sin su consentimiento”.

b) Art. 197.2, inciso 1.º: el apoderamiento, utilización o modificación de datos reservados de carácter personal o familiar de otro que figuren en un “archivo o registro”, público o privado. Son *reservados* aquellos datos desconocidos u ocultos, entendiéndose por tales aquellos que el sujeto activo no conozca o no esté seguro de conocer, y que el sujeto pasivo no desea que sean descubiertos¹¹⁵. Los actos han de perpetrarse sin la autorización de la persona a la que se refieran esos datos y, además, “en perjuicio de tercero”. El TS ha clarificado, por un lado, que este perjuicio no significa un plus de tipicidad, sino que es intrínseco a la realización de la conducta sin la autorización de la persona; y, por el otro, que

¹¹⁰ STS 07-07-2012 (Cendoj, ECLI:ES:TS:2012:5740), FJ 2.º.

¹¹¹ El origen de la discusión reside en la doctrina anglosajona, representada por Brandeis y Warren, quienes conciben la *privacy* sencillamente como el “derecho a ser dejado en paz”. Cfr. BRANDEIS, L. y WARREN, S. D.: “The right to privacy”, *Harvard Law Review*, 4(5), 193-220, 1890, p. 195.

¹¹² STC 30-11-2000 (HJ, ECLI:ES:TC:2000:292).

¹¹³ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (DOUE).

¹¹⁴ Cfr. MOLINA FERNÁNDEZ, F. (dir.): *Memento Práctico Penal 2019*, Francis Lefebvre, 2019, § 9899.

¹¹⁵ STS 11-07-2001 (Cendoj, ECLI:ES:TS:2001:6029), FJ 6.º.

la expresión “tercero” incluye al sujeto pasivo, pese a la ambigüedad del precepto¹¹⁶. Es pacífico que la consumación del delito tiene lugar tan pronto como el sujeto activo conoce y tiene a su disposición los datos. Por último, se excluyen del ámbito objetivo del tipo las conductas “realizadas sobre datos de carácter personal con anterioridad a su registro o archivo”¹¹⁷.

c) Art. 197.2, inciso 2.º: en referencia a los mismos datos reservados arriba descritos, su acceso por cualquier medio y su alteración o utilización, “en perjuicio del titular de los datos o de un tercero”. Es confusa la inclusión de los actos de alteración y utilización en este punto: parece que ambos estarían capturados por el tenor del inciso inmediatamente anterior, que penaliza la modificación (casi indistinguible de la alteración) y la utilización (mismo verbo que se emplea en el inciso 1.º) de los datos archivados o registrados. Así las cosas, este tipo se limita a prohibir el *acceso* a los datos.

d) Art. 197.3: la difusión, revelación o cesión a terceros de los datos descubiertos o las imágenes captadas mediante la comisión de los tipos de los dos apartados previos.

e) Art. 197.4.b): la comisión de los tipos de los apartados 1.º y 2.º mediante la “utilización no autorizada de datos personales de la víctima”. Esta confusa redacción se referiría, según algunos autores, a aquellos casos en que se utilizan herramientas de intrusismo informático o jaqueo no accesibles al individuo promedio¹¹⁸. Adicionalmente, el art. 197.4 *in fine* castiga con una pena superior la comisión de estos hechos más la revelación de los datos descubiertos (es decir, se añade el desvalor de resultado del art. 197.3).

f) Art. 197.7: la revelación (vía difusión o cesión) a terceros de contenido audiovisual obtenido con el consentimiento de la víctima en un lugar fuera del alcance de terceros, “cuando la divulgación menoscabe gravemente la intimidad personal” de ese tercero.

g) Art. 201: en todo caso, se requiere la denuncia de la persona agraviada o de su representante legal para perseguir el delito.

Como se puede apreciar, estos tipos se han adaptado a aquellos casos en que el sujeto activo actúa en el plano digital. Al mismo tiempo, el papel de objeto material lo juegan, en todo caso, los datos personales (en el ámbito del art. 197.2, los datos personales reservados) que se descubren o revelan. Así pues, la identidad, especialmente en su ámbito digital, ocupa también aquí una posición relevante: para que se califiquen unos datos de *personales*, éstos deben referirse a una persona física identificada o identificable¹¹⁹.

¹¹⁶ Por todas, STS 11-07-2001 (*cit.*), FJ 3.º.

¹¹⁷ MOLINA FERNÁNDEZ, F. (dir.): *Memento...*, *op. cit.*, § 9900.

¹¹⁸ MOLINA FERNÁNDEZ, F. (dir.): *Memento...*, *op. cit.*, § 9914.

¹¹⁹ El art. 2 del Reglamento (UE) 2016/679 (*cit.*) define *datos personales* como: “Toda información sobre una persona física identificada o identificable [...]; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social [...]”.

C) *La seguridad de los sistemas informáticos. Intrusismo informático, abuso de dispositivo y daños informáticos*

En la introducción, hicimos referencia al Convenio de Budapest como uno de los textos pilares en el proceso de adaptación jurídico-penal a la ciberdelincuencia. En esta norma, se desarrolla un catálogo de figuras delictivas ordenado, igual que el Código Penal, en atención al bien jurídico protegido. Pues bien: los delitos de acceso ilícito a sistemas informáticos, interceptación ilícita de éstos, alteración de datos y abuso de dispositivos se agrupan bajo la rúbrica “Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos”. Por su parte, la Directiva 2013/40/UE¹²⁰, que recoge delitos similares es la directiva “relativa a los ataques contra los sistemas de información”.

La transposición de los citados delitos al ordenamiento penal español, realizada en la reforma de 2015, resultó en los siguientes tipos:

a) Art. 197 bis: sanciona (i) el acceso ilegal a un sistema informático través de la vulneración de sus medidas de seguridad por cualquier medio o procedimiento, y (ii) la interceptación de transmisiones no públicas de datos informáticos. En ambos casos, se exige que el ataque no esté “debidamente autorizado”. La FGE ha clarificado que, en el momento en que los actos tipificados en este precepto producen un daño a la privacidad, nos encontraremos en el ámbito del art. 197, que consumirá el desvalor de resultado este artículo¹²¹. En otro orden de cosas, Anarte Borrallo y Doval Pais sostienen que la “vulneración de medidas de seguridad” a la que se refiere el tipo exige que el acceso ilegal al sistema presente una mínima complejidad técnica¹²².

b) Art. 264: establece como conductas típicas borrar, dañar, alterar o hacer inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, siempre que se haga sin autorización (expresión en la que tienen cabida no sólo el consentimiento del dueño de los datos o soportes, sino también una “autorización legal”¹²³) y ocasionando resultados graves. Es mayoritaria la interpretación de que no se precisa causar un perjuicio a un tercero, de forma que lo importante es que el objeto dañado pierda valor económico¹²⁴. La sanción penal se ve agravada cuando la acción se comete mediante la utilización ilícita de datos personales de otro para facilitar el acceso al sistema o para ganarse la confianza de un tercero.

¹²⁰ Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo (BOE, 14-08-2013).

¹²¹ Cfr. Circular FGE 21-09-2017 (BOE, 3/2017).

¹²² Ello ocurre “cuando la clave de acceso aparece en la pantalla, bastando con pulsar la tecla *intro*”, así como cuando esa clave es tan sencilla como “123456” o “qwerty”. ANARTE BORRALLO, E. y DOVAL PAIS, A.: “Límites de la ley penal a propósito del nuevo delito de intrusión informática”, *Revista General de Derecho Penal*, 18, 2012, § 12.

¹²³ SJP n.º 31 Madrid 04-09-2019 (Cendoj, ECLI:ES:JP:2019:39), FJ 5.º.

¹²⁴ Cfr. COBO DEL ROSAL, M. (dir.): *Compendio...*, *op. cit.*, p. 483. Discuten también los autores si el daño debe afectar a la sustancia del bien, o basta con que incida en el valor de uso que éste tiene para su dueño.

c) Art. 264 bis: similar al anterior, prohíbe obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno, con la misma agravante de utilización ilícita de datos personales.

d) Arts. 197 ter y 264 ter: penalizan el abuso de dispositivos¹²⁵, esto es, los actos de producción, adquisición, importación o entrega a terceros, con vías a facilitar la comisión de los arts. 197 y 197 bis y los arts. 264 y 264 bis, respectivamente, de (i) un programa informático concebido o adaptado para cometer esos delitos, o (ii) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema.

Sucede que la ubicación sistemática de este grupo de delitos no concuerda con la que le dan las normas supranacionales de donde éstos proceden: de un lado, los arts. 197 bis y 197 ter están a continuación del ya analizado art. 197, que protege la intimidad, la propia imagen y, como hemos sostenido, la privacidad —conque también precisan de denuncia previa del agraviado—; del otro, el 264, el 264 bis y el 264 ter siguen al tipo genérico de daños. Así pues, cabe plantearse cuáles son, verdaderamente, los bienes jurídicos que se protegen.

Son varios los autores que han analizado esta cuestión respecto de los arts. 197 bis y 197 ter¹²⁶. Un sector es favorable a considerar que estamos ante un bien jurídico distinto de la privacidad, cuya principal diferencia reside en que se trata de un bien *colectivo*, no individual. Se han propuesto denominaciones como “funcionalidad informática”¹²⁷, “seguridad informática”¹²⁸ y “seguridad e intangibilidad de los sistemas informáticos”¹²⁹; esta última, con cierta acogida en la jurisprudencia¹³⁰. Voces contrarias a esta visión aseveran que la ubicación sistemática de los tipos impide hablar de un bien colectivo. Hablan de “libertad informática” —rescatando el término empleado por el TC—, “inviolabilidad de las comunicaciones informáticas”¹³¹, “inviolabilidad informática”¹³² o “intimidad de los sistemas informáticos”¹³³, siempre en el ámbito de la privacidad.

Si trasladamos el debate al ámbito de los daños informáticos, nos encontramos también ante dos alternativas: la protección de un bien colectivo, llamémosle también *seguridad de*

¹²⁵ Así lo llama la Circular FGE 21-09-2017 (*cit.*), p. 34.

¹²⁶ Una síntesis más detallada se expone en COLÁS TURÉGANO, A.: “El delito de intrusismo informático tras la reforma del CP español de 2015”, *Revista Boliviana de Derecho*, 21, 210-229, 2016, p. 215.

¹²⁷ MAYER LUX, L.: “El bien jurídico protegido en los delitos informáticos”, *Revista Chilena de Derecho*, 44(1), 235-260, 2017, p. 255. La autora concibe este bien respecto de delitos tipificados en el Código Penal chileno, aunque análogos a los indicados.

¹²⁸ TOMÁS-VALIENTE LANUZA, C.: “Delitos...”, *op. cit.*, p. 38.

¹²⁹ ANARTE BORRALLO, E. y DOVAL PAIS, A.: “Límites...”, *op. cit.*, § 4.

¹³⁰ Principalmente, *cfr.* SAP Girona 22-06-2015 (Cendoj, ECLI:ES:APGI:2015:940), FJ 3.º.

¹³¹ DE LA MATA BARRANCO, N. J.: “Reflexiones sobre el bien jurídico a proteger en el delito de acceso informático ilícito (art. 197 bis CP)”, *Cuadernos de política criminal*, 118, 43-86, 2016, p. 80.

¹³² En GALÁN MUÑOZ, A.: “La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales”, *Revista Penal*, 24, 90-107, 2009, p. 95. Este término no se utiliza en referencia a la reforma penal de 2015, sino al Convenio de Budapest.

¹³³ BARRIO ANDRÉS, M.: *Ciberdelitos...*, *op. cit.*, p. 66.

los sistemas (o seguridad *de los datos*), o bien la protección de la propiedad ajena, pues es éste el objeto tutelado en el tipo genérico de daños.

Personalmente, nos inclinamos a considerar que estamos ante un bien jurídico de carácter instrumental o colectivo. Afirmar lo contrario implicaría que los tipos sólo se realizarían cuando la acción estuviera *preordenada* a la lesión de la privacidad o la propiedad (según el caso) de la víctima, condición que no está expresa en los correspondientes artículos, lo que no es compatible con una concepción esencialmente objetiva del injusto como la que manejamos en este trabajo¹³⁴.

En conclusión, nos encontramos ante un grupo de conductas delictivas que tutelan la seguridad de los sistemas informáticos. Ello no es incompatible con que sea preceptiva la denuncia de la persona agraviada *ex art.* 201. Es más: aceptando la seguridad de los sistemas informáticos como bien jurídico, la condición de agraviado podría tenerla el creador (persona física) del sistema cuya seguridad se ha visto vulnerada, aun cuando en ese sistema no figuren sus datos personales. Tanto este requisito de previa denuncia como la “debida autorización” del art. 197 bis permiten la actuación de los llamados *sombreros blancos* o *jáqueres éticos*, personas expertas en ciberseguridad que penetran en sistemas informáticos con la finalidad de detectar e informar sobre posibles vulnerabilidades en su seguridad¹³⁵.

Queda por señalar cómo se ve afectada la identidad digital con la comisión de estos tipos. Respecto de los arts. 197 bis y 197 ter, se está adelantando la barrera punitiva frente a las agresiones a la privacidad tuteladas por el art. 197, y, por ende, también frente a ataques susceptibles de recaer sobre la identidad digital. En lo tocante a los daños informáticos, estaríamos ante un tipo más bien residual: si los datos informáticos o documentos electrónicos dañados o cuyo funcionamiento se ha obstaculizado están relacionados con la identidad digital, el desvalor de resultado producido se verá consumido, por lo general, por el art. 197 (en caso de daño) o el art. 197 bis (cuando se obstaculice o interrumpa el sistema).

D) *La libertad de obrar. Acoso moral por medios digitales*

Como válvula de cierre a la protección del libre desarrollo de la personalidad, el Código incorpora el delito de coacciones en el art. 172, cuyo objeto de protección es la libertad de obrar de las personas¹³⁶. Se castiga a aquél que “impidiere a otro con violencia hacer lo que la

¹³⁴ De la Mata Barranco, de la opinión opuesta, defiende que “datos aparentemente intrascendentes, en su interconexión virtual, [...] definen personalidades y trascienden [esa] aparente nimia importancia” (DE LA MATA BARRANCO, N. J.: “Reflexiones...”, *op. cit.*, Madrid, 2016, p. 80). Sin embargo, esta afirmación parece asumir que la única motivación que puede llevar a un agresor a realizar este delito es la *trascendencia* de esos datos, elemento (insistimos) no recogido en el tipo. Siguiendo el razonamiento de este autor, en el momento en que se pusiera de manifiesto una finalidad diversa, como obstaculizar la funcionalidad del sistema o transmitir su falta de seguridad a terceros, la acción devendría atípica (lo cual no concuerda con nuestra exposición).

¹³⁵ Circular FGE 21-09-2017 (*cit.*), p. 19.

¹³⁶ STS 22-11-1990 (Cendoj, ECLI:ES:TS:1990:12269) FJ 4.º.

Ley no prohíbe, o le compeliere a efectuar lo que no quiere, sea justo o injusto”, conducta de carácter abierto que en múltiples ocasiones será consumida por otros tipos penales¹³⁷.

Dicho esto, la reforma penal de 2015 incorporó un tipo autónomo junto con las coacciones que castiga, con una pena en abstracto inferior, el llamado acoso moral. Ubicado en el art. 172 ter, este tipo castiga aquellas conductas lesivas de la libertad de obrar que consistan, entre otras, en contactar (o intentar contactar) repetidamente con la víctima a través de cualquier medio de comunicación, o en provocar, mediante el uso indebido de sus datos personales, que terceras personas se pongan en contacto con ella. El precepto requiere que el acoso resulte en una alteración grave “en el desarrollo de su vida cotidiana”.

Nótese cómo la identidad digital se puede ver implícitamente afectada como resultado de estos actos: el perjuicio a la libertad se puede perpetrar, por ejemplo, a través de llamadas telefónicas o mensajes en una red social continuos, o compartiendo datos (el número telefónico) de la víctima que permitan contactar con ella.

¹³⁷ “Las coacciones son el delito subsidiario por excelencia, así todos los ataques a la libertad que no supongan al mismo tiempo un ataque a otro bien jurídico expresamente tipificado, se castigarán como coacciones”. MOLINA FERNÁNDEZ, F. (dir.): *Memento...*, *op. cit.*, § 8570.

IV. RELEVANCIA PENAL DE LAS SUPLANTACIONES EN REDES SOCIALES

En el capítulo anterior, han quedado de manifiesto las limitaciones que presenta el Derecho penal español para tutelar de manera indirecta la identidad digital, que se resumen en que determinados comportamientos que son típicos si se realizan en el espacio físico encuentran dificultades de subsunción al cometerse en el ciberespacio (singularmente, la usurpación de estado civil y la falsedad documental). Existe, en definitiva, una cierta inseguridad jurídica.

Por ello, dedicamos este capítulo a discutir una propuesta político-criminal en torno a la tutela de la identidad digital en un caso específico: la suplantación de la identidad de otra persona en las redes sociales. La elección de este caso radica en que se trata, desde nuestro punto de vista, de la agresión más grave que puede sufrir la identidad digital. Para acometer nuestro análisis, se distinguirá entre dos modalidades de suplantación de identidad digital, ilustrando cada una con un caso práctico. Se examinará la tipicidad que presenta cada supuesto, haciendo hincapié en los problemas de subsunción y concursales. Al final, se propondrá una posible reforma penal a fin de superar los problemas hallados.

1. EXAMEN DE TIPICIDAD A TRAVÉS DE DOS SUPUESTOS PRÁCTICOS

De manera acertada, Tomás-Valiente Lanuza¹³⁸ identifica dos clases de conductas que se pueden realizar para suplantar la identidad de otro en una red social: las que consisten en la creación de un *perfil falso* o ficticio en la que se muestren datos de la persona suplantada, y aquéllas que comportan el acceso al perfil —ya existente— de un tercero, con el consiguiente *apoderamiento* de su cuenta y sus datos. Los primeros son más frecuentes, quizá porque no precisan más que un conocimiento básico de internet. Los segundos, por su parte, requieren vencer las medidas de seguridad de la red social a través de algún instrumento técnico, de la intimidación o, simplemente, de la adivinación de las claves de acceso del usuario. Se pondrá, pues, un ejemplo de cada caso.

A su vez, para facilitar el examen de tipicidad, los hechos delictivos se agruparán en dos actos: aquél en que se produce la suplantación de identidad como tal, y el acto posterior, en el que se atacan otros bienes jurídicos. Sirviéndonos del latín, nos referiremos a estos dos actos como *ad supplantationem* e *in supplantatione*¹³⁹, respectivamente.

¹³⁸ TOMÁS-VALIENTE LANUZA, C.: “Delitos...”, *op. cit.*, p. 36.

¹³⁹ Literalmente, *ad supplantationem* ‘hacia la suplantación’ designa el conjunto de hechos o actos encaminados a suplantar al tercero, e *in supplantatione* ‘en la suplantación’ implica que la persona ya ha sido suplantada.

A) Suplantación a través de creación de cuenta falsa

Partimos del siguiente supuesto práctico¹⁴⁰:

En cierto momento, el sujeto A comienza a recibir en su móvil, de manera masiva, mensajes de WhatsApp con contenido audiovisual de carácter pornográfico. Asimismo, tanto en estos mensajes como en llamadas telefónicas, terceras personas le hacen propuestas sexuales a cambio de dinero. Por si fuera poco, hasta en tres ocasiones un desconocido se presenta en la puerta de su domicilio con intenciones similares. La intranquilidad y el ataque a su privacidad que A siente a raíz de estos hechos le empujan a cambiar de número de teléfono, y a colocar un cartel junto a su casa en el que se advierte que él no ofrece servicios de prostitución.

Semanas más tarde, dispuesto a descubrir quién está detrás de estos hechos, A descubre que fue todo un plan del sujeto B, con quien había tenido desavenencias en el pasado. Este sujeto, con la intención de perjudicar a A, había creado en una red social pornográfica un perfil falso en el que se mostraban una fotografía suya que no había sido previamente publicada en internet (aunque sí había sido tomada con su consentimiento), el nombre de usuario que utiliza A en su cuenta personal de Instagram, su número de teléfono y su domicilio.

a) Tipicidad *ad supplantationem*

Para llevar a cabo la suplantación de identidad, B se sirve de una página de internet, donde crea una cuenta que incluye un aspecto de la identidad digital de A: su número de teléfono. Además, para que la suplantación tenga más credibilidad¹⁴¹, se incorpora una fotografía de A y, aunque no su nombre de pila, sí su nombre en otra red social.

En vista de estas acciones, se discute la concurrencia de los siguientes tipos penales:

a) Falsificación de documento público (art. 392.1). Si aceptamos que la página donde se puede ver el perfil de A constituye un archivo ligado al contrato mercantil que se ha tenido que firmar para crear la cuenta, puede afirmarse que B está simulando un documento en su totalidad, de manera que puede inducir a error (primer supuesto del art. 390.1), así como falseando la intervención de A en un acto —la creación del perfil— en el que éste no ha intervenido en realidad (tercer supuesto). Debe apuntarse, sin embargo, que esta postura no goza todavía de una gran acogida jurisprudencial, a excepción del citado AAP Madrid.

b) Revelación de imágenes obtenidas con consentimiento de la víctima (art. 197.7), a raíz de la publicación de la fotografía comprometida de A sin su anuencia. Considerando el

¹⁴⁰ Este supuesto está inspirado en varios supuestos reales: uno acontecido en Madrid del que no se derivó un proceso penal, que llegó a conocimiento del autor de este trabajo a través de un tercero; el caso, todavía no resuelto, del AAP Madrid 25-05-2017 (*cit.*), y un asunto sustanciado en el seno de la AEPD, que se relata en EDITORIAL LA LEY: “Primera...”, *op. cit.*

¹⁴¹ En virtud del art. 16.1 CP, la conducta típica debe ser *idónea* para la comisión de un delito. Estudiar en profundidad los problemas de idoneidad en la suplantación en redes sociales escapa al propósito de este trabajo; por ello, hemos propuesto unos supuestos que no dejan dudas en torno a la idoneidad. Con todo, haremos otra referencia a esta cuestión en la sección de conclusiones de este epígrafe.

propósito con el que se utiliza la imagen, no habría dificultades a la hora de probar la lesión grave a la intimidad de A que exige el tipo penal. La revelación permite que la suplantación sea eficaz, de manera que entre este tipo y la falsedad documental —si asumimos que esta última concurre— se establecería una relación de concurso medial.

La ejecución de este segundo delito no es un requisito para realizar la suplantación, pues existen otras vías para lograr que terceras personas caigan en el engaño. Por ejemplo, podría haberse utilizado una fotografía de un tercero que sí se dedique a la prostitución; en tal caso, la conducta de suplantación devendría atípica (salvo si se estimara falsedad documental).

Cabe plantearse si la utilización del número de teléfono y el domicilio de A como datos del perfil es subsumible en el tipo de descubrimiento de datos reservados de carácter personal del art. 197.2 CP. El problema de esta subsunción es que la información descubierta debe estar almacenada en algún tipo de *registro* o archivo con carácter previo a la comisión del delito. No obstante, lo cierto es que se está dando la circunstancia del art. 197.4.b): se están usando datos personales de la víctima sin su consentimiento, sin que ello pueda resultar castigado por no ser el acto subsumible en el art. 197.2.

Finalmente, en la medida en que la fama de A se vería menoscabada a raíz de la creación de la cuenta, puede sugerirse la concurrencia de una injuria (art. 208). Con todo, ello es discutible por dos motivos: primero, porque el desvalor de resultado todavía no es, quizá, de entidad suficiente para que la injuria abandone el ámbito de ilícito civil; segundo, porque el honor de A es difícil de separar de su intimidad —dañada por el tipo del art. 197.2— en este caso concreto.

b) Tipicidad *in supplantatione*

Con posterioridad a la suplantación, A es contactado por terceros de forma abusiva vía mensajes y llamadas telefónicas, y, en algún caso, intentando visitarle a su domicilio.

Identificamos la posible subsunción de los hechos en dos figuras delictivas:

a) Usurpación de estado civil (art. 401). En efecto, el sujeto B está ejerciendo derechos propios de A al seguir masivamente a otras cuentas de la red social, transmitiendo en todo caso la impresión de que quien actuaba era la persona detrás de ese perfil. El desvalor del resultado tiene lugar cuando un número considerable de personas se ponen en contacto con A:

ello perjudica la seguridad del tráfico protegida por el art. 401 CP¹⁴². Con todo, se observa un problema de base: la cuenta falsa no contiene el nombre y los apellidos de la persona suplantada, elemento que la jurisprudencia exige (de manera prácticamente unánime) como condición necesaria para la realización del tipo, sino el nombre de usuario que utiliza la persona suplantada en otra red social. Por otro lado, entre esta falsedad *personal* y la falsedad *documental* antes descrita se establece un concurso de difícil determinación. Personalmente, creemos que se trata de un concurso de normas —por tutelar ambos tipos la fe pública—, pero la doctrina mayoritaria es contraria a esta opinión¹⁴³.

b) Acoso moral (art. 172 ter). Engañados por B, varias personas intentan contactar con A tanto por medios de comunicación como físicamente, lo que parece alterar gravemente el desarrollo de su vida cotidiana. La gravedad de la alteración se ve reflejada en el hecho de que A se ve obligado a cambiar su número telefónico, elemento que integra su identidad digital. De esta suerte, podríamos apuntar a B como autor *mediato* de un delito de acoso moral. El desvalor de resultado que se produce consume, sin duda, cualquier injuria que pudiera apreciarse en el acto *ad supplantationem*.

Pueden surgir dudas sobre si se ha falsificado un documento *privado*. A nuestro modo de ver, ello no sería posible: B se ha limitado a seguir (virtualmente) a otros perfiles para dar publicidad de los datos de A; pese a que esa acción puede generar una notificación en la cuenta del tercero, consideramos que esa notificación no puede calificarse de documento privado. Sólo cabría esa calificación si existiera una verdadera interacción con terceros.

Por estar protegiéndose bienes jurídicos diferentes, el concurso que se da entre la usurpación —en caso de apreciarse— y el acoso moral sería de delitos y, concretamente, real.

B) Suplantación a través de intrusismo informático

Utilizaremos como referencia el siguiente caso práctico¹⁴⁴:

¹⁴² Seguramente, Mendo Estrella discreparía en este punto. En su opinión, el tráfico jurídico —protegido por el art. 401 CP— presenta una “configuración mercantil o económica”, lo que comporta que la mera “distorsión de las relaciones sociales del suplantado” devenga atípica. No compartimos este extremo por dos motivos. Primero, pensamos que *tráfico jurídico* tiene un significado más amplio (al cabo, se trata de concepto indeterminado). Por el otro, el citado autor basa su postura, entre otras resoluciones, en un auto que rechazaba la existencia de un delito de usurpación de estado civil en el ámbito de Tuenti, una red social (hoy inexistente) que tenía carácter *privado* —al perfil de un usuario sólo podían acceder aquellos contactos que aquél agregase voluntariamente—, de forma que la trascendencia de la suplantación estaba “limitada al foro de contactos en que se actuaba”, como el propio auto indica. En fin, el comportamiento era atípico porque la arrogación de la identidad digital ajena no reunía las notas de persistencia y continuidad que exige la jurisprudencia. Cfr. AAP Segovia 25-03-2010 (Cendoj, ECLI:ES:APSG:2010:11A), FJ 4.º, y MENDO ESTRELLA, Á.: “Delitos...”, *op. cit.*, pp. 29-32.

¹⁴³ Boix Reig y Díaz López son algunos de los autores que postulan un concurso de delitos. En BOIX REIG, J.: *El delito...*, *op. cit.*, p. 44, y DÍAZ LÓPEZ, J. A.: *El delito...*, *op. cit.*, p. 214.

¹⁴⁴ La parte inicial de la redacción procede, en parte, de INTECO: *Guía...*, *op. cit.*, p. 18. Un caso similar se encuentra en la SAP Girona 22-06-2015 (*cit.*).

Como cada tarde después de trabajar, A se dispone a acceder a su cuenta personal de Twitter, pero, cuando introduce su nombre de usuario y contraseña, se le deniega el acceso: aparentemente, los datos introducidos no coinciden con los registros de la red. Al buscar su perfil a través del buscador de Twitter, comprueba que todavía existe, pero no logra recuperar su contraseña a través de su correo electrónico.

Días más tarde, el sujeto A observa que el perfil está siendo gestionado por alguien que no es él. Su suplantador, B, ha publicado información que le resulta perjudicial: en un tuit, ha compartido varias conversaciones mantenidas en el chat privado de Twitter; en otros, ha manifestado opiniones en su nombre, causando cierta polémica. Estas acciones se realizan de manera que los seguidores de A (más de 500 personas) piensan que es él quien está actuando. El sujeto B había logrado acceder a su cuenta mediante una herramienta de jaqueo, y no comenzó a disponer de ella (ni a leer los chats) hasta transcurridos varios días.

a) Tipicidad *ad supplantationem*

En supuestos como el relatado, en el que la suplantación tiene lugar mediante el apoderamiento de una cuenta que pertenece al suplantado, la situación cambia considerablemente. Los hechos únicamente pueden subsumirse en un tipo: el de intrusismo informático (art. 197 bis). En efecto, al acceder ilegalmente a su perfil de Twitter, el sujeto B está vulnerando las medidas de seguridad establecidas para impedir ese acceso. El tipo penal no precisa vulnerar la privacidad del individuo de la cuenta —según justificamos en el capítulo anterior—, por lo que el desvalor de resultado es considerable: junto con haber dañado la seguridad del sistema, B puede acceder a información privada de A (acceso que, en este momento, todavía no se ha producido). Puesto que el medio empleado para vulnerar las medidas de seguridad es una técnica avanzada de jaqueo, esta subsunción no ofrece dudas. Sí lo haría, según algunos autores, si se hubiera accedido al perfil mediante la mera adivinación de la contraseña y ésta careciese de una mínima complejidad técnica¹⁴⁵.

Así las cosas, a diferencia del primer caso analizado, la suplantación *per se* no supone un ataque a la intimidad o a la propia imagen —pues todavía no se han descubierto ni revelado datos de A— ni una afrenta a su honor. Tampoco parece haber falsedad documental: cabría plantearse si se ha *alterado* la cuenta del usuario suplantado en cuanto archivo electrónico ligado al contrato mercantil, pero ello es harto complicado de sostener, pues el contenido de ese contrato no se ha visto modificado.

Plantea ciertas dudas el tipo de daños informáticos (art. 264): el éxito en la suplantación de la cuenta de A no reside únicamente en haber podido acceder sin consentimiento a ella, sino en que A es incapaz de recuperarla, volviéndose los datos *inaccesibles*. Esta inaccesibilidad sería típica por el citado artículo siempre y cuando el resultado producido sea grave. En este sentido, la gravedad podría justificarse si se probara que la información contenida en el perfil

¹⁴⁵ ANARTE BORRALLO, E. y DOVAL PAIS, A.: “Límites...”, *op. cit.*, § 12.

de A es especialmente sensible o confidencial, pero, aun así, las diferencias entre este daño y el desvalor de resultado que está capturando el art. 197 bis serían prácticamente nulas.

b) Tipicidad *in supplantatione*

Una vez *en* la cuenta de Twitter suplantada, el sujeto B publica una serie de informaciones que perjudican a A, y que involucran nuevos tipos penales:

a) Usurpación de estado civil (art. 401). Sucede algo similar al primer supuesto analizado: al publicar tuits en nombre de A sin su autorización —con independencia de si su contenido es cierto o no—, el sujeto B se está arrogando facultades cuyo ejercicio no le corresponden. Puesto que se ha suplantado la cuenta *personal* de Twitter de A, entendemos que habría usurpación en todo caso, aunque no podemos olvidar que A podría no figurar con su nombre y sus apellidos en la red social —aun pudiendo ser reconocible por terceros—, factor que dificultaría nuevamente la apreciación del tipo. Desde nuestro punto de vista, la usurpación de elementos como el nombre de usuario o el correo electrónico debería ser suficiente, al tratarse de extensiones del nombre en el ciberespacio (según se argumentó en el capítulo II).

b) Descubrimiento y revelación de secretos (art. 197.4). De acuerdo con los hechos narrados, se entiende que B ha accedido a datos del perfil de A de carácter privado: los chats. Desde que tiene lugar ese acceso, su conducta es típica *ex* art. 197.2 por la injerencia en la intimidad de A. Además, si se considera que la conducta se ha realizado vía jaqueo, podría estimarse la agravante del art. 197.4, por concurrir la circunstancia de la letra *b*) del precepto (“la utilización no autorizada de datos personales de la víctima”), que, como señalábamos anteriormente, la doctrina vincula al intrusismo. En el momento en que B publica los datos, se produce la circunstancia agravante de revelación que señala *in fine* el citado art. 197.4. Por supuesto, este tipo consume el desvalor del art. 197 bis.

c) Injuria (art. 208). Junto con la revelación del contenido de los chats, el suplantador ha publicado otros tuits atribuyendo opiniones que A *no* piensa. Mientras que el daño que A pueda sufrir en su dignidad por el primer hecho queda consumido por el tipo del art. 197.4, no sucede lo mismo con el segundo grupo de tuits, que no son típicos por dicho precepto. Si se trata de un tipo de injuria o no, dependerá de que B haya actuado “con conocimiento de su falsedad o temerario desprecio hacia la verdad” sobre los hechos, juicio que, por la falta de detalles en el enunciado del caso, no procede realizar. Por lo demás, el hecho de que injuria se lleve a cabo vía suplantación no plantea problemas interpretativos.

d) Falsificación de documento privado (art. 395). Al publicar los tuits en nombre de A, el sujeto B está *simulando* que ha sido A quien ha decidido manifestar esas declaraciones a terceras personas. Con independencia de si lo manifestado es cierto o no, podríamos afirmar que B está falsificando un documento privado si aceptáramos la interpretación extensiva que

ya indicamos. El art. 395, que tipifica esta infracción, requiere la intención de “perjudicar a otro”; ello es fácil de alegar en este supuesto, en el que concurren otros tipos penales —que suponen un perjuicio—, de forma que la falsedad sería el *medio* para cometer dichos tipos. No obstante, de la misma forma que en el primer caso práctico, el concurso entre este tipo y la usurpación de estado civil se complica.

Parece que la relación entre la usurpación de estado civil y el delito de descubrimiento y revelación de secretos es de concurso medial de infracciones: al publicar información privada de A, el sujeto B está usurpando su estado civil, y lo está haciendo utilizando sus datos personales de forma no autorizada. Por su parte, dado que la injuria es de carácter incidental, entre ésta y los delitos anteriores se daría un concurso real en el caso de estudio, lo que no obsta a que, en otros supuestos, pudiera hablarse de concurso medial. Finalmente, las dos falsedades se encontrarían en concurso de normas, debiendo ser la usurpación (en caso de que llegáramos a apreciarla) aplicable en consunción de la falsificación documental.

C) Conclusiones. Otros problemas de tipicidad y concursales

Los múltiples *rodeos* interpretativos que deben darse al Código para capturar el máximo desvalor de resultado derivado de una suplantación en redes sociales resultan evidentes tras el análisis anterior. Es pertinente resumir los dos principales conflictos detectados:

a) El encaje de los actos de suplantación en alguno de los tipos de falsedades en vigor. Cuando ésta se realiza a través de un perfil ficticio (caso 1.º), es discutible si estamos ante una falsedad de documento mercantil al inicio, y más dudoso es que, al exteriorizarse la arrogación de facultades del sujeto suplantado, podamos hablar de una usurpación de estado civil en todo caso, especialmente si se utilizan elementos exclusivos de la identidad digital. Por su parte, si el suplantador se ha apoderado de una cuenta existente (caso 2.º), la posterior interacción con terceros usuarios de la red social¹⁴⁶ acaso podría considerarse una usurpación de estado civil, una falsedad documental o incluso ambas. De concurrir ambas, el problema se acentúa, pues no está claro hasta qué punto el concurso es de delitos o de normas (pese a que el grueso de la doctrina se decante por la primera opción, que estimamos más válida cuando se realiza el acto en el mundo físico, mas no cuando se trata del ciberespacio).

b) La confusión que generan algunos tipos del art. 197. Como decíamos en el capítulo III, la poca precisión de este precepto ha sido criticada fuera de los casos de suplantación en redes sociales. En este ámbito, surgen serias dudas de subsunción en lo referente a la creación de un perfil falso mediante información personal (reservada) de la víctima, pues, si bien la

¹⁴⁶ En el supuesto 1.º, decidimos —para simplificar la problemática— no incorporar una acción consistente en la interacción con terceros, si bien no sería extraño que ello aconteciera.

circunstancia del 197.4.b) parece concurrir —asumiendo que su sentido es equivalente al del tipo del art. 197 bis—, no está claro que se realice el 197.2, que emplea los inexactos términos “archivo o registro”.

Donde no encontramos un problema destacable es en lo tocante a las agresiones al honor o a la libertad de obrar: en la medida en que esas agresiones sean graves, los tipos penales correspondientes serán invocables, y generalmente la suplantación será el *medio* de comisión.

Naturalmente, la problemática en torno a la suplantación de la identidad digital no se agota en los casos prácticos que hemos examinado. Un tema en el que se pueden considerar múltiples variables es el de la *idoneidad* de la conducta. En redes sociales como Twitter, Instagram y Facebook, existen medios para informar a la plataforma de un jaqueo de cuenta; también es posible añadir un sello de verificación al perfil, lo que garantiza —a menos que se produzca el citado jaqueo— que quien está detrás de ese perfil es quien dice ser. Estas herramientas, entre otras, dificultan que una suplantación de identidad pueda prosperar¹⁴⁷.

Por otra parte, el fin último del suplantador no será siempre lesionar la privacidad, la integridad moral o el honor del suplantado: amenazas, daños informáticos, delitos contra la libertad sexual y, destacadamente, estafas —por medio del *phishing*¹⁴⁸— son otras de las figuras delictivas que pueden cometerse vía suplantación¹⁴⁹. Para finalizar, conviene recordar que nuestro examen se ha limitado a la parte esencialmente objetiva del delito, por lo que asuntos relacionados con la *culpabilidad* (sobre todo, el dolo) no han sido abordados¹⁵⁰.

2. DISCUSIÓN DE POLÍTICA CRIMINAL SOBRE LA SUPLANTACIÓN DE IDENTIDAD DIGITAL

A) Consideraciones previas

La seguridad jurídica recomienda adecuar la normativa penal a esta nueva fenomenología delictiva. A nuestro juicio, esta reconfiguración debe mantener la identidad como objeto de tutela indirecta de la ley penal. Construir *ex novo* una infracción penal que la proteja

¹⁴⁷ Cfr. ÉCJIA BERNAL, Á.: “Principales conductas antisociales de Internet (y III)”, *Diario La Ley*, 4, 2017, § IV.

¹⁴⁸ El *phishing* es, sin duda, una de las principales técnicas de suplantación, aunque no lo hemos tratado por afectar más a las empresas, las cuales carecen de *identidad* en los términos en los que nosotros la hemos definido.

¹⁴⁹ No hemos abarcado estos grupos de supuestos porque protegen bienes jurídicos no tan ligados a la personalidad —y, por tanto, a la identidad— como los anteriores. En efecto, la estafa protege el *patrimonio*, mientras que el tipo de daños informáticos puede cometerse sobre toda clase de *datos* (informáticos), no necesariamente identificativos. Acerca de los delitos contra la libertad e indemnidad sexuales, poco hay que decir. Por último, el contenido de unas amenazas suele estar ligado a otro bien (vida, intimidad, honor, patrimonio...), por lo que no consideramos tan pertinente su análisis.

¹⁵⁰ *V. gr.*, en una suplantación de identidad realizada a través de la creación de una cuenta falsa, no habría en ningún caso usurpación de estado civil cuando dicha suplantación se realice con finalidad humorística o satírica (por supuesto, la idoneidad de la conducta queda también en entredicho en estos supuestos). Este es el caso de múltiples perfiles *parodia* de Twitter e Instagram que utilizan nombres de personalidades famosas.

directamente no sería verosímil, por cuanto ataques absolutamente inocuos se verían trasladados a la *ultima ratio* del Derecho penal. El ámbito de sanción de estos comportamientos de escasa entidad ha de ser el civil, igual que sucede con los ilícitos civiles contra el honor, la intimidad o la propia imagen. Ello no sería inusual: la creación de un perfil falso en un supuesto similar al primero que examinamos fue objeto de sanción por la AEPD en 2011¹⁵¹. El hecho de que la frontera entre estas suplantaciones penalmente irrelevantes y aquéllas que merecen reproche penal sea imprecisa subraya la necesidad de revisar los tipos penales vigentes.

Para acometer esta propuesta, podemos optar por diferentes caminos:

a) Tipificar, como infracción autónoma, las suplantaciones de la identidad digital de otro que presenten carácter *grave*. En aras a la seguridad jurídica, el término *identidad digital* debería ser definido, y deberían indicarse criterios que permitan estimar la mayor (o menor) gravedad del daño, tarea no exenta de dificultades. Surgirían asimismo problemas en relación con el art. 197 bis CP. Esta es la alternativa que, *grosso modo*, proponía la FGE en 2014¹⁵², más tarde emulada por Magro Servet¹⁵³.

b) Adaptar el tipo del art. 401 CP para que contemple también la usurpación de estado civil por medios electrónicos, lo que capturaría con mayor precisión las suplantaciones de identidad *digital*. Ello sería, sin duda, apropiado, pues es evidente el carácter anacrónico de la usurpación de estado civil. Empero, seguirían existiendo dudas sobre si la arrogación de la dirección de correo electrónico, el número de teléfono o el nombre de usuario de otro, que no vayan expresamente acompañadas del nombre y los apellidos de su titular, serían típicas. Esta opción iría en línea con las reformas ya experimentadas por la estafa (*cf.* art. 248.2) o el examinado art. 197, entre otros delitos.

c) Establecer la suplantación de identidad *digital* como agravante específica de una serie de delitos, a saber, el acoso moral, las injurias o los delitos contra la privacidad. Esta es la tónica que ha seguido el legislador en las últimas modificaciones a la norma penal; la reforma que afectó a los delitos de homicidio y asesinato (arts. 138 a 142) es un fiel reflejo de ello.

¹⁵¹ EDITORIAL LA LEY: “Primera...”, *op. cit.*

¹⁵² “El que, en perjuicio de otro, suplantar 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”. FGE: *Memoria...*, *op. cit.*, pp. 748-749.

¹⁵³ A la propuesta de la FGE, el citado autor añade un segundo apartado: “Cuando el ofendido fuere alguna de las personas a las que se refiere el apartado 2 del artículo 173, se impondrá una pena de prisión de uno a dos años, o trabajos en beneficio de la comunidad de sesenta a ciento veinte días”. MAGRO SERVET, V.: “La tipificación...”, *op. cit.*, p. 11.

B) *Propuesta de reforma penal*

Optando por una vía a caballo entre las dos primeras, se propone modificar la ley penal en los términos que se exponen a continuación:

Primero. Modificar el tipo de usurpación de estado civil (art. 401) por un tipo de usurpación de identidad. La descripción típica sería: “El que usurpare *la identidad de otro...*” (la modificación se expresa en cursiva).

Segundo. Añadir, como segundo párrafo del nuevo art. 401, el siguiente inciso: “A los efectos de este artículo, se entenderá por identidad el conjunto de datos integrado por el nombre, las relaciones familiares y la nacionalidad de una persona física, incluyendo aquellas denominaciones alfanuméricas que pudiera tener esa persona en el plano digital y permitan su reconocimiento de forma análoga a los elementos anteriores”.

Tercero. Modificar el art. 197.2, de forma que afecte a “datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o informáticos, o en cualquier otro tipo de archivo o registro público o privado, *con inclusión de las agendas de contactos...*” (la adición, en cursiva).

Consideramos que esta propuesta despeja la mayoría de dudas que existen en casos como los examinados, a saber:

a) En primera instancia, dejaría de ser necesario entrar en la controvertida interpretación de las falsedades documentales, por cuanto el tipo de usurpación de identidad es lo suficientemente claro como para desviarlo a aquéllas. En el caso de que no fuese típica de usurpación por ser una suplantación inocua, tampoco creemos que pudiera reconducirse a alguna de las acciones del art. 390.1, pues éstas exigen, similarmente a la usurpación, una cierta credibilidad de la falsificación. Estos actos podrían ser castigados, en su caso, como ilícitos civiles.

b) Como corolario de lo anterior, se podría estimar razonablemente que la usurpación de identidad consume la falsedad documental cuando se realiza en el ciberespacio. Hemos apuntado que la doctrina más numerosa propone un concurso de delitos en todo caso, sin considerar que, cuando estamos extendiendo la calificación de documento a, por ejemplo, un tuit, resulta difícil justificar un *non bis in idem* entre la falsedad personal y la documental. Con esta propuesta de reforma, el conflicto queda resuelto: el concurso será de normas, y no de delitos (salvo, por supuesto, que en el caso concreto concurrieran dos acciones diferentes de falsedad, a modo de concurso real).

c) En tercer lugar, el innecesario debate sobre el contenido del estado civil quedaría relegado al plano del Derecho privado, eliminando toda inseguridad jurídica generada en torno al art. 401 CP. Bien es cierto que con añadir un inciso al precepto original definiendo lo

que debe entenderse por estado civil a efectos jurídico-penales se resolvería la cuestión, mas no sin el descontento de quienes —con razón— propugnan la equivalencia civil-penal del concepto de estado civil. Queremos insistir, por otra parte, en que la definición propuesta de *identidad* está fundada en el Derecho internacional.

d) Por último, la modificación del art. 197.2 permite integrar pacíficamente aquellas suplantaciones de identidad digital consistentes en la creación de un perfil falso en los que se difundan datos reservados de carácter personal del suplantado. Sostenemos que estos comportamientos merecen reproche penal en la medida en que la intimidad de la persona suplantada resulte dañada.

V. CONCLUSIONES

En las próximas líneas, exponemos las principales contribuciones que aporta este trabajo al estudio de los ciberdelitos.

Debido al creciente empleo de términos como *identidad digital* y similares, resultaba fundamental buscar una definición rigurosa de esta nueva realidad que pudiera asumirse en nuestro Derecho. La búsqueda de normas nacionales e internacionales nos llevó a concluir que, aunque no sea empleado habitualmente, existe un concepto jurídico de identidad que, a raíz de los profundos cambios en nuestras relaciones sociales, puede —y debe— ser adaptado al ámbito virtual o del ciberespacio.

Al analizar qué lugar ocupa este bien bajo la legislación penal vigente, enseguida se pudo comprobar su naturaleza de objeto *material*, que no jurídico, respecto de determinadas conductas típicas que atentan contra la fe pública, la privacidad, la seguridad de los sistemas informáticos y, en términos más generales, la libertad de obrar. Sin embargo, se evidenciaba al mismo tiempo que no en todas las ocasiones en que se protegía implícitamente la identidad a secas podía extenderse o adaptarse dicha protección a la identidad digital.

Después de un análisis general y teórico sobre esta cuestión, pasamos a lo práctico, esto es, a examinar las lagunas y dificultades de interpretación que existían en los casos concretos de suplantación de identidad digital, concretamente en redes sociales. Así, constatamos que se pueden distinguir dos clases de suplantación: aquéllas en las que el suplantador se apodera de una cuenta que era gestionada antes por el individuo suplantado, y las que consisten en la creación de un perfil falso de manera que el suplantador actúa como si fuera la víctima. Al mismo tiempo, se destaca lo práctico de diferenciar, para un mejor examen de las conductas, entre los actos dirigidos a la suplantación (*ad supplantationem*) y los que se llevan a cabo con posterioridad a ésta (*in supplantatione*).

En este punto, el desvalor de resultado de las conductas no termina de superar unos cánones de seguridad jurídica mínimos, debido, principalmente, a la imprecisión del art. 401 CP, el tipo de usurpación de estado civil —que obliga, a su vez, a hacer una interpretación extensiva de las falsedades documentales—, y de varios párrafos del art. 197 CP, el tipo de descubrimiento y revelación de secretos. Por ende, se proponen varias modificaciones a la norma penal que, en nuestra opinión, permiten solucionar los principales conflictos interpretativos.

Este trabajo pretende ser una contribución más al creciente debate en torno a la tipicidad de las suplantaciones de identidad en internet, aunque creemos que permite arrojar luz sobre gran parte de las incógnitas que le rodean y que ahonda en las aportaciones más importantes que se han realizado hasta la fecha. Por supuesto, restan cuestiones por analizar: en concreto, cuán estrecha pudiera llegar a ser la línea entre el delito y el ilícito penal es un asunto que merece ser examinado.

BIBLIOGRAFÍA

1. DOCTRINA CIENTÍFICA

- AECE: “La suplantación de una identidad digital”, *Cont4bl3*, 45, 38, 2013.
- ALONSO LECUIT, J.: *Identidad digital y seguridad online*, Real Instituto Elcano, Madrid, 2020. Disponible en <realinstitutoelcano.org/> (última consulta: 16-06-2020).
- ANARTE BORRALLA, E. y DOVAL PAIS, A.: “Límites de la ley penal a propósito del nuevo delito de intrusión informática”, *Revista General de Derecho Penal*, 18, 2012.
- ARISTÓTELES: *Ética a Nicómaco*, Alianza Editorial, Madrid, 2005.
- BARRIO ANDRÉS, M.: *Ciberdelitos: amenazas criminales del ciberespacio*, Reus, Madrid, 2017.
- BICARREGUI GARAY, J.: “El fraude on-line: Nuevo escenario, vieja picaresca”, *Boletín de Estudios Económicos*, 194, 311-332, 2008.
- BOIX REIG, J.: *El delito de usurpación de estado civil*, Universidad de Valencia, Valencia, 1980.
- BRAGG, M., y otros: “Authenticity”, *In Our Time*, BBC Radio, 2019. Disponible en <bbc.co.uk/programmes/m00035z4> (última consulta: 16-06-2020).
- BRANDEIS, L. y WARREN, S. D.: “The right to privacy”, *Harvard Law Review*, 4(5), 193-220, 1890.
- COBO DEL ROSAL, M. (dir.): *Compendio de Derecho penal español*, Marcial Pons, Madrid, 2000.
- COLÁS TURÉGANO, A.: “El delito de intrusismo informático tras la reforma del CP español de 2015”, *Revista Boliviana de Derecho*, 21, 210-229, 2016.
- DAVARA RODRÍGUEZ, M. Á.: “Suplantación de identidad en la Red”, *El consultor de los ayuntamientos*, 20, 2012.
- DESCARTES, R.: *Discurso del método*, trad. M. García Morente, Austral-Espasa Calpe, Madrid, 2010.
- DE HIPONA, A.: *Del libre albedrío*, trad. E. Seijas, Federación Agustiniana Española, 2005. Disponible en <augustinus.it/spagnolo/libero_arbitrio/index2.htm> (última consulta: 16-06-2020).
- DE LA MATA BARRANCO, N. J.: “Reflexiones sobre el bien jurídico a proteger en el delito de acceso informático ilícito (art. 197 bis CP)”, *Cuadernos de política criminal*, 118, 43-86, 2016.
- DE MONTALVO JÄÄSKELÄINEN, F. y otros: *Informe de Comité de Bioética de España sobre el derecho de los hijos nacidos de las técnicas de reproducción humana asistida a conocer sus orígenes biológicos*, Comité de Bioética de España, Madrid, 2020.
- DÍAZ LÓPEZ, J. A.: *El delito de usurpación del estado civil*, Dykinson, Madrid, 2010.
- DÍEZ-PICAZO, L. y GULLÓN, A.: *Sistema de Derecho civil. Vol. I*, Tecnos, Madrid, 1989.

- ÉCIJA BERNAL, Á.: “Principales conductas antisociales de Internet (y III)”, *Diario La Ley*, 4, 2017.
- EDITORIAL LA LEY: “Primera sanción de la AEPD al responsable de crear un perfil falso en una red social”, *Diario La Ley*, 7720, 2011.
- ENCABO VERA, M. A.: *Derechos de la personalidad*, Marcial Pons, Madrid, 2012.
- ESCRIBANO TORTAJADA, P.: “Algunas cuestiones sobre la problemática jurídica del derecho a la intimidad, al honor y a la propia imagen en internet y las redes sociales”, en A. Fayos Gardó (dir.): *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Dykinson, Madrid, 2015.
- FGE: *Memoria elevada al Gobierno de S.M. presentada al inicio del año judicial por el Fiscal General del Estado*, Ministerio de Justicia, Gobierno de España, Madrid, 2014. Disponible en <fiscal.es/memorias/memoria2014/FISCALIA_SITE/recursos/pdf/MEMFIS14.pdf> (última consulta: 16-06-2020).
- FREUD, S.: *El yo y el ello y otros escritos de metapsicología*, trads. R. Rey Ardid y L. López-Ballesteros y de Torres, Alianza Editorial, Madrid, 2012.
- GALÁN MUÑOZ, A.: “La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales”, *Revista Penal*, 24, 90-107, 2009.
- GÓMEZ BENGOCHEA, B.: *Derecho a la identidad y filiación*, Dykinson, Madrid, 2007.
- GONZÁLEZ RUS, J. J., y otros: “Delito e informática: algunos aspectos”, *Cuadernos penales José María Lidón*, 4, 2007.
- GORDON BENITO, I.: “Suplantaciones de identidad online. Claves (re)interpretativas del delito de usurpación de estado civil (1)”, *La Ley Penal: revista de derecho penal, procesal y penitenciario*, 143, 2020.
- HUSSERL, E.: *Meditaciones cartesianas*, trads. J. Gaos y M. García-Baro, Foro de Cultura Económica, México, 1996.
- HOOTSUITE y WE ARE SOCIAL: *Digital 2020: Spain*, 2020. Disponible en <datareportal.com/reports/digital-2020-spain> (última consulta: 16-06-2020).
- INCIBE: *Ciberseguridad en la identidad digital y la reputación online*, Ministerio de Asuntos Tecnológicos y Transformación Digital, Gobierno de España, 2016. Disponible en <incibe.es/protege-tu-empresa/guias/guia-ciberseguridad-identidad-online> (última consulta: 16-06-2020).
- INTECO: *Guía para usuarios: identidad digital y reputación online*, Ministerio de Industria, Energía y Turismo, Gobierno de España, Madrid, 2012. Disponible en <asesores.com/upload/590.pdf> (última consulta: 16-06-2020).
- KANT, I.: *Fundamentación de la metafísica de las costumbres*, trad. M. García Morente, Biblioteca Virtual Miguel de Cervantes, 1999. Disponible en <cervantesvirtual.com/obra-visor/fundamentacion-de-la-metafisica-de-las-costumbres--0/html/> (última consulta: 16-06-2020).

- KIERKEGAARD, S.: *Edifying discourses: A selection*, trads. D. F. Swenson y L. M. Swenson, Harper & Brothers, Nueva York, 1958.
- KIERSZENBAUM, M.: “El bien jurídico en el Derecho penal. Algunas nociones básicas desde la óptica de la discusión actual”, *Lecciones y Ensayos*, 86, 187-211, 2009.
- MAGRO SERVET, V.: “La tipificación penal de la suplantación de identidad en el uso de las redes sociales”, *Diario La Ley*, 9005, 2017.
- MANTILLA MOLINA, R. L.: “Sobre el concepto de *status*”, *Revista de la Facultad de Derecho de México*, 29, 1958. Disponible en <revistas-colaboracion.juridicas.unam.mx/index.php/rev-facultad-derecho-mx/article/view/25609/23007> (última consulta: 16-06-2020).
- MARTÍN SIERRA, Á.: *Concepto y límites del ‘legal smart contract’*, Universidad Pontificia Comillas, Madrid, 2020.
- MASSIP, J., y otros: *Commission Internationale de l’État Civil (CIEC)*, Kluwer Law Online, 2018. Disponible en <ciec1.org> (última consulta: 16-06-2020).
- MATUS ACUÑA, J. P. y HERNÁNDEZ BASUALTO, H.: “Anteproyecto de Código Penal Chileno de 2005, elaborado por la Comisión Foro Penal”, *Política Criminal*, 1(1), 1-92, 2005.
- MAYER LUX, L.: “El bien jurídico protegido en los delitos informáticos”, *Revista Chilena de Derecho*, 44(1), 235-260, 2017.
- MENDO ESTRELLA, Á.: “Delitos y redes sociales: Mecanismos formalizados de lucha y delitos más habituales. El caso de la suplantación de identidad”, *Revista General de Derecho Penal*, 22, 2014.
- MOLINA FERNÁNDEZ, F. (dir.): *Memento Práctico Penal 2019*, Francis Lefebvre, 2019. Disponible en <online.elderecho.com> (última consulta: 16-06-2020).
- NIETZSCHE, F.: *Crepúsculo de los ídolos o cómo se filosofa con el martillo*, trad. A. Sánchez Pascual, Alianza Editorial, Madrid, 2013.
- OBREGÓN GARCÍA, A. y GÓMEZ LANZ, J.: *Derecho Penal. Parte General: Elementos básicos de teoría del delito*, Tecnos, Madrid, 2015.
- QUINTERO OLIVARES, G., y otros: *Comentarios al Código Penal Español*, Aranzadi, Madrid, 1995.
- RODRÍGUEZ DEVESA, J. M. y SERRANO GÓMEZ, A.: *Derecho Penal Español. Parte Especial*, Dykinson, Madrid, 1995.
- RODRÍGUEZ FERNÁNDEZ, M. P.: “Suplantación electrónica de identidad. Posible respuesta jurídica penal”, *Diario La Ley*, 7906, 2012.
- RUNDLE, M., y otros: *At a crossroads: “personhood” and digital identity in the information society*. Dirección de Ciencia, Tecnología e Industria de la OCDE, 2008. Disponible en <oecd.org/dataoecd/31/6/40204773.doc> (última consulta: 16-06-2020).
- SIEBER, U.: *Legal aspects of Computer-Related Crime in the Information Society. COMCRIME study*, Universidad de Würzburg, 1998. Disponible en <oas.org/juridico/english/COMCRIME%20Study.pdf> (última consulta: 16-06-2020).

STEPHAN, M. J., y otros: “Identity burglary”, *Texas Review of Law & Politics*, 13(2), 401-418, 2009.

TOMÁS-VALIENTE LANUZA, C.: “Delitos contra la intimidad y redes sociales (en especial, en la jurisprudencia más reciente)”, *Revista de Internet, Derecho y Política*, 30, 30-41, 2020.

VILLACAMPA ESTIARTE, C.: *La falsedad documental: Análisis jurídico-penal*, Universitat de Lleida, Lleida, 1998. Disponible en <tesisenred.net> (última consulta: 16-06-2020).

2. DOCTRINA JURISPRUDENCIAL Y ADMINISTRATIVA

AAP Madrid 25-05-2017 (Cendoj, ECLI:ES:APM:2017:1634A).

AAP Segovia 25-03-2010 (Cendoj, ECLI:ES:APSG:2010:11A).

ATSJ Andalucía 17-11-2003 (Cendoj, ECLI:ES:TSJAND:2003:270A).

Circular FGE 21-09-2017 (BOE, 3/2017).

Informe AEPD 16-02-2011 (AEPD, 0437/2010).

SAN 17-09-2008 (Cendoj, ECLI:ES:AN:2008:3250).

SAP Girona 22-06-2015 (Cendoj, ECLI:ES:APGI:2015:940).

SAP Zaragoza 13-04-2011 (Cendoj, ECLI:ES:APZ:2011:1002).

SJP n.º 31 Madrid 04-09-2019 (Cendoj, ECLI:ES:JP:2019:39).

STC 02-12-1998 (HJ, ECLI:ES:TC:1988:231).

STC 26-02-2001 (HJ, ECLI:ES:TC:2001:49).

STC 03-07-2006 (HJ, ECLI:ES:TC:2006:216).

STEDH 07-07-1989 (HUDOC, ECLI:CE:ECHR:1989:0707JUD001045483).

STS 11-07-2001 (Cendoj, ECLI:ES:TS:2001:6029).

STS 01-06-2009 (Cendoj, ECLI:ES:TS:2009:3961).

STS 15-06-2009 (Cendoj, ECLI:ES:TS:2009:3931).

STS 04-05-2012 (Cendoj, ECLI:ES:TS:2012:3030).

STS 12-06-2012 (Cendoj, ECLI:ES:TS:2012:3999).

STS 07-07-2012 (Cendoj, ECLI:ES:TS:2012:5740).

STS 02-03-2016 (Cendoj, ECLI:ES:TS:2016:923).

3. LEGISLACIÓN

Constitución Española (BOE 29-12-1978).

Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo (BOE, 14-08-2013).

Instrumento de Ratificación de la Convención sobre los Derechos del Niño, adoptada por la Asamblea General de las Naciones Unidas el 20 de noviembre de 1989 (BOE, 31-12-1990).

Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 (BOE, 17-09-2010).

Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (BOE 08-01-2000).

Ley 20/2011, de 21 de julio, del Registro Civil (BOE 22-07-2011).

Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (BOE 14-05-1982).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales (BOE 06-12-2018).

Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil (BOE 25-07-1889).

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (DOUE 04-05-2016).

4. BASES DE DATOS

Sistema Estadístico de Criminalidad, Ministerio del Interior, Gobierno de España, 2020. Disponible en <estadisticasdecriminalidad.ses.mir.es> (última consulta: 16-06-2020).

Versión en línea del *Diccionario de la Lengua Española*, RAE, 2020. Disponible en <dle.rae.es> (última consulta: 16-06-2020).

Versión en línea del *Diccionario del español jurídico*, RAE y CGPJ, 2020. Disponible en <dej.rae.es> (última consulta: 16-06-2020).