La “identidad digital” en internet: creación de perfiles falsos en redes sociales

“Digital identity” on the net: the creation of fake profiles on social media

María González García Viñuela
Magíster en Derecho de la ciberseuridad y entorno digital
Universidad de Valladolid
Castilla y León, España
https://orcid.org/0009-0005-9282-9514

https://doi.org/10.59659/rifed.v13.2025.ch14

Resumen

Los avances tecnológicos de las últimas décadas han aumentado la preocupación por la protección de los derechos de la personalidad (honor, intimidad, propia imagen y protección de datos) en internet. El hecho de que la Red no tenga barreras territoriales dificulta la persecución y sanción de este tipo de conductas. Ante esta nueva realidad los Estados han comenzado a incorporar expresamente en sus normas sustantivas penales el castigo de los ciberdelitos. Los ordenamientos nacionales también cuentan con mecanismos en vía civil para el castigo de las conductas menos graves. Sin embargo, no se ha planteado la creación de instrumentos mundiales que respondan a la persecución de este tipo de conductas, teniendo en cuenta su carácter transnacional.

Palabras clave
Identidad digital, derecho al honor, intimidad y propia imagen; derecho a la protección de datos; ciberdelincuencia; perfiles falsos en redes sociales

Abstract

Technological advances in recent decades have brought with them concerns about how to protect personal rights (like honor, privacy, self-image, and data protection) on the Net. The fact that the Internet has no territorial barriers makes it difficult to prosecute and punish this type of behavior. Faced with this new reality, States have begun to expressly incorporate the punishment of cybercrime into their substantive crimi-

nal laws. National legal systems also have civil mechanisms in place to punish less serious conducts. However, given the transnational nature of cybercriminality, the creation of global instruments that respond to and prosecute cybercrime has not been considered.

Keywords
Digital identity; right to honor, privacy, and personal image; right to data protection; cybercrime; fake profiles on social media

INTRODUCCIÓN

Desde mediados del siglo XX se han producido tres cambios relevantes con repercusión en la evolución social: la Sociedad de la Información a través de la llamada "Revolución Informática"; la Sociedad de Riesgos; y, la aparición de la Sociedad Global, que ha supuesto el desvanecimiento de las fronteras nacionales (Anguita Osuna, 2018: 108).

La tecnología avanza a mayor ritmo que la regulación legal. Para tratar de hacer frente a las nuevas formas de comisión de delitos, parece necesaria una legislación, permanentemente revisada y actualizada, que reúna y sistematice todos los delitos cibernéticos. Son pocos los países que disponen de una legislación adecuada para hacer frente a este nuevo enfoque de la criminalidad.

Para combatir la delincuencia que tiene lugar en el ciberespacio son necesarios medios especializados capaces de ofrecer una respuesta eficaz. El aumento exponencial de los ciberdelitos exige a los Estados no solo una regulación sustantiva y procesal adecuadas, sino también que cuente con Fuerzas y Cuerpos de Seguridad especializados, competentes para detectar y perseguir a los ciberdelincuentes.

La ciberdelincuencia en España ha pasado de los 40.000 delitos, en 2011; a los 375.000, en 2022. En el período comprendido entre 2011 y 2016, se aprecia un crecimiento aritmético, que se ha transformado en geométrico de 2017 a 2022. Dentro de la modalidad de ciberdelitos, los fraudes informáticos, amenazas y coacciones y falsificación informática

son, respectivamente, los más cometidos. Este trabajo se centra en la creación de perfiles falsos en redes sociales, tipificado en el ordenamiento jurídico español como una modalidad del delito de coacciones, por el impacto que tiene en la identidad digital.

Planteamiento de la cuestión

La creación de perfiles en redes sociales puede vulnerar los derechos tradicionales de la personalidad (honor, intimidad y propia imagen) y el derecho a la protección de datos. La regulación prevista para estos derechos puede resultar insuficiente o no del todo adecuada para garantizar el reproche, tanto en vía civil como penal para los casos más graves, de este tipo de conductas. Por ello, cabe plantearse si, tras el desarrollo tecnológico alcanzado en las últimas décadas, la protección prevista para estos derechos es suficiente para dar una respuesta jurídica adecuada y suficiente al daño reputacional que se puede ocasionar a una persona con este tipo de conductas.

A pesar de que la investigación se centra en el estudio de un ordenamiento jurídico concreto, el español, presenta también una dimensión internacional ya que, al tratarse de conductas realizadas en la Red, los eventuales autores y perjudicados pueden localizarse en cualquier país. De ahí, la necesidad de una regulación global.

Las conductas de creación de perfiles falsos están siempre relacionadas con la usurpación de identidad. El ordenamiento jurídico español, junto con la tradicional protección en vía civil de los derechos de la personalidad, introdujo, en 2022, un tipo penal para proteger a los usuarios frente a la creación de perfiles falsos en redes sociales.

Las principales cuestiones que se van a abordar y a las que se pretende dar respuesta son: (1) cuál de los ordenamientos, civil o penal, es más idóneo para hacer frente al extraordinario incremento de la creación de perfiles falsos en la Red; (2) si la conducta penal introducida en el Código Penal español en 2022 debería extenderse al resto de los países

para combatir los ciberdelitos; y, (3) cómo podría lograrse una cooperación transnacional eficaz en la lucha contra este tipo de intromisiones.

Para ello, se ha realizado, por un lado, un breve estudio de la regulación, europea y transnacional, examinando: qué países cuentan con una tipificación penal expresa de la creación de perfiles falsos en redes sociales; su ubicación sistemática; los bienes jurídicos afectados; y, los elementos típicos del delito en el ordenamiento jurídico español, y, por otro, se ha analizado la posibilidad de aplicar otro tipo de sanción, civil o incluso administrativa para el castigo de estas conductas.

Instrumentos europeos e internacionales en materia de delincuencia informática

La globalización está íntimamente relacionada con las nuevas tecnologías, fundamentalmente a través de la Red. Actualmente la Red cuenta con más de cinco millones de usuarios, lo que representa más de la mitad de la población mundial, entre los que también se encuentran individuos o grupos de individuos que realizan actividades ilícitas, los ciberdelincuentes (Cocchini, 2021: 70). Esto ha llevado a numerosos países a la convicción de la necesidad de una legislación sobre delincuencia informática, que facilite la investigación, persecución y sanción de los delitos cometidos a través de las Tecnologías de la Información y la Comunicación (TIC).

La primera respuesta sobre delincuencia informática se esboza en el Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos, denominado «Manual Tallin», redactado por la ONU en 1977.

En el ámbito europeo, pero de aplicación transnacional, el Consejo de Europa redactó el Convenio Europeo sobre Ciberdelincuencia, aprobado en Budapest el 23 de noviembre de 2001, que establece pautas de actuación en los ámbitos penal y procesal (Corcoy Bidasolo, 2007, pp. 8-9), siendo actualmente el texto más relevante en esta materia. Ha sido

suscrito por 54 países, tanto Estados miembros de la UE como terceros países, entre los que se encuentran potencias mundiales como Estados Unidos.

Se trata del primer Tratado de carácter internacional que aborda los delitos informáticos a través de leyes nacionales y la cooperación entre Estados. En este Convenio se establecen tres objetivos esenciales: (1) armonizar el Derecho penal material, (2) promulgar medidas procesales en el ámbito digital y (3) establecer un régimen activo y funcional de cooperación internacional.

Este texto presenta algunas deficiencias. Uno de sus principales fallos es la excesiva libertad que otorga a los Estados para tipificar las conductas en los ordenamientos internos, lo que dificulta la uniformidad en la aplicación del Derecho penal. El otro es que el rápido avance de la tecnología y la irrupción de la inteligencia artificial hacen que este instrumento se haya quedado obsoleto.

Concepto de ciberdelincuencia

La construcción del concepto de ciberdelincuencia es eminentemente doctrinal. Algunos autores utilizan los términos «cibercrimen» o «ciberdelito» para referirse a aquellas conductas que aprovechan las comunicaciones electrónicas para la comisión de una acción delictiva (Barrio Andrés, 2018: 38). Se pone el acento en los medios de comisión del delito, definiéndolos como delitos perpetrados en el ciberespacio o espacio virtual (Subijana Zunzunegui, 2008: 171).

Romeo Casabona (2006) introduce un elemento esencial, la falta de consentimiento, al definir la ciberdelincuencia como el "conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en entornos TIC, perpetradas sin consentimiento o autorización, de tal manera que se afecten bienes jurídicos diversos ya sean de naturaleza individual o supraindividual" (Romeo Casabona, 2006: 9). Este elemento es fundamental en la tipificación que reciente-

mente se ha introducido en el ordenamiento jurídico español del delito de creación de perfiles falsos.

El Derecho penal como ultima ratio

El Derecho penal debe responder ante las nuevas amenazas haciendo uso de los mecanismos de que dispone, pero sin conculcar sus principios estructurales, en especial, el principio de última ratio (Barrio Andrés, 2011: 279), manifestación del principio de intervención mínima (Luzón Peña, 2016: 42), conforme al cual, el Derecho penal solo debe intervenir ante los conflictos sociales cuando sea estrictamente necesario (Cancio Meliá y Pérez Manzano, 2019: 80); y, por supuesto, el principio de legalidad, como límite impuesto por el Estado de Derecho al ejercicio del ius puniendi, que se concreta en el aforismo nullum crime nulla poena sine lege y que supone que no puede imponerse ninguna pena que no esté prevista en la Ley (Muñoz Conde y García Arán, 2022: 91). Por tanto, es necesario delimitar cuáles son las conductas más graves, que precisan del derecho penal para su reproche; y, para las demás, es suficiente la sanción civil.

La identidad digital

No cabe duda que las comunicaciones, la seguridad y el acceso a la información han experimentado un enorme progreso gracias a la mejora de las tecnologías. Sin embargo, también ha traído consigo nuevas amenazas como el aumento de la delincuencia cometida a través de la red, entre la que se encuentra el robo de identidad personal, que afecta a la vida íntima de las personas.

Las cuentas de correo electrónico, los perfiles editados en las redes sociales, los chats, los foros o la mensajería instantánea integran la identidad digital de la persona concebida como el conjunto de datos que permiten que se comunique en la Red, intervenga en redes sociales y opere en las páginas web (De Prada Rodríguez y Santos Alonso, 2013: 225). Por tanto, son datos que identifican o hacen identificables a las personas

en las interacciones online.

En el contexto de la sociedad tecnológica, dominada por la comunicación a través de la Red, el concepto de «identidad» encuentran nuevos desafíos como el anonimato, los pseudónimos, los perfiles falsos y la suplantación de identidad digital. La identidad se puede definir como el conjunto de atributos y características que permiten individualizar a la persona en sociedad, pertenecientes a un individuo determinado, o compartidos por todos los miembros de una determinada categoría o grupo social (Borghello y Temperini, 2016: 291-292). Hoy en día no cabe duda de que existe una identidad digital que "no sólo nos representa de alguna manera, sino que está en constante interacción con nuestra identidad física y moral", (Tarodo Soria, 2025: 410). Si bien la suplantación de la identidad digital puede adoptar diferentes formas, los elementos esenciales y la finalidad no varían. Esta finalidad consiste en obtener la información que permita la identificación de la persona y el uso posterior de la misma para hacerse pasar por el verdadero titular de tales credenciales. Estas acciones suelen llevar consigo consecuencias perjudiciales para el individuo, tanto personales, tales como la pérdida reputacional o daños a su honor e imagen personales, como patrimoniales (pérdidas económicas) (Borghello y Temperini, 2016: 297-298).

METODOLOGÍA

Para la elaboración de este artículo se ha utilizado la metodología propia de la Ciencia jurídica. En particular, la Ciencia del Derecho penal, dividida en dos grandes ramas: la orientación criminológica, que estudia el delito como fenómeno social y biopsicológico; y la orientación jurídico-dogmática que estudia el delito y sus consecuencias como fenómeno jurídico previsto en las normas y que precisa ser interpretado y aplicado (Muñoz Conde y García Arán, 2022: 177), siendo este el enfoque utilizado en este trabajo. Y la Ciencia del Derecho civil, que supone el estudio sistemático y analítico de las normas que regulan las relaciones entre personas, conforme a las reglas de interpretación y aplicación

previstas en el art. 3.1 CC. Así, las normas civiles se deben interpretar atendiendo al sentido propio de las palabras, en relación con el contexto; los antecedentes históricos y legislativos; y, la realidad social del tiempo en que deben aplicarse; y deben atender fundamentalmente al espíritu y finalidad de la propia norma.

RESULTADOS

La preocupación por adoptar una legislación específica frente al crecimiento de los delitos informáticos que se sirven de una usurpación de la identidad utilizando datos de identificación personal para la comisión de otros delitos tiene su origen en la Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo y al Comité de las Regiones, de 22 de mayo 2007. La razón de su tipificación radicaría en la necesidad de facilitar la cooperación judicial y policial en todos los Estados miembros (Comisión Europea, 2007: 8).

La Directiva 2013/40/UE establece un enfoque integrado contra la ciberdelincuencia y aboga por el establecimiento de medidas eficaces contra la usurpación y otras infracciones relacionadas con la identidad. En 2014, haciéndose eco de esta Directiva, la Fiscalía General del Estado alertaba ante el incremento de acciones de usurpación de la identidad en foros, chats, redes sociales y, en general, en medios de comunicación electrónicos (FGE, 2014: 742), y defendía la necesidad de una tipificación específica de estas conductas en un capítulo independiente bajo la rúbrica de la suplantación de la identidad online, dentro del Título XVIII del Libro II CP, relativo a las falsedades (FGE, 2014: 748). Esta no fue la ubicación elegida por el legislador a la hora de su tipificación expresa.

Tipificación expresa de los ciberdelitos

Para la tipificación en el plano sustantivo de los ciberdelitos a nivel comparado, se ha recurrido a dos técnicas normativas. Algunos países como Chile, Estados Unidos, Francia, Gran Bretaña, Holanda o Venezuela han optado por el recurso a las leyes penales especiales. Otros

países como Alemania, Argentina, Austria, España, Italia o Portugal se han decantado por la tipificación de las nuevas figuras delictivas en su propio CP (Barrio Andrés, 2018: 57).

En particular, numerosos países cuentan con una tipificación específica de la suplantación de la identidad digital (Solari Merlo, 2023: 202). Aquí nos referiremos a aquéllos que castigan la suplantación de la identidad en sentido estricto, dejando los que castigan la apropiación de datos como acto previo a la comisión de otros delitos.

Los primeros países en tipificar expresamente la suplantación de identidad digital fueron Estados Unidos (en concreto, el Estado de California) y Francia en 2011. En el caso de Francia, el art. 226.4.1 de su Ley castiga la usurpación de la identidad de tercero o el uso de uno o más datos que permitan identificarlo con el fin de perturbar su tranquilidad o atentar contra su honor, haciendo expresa mención a la imposición de la misma pena cuando el delito se cometa "en una red pública de comunicación en línea". En 2013 introdujeron esta conducta delictiva, en sus respectivos ordenamientos, Costa Rica y Perú. Otros países europeos que castigan estos hechos son Suecia (2015), Países Bajos (2016), Alemania (2017) y recientemente Dinamarca (2022). En Suecia y Países Bajos, la conducta tipificada se refiere al uso de datos personales que siendo identificativos de una persona sean susceptibles de causar un daño financiero o un «inconveniente más que menor», o cualquier perjuicio derivado de ese uso, respectivamente. En el caso de Alemania, la tipificación es análoga en algunos aspectos a la española, pues también requiere que se lleve a cabo sin autorización, pero difiere en que exige expresamente que pueda perjudicar significativamente y de forma reiterada el modo de vida de la persona suplantada (Ibid.: 203-206).

Otros países como Brasil, Chile, Colombia, Ecuador e Italia no tipifican el delito de suplantación de la identidad digital de forma expresa pero esta conducta queda recogida en el delito genérico de suplantación de la identidad, es decir, que la regulación del delito tradicional de su-

plantación de identidad es aplicable también a su comisión a través de las TIC. El art. 494 del CP italiano castiga la sustitución ilícita de una persona atribuyéndose, a sí mismo o a otra persona, un nombre o estado falso o cualquier otra cualidad a la que la Ley atribuya efectos jurídicos, cuando el hecho no sea constitutivo de otro delito contra la fe pública (Ibid.: 207-208).

Finalmente, hay países que cuentan con Proyectos de reforma de sus legislaciones, pero que todavía no han incorporado este delito en sus respectivos ordenamientos jurídicos. Esto es así en Argentina, México o Uruguay (Ibid.: 208-209).

En España, la tipificación específica y generalizada de los delitos tecnológicos se produce con la LO 1/2015, de 30 de marzo. Esta reforma supuso la transposición de la Directiva 2013/40/UE. En particular, se introdujeron los delitos de stalking (art. 172 ter 1 CP), intrusismo informático (art. 197 CP), estafa informática (actual art. 248 CP, tras la LO 14/2022), daños informáticos (art. 264 CP) y el child grooming (actual art. 183 CP, LO 10/2022).

Introducción expresa de la conducta de creación de perfiles falsos en redes sociales

El art. 172 ter CP, castiga las conductas de acoso permanente a una persona como delito contra la libertad, modalidad en la que encajan algunas conductas de suplantación de la identidad de un tercero. Este precepto castigaba conductas de acoso que incidieran en la libertad de las personas realizadas con la finalidad específica de adquirir productos o mercancías, contratar servicios o hacer que terceras personas contacten con la víctima. El Preámbulo de la LO 1/2015 pone de manifiesto que esta modificación viene a ofrecer una respuesta a conductas de cierta gravedad que no podían ser calificadas y castigadas como amenazas ni coacciones. En él se señala que hay conductas de determinada gravedad que, sin llegar a suponer un anuncio explícito o no de la intención de causar un mal (amenaza) o sin el empleo directo de violencia para coartar la

libertad de la víctima (coacción), se menoscaba gravemente su libertad sometiéndola a una vigilancia o persecución constante mediante actos de hostigamiento. Con tal redacción, sin embargo, quedaban al margen los supuestos denunciados por la FGE en los que se pretendía que el castigo tuviera lugar por el mero hecho de hacerse pasar por un tercero en las relaciones online, es decir, "utilizar falsamente o usurpar la identidad real de otra persona, de tal modo que esa conducta sea susceptible de conducir a error sobre la verdadera identidad, cualquiera que sea la finalidad que con ello se pretenda" (FGE, 2014: 743-744).

La creación de perfiles falsos se incorpora como delito autónomo en el art. 172 ter CP, introducido por la LO 10/2022, tipificándose como una modalidad de acoso en el Capítulo III, de las coacciones, del Título VI, delitos contra la libertad. Con anterioridad a esta reforma, la suplantación de la personalidad ajena en redes sociales era considerada por la doctrina como una figura diferente del delito de usurpación civil del art. 401 CP, pues éste exige una clara suplantación constante de una persona por parte de otra, no solo mediante acciones virtuales y esporádicas sino con la intención de permanencia temporal (Velasco Núñez y Sanchís Crespo, 2019: 225-226). En ocasiones se ha mantenido que la creación de un perfil falso en una red social es constitutiva de un delito de falsedad en documento privado mercantil de acuerdo con el art. 392, en relación con el art. 390.1.1º CP. Incluso, de forma minoritaria, se ha considerado como un delito de revelación de datos personales o como un delito de coacciones (De Prada Rodríguez y Santos Alonso, 2013: 225-226). Finalmente, algunos autores han planteado la posibilidad de castigar estas conductas a través del delito de stalking del art. 172 ter 1. 3ª CP.

La jurisprudencia ha venido castigando este tipo de conductas como injurias, vejaciones injustas o falsedad en documento mercantil, de lo que se desprende que las conductas más graves ya encontraban acomodo en el CP antes de la introducción de un tipo autónomo que se refiere expresamente a la creación de este tipo de perfiles en la Red y, por tanto, a efectos de condena, no puede entenderse que la conducta en sí

sea nueva.

Análisis de los aspectos más relevantes del delito

El origen de la criminalización del delito de stalking se sitúa en Estados Unidos en los años 90 tras el asesinato de varias personas. Posteriormente se tipificó como delito en el Derecho anglosajón y más tarde llegó a Europa continental.

Los aspectos más relevantes de dicha conducta, tal y como se define en el artículo 172 ter 5 del Código Penal español, son: (1) los bienes jurídicos protegidos y (2) los requisitos para que la conducta sea perseguida y castigada como delito.

Bien jurídico protegido

En cuanto a la ubicación sistemática del delito, atendiendo al bien jurídico protegido, distinguimos tres bloques: delitos contra el patrimonio (Estados Unidos –California– y Costa Rica); delitos contra la fe pública (Brasil, Chile, Colombia, Italia, Países Bajos, Perú y el Proyecto de Argentina) y delitos relativos a la persona o a la personalidad (Alemania, Dinamarca, Ecuador, Francia, Suecia y las propuestas de México y Uruguay). Los ordenamientos que primero tipificaron estas conductas lo hicieron, con carácter general, asociadas al patrimonio; mientras que posteriormente se fueron vinculando a los delitos contra la libertad y la seguridad, (como España); y los que recogen la modalidad virtual junto con el delito genérico de usurpación del estado civil, asocian la conducta a la vulneración de la fe pública (Solari Merlo, 2023: 210).

En el ordenamiento jurídico español, con carácter general, el bien jurídico común a los tres capítulos del Título VI del Libro II CP es la libertad del individuo en los términos recogidos en el art. 17 CE. No obstante, las conductas tipificadas en cada uno de los capítulos de este título afectan a una concreta manifestación de esa libertad. En el caso de las coacciones, es la libertad general de actuación, es decir, que se tutela la libertad de llevar a cabo lo decidido previamente (Cuerda Arnau, 2022:

172). La jurisprudencia del TS señala, como criterio de distinción entre las coacciones y las amenazas, el efecto producido sobre la libertad del sujeto pasivo de la acción que, en el caso de las amenazas, será cuando incida sobre el proceso de formación de sus decisiones voluntarias, mientras que en el de las coacciones será cuando afecte a su voluntad de obrar (STS 2183/2000). De este modo, el sujeto amenazado ve perturbado su derecho al sosiego y a la tranquilidad personal en el normal desarrollo de su vida, así como el derecho a comportarse y decidir libremente, sin ningún tipo de intimidación; mientras que, en la coacción el individuo ha decidido libremente lo que quiere hacer o no hacer, y es en el momento de la ejecución cuando el sujeto activo del delito infiere violentamente en su libertad (Cuerda Arnau, 2022: 172).

Dentro de este bien jurídico, cabe plantearse si en el caso de creación de perfiles falsos, la manifestación de la libertad que es objeto de protección es la libertad entendida como libertad general de actuación del sujeto o libertad de obrar, o si, como ya se ha mencionado, estamos ante un delito pluriofensivo que afecta a otros bienes jurídicos como la integridad moral al exigirse que se ocasione a la víctima una situación de humillación, hostigamiento o acoso, la intimidad o incluso la propia imagen, siendo entonces más conveniente una ubicación diferente de esta figura.

Esta última es la opinión de un amplio sector doctrinal, que considera que el bien jurídico protegido es el binomio libertad-seguridad (Baucells I Lladós, 2014: 10; Gutiérrez Castañeda, 2013: 584; De La Cuesta Arzamendi y Mayodormo Rodrigo, 2011: 43-45). Esta consideración supone que tales conductas afectarían además de a la libertad de obrar, a la libertad entendida como proceso de formación de la voluntad.

En segundo lugar, atendiendo al requisito de crear en la víctima una determinada situación, el bien jurídico protegido es la integridad moral. Las torturas y otros delitos contra la integridad moral se regulan en el Título VII del Libro II CP (arts. 173 a 177 CP) y el Título VII bis,

que castiga la trata de seres humanos (art. 177 bis CP). La integridad moral, está consagrada en el art. 15 CE como un derecho fundamental, y se entiende como un atributo de la persona dotado de autonomía propia e independiente de los derechos a la vida, a la integridad física, a la libertad o al honor. Se concibe como el derecho de la persona a ser tratada conforme a su dignidad, sin ser humillada o vejada, con independencia de su situación o relaciones con otras personas. El TC español viene sosteniendo que el derecho a la integridad moral protege la inviolabilidad del ser humano no solo contra ataques dirigidos a causar lesión en su cuerpo o espíritu sino contra cualquier clase de intervención en ellos que no cuente con el consentimiento del titular (STC 137/1990).

Un sector doctrinal venía considerando que el bien jurídico protegido era la integridad moral, si bien matizando que cualquier atentado contra la integridad moral exige que se produzca un sentimiento de humillación y envilecimiento que no son consustanciales a algunas modalidades de acoso (Villacampa Estiarte, 2010: 46).

Finalmente, también podrían verse afectados los derechos a la intimidad personal y la propia imagen, consagrados como derechos fundamentales en el art. 18.1 CE, especialmente el derecho a la propia imagen, ya que el tipo habla específicamente del uso de la imagen de una persona. Estos delitos se regulan en el Título X CP, que consta de dos capítulos, respectivamente relativos al descubrimiento y revelación de secretos (Capítulo I, arts. 197 a 201 CP) y al allanamiento de morada, domicilio de las personas jurídicas y establecimientos abiertos al público (Capítulo II, arts. 202 a 204 CP).

El derecho a la intimidad, tiene por objeto garantizar al individuo un ámbito reservado de su vida, ligado al respeto de su dignidad como persona, prevista en el art. art. 10.1 CE, frente a la acción y el conocimiento de los demás, atribuyendo a su titular el poder de defender ese ámbito reservado, no sólo personal sino también familiar, frente a su divulgación por terceros y a una publicidad no querida (STC 58/2018).

La garantía de la vida privada de una persona y de su reputación tiene en la actualidad una dimensión positiva que excede el ámbito del derecho a la intimidad consagrado en el art. 18.1 CE y se traduce en un derecho de control sobre los datos del propio individuo. Así, la llamada «libertad informática» es el derecho a controlar el uso de los datos contenidos en un programa informático (habeas data) y engloba, entre otros aspectos, la oposición de una persona a que sus datos personales sean usados para fines distintos del interés legítimo que justificó su obtención (STS 1465/2022).

Respecto a estos bienes jurídicos, la aprobación definitiva del CP de 1995, en aplicación del carácter fragmentario y parcial del Derecho penal no incluyó la mera utilización de imágenes como recogía el Anteproyecto, al considerar que la protección de este bien jurídico está suficientemente garantizada con la LO 1/1982, de 5 de mayo. Por tanto, el Derecho penal no protege la propia imagen como bien jurídico autónomo ni directa ni indirectamente, sin perjuicio de que, a través de las imágenes entendidas como objeto material del delito, se puedan lesionar otros objetos formales como el honor y la intimidad, protegidos por la Ley penal (De Las Heras Vives, 2018: 450).

Algunos autores consideran la identidad digital como un bien jurídico autónomo que debería ser objeto de tutela. La identidad digital está íntimamente relacionada con el libre desarrollo de la personalidad y con otros bienes objeto de tutela penal en nuestro ordenamiento jurídico como el honor, la intimidad y la propia imagen cuando las conductas se desarrollan en el espacio virtual (Solari Merlo, 2021: 411). La suplantación online se define como aquellos actos en los que el sujeto interactúa en el espacio virtual haciéndose pasar por un tercero y sin su consentimiento. No se trata de un mero enmascaramiento de la realidad sino de un límite al disfrute de la personalidad en internet (Ibid.: 411).

Por tanto, de conformidad con lo anteriormente expuesto, cabe plantearse cuál es el bien jurídico protegido en la suplantación de iden-

tidad digital, tal como está regulada en el CP español. La referencia a la creación de una situación de acoso, hostigamiento o humillación como requisito indispensable para que el hecho de abrir un perfil falso en redes sociales, páginas de contacto u otro medio de difusión pública sin consentimiento del sujeto pasivo encaje en la conducta típica, puede interpretarse en el sentido de que en cualquier caso se estaría atentando contra la integridad moral, mientras que si se atiende a la ubicación sistemática de la figura delictiva, el bien jurídico tutelado sería la libertad. En mi opinión se trata de un delito pluriofensivo en el que los bienes tutelados son tanto la libertad como la integridad moral, así como el honor, la intimidad y la propia imagen del titular del perfil creado y, fundamentalmente, la identidad digital.

Todos estos bienes jurídicos tutelados, en caso de tipificación expresa del delito, debería ubicarse en un título propio, que llevara como rúbrica "de los delitos contra la identidad digital", reubicando en él todas las figuras delictivas que constituyen delitos contra las personas y que afectan también a estos bienes jurídicos cuando se cometan a través de las TIC.

Conducta típica: elementos

El art. 172 ter 5 CP castiga una suerte de suplantación momentánea de la identidad que consiste en el uso de la imagen, real o no, de un tercero, sin su consentimiento, para realizar alguna de estas conductas: publicar anuncios o abrir perfiles falsos en redes sociales, páginas de contacto o cualquier otro medio de difusión pública (Sánchez Benítez, 2023: 50-51). Estamos ante un delito de resultado, cuya consumación requiere que se cause una situación de «acoso, hostigamiento o humillación».

Para que el hecho encaje en la conducta prevista en el tipo penal es necesaria no solo la apertura del perfil falso, sino también la concurrencia de unos requisitos adicionales como son: la falta de consentimiento del titular del perfil abierto y que tenga lugar en redes sociales, páginas

de contacto o cualquier medio de difusión pública. Además, esta conducta, tiene que causar a la víctima una situación de acoso, hostigamiento o humillación.

Inexistencia de consentimiento

El consentimiento es un elemento relevante de este tipo penal, ya que determinará la existencia o no de responsabilidad penal.

La prestación del consentimiento por el titular del bien jurídico protegido plantea algunos problemas que tienen difícil solución. Por un lado, la libertad, pues el consentimiento supone la manifestación externa de la libertad del sujeto, por lo que la autonomía y la libertad constituyen el punto de partida de la imputación penal. Por otro lado, la disponibilidad de los bienes jurídicos, es decir, si los bienes jurídicos individuales son disponibles o no, y en caso de serlo, si lo son todos o sólo algunos (Íñigo Corroza , 2022: 170). Para poder dar respuesta a estas cuestiones hay que delimitar qué se entiende por consentimiento, cuál es el bien jurídico afectado y cuáles son las circunstancias del caso concreto.

El consentimiento se puede definir como la exteriorización libre y voluntaria de la voluntad del sujeto. La doctrina penal no solo española, sino también la alemana y anglo-americana, debaten sobre si el consentimiento debe entenderse como acuerdo, asentimiento, conformidad o ejercicio de autonomía. La manifestación del titular del bien jurídico a la injerencia en éste, que determine la inexistencia del delito, puede deberse a que esa exteriorización de la voluntad convierta el hecho en atípico o a que excluya la antijuridicidad de la conducta (Ibid.: 172). En los mismos términos se pronuncia otro sector doctrinal, que sostiene que el consentimiento puede operar excluyendo la tipicidad en los casos en que la definición positiva del delito precisa la voluntad adversa del sujeto pasivo, ya que en estos casos no existe lesión o puesta en peligro del bien jurídico tutelado; o destruyendo la antijuridicidad de la acción, pero persistiendo la estructura típica del delito (Quintano Ripollés, 1950: 329).

Finalmente, otros autores sostienen que, cuando el consentimiento es jurídicamente válido por haberlo emitido el titular del bien jurídico con plena capacidad y sin que concurra ningún vicio de la voluntad se diferencian tres supuestos. En primer lugar, aquéllos en los que de entrada no hay tipicidad por falta de relevancia jurídica (negativa) y de todo indicio injusto. En segundo lugar, aquéllos en los que el consentimiento jurídicamente válido es eficaz y permite la conducta, que de entrada es atípica por suponer la lesión o puesta en peligro del bien jurídico y por la falta de adecuación social, por considerar que se trata de una conducta socialmente normal y cotidiana, de manera que el permiso o autorización por el consentimiento supone una causa de justificación debida a la ponderación de intereses. En tercer lugar, en algunas figuras delictivas, el propio precepto penal pone de relieve que, además de la exención del consentimiento válido excluyente de la antijuridicidad, el consentimiento de hecho del sujeto pasivo, aunque en términos jurídicos sea plenamente válido no excluyendo la antijuridicidad del acto, es suficiente para excluir la ilicitud penal de la conducta consentida. Por tanto, el consentimiento fáctico será causa de exclusión solo de la tipicidad penal siempre que concurran determinadas condiciones que dependen de cada tipo (Luzón Peña, 2016: 360-362).

En segundo lugar, respecto a la disponibilidad del bien jurídico, el CP encierra intereses diversos, como pueden ser los que afectan a la realidad básica del individuo (vida, salud e integridad), los relativos a la proyección de su persona (libertad en sus diversas manifestaciones, ya sea libertad sexual, libertad de obrar e intimidad), intereses funcionales (los que protegen el honor, el patrimonio, la institución de la familia o la inviolabilidad del domicilio) y los intereses relativos a la protección de las condiciones de vida en sociedad (salud pública, medio ambiente, seguridad vial, orden socioeconómico, orden público, Constitución, Administración Pública o Administración de Justicia). Los más relevantes son los vinculados de forma mediata o inmediata a la persona, es decir, los bienes jurídicos individuales como son la vida, la integridad física y

moral, el patrimonio, la intimidad, el honor, la libertad ambulatoria, la libertad sexual y la libertad general de actuación (Íñigo Corroza, 2022; 172-173). En este caso, estamos ante un bien jurídico pluriofensivo de carácter individual, como son la libertad de obrar, la intimidad, la integridad moral, la identidad digital y la propia imagen.

Creación de anuncios o perfiles falsos

En una primera aproximación al concepto de anuncio o perfil falso, podemos definirlo como aquel que no cumple con los términos y condiciones que establece una determinada plataforma, no pertenecen al titular del perfil o simulan pertenecer a este. Este tipo de perfil se crea con fines de cometer diferentes delitos como stalking, ciberbullying, delitos pornográficos, delitos que atentan contra la reputación digital, manipulación mediática, etc. (Rodas Sandoval, 2018: 67). A nivel operacional, se entiende por perfil falso a efectos de cualquier investigación, aquel que sea creado por cualquier usuario con el fin de manipular, usurpar o generar una nueva identidad digital, para crear cualquier tipo de contenido (Ibid.)

Difusión a través de las redes sociales

El concepto de redes sociales se entiende como una aplicación online que permite al usuario, de forma descentralizada, crear perfiles públicos basados en un nombre y a los que se pueden acompañar imágenes, fotografías, videos, textos y otros datos, que permiten interactuar con terceras personas de forma remota; compartir información; generar contenidos, así como participar en movimientos sociales y corrientes de opinión.

Situación de acoso, hostigamiento o humillación

Para que la conducta típica consistente en utilizar la imagen de una persona sin su consentimiento, con la finalidad de abrir perfiles falsos en redes sociales sea punible se exige que la misma ocasione a la víctima una situación de acoso, hostigamiento o humillación.

El acoso, en defecto de un concepto legal, se puede definir como aquellas acciones que, sin llegar a producir el anuncio expreso de causar un mal o el empleo directo de violencia para coartar la libertad de la víctima, se llevan a cabo de manera reiterada con la finalidad de menoscabar gravemente la libertad y el sentimiento de seguridad de la víctima con independencia de su sexo, sometiéndola a una persecución o vigilancia constante, o realizando otros actos continuos de hostigamiento. Estas conductas de acoso tienen como objetivo el control, la búsqueda de intimidad y la necesidad de manipulación de la vida y actividades de la víctima, provocando inseguridad y miedo vinculados causalmente al hostigamiento, así como inferirle sentimientos de temor por su integridad física, de persecución y desestabilización, e incluso, vejación y humillación (Martínez Atienza, 2020: 18). El elemento esencial del acoso es el patrón de comportamiento intrusivo en la vida de otra persona contra su voluntad, del que se desprende un riesgo objetivo de causar un mal o desagrado a una persona con el consiguiente desasosiego, preocupación e incluso miedo experimentado de forma razonable por la víctima (De La Cuesta Arzamendi y Mayordomo Rodrigo, 2011: 23-24).

Exigibilidad de los requisitos del art. 172 ter 1 CP

Por último, es necesario analizar si también se exige la concurrencia de los requisitos del delito de stalking del art. 172 ter 1 CP. Estos requisitos son: repetición de la conducta, falta de legitimidad y alteración de la vida cotidiana. Algunos autores consideran que, por su ubicación sistemática, existe una conexión entre ambos delitos y, por lo tanto, deben exigirse (Díaz y García-Conlledo, 2023); mientras que otros lo consideran un artículo independiente y no exigen la concurrencia de estos requisitos (Sánchez Benítez, 2023). La ubicación sistemática del delito de creación de perfiles falsos en redes sociales, entre los delitos contra la libertad, como modalidad de coacción no es, a mi juicio, correcta, por lo que considero que los requisitos del delito de stalking no son exigibles para la creación de perfiles falsos en redes sociales. Los bienes jurídicos protegidos en los delitos convencionales no son suficientes para la ade-

cuada recriminación de este tipo de conductas en la red. Este delito debería tipificarse en un título separado donde se proteja la identidad digital como derecho autónomo.

Delimitación entre el reproche penal y la sanción civil

No todos los supuestos de creación de un perfil falso, sin consentimiento, utilizando la imagen de una persona producen una situación de acoso, hostigamiento o humillación, por lo que en estos casos la conducta no es punible penalmente.

El ordenamiento jurídico español cuenta con mecanismos de respuesta en vía civil a través de la LO 1/1982. Estas conductas encuentran acomodo en el elenco, no exhaustivo, de intromisiones ilegítimas en los mencionados derechos, previsto en el art. 7, haciendo una interpretación extensiva de lo establecido en el número 6, según el cual, se consideran intromisiones ilegítimas en el ámbito de protección delimitado en el art. 2 de esta LO, la utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga. En este precepto, a diferencia del tipo penal que se refiere únicamente al uso de la imagen, se protege la intromisión en los derechos al honor, la intimidad y la propia imagen no solo por el uso de la imagen, sino también de otros datos identificativos de una persona como el nombre o la voz. Dentro del término «de naturaleza análoga» a los fines comerciales o publicitarios, se pueden entender incluidos los fines de realizar anuncios o crear perfiles falsos. Además, a diferencia de la vía penal, en la civil es posible la tutela de los derechos al honor, intimidad y propia imagen también de las personas fallecidas.

Sin embargo, en los casos en los que con la creación del perfil falso se produzca tal situación de acoso, hostigamiento o humillación, considero que sí es necesaria la intervención del Derecho penal, pero que no es necesaria la tipificación expresa del delito, porque podía castigarse por dos vías, bien a través del tipo básico de los delitos contra la integridad moral, previsto en el art. 173.1 CP, o como delito de stalking del art.

172 ter 1. 3ª CP. De establecer una tipificación expresa de estas conductas, debería hacerse en un título autónomo cuyo bien jurídico protegido sea la identidad digital.

DISCUSIÓN

Aunque los sistemas del Common Law, a diferencia de los sistemas de Derecho continental, no siguen esta vocación codificadora, también cuentan con mecanismos para determinar qué conductas son perseguibles, por lo que la cuestión de si el derecho penal es la mejor forma de combatirlas también les concierne; y cuentan con mecanismos de derecho civil para las conductas menos graves.

Para concluir, intentaré responder a las tres preguntas que planteé al principio de este artículo.

1. La respuesta penal no es siempre la más idónea para hacer frente al incremento de los atentados contra la dignidad en internet. El Derecho penal debe reservarse para los casos más graves en los que se pone en peligro la convivencia social. No todos los supuestos de creación de perfiles falsos, sin consentimiento, que utilizan la imagen de una persona generan situaciones de acoso, hostigamiento o humillación, por lo que en estos casos la conducta no es punible penalmente. Los ordenamientos jurídicos deben contar con otros mecanismos de respuesta para estos otros casos, en procedimientos civiles y administrativos.

El ordenamiento jurídico ya contaba con cauces suficientes para el castigo de estas conductas sin necesidad de creación expresa de un tipo autónomo. Sin embargo, si considero necesario contar con algún instrumento jurídico de ámbito mundial donde se recojan las conductas delictivas cometidas a través de la Red. El hecho de que este tipo de delitos se pueda cometer en cualquier lugar dificulta su identificación y sanción, por lo que un instrumento global permitiría, al menos, delimitar de manera unánime cuales son las conductas más peligrosas, cómo se deben tipificar y donde se debe enjuiciar al sujeto responsable. Para los

demás casos, los Estados deben gozar de más libertad para determinar, en vía civil o en su caso administrativa, la sanción de estas conductas.

2. La regulación proporciona seguridad jurídica. Sin embargo, una regulación excesiva supone la quiebra de los principios generales del propio Derecho penal, como el de última ratio o intervención mínima, conforme al cual el Derecho penal solo debe perseguir las conductas más peligrosas para la convivencia social. La idoneidad de la introducción de figuras jurídicas similares a la prevista en el art. 172 ter 5 CP español depende de la posibilidad de su armonización con los demás preceptos del ordenamiento jurídico en cuestión y de la posibilidad de aplicación de otras figuras ya previstas para el castigo de estas conductas.

La creación de perfiles falsos en redes sociales ya era reprochable penalmente y venía siendo castigada por la jurisprudencia española con arreglo a distintos tipos previstos en el CP. Por tanto, no estamos ante una nueva conducta delictiva, sino ante la tipificación expresa de una conducta ya castigada con anterioridad a su introducción en el art. 172 ter 5 CP. No obstante, la jurisprudencia no seguía un criterio unánime en la calificación de estos hechos, sino que los castigaba inicialmente como un delito de usurpación del estado civil, y, en otros casos, aunque en menor medida, como delitos de injurias, vejaciones injustas o falsedad en documento mercantil. Si bien todos estos tipos son suficientes para el castigo penal de esta conducta, no es menos cierto que los delitos tecnológicos pueden suponer la vulneración de otros bienes jurídicos diferentes a los protegidos en los delitos cometidos en el espacio físico; por ejemplo, el derecho a la identidad digital. Entiendo que, si consideramos que es necesaria la protección de otros bienes jurídicos, estaría justificada la tipificación expresa de estos delitos cometidos a través de la Red, pero en ese caso, deberían ubicarse sistemáticamente en un título propio.

3. La creación de instrumentos globales para hacer frente a la ciberdelincuencia y su enjuiciamiento, teniendo en cuenta su carácter transnacional, no se ha considerado más allá del Convenio de Budapest

de 2001. La excesiva libertad concedida a los Estados para tipificar las conductas en su legislación nacional y el rápido avance de las tecnologías dificultan la uniformidad en la aplicación de la Ley penal. Este texto, aunque supone un paso adelante en el intento de cooperar en la lucha contra la ciberdelincuencia, no es suficiente. La rápida evolución tecnológica y el impacto de la inteligencia artificial, parece evidenciar una necesidad de actualización del Convenio, así la aprobación de otras normas transnacionales.

La existencia de cooperación entre los Estados con el fin de lograr un mayor éxito en el enjuiciamiento de la ciberdelincuencia es una cuestión de voluntad política. Ningún instrumento jurídico es universalmente vinculante; solo son vinculantes para los Estados que se adhieren a ellos y los ratifican.

Referencias bibliográficas

Anguita Osuna, J. E. (2018). Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea. Revista de Estudios en Seguridad Internacional, 4(1), 107–126. https://doi.org/10.18847/1.7.7

Barrio Andrés, M. (2011). La ciberdelincuencia en el Derecho español. Revista de las Cortes Generales, (83), 273–305. https://doi.org/10.33426/rcg/2011/83/473

Barrio Andrés, M. (2018). Delitos 2.0: Aspectos penales, procesales y de seguridad de los ciberdelitos. Wolters Kluwer.

Baucells i Lladós, J. (2014). La irreflexiva criminalización del hostigamiento en el proyecto de Código Penal. Revista General de Derecho Penal, (21), 1–17.

Borghello, C., & Temperini, M. G. I. (2016). Suplantación de identidad digital como delito informático. En M. Kieffer (Coord.), Cibercrimen: Aspectos de Derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios en Internet (pp. 291–311). B de F.

Cancio Meliá, M., & Pérez Manzano, M. (2019). Principios del Derecho penal (II). En J. A. Lascuraín Sánchez (Coord.), Manual de introducción al Derecho penal (pp. 69–90). BOE.

Cocchini, A. (2021). Los ciberataques de los actores no estatales y la "ciberdiligencia debida" de los Estados. Revista UNISCI, 19(55), 69–98. https://doi.org/10.31439/unisci-106

Corcoy Bidasolo, M. (2007). Problemática de la persecución penal de los denominados delitos informáticos: Particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos. Eguzkilore: Cuaderno del Instituto Vasco de Criminología, (21), 7–32. http://hdl.handle.net/10810/25001

Cuerda Arnau, M. L. (2022). Delitos contra la libertad (II): Amenazas. Coacciones. En J. L. González Cussac (Coord.), Derecho penal: Parte especial (7.ª ed., pp. 171–199). Tirant lo Blanch.

De la Cuesta Arzamendi, J. L., & Mayordomo Rodrigo, V. (2011). Acoso y Derecho penal. Eguzkilore: Cuaderno del Instituto Vasco de Criminología, (25), 21–48. https://www.ehu.eus/es/web/ivac/cuaderno-eguzkilore-25

De las Heras Vives, L. (2018). El derecho a la propia imagen en España: Un análisis desde el Derecho constitucional, civil y penal. Actualidad Jurídica Iberoamericana, (8), 435–453. https://revista-aji.com/articulos/2018/8/435-453.pdf

De Prada Rodríguez, M., & Santos Alonso, J. (2013). Suplantación de identidad en internet: Necesidad de reforma del Código Penal. Anuario Jurídico Villanueva, (7), 215–229. https://digiuv.villanueva.edu/handle/20.500.12766/338

Díaz y García Conlledo, M. (2023). Comentario al art. 172 ter CP. En M. L. Cuerda Arnau (Dir.), Comentarios al Código Penal (1.ª ed., t. I, pp. 1137–1142). Tirant lo Blanch.

Gutiérrez Castañeda, A. (2013). Acoso - stalking: Art. 173 ter. En L. Álvarez García (Dir.), Estudio crítico sobre el anteproyecto de reforma penal de 2012 (1.ª ed., pp. 581–588).

Íñigo Corroza, E. (2022). El consentimiento de la víctima: Hacia una teoría normativa de la acción del que consiente. Anuario de Derecho Penal y Ciencias Penales, 75, 167–203. https://revistas.mjusticia.gob.es/index.php/ADPCP

Luzón Peña, D. M. (2016). Lecciones de Derecho penal: Parte general (3.ª ed.). Tirant lo Blanch.

Martínez Atienza, G. (2020). El acoso y su protección especialmente penal. Experiencia.

Muñoz Conde, F., & García Arán, M. (2022). Derecho penal: Parte general (11.ª ed.). Tirant lo Blanch.

Quintano Ripollés, A. (1950). Relevancia del consentimiento de la víctima en materia penal. Anuario de Derecho Penal y Ciencias Penales, 2(3), 321–344. https://revistas.mjusticia.gob.es/index.php/ADPCP/article/view/541

Rodas Sandoval, M. C. (2018). Análisis sobre el uso de perfiles falsos de figuras políticas en Guatemala a través de la red social Twitter durante los años 2015-2017 [Tesis, Universidad Rafael Landívar].

Romeo Casabona, C. M. (2006). De los delitos informáticos al cibercrimen: Una aproximación conceptual y político-criminal. En C. M. Romeo Casabona (Coord.), El cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas político-criminales (pp. 1–43). Colmenares.

Sánchez Benítez, C. (2023). Tratamiento jurídico-penal del acoso en España, especial referencia a las Leyes Orgánicas 4/2022, de 12 de abril y 10/2022, de 6 de septiembre. BOE.

Solari Merlo, M. N. (2021). Encaje jurídico de las conductas de suplantación en la era digital. En P. Simón Castellano & A. Abadías Selma (Coords.), Cuestiones penales a debate (pp. 405–429). J. M. Bosch Editor.

Solari Merlo, M. N. (2022). Suplantación de identidad digital: ¿Necesidad de criminalización? Cuadernos de Política Criminal, (136), 125–163.

Solari Merlo, M. N. (2023). La identidad digital ante el Derecho penal. Thomson Reuters Aranzadi.

Subijana Zunzunegui, I. J. (2008). El ciberterrorismo: Una perspectiva legal y judicial. Eguzkilore: Cuaderno del Instituto Vasco de Criminología, (22), 169–187. https://www.ehu.eus/documen-

ts/1736829/2176658/Eguzkilore+22.pdf

Tarodo Soria, S. (2025). Patient autonomy in the context of digital health. Bioethics, 39(5), 404–413. https://doi.org/10.1111/bioe.13410

Velasco Núñez, E., & Sanchís Crespo, C. (2019). Delincuencia informática: Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal penal de 2015. Tirant lo Blanch.

Villacampa Estiarte, C. (2010). La respuesta jurídico-penal frente al stalking en España: Presente y futuro. ReCRIM: Revista de l'Institut Universitari d'Investigació en Criminologia i Ciències Penals de la UV, (4), 33–57. http://www.uv.es/recrim/recrim10/recrim10a03.pdf

Otras Fuentes y Legislación

Comisión Europea. (2007). *Hacia una política general de lucha contra la ciberdelincuencia* [COM(2007) 267 final]. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52007DC0267

Consejo de Europa. (2001). *Convención sobre cibercrimen.* Budapest. https://rm.coe.int/1680081561

Consejo de Europa. (2011). *Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica.* Estambul. https://rm.coe.int/1680462543

Constitución Española. (1978). *Constitución Española* (BOE núm. 311, de 29 de diciembre de 1978). https://www.boe.es/eli/es/c/1978/12/27/(1)/con

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. (2013). https://eur-lex.europa.eu/eli/dir/2013/40/oj

Fiscalía General del Estado. (2014). Memoria elevada al Gobierno de S. M. presentada al inicio del año judicial por el Fiscal General del

Estado Excmo. Sr. D. Eduardo Torres-Dulce Lifante. https://www.fiscal.es/memorias/memoria2014/FISCALIA_SITE/recursos/pdf/MEMFIS14.pdf

Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. (1982). https://www.boe.es/eli/es/lo/1982/05/05/1/con

Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. (2000). https://www.boe.es/eli/es/lo/2000/01/12/5/con

Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. (2010). https://www.boe.es/eli/es/lo/2010/06/22/5

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. (1995). https://www.boe.es/eli/es/lo/1995/11/23/10/con

Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. (2015). https://www.boe.es/eli/es/lo/2015/03/30/1/con

Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. (1889). https://www.boe.es/eli/es/rd/1889/07/24/(1)/con

Jurisprudencia

Tribunal Constitucional de España. (2018, junio 4). STC 58/2018 [ECLI:ES:TC:2018:58]. https://hj.tribunalconstitucional.es/es/Resolucion/Show/25683

Tribunal Constitucional de España. (1990, julio 19). STC 137/1990 [ECLI:ES:TC:1990:137]. https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/1562

Tribunal Supremo de España. (2022, abril 20). STS 1465/2022 [ECLI:ES:TS:2022:1465]. https://www.poderjudicial.es/search/

AN/openDocument/645033570cfa79da/20220429

Tribunal Supremo de España. (2000, marzo 18). STS 2183/2000 [ECLI:ES:TS:2000:2183]. https://www.poderjudicial.es/search/AN/openDocument/83fd36b86a65c6f3/20030830