IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

Dosier «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes»

ARTÍCULO

Delitos contra la intimidad y redes sociales (en especial, en la jurisprudencia más reciente)

Carmen Tomás-Valiente Lanuza
Universitat de les Illes Balers

Fecha de presentación: mayo de 2018
Fecha de aceptación: julio de 2018
Fecha de publicación: septiembre de 2018

Resumen

Las redes sociales constituyen vehículos de exhibición de la propia intimidad a la vez que canales especialmente idóneos para la exposición de la ajena. En esta última variante, en los últimos años han devenido en medio comisivo preferente de delitos de revelación de secretos del artículo 197 Cp en sus distintas modalidades (el encaje en una u otra dependerá del modo en que se haya accedido al material íntimo objeto de la difusión); el usuario de la red es aquí el autor del delito contra la intimidad ajena (apartado 1). De otro lado, en cambio, el usuario de una red social se coloca también a sí mismo en una posición vulnerable (apartado 2), puesto que aquello que publica a un círculo cerrado de destinatarios (los «amigos»), que eventualmente puede afectar a su intimidad, es susceptible de ser redifundido por alguno de estos, conducta que, pese a todo, no consideramos penalmente típica. En tercer lugar, la jurisprudencia más reciente empieza a ocuparse de supuestos de acceso no consentido al espacio de un usuario en una red social (apartado 3), en los que entra en juego la figura de intrusismo informático del artículo 197 bis.

Palabras clave

red social, intimidad, descubrimiento y revelación de secretos, intrusismo informático

Tema

protección penal de la intimidad

Privacy offences and social networks (particularly in the most recent case-law)

Abstract

Social networks constitute new windows for displaying one's own private life, while also being particularly suitable channels for exposing the privacy of others. In this last sense, they have recently become a most frequent vehicle for the crime of disclosing secrets, contained in Article 197 of the criminal code in its different forms (the conduct's specific classification among them depends on how the shared intimate material was obtained). Here, the user of the network is the perpetrator of the privacy offence (section 1). On the other hand, social network users also place themselves in a vulnerable position (section 2), since everything they intend to show to a closed circle of recipients (their "friends"), which may eventually affect their privacy, can afterwards be passed on by any of these people—a conduct which, despite everything, we do not consider criminal. Thirdly, the most recent case-law has begun to deal with cases of non-consensual access to a user's space in a social network (section 3), where article 197 bis crime of computer hacking comes into play.

Keywords

social network, privacy, discovery and revealing of secrets, computer hacking

Topic

criminal protection of intimacy

Introducción

El uso masivo de las redes sociales (especialmente de las denominadas «de ocio») ha modificado de modo muy relevante –afirmarlo constituye ya un lugar común– la manera de entablar y mantener relaciones interpersonales, en un nuevo escenario en el que –entre otros muchos factores– resulta fundamental la transformación del papel desempeñado por la intimidad de los usuarios. Las redes sociales sirven, ante todo, como canal de exposición o comunicación (en abierto o a círculos más o menos restringidos de destinatarios) de la propia intimidad (fotos, vídeos, información sobre gustos, actividades, etc.), aunque obviamente también operan como vehículo de difusión de lo que puede afectar a la intimidad de terceros no usuarios que no hayan prestado su consentimiento a dicha exposición.[1]

En estas páginas intentaremos diseccionar (o cuando menos sistematizar), sobre la base de la jurisprudencia más reciente, las cuestiones jurídico-penales específicamente suscitadas por la utilización de una red social en la comisión de hechos eventualmente incardinables en los delitos de descubrimiento y revelación de secretos (artículo 197), aunque también se planteará la aplicabilidad del delito de intrusismo informático del artículo 197 bis Cp a supuestos en los que la red social opera no como instrumento de la comisión del delito, sino como objeto material mismo de la conducta (como sucede en los casos de acceso no consentido a la página de un usuario).

1. La red social como vehículo de difusión de la intimidad de terceros distintos del usuario

Dejando en este momento al margen las peculiaridades de la protección de la libertad informática o *habeas data*

1. Una interesante introducción al fenómeno de las redes sociales, en tanto nuevo marco de hechos penalmente relevantes contra diversos bienes jurídicos (intimidad, inviolabilidad informática, honor, propiedad intelectual, etc.) con los usuarios como posibles autores y víctimas, puede encontrarse en Picotti (2013, pág. 76-81).

por el artículo 197.2, la tutela penal de la intimidad por el artículo 197 se articula básicamente, como es sabido, en torno al modo de acceso (ilícito o lícito) a aquello en lo que se plasma la intimidad (documentos, cartas, mensajes, fotografías, vídeos...). Hasta la reforma del precepto por la LO 1/2015, nuestro ordenamiento solo sancionaba el acceso ilícito (descubrimiento) y la eventual revelación de lo así conocido.[2] A partir de la citada reforma, la revelación de lo ilícitamente conocido conserva un mayor reproche penal, pero también es típica, en los términos que enseguida se comentarán, la difusión (siempre no consentida) de imágenes o grabaciones de contenido íntimo previamente obtenidas con consentimiento del sujeto pasivo (se tipifica por tanto, y con una pena menor que la variante anterior, la revelación de lo que el autor ha conocido lícitamente).

1.1. Revelación o difusión de aquello a lo que se ha accedido ilícitamente (artículos 197.1 y 197.3 Cp)

1.1.1. Los accesos ilegítimos típicos (del artículo 197.1) previos a la difusión.

El ámbito tradicional de protección penal del bien jurídico (el único típico antes de 2015) viene dado por el acceso ilegítimo a la intimidad, en cualquiera de las modalidades descritas por el prolijo apartado 1 (apoderarse de documentos, mensajes, fotos, etc.; interceptar las comunicaciones; o utilizar de artificios técnicos de escucha o grabación del sonido o de la imagen), a partir de lo cual la conducta puede detenerse en ese mero descubrimiento de la intimidad ajena (al que dicho apartado asigna una pena de uno a cuatro años de prisión más multa) o avanzar hasta la ulterior revelación de lo descubierto a terceras personas (lo que da lugar al tipo agravado del apartado 3, con pena de dos a cinco años). En relación con esta segunda conducta, en la práctica las redes sociales, junto con la mensajería telefónica (sobre todo a través de la aplicación WhatsApp), juegan un papel destacado como canales de revelación o difusión, lo que normalmente comporta un grado de lesividad más intenso (en función del número de personas con acceso al perfil del usuario) que en las revelaciones dirigidas a un número menor de destinatarios.

En todo lo que se refiere a la satisfacción de los requisitos típicos del artículo 197.1, sobre los que se construye la posterior conducta de revelación, la intervención de la red social como instrumento de esta última no introduce, como es lógico, ninguna diferencia. Es necesario que antes de la revelación o difusión se haya producido alguna de las conductas invasoras de la intimidad del citado apartado, cuyos requisitos típicos han de haberse cumplido en su totalidad (con los problemas interpretativos a que pueden dar lugar, por ejemplo, el concepto de apoderamiento,[3] o la determinación de aquello que puede entenderse que afecta a la intimidad).[4] Todo ello se satisface, sin duda, en los supuestos que la jurisprudencia nos demuestra más frecuentes en la práctica, aquellos en los que se difunden fotografías o vídeos de carácter sexual obtenidos sin consentimiento de la persona que en ellos aparece, y que obran en poder del autor de la difusión bien porque previamente se ha «apoderado» de ellos (así, si entra sin autorización en el correo electrónico de la víctima o en su teléfono móvil, y se descarga las imágenes que allí encuentra),[5] bien porque él mismo ha utilizado artificios de captación de imágenes

2. Salvo en el caso de la revelación de secretos conocidos por razón del oficio o profesión (artículo 199), cuyo presupuesto es siempre el acceso lícito a la información.
3. ¿Constituye apoderamiento la mera lectura de lo que otro ha dejado –con mayor o menor grado de descuido– a la vista de terceros? ¿Y fotografiarlo? De este último supuesto, afirmando la tipicidad, se ocupa la SAP Ciudad Real 180/2017, de 30 de noviembre. De todos es conocido, por otra parte, el reciente suceso de la captación con cámaras de televisión (y posterior difusión) de mensajes privados intercambiados entre dos políticos catalanes, que aparecían en la pantalla del teléfono móvil de uno de ellos, a la vista del equipo periodístico.
4. Así, la captación de fotografías en plena calle de dos personas besándose, realizada sin consentimiento de los fotografiados, no encaja en el apartado 1 (ni su posterior revelación, por tanto, en el apartado 3) por mucho que aquello que evidencien (en el supuesto de la SAP Jaén 76/2017, de 31 de enero, una relación extramatrimonial) sí pueda formar parte de la intimidad del fotografiado. Conductas de este tipo (captación y difusión de imágenes que no pueda decirse que afecten a la intimidad, teniendo en cuenta el lugar en el que se toman y su propio contenido) han de remitirse necesariamente a la protección civil de la propia imagen. Absuelve por ello acertadamente la SAP Madrid 539/2017, de 26 de junio, a quien graba en la calle y difunde luego en su Facebook un vídeo de un niño de dos años cuando, acompañado por su padre, tiene una fuerte rabieta.
5. SAP Málaga 396/2015, de 9 de septiembre. Aunque la sentencia no entre en ello en absoluto, los hechos suscitan un viejo problema de tipicidad del artículo 197.1, que se produce cuando el autor se apodera ilícitamente de material íntimo (en este caso, fotos que se descarga del móvil de su expareja), pero dándose la circunstancia de que la persona cuya intimidad se refleja no es la «dueña» del material (en este supuesto, quien aparece en las fotos no es el dueño del móvil, sino su nueva pareja, desnuda). Se suscita entonces la duda de si se

de la víctima de modo subrepticio[6] (o advertido pero no consentido, como cuando se graba una agresión, que no necesariamente tiene que serlo contra la libertad sexual).[7]

1.1.2. La difusión en cadena a través de las redes

En este contexto, la peculiaridad planteada por el uso de redes sociales como instrumento de revelación del material íntimo se refiere a la conducta de redifusión o reenvío, cuando es realizada por quienes no han intervenido en su ilícita obtención; conducta que, siempre que el sujeto conozca dicho origen ilícito, es sancionada por el artículo 197.3 párrafo segundo con la pena de uno a tres años de prisión más multa. Pues bien, en principio, en la medida en que cada sujeto que comparte el material en sus redes sociales amplía sucesivamente el círculo de conocedores, con cada redifusión se produce una nueva lesión del bien jurídico protegido, cuya relevancia penal a la luz del precepto mencionado no plantea problemas.[8]

1.1.3. El indebido recurso al artículo 197.2 Cp para soslayar la atipicidad del acceso previo a la difusión

Una vez sentada la necesidad de un acceso ilegítimo al material íntimo –típica del artículo 197.1– para poder luego sancionar *ex* artículo 197.3 su descubrimiento o revelación (en las redes o de cualquier otro modo), lo que no resulta de recibo es pretender soslayar los problemas de encaje en el artículo 197.1 por la vía (empleada con frecuencia creciente por las audiencias provinciales) de subsumir la conducta en el apartado 2 del artículo 197, en el que se consagra la protección penal de la llamada libertad informática o *habeas data*.[9] La cuestión requiere un examen algo más detenido.

La razón de ser del mencionado 197.2 (cuya atormentada redacción ha pretendido desentrañarse a través de variadas interpretaciones doctrinales) se encuentra en la protección del derecho del ciudadano a controlar sus datos personales en un contexto concreto: el de los riesgos de conocimiento y utilización no consentidos generados a partir fundamentalmente de su tratamiento informatizado. Lo que se protege son datos personales reservados (y constituye objeto de importante discrepancia cuáles de ellos puede entenderse que afectan a la intimidad merecedora de protección penal, siempre subsidiaria de la administrativa) recogidos en archivos o registros (en primera instancia, el legislador se refiere a los informatizados, aunque también admite los que no lo sean). Pues bien: siendo esto así, resulta totalmente inadecuado entender, como han propuesto diversas audiencias en los últimos años, que lo almacenado –especialmente relevante en la práctica, las fotografías o vídeos– en un dispositivo informático, como es el caso de un teléfono móvil, constituye dato *registrado* en el sentido del mencionado precepto. Adoptar esta argumentación como base para sancionar la posterior revelación de lo almacenado aboca a una ampliación potencialmente ilimitada del espacio típico del 197.2 y, a la postre, deja vacío de sentido el apartado 1: cualquier foto y cualquier documento, incluso inicialmente en papel, es susceptible de ser digitalizado y almacenado en dispositivos como móviles u ordenadores; con la argumentación que ahora discutimos, por mucho que el acceso a ellos hubiera sido lícito, su revelación sería punible por el 197.3 tomando como base el 197.2. Y lo mismo sucede (quedaría sin sentido la tipificación expresa) en relación con el nuevo apartado 7 que enseguida examinaremos.[10]

satisface la tipicidad en la medida en que el artículo 197.1 se refiere al apoderamiento de los papeles, documentos, etc. de una persona, realizada con ánimo de vulnerar «su» intimidad.

6. Así, SAP Madrid 671/2015, de 28 de septiembre (grabación no consentida de vídeo sexual y posterior difusión, que aquí se produce a través de páginas web de contenido pornográfico); SAP Madrid 657/2017, de 15 de noviembre (toma una foto de su novia dormida con un pecho desnudo, y tiempo después la envía a la nueva pareja de ella, además de colgarla en su Facebook). *Vid* igualmente SAP Tarragona 453/2016, de 29 de diciembre, donde la presencia o no de consentimiento resulta discutible.
7. SAP Málaga 452/2009, de 16 de septiembre.
8. No existe en España, en lo que se nos alcanza, ninguna sentencia sobre un caso de este tipo. Sí es conocido, en cambio, el supuesto sometido a enjuiciamiento en Dinamarca en el momento de escribirse estas líneas, relativo a la difusión por redes sociales de un vídeo sexual grabado sin consentimiento de sus protagonistas, y compartido sucesivamente por centenares de personas (<http://www.lavanguardia.com/vida/20180220/44929353263/dinamarca-juicio-video-sexual-adolescentes-condenas.html>) [Fecha de consulta: 14/0318].
9. El 197.2 impone las mismas penas que el apartado 1 al que «sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero».
10. SAP Barcelona 742/2017, de 7 de septiembre, que expresamente concibe el teléfono móvil como «soporte informático donde consta un registro de archivos de carácter personal», lo que le sirve para sancionar la conducta de revelación de vídeos sexuales cuya obtención,

1.2. La revelación de material íntimo obtenido (lícitamente) con consentimiento del sujeto pasivo: el artículo 197.7

1.2.1. Conductas no abarcadas por la nueva tipificación

Como se ha comentado ya, hasta la reforma operada por la LO 1/2015, la tipicidad de las conductas de revelación se constreñía a las que tuvieran por objeto aquello previamente descubierto de modo ilícito; la revelación de lo obtenido con consentimiento de la otra persona (que en la práctica suele tener por objeto fotografías o vídeos de carácter sexual finalmente difundidos por la antigua pareja del sujeto pasivo) no encajaba en la descripción típica, por más que la difusión fuera no consentida y con independencia del innegable menoscabo, a veces muy grave, que pudiera comportar (como acontece cuando tal difusión se produce a través de una red social). La citada reforma modifica sustancialmente este panorama, si bien no con el alcance, a mi juicio, que gran parte de la doctrina parece atribuirle.[11] En efecto: como ya he tenido oportunidad de poner de manifiesto en otro lugar,[12] la dicción del nuevo apartado 7 del artículo 197 comprende la difusión de lo que el *propio autor de la difusión* ha obtenido previamente (al grabar o fotografiar por sí mismo al sujeto pasivo), pero a mi juicio no abarca los supuestos en que las imágenes han sido obtenidas por la víctima (que se graba o fotografía a sí misma) para luego facilitarlas a quien ulteriormente las difunde sin su consentimiento. Asiste sin duda toda la razón a quienes señalan que no era esta la intención del legislador, que pretendía –aun sin cuidar la redacción para conseguirlo– incluir también los supuestos aquí discutidos[13] (que de hecho la jurisprudencia demuestra muchísimo más frecuentes que los primeros); la cuestión es, sin embargo, si una apelación a tales propósitos justifica una interpretación amplia del tipo que (a mi entender) desbordaría su tenor literal con la consiguiente vulneración del principio de legalidad.[14] En este mismo sentido se ha pro-

según la propia sentencia reconoce, no encajaba en el apartado 1; SAP Málaga 107/2016, de 23 de marzo (sobre la que volveremos *infra* al tratar la conducta de creación de perfiles falsos), que castiga por el 197.2 al sujeto que –con la finalidad de hacerla objeto de requerimientos sexuales por terceros– crea un perfil falso en una red social a nombre de su expareja e inserta, además de mensajes provocativos, una foto de ella (por lo demás no íntima sino inocua, y que el autor poseía legítimamente), que es considerada por la AP un dato de carácter personal cuya inserción en el perfil subsume bajo la conducta típica de utilización del dato en perjuicio del titular; SAP Burgos 136/2017, de 2 de mayo, que recurre al 197.2 para sancionar a un sujeto que publica en sus redes sociales algunos documentos (que poseía legítimamente como parte en el proceso) en los que figuraban «datos sensibles» (no se dice cuáles) de su expareja –pese a no haberse extraído los datos de archivo o registro alguno en el sentido del precepto, la AP considera que el acusado «utilizó dolosamente datos personales [de la querellante] divulgando en las redes sociales y sin su consentimiento los mismos y la situación de enfrentamiento familiar y personal existente con ella con la intención de causarle un perjuicio personal y social con dicha divulgación a la que terceras personas tenían un acceso libre»–. Con pocas explicaciones, también en un caso de difusión de una foto (sin que quede claro cómo se accedió a ella), SAP Burgos 189/2016, de 13 de mayo; por su parte, aunque absuelva, se plantea el 197.2 en un caso de difusión de un vídeo enviado por WhatsApp AAP Cádiz 445/2016, de 10 de noviembre. Correctamente en cambio, en el sentido aquí defendido y con un rechazo expreso de la aplicación del 197.2, SAP Lleida 389/2016, de 25 de octubre.

Vid. igualmente SAP Pontevedra 320/2017, de 12 de diciembre, que absurdamente condena por el artículo 197.2 cuando en realidad aquí sí se satisfacen los requisitos del apartado 1, al haber entrado el sujeto en mensajes enviados por su expareja desde su cuenta de Facebook. Por otro lado, obviamente nada de lo anterior es óbice para la sanción (*ex* artículo 197.3 en relación con el 197.2) de la revelación –en redes sociales o de otro modo– de lo que realmente constituyan datos personales reservados a los que se haya accedido sin autorización (pensemos, por ejemplo, en quien publica en su Facebook datos sanitarios de una o varias personas, que conozca por haber accedido sin autorización a registros informatizados de sus historias clínicas).

11. Artículo 197.7: «Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquella *que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros,* cuando la divulgación menoscabe gravemente la intimidad personal de esa persona» (la cursiva es mía).
12. Me permito remitir a Tomás-Valiente Lanuza (2015, pág. 670-671).
13. Morales Prats (2016, pág. 1466-73). Lo cierto es que es difícilmente comprensible que se rechazaran las enmiendas presentadas por el Grupo Entesa pel Progrés de Catalunya y el Grupo parlamentario Socialista orientadas a la expresa inclusión en el precepto de los supuestos de envío del material íntimo por el sujeto pasivo.
14. Al margen de este aspecto muy discutible del tipo de *lege lata*, el delito plantea un interesante debate en cuanto a su justificación político-criminal, en el que aquí no puede ahondarse. Baste bosquejar la presencia de vectores contrapuestos: la indudable relajación de la autoprotección de la intimidad en la que incurre quien cede a otro imágenes íntimas se alza como argumento central entre sus

nunciado algún autor y alguna sentencia muy reciente;[15] pero lo cierto es que la mayoría de la doctrina opta por la interpretación amplia aquí criticada, al igual que la práctica totalidad de los tribunales que han tenido ocasión de pronunciarse al respecto, que dan por sentada (cosa que por cierto era previsible) la admisión como objeto material del delito de lo enviado por quien se graba o fotografía a sí mismo.[16]

Al margen de todo este debate, ha de advertirse, por otra parte, que a diferencia del artículo 197.3 segundo párrafo –que como se ha comentado prevé la (re)difusión eventualmente en cadena por terceras personas que no han intervenido en la obtención del material íntimo pero conocen su origen ilícito–, en esta sede no se contemplan ulteriores revelaciones por terceros (cuya consideración como típicas supondría, entre otras cosas, el carácter totalmente superfluo del 197.3.2.º).[17]

2. La red social como vehículo de exposición de la propia intimidad. La redifusión de lo recibido por los incluidos en la red social

Asumamos ahora, a efectos argumentativos (y porque como se ha dicho esta es claramente la interpretación más defendida por doctrina y jurisprudencia), que el objeto típico del artículo 197.7 abarcara no solo las imágenes o vídeos obtenidos por quien posteriormente los revela o difunde, sino también los que voluntariamente le ha hecho llegar la persona cuya intimidad se ve «gravemente» afectada por la ulterior revelación. Pensemos en quien voluntariamente expone en su red social –al círculo más o menos restringido de sus «amigos»– imágenes que pueda considerarse que menoscaban su intimidad (no suele difundirse por las redes material comprometedor de uno mismo en el ámbito sexual, pero sí, por ejemplo, imágenes en fiestas, con amigos, etc., que según los casos –por ejemplo, si el protagonista aparece bebido o fumando droga– podrían llegar a afectar al bien jurídico);[18] y añádase a ello el que alguno de los destinatarios difunda las imágenes fuera de ese círculo al que iban inicialmente dirigidas. ¿Podría esta difusión considerarse típica del artículo 197.7?

Varios factores aconsejan una respuesta negativa. Ciertamente, el hecho de que el envío inicial se dirija a una pluralidad de destinatarios (los «amigos» en la red, o terminología similar) no impide *per se* (por más que el legislador parece estar partiendo de un destinatario individual) que cada uno de los que ulteriormente difundieran pudiera ser considerado sujeto activo del delito; sin embargo, este dato sí que incide sustancialmente en la interpretación de la afectación del bien jurídico y en el papel de los deberes de autoprotección razonablemente exigibles al usuario de una red social. En efecto: si las imágenes se difunden a

detractores –como mejor exponente de esta crítica Morales Prats (2016 , pág. 1466-73)–, mientras que los partidarios de la tipificación suelen destacar la enorme entidad de la lesión del bien jurídico inherente a la conducta (máxime si, como es habitual, la difusión se produce en internet).

15. Mendo Estrella (2016, pág. 19 y sig.); González Collantes (2015, pág. 69-70); SAP Barcelona 302/2017, de 24 de abril.
16. SAP Guadalajara 111/2015, de 23 de septiembre y SAP Alicante 452/2016, de 3 de noviembre (aunque ambas absuelven por atipicidad en el momento de los hechos, anteriores a la creación del tipo); SAP Sevilla 314/2017, de 28 de junio; SSAP Valencia 488/2016, de 25 de noviembre, y 528/2017, de 7 de septiembre; SAP Valladolid 290/2017, de 6 de octubre. Sorprende que esta última sentencia condene por el artículo 197.7 a una mujer que detecta en el teléfono de su pareja fotos y vídeos sexuales de otra mujer, los cuales cuelga en Facebook y YouTube. Al margen del problema interpretativo mencionado *supra* en el texto (los vídeos fueron enviados por la propia víctima, y no «obtenidos» por quien difunde), la conducta no encajaría siquiera en la interpretación extensiva del precepto que aquí se rechaza (pues en modo alguno ha obtenido las imágenes y vídeos de modo consentido, ni siquiera como receptora del envío). Del relato de los hechos probados parece deducirse, en cambio, la existencia de un acceso ilegítimo a las imágenes (que se descarga, parece que inadvertidamente, del móvil de su pareja), si bien la tipicidad final de la conducta *ex* artículo 191.1 y 3 exigiría detenerse en el problema mencionado *supra* en nota 5 (las imágenes reflejan la intimidad de una tercera persona). En la doctrina, por todos, Morales Prats (2016, pág. 1466-73).
17. De ahí la incorrección de la SAP Las Palmas de Gran Canaria 81/2017, de 14 de marzo, que aunque absuelva por inaplicabilidad retroactiva del nuevo apartado 7, da por buena la tipicidad de la conducta de una joven que difunde unas fotos de otra menor (desnuda), que esta última había enviado a un sujeto que a su vez las había reenviado a la primera. A mi entender, el precepto no abarca ni la conducta de él (que no obtuvo las fotos por sí mismo, sino que las recibió de la víctima), ni desde luego la de la ulterior redifusora (que sería atípica incluso aunque la conducta del inicial destinatario de las fotos sí se considerara abarcada por el tipo).
18. Obsérvese que, aunque hubiera sido deseable en aras de una mayor restricción del tipo, el 197.7 no limita su objeto material a vídeos o fotos eróticos.

una pluralidad de destinatarios (y obviamente el argumento se refuerza cuanto más amplio sea el círculo de estos) se debilita la posibilidad de considerar que ulteriores difusiones (por mucho que se proyectaran fuera del círculo inicialmente consentido por el protagonista) menoscaban gravemente el bien jurídico intimidad; a ello se añade la absoluta renuncia del sujeto a desplegar unos mínimos deberes de autoprotección del bien jurídico, puesto que el envío a una pluralidad de destinatarios supone una total pérdida de control sobre el material remitido.[19] Resulta conveniente, por tanto, una interpretación restrictiva del precepto que abarque la tipicidad tan solo de aquellos supuestos en los que claramente pueda estimarse que la víctima (pese a la relajación de la autoprotección ínsita ya en el envío a una sola persona) desea mantener el material fuera del alcance de más sujetos.

3. La red social como objeto de acceso no consentido

3.1. Precisiones iniciales

Procede ahora plantearse la posibilidad de que la red social se configure como el objeto mismo de un acceso no consentido –así, como ejemplo más frecuente en la práctica, el producido a la página de un usuario en redes como Facebook, Tuenti, Instagram, etc.–, conducta que interesa examinar a la luz del delito de intrusismo informático del artículo 197 bis (precepto al que la LO 1/2015 traslada, con algunas modificaciones, el delito de *hacking* previamente tipificado *ex novo* en el artículo 197.3 por la Ley de reforma 5/2010).

3.1.1. Distinción de las conductas de creación de un perfil falso

Aunque resulte harto evidente, quizás no esté de más destacar, como precisión inicial, que el acceso no consentido al espacio ajeno en una red social no ha de confundirse con otra conducta muy distinta (objeto de un número creciente de sentencias) como es la de crear en la red social un perfil ficticio a nombre de otra persona a la que de algún modo se quiere perjudicar. Dependiendo de para qué se utilice dicho perfil falso, este comportamiento podrá resultar atípico[20] o dar lugar a algún delito: contra la intimidad del artículo 197.1 si el espacio se utiliza para difundir material íntimo obtenido de manera ilícita, o del 197.7 si el objeto difundido fueran fotos o vídeos de carácter íntimo obtenidos con consentimiento del sujeto pasivo (siempre en este caso que los hechos sean posteriores a la entrada en vigor de la reforma de 2015);[21] de la nueva figura de *stalking* o acoso del artículo 172.3. si (como en varios casos enjuiciados en los últimos años) se utilizara repetidamente la página y los datos de la víctima para, haciéndose pasar

19. Como acertadamente expresa el AAP Cádiz 445/2016, de 10 de noviembre, es difícil hablar de intimidad «en relación con episodios o incidencias (grabación de vídeo) que han sido aireadas, difundidas y divulgadas por quien invoca esa "confidencialidad", pues como tal debemos entender quien lo sube a un grupo de 27 personas». La denunciante, en efecto, había remitido un vídeo con imágenes suyas en un bar (no se aclara en los hechos su contenido) a un grupo de WhatsApp de 27 personas, alguien del grupo lo remitió a terceros, y las imágenes terminaron finalmente colgadas en una página web. La sentencia parte de la consideración del vídeo como dato inicialmente comprendido por el 197.2 (proceder que se ha criticado *supra*), y concluye que las circunstancias mencionadas no permiten calificarlo de «reservado»; el marco de discusión correcto ha de ser, como se ha explicado, el apartado 7, pero en cualquier caso las consideraciones de la AP conducen a la valoración correcta sobre la inexistencia del menoscabo grave de la intimidad exigido por este último precepto.
20. De atípicos merecerían ser calificados, a mi juicio, los hechos enjuiciados en la SAP Madrid 658/2017, de 16 de octubre. Aunque finalmente absuelva por falta de pruebas, la sentencia parece sin embargo asumir una imprecisa tipicidad (como delito contra la intimidad) de la conducta, consistente en la apertura por el acusado de tres cuentas en Instagram, Facebook y Tuenti a nombre de su expareja, en las que cuelga «fotografías de su vida privada sin su consentimiento» –sin mencionarse en modo alguno que estas fueran íntimas ni cómo se habían obtenido–. La ulterior referencia a que «con la creación de dichas cuentas pudo [el acusado] obtener datos de los contactos de la denunciante (números de teléfono de sus allegados o de su agente de prensa), que le permitieron obtener información de la misma» no parece tampoco subsumible en ninguno de los tipos contra la intimidad.
21. SSAP Pamplona 189/2016, de 12 de septiembre y 155/2016, de 30 de junio (que absuelve de delito contra la intimidad al ser los hechos previos a la reforma de 2015, pero condena por delito contra la integridad moral del artículo 173). Llama la atención la ligereza de la SAP Málaga 4/2015, de 15 de enero, que en un supuesto de creación de un perfil falso con difusión de fotografías del suplantado (se insinúa que de carácter íntimo) confirma la condena por el artículo 197 sin especificar en ningún momento el apartado en el que se subsume la conducta, y además con particular insistencia en la irrelevancia del origen de las imágenes (lo importante según el tribunal es que se publica sin autorización fotografías obtenidas «sea legal o ilegalmente, sea con autorización o sin ella»), cuando precisamente tales datos son esenciales para la correcta subsunción de la difusión.

por ella, ofrecer servicios sexuales y conseguir así hacerla objeto de contactos por parte de terceros;[22] contra la integridad moral del artículo 173.1;[23] o, en fin, y en casos muy concretos, de delito de usurpación de estado civil del artículo 401 Cp.

3.1.2. Aplicación preferente del delito de descubrimiento (y eventualmente de revelación) de secretos del artículo 197.1 y 2 (y en su caso 3)

Centrándonos ya en la conducta de entrada no consentida en la página de un usuario de una red social, una segunda precisión que ha de quedar sentada desde el inicio es que el artículo 197 bis no puede acoger conductas que tienen ubicación preferente en el delito de descubrimiento de secretos del 197 apartados 1 y 2 (en su caso, seguidos de una revelación del apartado 3); de hecho, así opera la jurisprudencia cuando condena solo por estos tipos en casos en los que se produce una entrada no autorizada a un sistema informático que pudiera resultar típica *per se* de intrusismo (por ejemplo, un acceso –venciendo las medidas de protección– al correo electrónico de otra persona, al ordenador ajeno, a un registro o archivo informático de un banco, una empresa, la Seguridad Social, etc.), pero ello se utiliza para acceder a material íntimo o a datos personales reservados (se leen mensajes del correo o se ven fotos de carácter íntimo archivadas en el ordenador, objetos materiales del 197.1, o se realiza cualquiera de las conductas típicas sobre los datos registrados –de clientes, pacientes, etc.– en el caso del 197.2).[24] Por esta razón, si tenemos en cuenta que la mayoría de las redes sociales incorporan el servicio de intercambio de mensajes individuales con otro usuario, entiendo que el descubrimiento de estos por quien previamente se ha introducido sin permiso en la página debe encuadrase directamente en el primer apartado del artículo 197, que absorbe todo el desvalor del hecho (concurso de leyes resuelto por principio de consunción).[25]

Sin abandonar todavía la reflexión sobre las posibilidades de aplicar preferentemente el artículo 197.1 a la conducta de entrada no consentida en una red social, en principio parece claro que –a menos que se produjera la apertura de mensajes individualizados que acaba de mencionarse– dicha entrada no daría lugar *per se* a un delito de descubrimiento de secretos; como se ha comentado ya en apartados anteriores, parece lógico entender que lo que un usuario ha mostrado voluntariamente a otros a través de la red social (pensemos sobre todo en fotografías o vídeos, incluso aunque estas tuvieran un carácter inicialmente íntimo)[26] deja de pertenecer a su intimidad, al menos (entiendo) en el grado en que sería acreedora de protección penal. Es cierto que en el caso que nos ocupa quien entra en la página de la red social sin consentimiento del titular no pertenece al círculo de personas con las que este ha querido compartir su (inicial) intimidad (que son solo aquellos previamente aceptados por él como destinatarios), y en este sentido la calificación de la conducta podría ofrecer más dudas. La cuestión merecería sin duda una reflexión más detenida de la que puede acometerse en estas páginas; con todo, creo que aquello que ya se ha compartido con terceros (en un círculo que, si hablamos de redes sociales, siempre implica ya una cierta amplitud) no entraría en el círculo de la intimidad penalmente protegible. En tales casos de inaplicabilidad del artículo 197.1 sí podría plantearse ya, en cambio, la entrada en juego del intrusismo informático del 197 bis, un delito de contornos nada precisos y a día de hoy todavía muy poco aplicado por los tribunales (situación que no brinda demasiados

22. Esta, tras la entrada en vigor de la reforma, sería la ubicación apropiada para la conducta enjuiciada en la SAP Málaga 107/216, de 23 de marzo, que sin embargo condena, con el recurso argumental ya criticado *supra* en el texto, por el artículo 197.2 (al haberse incluido en el perfil falso una foto de la víctima –por lo demás inocua– que el sujeto tenía almacenada –lícitamente– en su teléfono móvil, foto que la sentencia considera dato personal).
23. Sobre la aplicabilidad de este y otros tipos en casos de acoso repetido a y entre menores, con las redes sociales como medio comisivo muy habitual, *vid.* Miró Llinares (2013, pág. 65 y sig.). Antes de la creación de tipos más específicos de acoso, no era extraño en la jurisprudencia, sobre todo de menores, el recurso a los delitos contra la intimidad en supuestos que claramente no satisfacían los requisitos del artículo 197 (a modo de ejemplo, SAP Murcia 7/2010, de 29 de enero).
24. SAP Barcelona 314/2015, de 8 de abril.
25. SAP Pontevedra 320/2017, de 12 de diciembre (entrada a la página de Facebook de su expareja y apertura de mensajes privados que este se intercambia con otra mujer). Se condena (incorrectamente) por el artículo 197.2 y ni siquiera se plantea la concurrencia de intrusismo informático.
26. Pensemos en el caso (bien real) de jóvenes que cuelgan en su Instagram o en su muro de Facebook imágenes en las que aparecen consumiendo droga (por ejemplo, fumando marihuana).

asideros para valorar la posibilidad de que el tipo abarque las conductas que nos ocupan).[27]

3.2. Las dificultades interpretativas del intrusismo informático del artículo 197 bis. Su proyección sobre la valoración de la conducta de acceso no consentido al espacio de un usuario en una red social

La introducción en nuestro ordenamiento del delito de *hacking* o intrusismo informático por la LO 5/2010, y su posterior reforma por la LO 1/2015, ha generado una notable controversia doctrinal en torno a la delimitación del bien jurídico protegido por el artículo 197 bis, en la que juega un papel destacado la ubicación sistemática del precepto en la que el legislador ha persistido (pues incluso tras la reforma de 2015 continúa situándolo en el capítulo de los delitos contra la intimidad). El ejemplo de la conducta de acceso no consentido a una red social puede servir como buen botón de muestra de las dificultades interpretativas (inevitables a la luz de la función teleológica desempeñada por el bien jurídico) a que todo ello está dando lugar.

Simplificando un tanto la cuestión dadas las limitaciones de espacio a las que debemos sujetarnos en esta contribución, el núcleo del problema se cifra en hasta qué punto la conducta intrusa, para resultar típica, habría de lesionar o siquiera poner en peligro la intimidad ajena, cuestión sobre la que existen indicadores contradictorios. Por una parte, es cierto que la mencionada ubicación sistemática del precepto en el seno de los delitos contra la intimidad parecería dar pie a la exigencia, siquiera en clave de generación de un peligro, de una conexión con dicho bien jurídico, y en ese sentido se pronuncia un sector importante de la doctrina, que también suele aludir al carácter excesivamente indeterminado del bien jurídico seguridad informática.[28] De otro lado, sin embargo, parece claro que tal vinculación *excluyente* al bien jurídico intimidad no se corresponde con el sentido de la normativa internacional origen de la tipificación del intrusismo, que indudablemente –baste leer los detallados considerandos de la Directiva 2013/40/UE– apunta a la seguridad informática como bien jurídico protegido en tanto presupuesto imprescindible de la actividad económica y social, los servicios públicos e infraestructuras, la seguridad nacional, etc.;[29] un bien jurídico instrumental (con todo lo que ello pueda tener de discutible, sin duda, en tanto exponente –uno más entre tantísimos otros incorporados a nuestro Código penal en los últimos años[30]– de un claro adelantamiento de las barreras penales de protección), al servicio de múltiples intereses que a mi entender abarcan pero a la vez exceden con mucho la intimidad.[31] La opción por este bien jurídico, de contornos ciertamente poco precisos, obliga de *lege lata*, por descontado, a una interpretación restrictiva del precepto en aras de su compatibilización (ha de reconocerse que compleja) con el principio de ofensividad; de modo provisional, puesto que la cuestión merece un desarrollo mucho más detenido, podrían sugerirse algunas posibilidades en este sentido, que aplicaremos ya sobre el ejemplo del acceso no consentido al espacio de un usuario en una red social.[32]

27. *Vid.* los hechos de la ya citada SAP Vigo 462/2017, en los que parece que el autor se introduce en la página de Tuenti de su expareja, sin que conste apertura de mensajes privados. En todo caso, la sentencia no se plantea el intrusismo informático; sí condena en cambio por delito contra la integridad moral al haber colgado mensajes procaces haciéndose pasar por la víctima para conseguir hacerla objeto de contactos por terceros.
28. Por todos, Doval Pais y Anarte Borallo (2016, pág. 517-520); esta parece ser la postura finalmente de Colás Turégano (2016, pág. 218). *Vid.* igualmente las amplias reflexiones de de la Mata Barranco y Barinas Ubiñas (2014, pág. 59 y sig.) y las de Galán Muñoz (2009, pág. 93-98), que opta por la inviolabilidad informática como bien jurídico claramente individual, desde una perspectiva en todo caso muy crítica con la marcada tendencia del legislador a escudarse en la normativa internacional como coartada de opciones político-criminales, como en este caso, excesivamente expansivas.
29. 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 (base de la tipificación de 2010).
30. Muy ilustrativo al respecto el reciente trabajo de Alonso Rimo 2017, con mención expresa en pág. 53 del artículo 197 *ter*, que el autor considera, a diferencia de lo aquí propuesto, tipificación expresa de actos de preparación de delitos contra la intimidad.
31. Por esta configuración del bien jurídico me decantaba en Tomás-Valiente Lanuza (2015, pág. 675). En este sentido también, entre otros, Carrasco Andrino (2010, pág. 249), o Jorge Barreiro y Guérez Tricarico (2017, n.m. 9947).
32. Imprescindible sobre la tipicidad como intrusismo del acceso a redes sociales, Jorge Barreiro y Guérez Tricarico (2017, ns. ms. 9945-9950). *Vid.* igualmente Picotti (2013, pág. 86-88), a favor de la tipicidad como intrusismo informático (en la legislación italiana) de la entrada no consentida en el espacio de un usuario en la red social.

En primer lugar, podría proponerse una interpretación que exija una especial insidiosidad del medio de acceso al sistema informático, que acentúe el desvalor objetivo de acción y revele una mayor energía criminal en la conducta de vencer las barreras de protección dispuestas por el titular del sistema de información: de acuerdo con esta idea, la entrada en el sistema habría de producirse gracias a una especial destreza o habilidad informática, lo que excluiría del tipo los accesos posibilitados por el hecho de que el sujeto simplemente conozca o disponga de la contraseña (si de este mecanismo de protección se trata) establecida por el usuario, sea porque en algún momento del pasado se le ha permitido tenerla, porque ha observado al usuario tecleándola, etc., supuestos que en puridad no habrían de considerarse *hacking*; precisamente esto es lo que ocurre en la mayoría de los casos (todavía pocos) de entrada no consentida en redes sociales que han llegado a los tribunales, protagonizados por quien había sido pareja del titular de la cuenta (casos en los que, sin embargo y en contra de lo aquí propuesto, se ha tendido a la condena).[33]

Un segundo criterio de reducción teleológica del tipo pasaría por exigir de la conducta la constatación de su peligrosidad para algún bien jurídico identificable (ya sea de titularidad individual –intimidad en el caso que ahora nos interesa– o colectiva –buen funcionamiento de servicios públicos o infraestructuras esenciales, etc.). En lo que aquí importa, no puede perderse de vista, como indican Jorge Barreiro y Guérez Tricarico, la gran diversidad de grados y matices con que la intimidad personal puede verse afectada por la participación en una red social, pues junto con espacios susceptibles de acoger informaciones más próximas a lo íntimo –la cuenta de usuario de redes como Facebook o Tuenti– existen otros en los que la implicación puede considerarse mínima –chats o foros sobre temas irrelevantes.[34]

En tercera instancia, el elemento típico del vencimiento de medidas de protección (reflejo de ese especial desvalor de acción antes aludido, pero también de la exigencia al titular del sistema de información de la puesta en práctica de sus deberes de autoprotección) se muestra susceptible de interpretaciones más o menos restrictivas. En esta línea podría considerarse atípico, por ejemplo, el acceso a lo protegido con medios fácilmente vencibles; en el ámbito de las redes sociales, esto sucedería cuando el usuario no hubiera hecho uso adecuado de las herramientas de configuración de la privacidad ofrecidas por la red.[35]

Por último, ya en el ámbito concursal, en tanto tipo de peligro para bienes jurídicos identificables más allá del bien instrumental de la seguridad informática, el desvalor del delito de acceso habría de estimarse absorbido por la consumación de otros delitos a los que se encuentre preordenado, lo que, como se ha indicado ya, sucederá –en el caso de entrada en redes sociales– siempre que se abran mensajes intercambiados en privado entre el titular y un tercero, que darán lugar al delito contra la intimidad del artículo 197.1.[36] En este contexto concursal, si el intruso

33. *Vid.* SAP Álava 74/2013, de 7 de marzo (que confirma la condena en un caso de entrada en Facebook de la expareja, en el que, aunque no se explicita, parece que la contraseña se conocía previamente); SAP Girona 504/2014, de 22 de septiembre (que parte de la tipicidad como intrusismo informático de la entrada en Facebook –parece que también en los casos aludidos en el texto–, si bien finalmente absuelve por no estar probada la falta de autorización); SAP Girona 358/2015, de 22 de junio (que condena por intrusismo la entrada en la página de Facebook de su expareja, cuya contraseña conocía al haber visto a esta última tecleándola). *Vid.* en cambio SAP Vigo 462/2017, a raíz de lo que parece una entrada no consentida en la página de Tuenti de la expareja, sin que se plantee el intrusismo (sí se condena en cambio por delito contra la integridad moral al haber colgado el autor mensajes procaces haciéndose pasar por la mujer para que fuera objeto de contactos por terceros, como efectivamente ocurrió). Considera que una entrada en la página de Tuenti sí hubiera sido típica de intrusismo de haberse encontrado ya en vigor el delito, SAP Madrid, 402/2012, de 17 de julio.
34. Jorge Barreiro y Guérez Tricarico (2017, ns. ms. 9945 y 9949). Irrelevancia que no puede predicarse por igual de todos los foros o chats (piénsese, por ejemplo, en chats privados sobre preferencias sexuales).
35. En este sentido, entienden Jorge Barreiro y Guérez Tricarico (2017, n.m. 9950), que, de considerase inicialmente típica la entrada no autorizada en un chat privado (así, la realizada por un inicial usuario luego vetado), la afirmación final de la tipicidad dependería del grado de complejidad del «baneo» o barrera impuesta, pues algunas modalidades resultan muy fácilmente superables por un usuario medianamente avezado.
36. Lo mismo sucederá si al intrusismo sigue la comisión de otros delitos, como (por citar el ejemplo que parece más relevante) daños informáticos del artículo 264 Cp. De hecho, es esta figura (y sobre todo el tipo cualificado de su apartado 2, en sus circunstancias 3.ª y 4.ª, cuando los daños informáticos hayan perjudicado gravemente servicios esenciales, o hayan afectado al sistema informático de una infraestructura crítica, o se hubiera creado una situación de peligro grave para la seguridad del Estado o de la UE) la que parece conectarse de modo más directo con el espíritu de la Directiva.

accede a los datos personales facilitados por el usuario en la configuración de su perfil (dirección de correo electrónico, dirección postal, número de teléfono, profesión, etc.) podría quizás plantearse la entrada en juego del artículo 197.2 (puesto que aquí sí sería más defendible entender que se encuentran archivados en un registro informático); ello dependerá, no obstante, del entendimiento más o menos restrictivo que se defienda de los «datos personales *reservados*» objeto material de dicho delito, que a mi entender, como ya he defendido en otro lugar, no deben identificarse sin más con los datos personales objeto de protección administrativa.[37] Al no aplicarse entonces el tipo directamente protector de la intimidad, queda abierta la subsunción de la conducta bajo el intrusismo del 197 bis, que en todo caso convendría sujetar a los parámetros restrictivos arriba mencionados.

Bibliografía

ALONSO RIMO, A. (2017). «¿Impunidad general de los actos preparatorios? La expansión de los delitos de preparación». *InDret* 4/2017, pág. 1-79

CARRASCO ANDRINO, M. (2010). «El delito de acceso ilícito a los sistemas informáticos (arts. 197 y 201)». En: F. J. ÁLVAREZ GARCÍA y J. L. GONZÁLEZ CUSSAC. (dirs.). *Comentarios a la Reforma Penal de 2010*. Valencia: Tirant lo Blanch, pág. 249-256.

COLÁS TURÉGANO, A. (2016). «El delito de intrusismo informático tras la reforma del Código penal español de 2015». *Revista Boliviana de Derecho*. N.º 21, pág. 210-229.

DE LA MATA BARRANCO, N.; BARINAS UBIÑAS, D. (2014). «La protección penal de la vida privada en nuestro tiempo social: ¿necesidad de redefinir el objeto de tutela?». *Revista de Derecho penal y Criminología*, 3.ª *época*. *Nº* 1, *pág*. 13-92.

DOVAL PAIS, A.; ANARTE BORALLO, E. (2016). «Lección XIX: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio (1). Delitos de descubrimiento y revelación de secretos». En: J. BOIX REIG. *Derecho penal Parte Especial*, vol. I, 2.ª ed. Madrid: Iustel, pág. 493-549.

GALÁN MUÑOZ, A (2009). «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*. N.º 24, pág. 90-107.

GONZÁLEZ COLLANTES, T. (2015). «Los delitos contra la intimidad tras la reforma de 2015: luces y sombras». *Revista de Derecho penal y Criminología*, 3.ª Época. N.º 13, pág. 51-84.

JAREÑO LEAL A. (2008). *Intimidad e imagen: los límites de la protección penal*. Madrid: Iustel, 144 pág.

JORGE BARREIRO, A.; GUÉREZ TRICARICO, P. (2017). «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio». En: F. MOLINA FERNÁNDEZ (dir.). *Memento penal* 2017. Madrid: Francis Lefevre, ns. ms. 9850-10039.

MENDO ESTRELLA, A. (2016). «Delito de descubrimiento y revelación de secretos: acerca de su aplicación al sexting entre adultos». *Revista Electrónica de Ciencias Penal y Criminología*. N.º 18-16, pág. 1-27.

MIRÓ LLINARES, F. (2013). «Derecho penal, cyberbullying y otras formas de acoso (no sexual) en el ciberespacio». En: M. J. PIFARRÉ (coord.). «Internet y redes sociales: un nuevo contexto para el delito» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 16, pág. 61-75.

37. Tomás-Valiente Lanuza (2015, pág. 664-5), donde me acojo a interpretaciones restrictivas del objeto material del artículo 197.2 como la sugerida por Jareño Leal (2008, pág. 61 y sig.).

MORALES PRATS. F. (2016). «Comentario al art. 197 Cp». En: G. QUINTERO OLIVARES F. MORALES PRATS (2016). *Comentarios al Código penal de 1995. Tomo I, pág. 1434-1473.* 7.ª ed. Cizur Menor: Aranzadi.

PICOTTI, L. (2013). «Los derechos fundamentales en el uso y abuso de las redes sociales en Italia: aspectos penales». En: M. J. PIFARRÉ (coord.). «Internet y redes sociales: un nuevo contexto para el delito» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 16, pág. 76-90.

TOMÁS-VALIENTE LANUZA, C. (2015). «Capítulo I. Del descubrimiento y revelación de secretos». En: M. GÓMEZ TOMILLO. *Comentarios prácticos al Código penal,* Tomo II. Cizur Menor: Aranzadi, pág. 653-698.

Cita recomendada

TOMÁS-VALIENTE LANUZA, Carmen (2018). «Delitos contra la intimidad y redes sociales (en especial, en la jurisprudencia más reciente)». En: Albert GONZÁLEZ JIMÉNEZ (coord.). «Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes». *IDP. Revista de Internet, Derecho y Política*. N.º 27, págs. 30-41. UOC [Fecha de consulta: dd/mm/aa]
<http://dx.doi.org/10.7238/idp.v0i27.3147>

Sobre la autora

Carmen Tomás-Valiente Lanuza
carmen.tomas-valiente@uib.es

Profesora titular de Derecho Penal
Universitat de les Illes Balears

http://www.uib.es/es/personal/ABjMzNTQwMw/

Facultat de Dret (edifici Gaspar Melchor de Jovellanos)
Universitat de les Illes Balears
Cra. de Valldemossa, km 7.5. Palma (Illes Balears)