FACULTAD DE DERECHO

LA PROTECCIÓN PENAL DEL DERECHO A LA INTIMIDAD EN EL MARCO DE LAS NUEVAS TECNOLOGÍAS

Autor: Alejandra Sánchez Ballesteros
5º E3 D
Derecho Penal
Tutor: Miriam Cabrera Martín

Madrid
Abril 2018

RESUMEN

El propósito de este trabajo es estudiar la protección penal del bien jurídico intimidad tras la reforma del Código Penal, centrando la atención en el marco de las nuevas tecnologías, por entender que han sido uno de los motores principales de los cambios producidos. Se dedica especial atención a los delitos recogidos en los artículos 197.7 y 197 bis CP, por considerarse que son las figuras más novedosas y que plantean mayores problemas interpretativos.

PALABRAS CLAVE: intimidad; Código Penal; nuevas tecnologías; Internet; *sexting*; *hacking;* bien jurídico; intrusismo informático.

ABSTRACT

The purpose of this paper is to study the criminal protection of the legal privacy after the reform of the Spanish Criminal Code, focusing attention on the framework of new technologies, understanding that they have been one of the main engines of the changes produced the last years. Special attention is given to the crimes included in articles 197.7 and 197 bis CP, as they are the most novel and have major interpretative problems.

KEY WORDS: privacy, Spanish Criminal Code; new technologies; Internet; sexting; hacking; legal right; informatic intrusion.

ÍNDICE DE CONTENIDO

LISTA DE ABREVIATURAS

AP	Audiencia Provincial
BOE	Boletín Oficial del Estado
CE	Constitución Española
Coord.	Coordinador
CP	Código Penal
Dir.	Director
Ed.	Editor
FJ	Fundamento Jurídico
LO	Ley Orgánica
nº.	Número
núm.	Número
op. cit.	Obra citada
p.	Página
pp.	Páginas
SAP	Sentencia de la Audiencia Provincial
STC	Sentencia del Tribunal Constitucional
STS	Sentencia del Tribunal Supremo
TC	Tribunal Constitucional
TS	Tribunal Supremo

1. INTRODUCCIÓN

El siglo XXI se encuentra marcado por una revolución tecnológica. La aparición de Internet ha provocado un salto cualitativo en la sociedad, ha revolucionado nuestra forma de vivir. Hoy en día, Internet es la forma más común de comunicación personal, laboral y social; pone en contacto millones de ordenadores, ha eliminado fronteras y todo ello sin que haya una autoridad que lo gobierne. Las tecnologías de la información están transformando nuestra sociedad invadiendo todas las facetas, hasta el punto de que cualquier usuario puede tener acceso a la información almacenada en sistemas informáticos.

Si bien los beneficios y facilidades que ha aportado y sigue aportando son muchos, este desarrollo tiene un lado negativo, pues ha fomentado la aparición de nuevas formas de criminalidad; las redes informáticas se utilizan para cometer nuevos delitos, como, por ejemplo, el acceso ilegal a sistemas informáticos, así como delitos tradicionales. Por ello, a remolque de las nuevas tecnologías nos encontramos ante un nuevo Derecho penal, consecuencia de las modificaciones que están provocando en las conductas delictivas.

Dada la velocidad a la que se desarrollan los cambios y la magnitud de los mismos, el sistema normativo penal era insuficiente e impotente ante este nuevo tipo de criminalidad, de ahí que se haya reformado el Código Penal en numerosas ocasiones desde su publicación en 1995, siendo las de 2010 y 2015 las más importantes. De este modo, el Código Penal ha tratado de dar respuesta a las nuevas conductas que han ido surgiendo, a través de los llamados "ciberdelitos".

Tras la aparición de Internet y demás avances tecnológicos, se puede hablar de dos tipos de delitos relacionados con la informática. Por un lado, se encuentran los delitos cuyo único medio de comisión es la red, donde se enmarca el delito de *hacking* que se analizará en apartados posteriores. Por otro lado, encontramos las infracciones tradicionales que se han visto alteradas por la utilización de las redes telemáticas como instrumento, modificando así, las conductas típicas preexistentes. Entre estos últimos delitos se encuentran el fraude por internet, comúnmente conocido como *phishing*, los

atentados contra la propiedad intelectual e industrial y, los ataques a la intimidad como consecuencia de la difusión de contenidos, como es el caso del artículo 197.7 CP, que también se explicará a lo largo de este trabajo, entre otros.

Con la modificación de las conductas típicas existentes y la aparición de nuevas figuras delictivas, los bienes jurídicos protegidos también se han visto afectados. En este sentido, cabe destacar la importancia que ha tenido la protección del derecho a la intimidad, que ha sufrido modificaciones en las dos últimas grandes reformas del Código Penal llevadas a cabo. Asimismo, han surgido nuevos bienes jurídicos, como puede ser la seguridad en las redes y sistemas informáticos.

El propósito de este trabajo es estudiar la protección penal del bien jurídico intimidad tras la reforma del Código Penal, centrando la atención en el marco de las nuevas tecnologías, por entender que han sido uno de los motores principales de los cambios producidos. Se dedica especial atención a los delitos recogidos en los artículos 197.7 y 197 bis CP, por considerarse que son las figuras más novedosas y que plantean mayores problemas interpretativos.

En el preámbulo de la Ley Orgánica 1/2015, de 30 de marzo, por la que se reforma el Código Penal, se hace referencia a las modificaciones en materia de delitos de descubrimiento y revelación de secretos, así como de delitos de daños informáticos, como consecuencia de la incorporación al ordenamiento jurídico español de la Directiva 2013/40/UE, del Parlamento y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas informáticos. La reforma se planteaba, por tanto, como una exigencia internacional.

Además, de acuerdo con la Fiscalía General del Estado, las modificaciones en los tipos penales responden también a la voluntad del Legislador español de dar respuesta penal a determinados comportamientos, como es el caso de la divulgación de imágenes o grabaciones de una persona, tomadas con su consentimiento, pero, que se difunden sin

su autorización, afectando gravemente a su intimidad personal[1], conducta típica que será objeto de estudio en el presente trabajo.

La mencionada Directiva 2013/40/UE, sustituía la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los servicios de información, por la que se reformó el Código Penal en 2010. Dada la rápida evolución de la tecnología, en pocos años había surgido la necesidad de articular otras figuras delictivas o de modificar las existentes, para poder actuar penalmente frente a nuevas situaciones.[2] De ahí que se promulgase la Directiva de 2013, tras la cual se llevó a cabo la reforma del Código Penal de 2015.

Con la reforma del Código Penal de 2015, el artículo 197 del mismo sufre diversas modificaciones. De acuerdo con lo expuesto en el Preámbulo de la Ley Orgánica por la que se reforma el Código Penal, "se introduce una separación nítida entre los supuestos de revelación de datos que afectan directamente a la intimidad personal, y el acceso a otros datos o informaciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal"[3]. A grandes rasgos, las novedades son las siguientes: el nuevo artículo 197 bis recoge el delito de acceso ilegal a sistemas informáticos, antes recogido en el apartado 3 del artículo 197; los apartados 4,5,6 y 7 de este artículo pasan a numerarse como 3,4,5 y 6, respectivamente, y cambia el contenido del apartado 7, como se analizará más adelante.

Sin embargo, aunque la reforma fue oportuna, a causa de la situación político criminal ante la que se encontraba la sociedad, no por ello fue acertada en términos de contenido. Atendiendo a una interpretación estricta de lo que en ella se establece, los artículos 197.7 y 197 bis CP merecen una revisión y consecuente modificación, como se expondrá a lo largo de estas líneas.

[1] Circular 3/2017, sobre la reforma del código penal operada por la LO 1/2015 de 30 de marzo en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos.
[2] Circular 3/2017 *op. cit.*
[3] 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.

2. BIEN JURÍDICO PROTEGIDO: INTIMIDAD

A la hora de abordar el análisis jurídico-penal de una figura delictiva parece necesario comenzar explicando aquellos aspectos relacionados con el bien jurídico protegido, su determinación y su concreción. El bien jurídico protegido en los delitos de descubrimiento y revelación de secretos del artículo 197 CP, se considera que es la intimidad, como se desprende de la propia rúbrica del Título X del Libro II del Código Penal, en el que se encuentra ubicado el delito.

En un primer momento, la intimidad se protegía en su vertiente negativa consistente en el derecho a estar libre de intromisiones ilegítimas de terceros en el ámbito personal. Se trataba de proteger del alcance de terceros un espacio privado, a fin de que cada uno pudiera decidir quién podía o no podía participar de ese ámbito personal e individual, mediante la prohibición de intromisiones ajenas.

En la Constitución Española el derecho a la intimidad aparece recogido en el artículo 18. Dicho artículo se encuentra en el Título I "De los derechos y deberes fundamentales" y protege varios derechos, basados todos en la salvaguarda de la intimidad, aunque con diferentes matices[4]. En concreto, son los apartados primero y cuarto del artículo 18 los que contienen el derecho a la intimidad:

1. *Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
   (...)
   4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Este artículo se ha de poner en relación con los arts. 20.4 y 10.1 de la misma Ley Fundamental. El primero de ellos establece el límite a la libertad de expresión y el derecho a la información "especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia".[5] Por su parte, el

[4] ELVIRA PERALES, A., "Sinopsis artículo 18".
[5] Artículo 20.4 CE

artículo 10.1 CE establece que la dignidad de la persona, los derechos inviolables que le son inherentes y el libre desarrollo de la personalidad son fundamento del orden político y de la paz social.

Es en este sentido negativo en el que el derecho a la intimidad aparecía recogido en la Declaración Universal de Derechos Humanos de 1948, en virtud de cuyo artículo 12: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Posteriormente, el mismo derecho apareció recogido en otros textos, tanto a nivel nacional como internacional. En el ámbito internacional cabe destacar el camino marcado por Naciones Unidas; en este sentido, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966 supuso el reconocimiento definitivo de la intimidad como derecho fundamental en el ámbito internacional[6]. El citado artículo transcribe el texto literal recogido en la Declaración Universal de Derecho Humanos que se citaba en líneas anteriores.

El ámbito de la intimidad reconocido en el artículo 18 CE se limita, en el apartado primero a la prohibición de interferencias externas. De este modo, "lo que el artículo 18.1 CE garantiza es el secreto sobre nuestra propia esfera de vida personal y, por tanto, veda que sean los terceros, particulares o poderes públicos, quienes decidan cuáles son los contornos de nuestra vida privada"[7]. Esto es, recoge el derecho a la intimidad entendido como derecho de exclusión.

Por otro lado, en el apartado 4 del mismo artículo se hace referencia a la autodeterminación informativa: derecho a decidir qué datos, cuándo…; en definitiva, el poder de control de datos personales. En este sentido, el derecho a la intimidad implica "poder de acción del titular para exigir que determinados datos personales no sean conocidos, lo que supone reconocer un derecho a la autodeterminación informativa, entendido como libertad de decidir qué datos personales pueden ser obtenidos y tratados

[6] MARTÍNEZ DE PISÓN, J., "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" en MINISTERIOS DE JUSTICIA, BOLETÍN OFICIAL DEL ESTADO, BOE Y SOCIEDAD ESPAÑOLA DE FILOSOFÍA JURÍDICA Y POLÍTICA (ed.), *Anuario de Filosofía del Derecho*, Ministerio de Justicia y la Agencia Estatal Boletín Oficial del Estado, 2016, p. 411.
[7] STS núm. 176/2013 (Sala 2ª), de 21 de octubre FJ 7.

por otros"[8]. Ello supone un reconocimiento de las dos vertientes de la intimidad: la positiva y la negativa, reflejo de la evolución del bien jurídico intimidad[9].

Así, el Tribunal Supremo expone que "el derecho a la protección de los datos de carácter personal deriva del artículo 18.4 CE y consagra en sí mismo un derecho o libertad fundamental, que excede el ámbito propio del derecho fundamental a la intimidad (artículo 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona".[10] En sentido similar, el Tribunal Constitucional define la libertad informática como "derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención".[11]

Por lo tanto, entendemos la intimidad personal en un sentido moderno y actualizado. No sólo implica libertad negativa, la prohibición de interferencias externas, vinculada a la idea de secreto. También hace referencia, en un sentido positivo, al reconocimiento del bien jurídico *privacy*[12], que supone tener poder de control sobre los datos e informaciones relacionadas con uno mismo, situado en un contexto tecnológico que se proyecta sobre la sociedad actual, marcada por la sociedad 2.0[13].[14][15]

[8] SAP de Barcelona núm. 742/2017 (Sección 20ª), de 7 de septiembre FJ 8.

[9] Así lo refleja la STS núm. 586/2016 (Sala de lo Penal, Sección1ª), de 4 julio, FJ 4: "Se trata de una mutación histórica de innegable trascendencia conceptual, de un derecho de nueva generación que otorgaría a cada ciudadano el control sobre la información que nos concierne personalmente, sea íntima o no, para preservar, de este modo y en último extremo, la propia identidad, nuestra dignidad y libertad".

[10] STS núm. 803/2017, de 11 de diciembre de 2017, FJ 4.

[11] Sentencia del Tribunal Constitucional, de 30 de noviembre de 2000, Sentencia núm. 292/2000, FJ 5.

[12] Término adoptado de la cultura anglosajona.

[13] La expresión de "sociedad 2.0" hace referencia a la sociedad marcada por la revolución tecnológica, que trae consigo numerosos e importantes avances e innovaciones en el ámbito de las comunicaciones y la información. Se ha creado una sociedad en la que las relaciones interpersonales están basadas, en su mayor parte, en las nuevas tecnologías y en la red, creando así una cantidad innumerable de datos, susceptibles de afección. De este modo, las personas se han convertido, no sólo en consumidores de contenido informático sino, también, en creadores del mismo; se ha generalizado la creación de datos informáticos.

[14] JORGE BARREIRO, A., "Delitos contra la intimidad, derecho a la propia imagen e inviolabilidad del domicilio" (Actualizado por GUÉREZ TRICARICO, P.) en MOLINA FERNÁNDEZ, F. (coord.), *Memento Práctico Penal*, Francis Lefebvre, Madrid, 2016, p. 1030.

[15] Esta es la conclusión del análisis del texto constitucional y de las leyes que en nuestra legislación se encuentran destinadas a la salvaguarda del derecho a la intimidad.

Los primeros en definir el derecho a la intimidad fueron WARREN y BRANDEIS, en 1890[16], quienes querían proteger la esfera privada de las personas frente a los *paparazzi*, anticipándose a uno de los principales problemas que se plantean hoy en día en relación con la protección de la intimidad, como es el del desarrollo de los medios de comunicación, que buscan información en relación con el ámbito personal y familiar, y el de los límites que se puedan o deban establecer a los mismos. A esta nueva dimensión de la intimidad la denominaron *Right to be let alone,* es decir "el derecho a estar solo", o "el derecho a no ser molestado". De esta manera, gracias a WARREN y BRANDEIS, la protección a la denominada *privacy* fue cobrando importancia y reconocimiento.[17] En este sentido, el bien jurídico *privacy*, constituye una dimensión positiva del derecho a la intimidad, pues supone el derecho de control sobre los datos e información de cada uno, frente al sentido negativo de este derecho, que supone la prohibición de intromisión por parte de terceros al ámbito personal.

Asimismo, en nuestro Ordenamiento se refieren a la protección de la intimidad la 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, y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Sin embargo, pese a que queda claro el reconocimiento de la intimidad como un derecho fundamental de la persona, persisten dos cuestiones pendientes de resolver en relación con el mismo. Por un lado, se encuentra el problema de la falta de una definición unívoca del concepto de intimidad, tanto en el texto constitucional como en las leyes que desarrollan el derecho. En estas circunstancias, ha sido la jurisprudencia la encargada de ir delimitando el concepto, atendiendo al caso concreto.[18]

Por otro lado, suscita interés el debate acerca de la naturaleza singular o plural de los derechos recogidos en el artículo 18 CE, es decir, acerca de si el derecho al honor, a la

---

[16] WARREN, S. Y BRANDEIS, L., "Right to Privacy" *Harvard Law Review*, The Harvard Law Review Association, Vol. 4, No. 5, 1890, pp. 193-220.

[17] MARTÍNEZ DE PISÓN, J. "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" *op. cit.,* p. 412.

[18] FAYOS GARDÓ, A., *Derecho a la intimidad y medios de comunicación*, Centro de Estudios Políticos y Constitucionales, Madrid, 2000, p. 7 [*non vidi,* citado en MARTÍNEZ DE PISÓN, J. "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" *op. cit*., p. 416].

intimidad personal y familiar y a la propia imagen, forman parte del mismo derecho a la intimidad o si constituyen diferentes derechos. La doctrina mayoritaria entiende que son tres derechos autónomos, que a su vez constituyen derechos de la personalidad. En este sentido, la jurisprudencia ha establecido en numerosas ocasiones, que "los derechos a la intimidad personal y a la propia imagen garantizados por el artículo 18.1 CE forman parte de los bienes de la personalidad que pertenecen al ámbito de la vida privada"[19], con lo cual, se puede hablar del derecho a la intimidad como derecho de carácter personalísimo. Se entiende que el derecho a la intimidad forma parte de un espacio de intimidad personal y familiar, al margen de la intrusión de terceros, y merece necesaria protección consecuencia del alcance de los medios de comunicación e información, por la vulnerabilidad de la intimidad frente a estos[20].

[19] STS de 30 de diciembre de 2009 citada en SAP de Las Palmas núm. 22/2011 (Sección 1ª), de 20 de enero, FJ 3.
[20] SAP de Barcelona núm. 742/2017 (Sección 2ª), de 7 de septiembre, FJ 1.

3. SISTEMÁTICA DE LOS DELITOS DE DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS

En el presente epígrafe se expone brevemente el contenido del Capítulo I integrado en el Título X del Código Penal, resaltando los aspectos más relevantes de cada artículo, a fin de reflejar una visión general sobre el panorama de los delitos de descubrimiento y revelación de secretos

- Artículo 197.1 CP: En el apartado 1 del artículo 197 se encuentra el que constituye el tipo básico de los delitos de descubrimiento y revelación de secretos, mediante el que se tutela la intimidad personal en su vertiente negativa, es decir, como el derecho de la persona a excluir determinadas informaciones del conocimiento de terceros. Se trata de un tipo mixto alternativo[21] que puede consumarse de dos maneras, bien mediante el apoderamiento de papeles, cartas, mensajes de correo electrónico u otros documentos o efectos personales, bien mediante la interceptación de las telecomunicaciones o la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido de la imagen u otra señal de comunicación. Cabe añadir que, de acuerdo con la doctrina y la jurisprudencia, "para la consumación del delito basta con el acto de apoderamiento o de interceptación, sin que sea necesario acceder o captar los contenidos íntimos de la vida privada"[22].

- Artículo 197.2 CP: En este apartado se regula el delito de descubrimiento y revelación de secretos en relación la intimidad informática (derecho de control sobre los datos personales informatizados).[23] Las conductas típicas suponen el apoderamiento, uso o modificación de datos, y el objeto material del delito son los datos registrados en ficheros o soportes electrónicos, informáticos o telemáticos, u otro tipo de archivo o registro público o privado. De este modo, se tutela la intimidad informática que, como se ha explicado anteriormente, implica el derecho de control sobre los datos e informaciones relacionadas con uno

[21] OTERO GONZÁLEZ, P., "Delitos contra la intimidad, derecho a la propia imagen e inviolabilidad del domicilio" en ORTIZ DE URBINA GIMENO, I. y AYALA GÓMEZ, I. (coord.), *Memento Práctico. Penal Económico y de la Empresa*, Francis Lefebvre, Madrid, 2016-2017, p. 360.
[22] SAP de Islas Baleares núm. 197/2017 (Sección 1ª), de 31 julio, FJ 2.
[23] SAP de Granada núm. 486/2014 (Sección 1ª), de 18 de septiembre, FJ 2.

mismo. Básicamente, consiste en el delito de descubrimiento y revelación de secreto cometido en soporte electrónico.[24]

Al igual que sucede en los supuestos del apartado anterior, basta con el mero acceso a los datos para consumar el delito.[25] La conducta típica exige la falta de autorización por parte del sujeto pasivo y que se lleve a cabo en perjuicio de un tercero, sin necesidad de que ese tercero sea el titular de los datos.

De acuerdo con la jurisprudencia lo característico de ese delito es que protege los "datos propios de la intimidad de una persona guardados en bases de datos no controlados por el titular del derecho, y, por ende, sujetas a especiales normas de protección y de acceso que el autor quiebra para acceder. El carácter sensible de los datos a los que se accede incorpora el perjuicio típico".[26] Conforme a la jurisprudencia, se consideran datos sensibles a estos efectos todos los datos personales automatizados (siempre que pertenezcan al ámbito privado y personal o familiar del sujeto)[27], sin distinciones; cuando se trata de datos especialmente sensibles que conforman el núcleo duro de la intimidad (ideología, religión, salud y vida sexual)[28] se habrá de acudir al tipo penal del artículo 197.4 CP.

- Artículo 197.3 CP: Constituye un tipo agravado de los anteriores apartados que se aplica cuando la acción delictiva supone una mayor afectación a la intimidad. Esta mayor afectación se produce por la relevación, difusión o cesión de los datos, hechos o imágenes obtenidos. Es requisito haber cumplido, en primer lugar, con los requisitos del tipo básico recogido en los apartados 1 y 2 del mismo artículo para que la acción se pueda subsumir en el tipo gravado en cuestión.[29] De no ser así, habría que acudir al artículo 199.2 CP.

[24] De acuerdo con el Auto de la AP de La Rioja núm. 171/2017 (Sección 1ª), de 19 de mayo, FJ 2: "No tienen por qué ser informáticos, porque se acoge también a cualquier otro tipo de archivo o registro público o privado".
[25] SAP de Guadalajara núm. 31/2017 (Sección 1ª), de 4 diciembre, FJ 2.
[26] Auto del TS (Sala de lo Penal, Sección 1ª) núm. 199/2018, de 18 enero, FJ 1.
[27] STS núm. 532/2015 (Sala de lo Penal, Sección 1ª), de 23 septiembre, FJ5.
[28] FAYOS GARDÓ, A., *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Dykinson, Madrid, 2015, p. 127.
[29] Auto de la AP de Madrid (Sección 30ª) núm. 286/2017, de 29 marzo, FJ 3.

- Artículo 197.4 CP: Constituye un tipo agravado que presenta dos modalidades: Por un lado, que el sujeto activo de las conductas básicas recogidas en los apartados 1 y 2 del mismo artículo sea la persona encargada o responsable del fichero en el que se encontraban ubicados los datos objeto del delito. Por otro lado, cuando las mismas conductas se lleven a cabo mediante la utilización de los datos personales de la víctima sin su autorización, esto es, mediante el uso indebido de una contraseña o una clave de acceso, por ejemplo.

- Artículo 197.5 CP: Constituye un tipo cualificado previsto para cuando la conducta afecte a datos personales especialmente sensibles, estos son los relativos a la ideología, la religión, la vida sexual y la salud. Caben dos modalidades de comisión de este delito: por un lado, que la acción típica de los apartados anteriores afecte a datos especialmente sensibles en sentido estricto, es decir, a los indicados anteriormente, y por otro, que los datos pertenezcan a un menor de 18 años o a una persona discapacitada que necesite especial protección.

- Artículo 197.6 CP: Constituye un tipo agravado por razón de los fines lucrativos, de tal manera que, el delito cometido esté motivado por la obtención de un beneficio económico. Si además afecta al núcleo duro de la intimidad se prevé un tipo hiperagravado.

- Artículo 197.7 CP: Es una de las figuras más novedosas introducidas tras la reforma de 2015, razón por la cual su análisis será abordado de una manera más precisa en el siguiente apartado. La conducta típica supone la difusión, revelación o cesión a terceros de imágenes o grabaciones audiovisuales del sujeto pasivo sin su autorización "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"[30]. Cabe apreciar la confusión que suscita la literalidad del texto legal, motivo por el que se estudiará con más detalle a continuación.

[30] Artículo 197.7 CP

- Artículo 197 bis CP: En este artículo se regula el delito de intrusismo informático, que sanciona el acceso ilegal a sistemas de información[31]. Cabe destacar, introduciendo el debate que se tratará más adelante, que es cuestionable la ubicación de este artículo dentro de los delitos contra la intimidad personal. En este sentido, se discute acerca de cuál es el bien jurídico protegido, pues una parte de la doctrina, que defiende que la ubicación es la correcta, considera que es la intimidad, mientras que el sector mayoritario entiende que se trata de un nuevo bien jurídico, la seguridad de los sistemas informáticos, y por ello, ubicar este precepto con los demás delitos contra la intimidad es desafortunado e inapropiado. Este debate se expondrá más adelante, en el apartado 5.2 del presente trabajo.

- Artículo 197 ter CP: Se adelantan las barreras de la intervención penal en relación con las conductas tipificadas en los apartados 1 y 2 del artículo 197 y en el artículo 197 bis, sancionando las conductas preordenadas al *hacking*. Se castigan, por tanto, las conductas previas de producción, adquisición para su uso, importación o facilitación a terceros de un programa informático que sirva para cometer dichos delitos, o de una contraseña de ordenador, código de acceso o similar que permitan acceder a un sistema informático, total o parcialmente.[32] Se trata de un supuesto de conversión en delito autónomo de lo que en otro caso serían meros actos preparatorios, del mismo modo que se hace en el ámbito de las falsedades (artículo 400 CP), en el de la estafa (artículo 248.2.b CP) o en el de los delitos contra la propiedad intelectual (artículo 270.6 CP).

- Artículo 197 quarter CP: Constituye un tipo cualificado para el caso en el que los delitos anteriores se cometan en el seno de una organización o grupo criminal

[31] Circular 3/2017 *op. cit.*
[32] JORGE BARREIRO, A., "Delitos contra la intimidad, derecho a la propia imagen e inviolabilidad del domicilio", *op. cit.,* p. 1048.

- Artículo 197 quinquies CP: En este artículo se contempla la posibilidad de que las personas jurídicas respondan por los delitos comprendidos en los artículos 197, 197 bis y 197 ter CP sea una persona jurídica.

- Artículo 198 CP: Regula el supuesto en el que el sujeto activo que realiza las conductas anteriores es una autoridad o funcionario público.

- Artículo 199 CP: Hace referencia al delito de revelación de secretos cuando se vulnera el secreto profesional, por revelarse los secretos del sujeto pasivo conocidos por razón de profesión, oficio o de relaciones laborales.

- Artículo 200 CP: Consiste en el descubrimiento, revelación o cesión de datos reservados referidos a las personas jurídicas. Si bien hace alusión a los datos referidos a las personas jurídicas, se entiende que se proyecta sobre datos con trascendencia en las personas físicas, esto es, datos sobre los socios o empleados de una sociedad, por ejemplo, y no datos o información de tipo societario o empresarial. En este último caso, habría que acudir a los artículos 278 y siguientes del Código Penal.[33]

- Artículo 201 CP: Hace referencia a la acción penal y denuncia de los delitos anteriores. El proceso penal contra los delitos hasta ahora mencionados es necesario que comience con una denuncia interpuesta por la persona agraviada o su representante legal, o por el Ministerio Fiscal cuando la víctima sea un menor de edad, una persona con discapacidad que necesite protección especial o una persona desvalida. No obstante, esta denuncia no será necesaria cuando el delito afecte al interés general o a una pluralidad de demandados, o se trate del delito descrito en el artículo 198. Además, el perdón del ofendido o de su representante legal, en su caso, extingue la acción penal.

[33] OTERO GONZÁLEZ, P., "Delitos contra la intimidad, derecho a la propia imagen e inviolabilidad del domicilio", *op. cit.,* p. 382.

4. ARTÍCULO 197.7

> Artículo 197.7 CP: *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 pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.*

Las nuevas tecnologías favorecen la captación de imágenes y su posterior difusión, gracias a las prestaciones que traen consigo en el ámbito de la información y la comunicación. Como consecuencia de los avances tecnológicos, una parte de nuestra actividad o entorno íntimo pasa a estar recogido en sistemas informáticos, formando parte de nuestra intimidad informática. En este sentido, se ha generado tal situación en la que una vez se difunden los contenidos de dicha intimidad mediante los nuevos sistemas de comunicación (como puede ser la aplicación "*Whatsapp")* se pierde la capacidad de control de los mismos. De este modo, han ido surgiendo situaciones que, dada la velocidad a la avanzaban las nuevas tecnologías, no tenían acomodo con la regulación anterior. Un ejemplo es el caso en el que las imágenes o grabaciones audiovisuales difundidas se hubieran grabado con el consentimiento de la víctima, pero su posterior difusión no ha sido autorizada por la misma, ni expresa ni tácitamente.

Con la introducción de esta figura tras la reforma del CP en 2015, se entiende que el legislador trató de dar respuesta penal a ese tipo de situaciones, ya que con la anterior legislación se regulaban únicamente los supuestos de captación de imágenes o grabaciones en los que la acción se hubiera llevado a cabo sin anuencia de la víctima. Antes de la incorporación de esta figura al CP, los casos en los que las imágenes o grabaciones audiovisuales difundidas se hubieran grabado con el consentimiento de la víctima normalmente eran atípicos; en ningún caso, se trataban como un delito contra la

intimidad.[34] Si bien, se dio lugar a otras soluciones. En el ámbito penal, las soluciones más comunes resolvían declarando la comisión de un delito contra la integridad moral[35] o condena por delito de injurias[36]. Sin embargo, en otras ocasiones, tuvieron lugar pronunciamientos absolutorios y remisión a los tribunales civiles, aplicando la Ley Orgánica 1/1982 de 5 mayo, *de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.*[37][38]

Es por eso que, dada la variedad de soluciones que se planteaban ante tales situaciones, se considera, cuanto menos, oportuna y acertada la introducción y tipificación de esta figura. Se trata de una conducta consecuencia de la combinación entre las tecnologías de la comunicación y de Internet, ya que, a través de este último, se han desarrollado canales de comunicación, ámbito en el que cabe destacar el incremento de la vulnerabilidad del bien jurídico y que trae consigo la rápida y fácil difusión a través de métodos digitales.

La principal característica y nota diferenciadora de este delito respecto a los contenidos en los anteriores apartados del artículo 197 es el consentimiento de la víctima a que se tomen o graben las imágenes o el contenido audiovisual que constituye el objeto del delito. De esta manera, se puede afirmar que el ataque a la intimidad se produce en una

[34] Véase como ejemplo de esta situación en SAP de Lleida núm. 90/2004, de 25 de febrero de 2004, FJ 1, en la que los hechos declarados y probados consisten en la grabación consentida en una cinta de vídeo de imágenes de la querellante y del acusado mientras mantenían relaciones sexuales, así como su posterior difusión, sin autorización de la víctima, a terceros que la visionaron. En dicha sentencia se establece que "la difusión de la cinta de vídeo por el mismo no tiene encaje jurídico penal entre los delitos contra la intimidad, ya que para ello es preciso que los datos o las imágenes que se revelan hayan sido descubiertos o captados por el sujeto activo mediante una intromisión o injerencia ilícita en la intimidad ajena, que no concurre cuando, como es el caso, el sujeto pasivo ha prestado su consentimiento para la grabación de las imágenes".

[35] Véase como ejemplo en SAP de Santa Cruz de Tenerife núm. 419/2015 (Sección 2ª), de 28 de septiembre de 2015, FJ 3, en la que los hechos narran que la víctima había mandado un video erótico suyo vía *whatsapp* al sujeto activo quien, en contra de la voluntad de la víctima lo conservó y lo mandó a un tercero. Así, dicha sentencia establece que "hay prueba directa de los hechos de carácter personal, (…), para denigrar y agraviar a la que fuera su novia, utilizando el video que esta última le envió por *whatsapp* con el ruego de que lo borrase, para difundirlo a terceros y llevar a cabo una reprobable campaña para denigrar a Miriam y atentar contra su dignidad, tras concluir la relación con ella, que produjo a esta última un serio daño moral hasta el punto de solicitar apoyo sicológico y precisar tratamiento siquiátrico".

[36] Véase como ejemplo en la anteriormente citada Sentencia de la Audiencia Provincial de Lleida, de 25 de febrero de 2004, en la que se condena la conducta como delito de injurias grave.

[37] COLÁS TURÉGANO, A., "Nuevas conductas delictivas contra la intimidad (arts. 197, 197 bis; 197 ter) en MATALLIN EVANGELIO, A., y GÓRRIZ ROYO, E. (coord.), GONZÁLEZ CUSSAC, J. (dir.), *Comentarios a la Reforma del Código Penal de 2015*, Tirant lo Blanch reformas, Valencia, 2015, p. 666.

[38] Así, la SAP de Granada núm. 351/2014 (Sección 1ª), de 5 junio, ¸ revocó la sentencia de instancia y absolvió al menor que difundió mediante su móvil una foto que le había enviado una menor por *whatsapp* en la que se encontraba ésta desnuda, por considerarlo un supuesto atípico.

segunda fase – la primera fase sería la de la obtención de las imágenes - ya que el sujeto activo ha tenido acceso a esta intimidad por consentimiento de la víctima, quien, a su vez, ha consentido este conocimiento basándose en una relación de confianza, con la voluntad en cierto modo implícita de que el contenido no se difunda.[39]

Los elementos esenciales del delito son:

Sujeto pasivo: Es el titular del bien jurídico protegido, la persona cuyas imágenes de contenido reservado se difunden, revelan o ceden a terceros sin su consentimiento.

Sujeto activo: Es la persona que ha obtenido el contenido audiovisual, con consentimiento de la víctima, y que después lo difunde sin autorización de ésta. Se excluye de este delito a los terceros que no intervengan en la acción inicial pero que posteriormente reenvíen las imágenes. En estos casos, el ataque a la intimidad ya se ha consumado con la primera divulgación, las imágenes ya han perdido el carácter de secreto, por lo que no tendría sentido volver a castigar el atentado contra la intimidad por esta vía. Habría que analizar si tendrían cabida en la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen estas conductas.

Además, se configura como un delito especial, dado que no cualquiera puede cometerlo, sino quien haya obtenido las imágenes con permiso de la víctima; sin esta autorización, no hay conducta típica y, por consiguiente, no se ha cometido este delito.

Conducta típica: Consiste en la difusión, revelación o cesión de imágenes o grabaciones audiovisuales de la persona afectada a terceros sin tener autorización de aquélla, pero habiendo sido obtenidas las imágenes o grabaciones con su anuencia. Es decir, por un lado, es requisito que la obtención de las imágenes objeto del delito se haya producido anteriormente de forma lícita, pues de lo contrario se incurriría en otro delito diferente, y, por otro, se requiere que, posteriormente, estas imágenes se difundan o cedan sin autorización de la víctima. En la conducta típica existen tres elementos:

[39] OTERO GONZÁLEZ, P., "Delitos contra la intimidad, derecho a la propia imagen e inviolabilidad del domicilio" *op. cit.*, p. 375.

- Obtención de imágenes: Hay un aspecto claro al respecto y es que el titular de la intimidad debe haber accedido a que se graben dichas imágenes. Ahora bien, de la literalidad del texto legislativo no se desprende de manera clara cómo debe obtener las imágenes el sujeto activo. El artículo se refiere al "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"[40]. Ante la literalidad del precepto cabe plantearse lo siguiente: ¿Qué tiene que hacer el sujeto activo del delito? ¿Basta con que difunda? ¿O también es necesario que obtenga él las imágenes? Habría que discutir si resulta preciso que el sujeto sea el que obtenga el contenido audiovisual y si eso deja fuera los casos en los que sea la propia víctima quien haya captado las imágenes y las haya enviado a quien luego las difunde, como ocurre en el *sexting*[41].

  Autores como MORALES PRATS[42], entienden que este nuevo precepto penal da respuesta al debate que generó el polémico caso de Olvido Hormigos. Ésta había enviado por teléfono voluntariamente imágenes suyas a un amigo (*sexting*), quien sin su consentimiento las divulgó. No obstante, ¿realmente cabe subsumir esta conducta en el tipo penal del artículo 197.7 CP?

  El verbo *obtener* se puede interpretar como equivalente a captar, en cuyo caso, el sujeto activo sería el que tendría que tomar por sí mismo las imágenes en un lugar reservado. Si nos ceñimos a esta interpretación, los supuestos de *sexting* no se podrían incluir, porque en este caso, obtener con su anuencia en un domicilio implica que el sujeto activo grabe las imágenes bajo la autorización de la víctima en un lugar privado, no que sea la víctima la que las capte y luego las envíe. En esta línea, con la consiguiente exclusión de los supuestos de *sexting*, se ha pronunciado la AP de Barcelona exponiendo que:

[40] Artículo 197.1 CP
[41] Contracción de los términos *sex* (sexo) y *texting* (texto, mensaje); consiste en el envío, por la red o cualquier terminal telefónico, de imágenes o vídeos de contenido sexual con consentimiento, grabados y protagonizados por el propio emisor.
[42] MORALES PRATS, F., "La reforma de los delitos contra la intimidad artículo 197 CP" en QUINTERO OLIVARES, G., (dir.) *Comentario a la reforma penal de 2015*, Thomson Reuters Aranzadi, Madrid, 2015, p.462.

"Se trata de una conducta que sólo puede ser cometida por aquél que ha obtenido las imágenes o grabaciones audiovisuales con el consentimiento de la víctima. En apoyo de tal interpretación cabe añadir, además, que la redacción exige que las imágenes o grabaciones de la persona afectada se hubieran obtenido "en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros", lo que cierra la posibilidad de que la persona investigada, encausada o acusada hubiera "obtenido" la grabación mediante la recepción de las imágenes o grabaciones en lugar distinto del domicilio de la persona afectada. Y, siendo así, la única interpretación lógica es la que precisa de la captación de la imagen o grabación directamente por el sujeto activo del delito "con la anuencia" de la víctima."[43]

Sin embargo, el verbo *obtener* también se puede interpretar como sinónimo de conseguir o tener. Conforme a esta segunda interpretación no sería necesario que el sujeto activo captara las imágenes; basta con que posteriormente las hubiera conseguido u obtenido de algún modo. En ese caso, resultaría admisible que las imágenes las hubiera captado un tercero o la propia víctima, lo que permitiría incardinar en el tipo penal supuestos de *sexting* como el del caso Hormigos.[44]

El problema es que, si se sigue este segundo sentido del término, lo que no tiene sentido es que se exija que el sujeto activo haya obtenido/conseguido las imágenes en un lugar reservado. En este sentido, hay que tener en cuenta que el artículo dice "que hubiera obtenido con su anuencia en un domicilio". La cuestión es si ello implica que el sujeto activo debería encontrarse en un domicilio u otro lugar fuera del alcance de la mirada de terceros al recibirlas. En este caso y a modo de ejemplo, ¿no se subsumiría una situación en la que un sujeto recibe las imágenes íntimas que le envía su pareja mientras está en un bar con sus amigos? Parece que lo lógico sería entender que el lugar reservado hace referencia al de la grabación de las imágenes y no al de la recepción de las mismas, pero el texto legal resulta confuso al respecto. Dependiendo de la interpretación que se siga el caso de Olvido Hormigos entraría o no en el vigente tipo penal.

---

[43] SAP de Barcelona núm. 302/2017 (Sección 6ª), de 24 de abril, FJ 2.

[44] Esto era lo que pretendía el legislador. En este sentido, de acuerdo con lo expuesto en SAP de Barcelona núm. 302/2017 (Sección 6ª), de 24 de abril, FJ 2, con la incorporación de esta figura "se trataba, en definitiva, de abordar el fenómeno conocido como "sexting" a raíz de un suceso mediático ocurrido en el año 2012", haciendo alusión al citado caso Hormigos.

Con toda seguridad, el carácter confuso del artículo obedece a un fallo de redacción porque parece claro cuál era la pretensión del legislador al introducir este artículo y que ésta no era dejar fuera los casos de *sexting*. El Preámbulo de la Ley de reforma del CP que introdujo esta nueva figura establecía que "los supuestos a los que ahora se ofrece respuesta son aquellos otros en los que las imágenes o grabaciones de otra persona se obtienen con su consentimiento, pero son luego divulgados contra su voluntad, cuando la imagen o grabación se haya producido en un ámbito personal y su difusión, sin el consentimiento de la persona afectada, lesione gravemente su intimidad"[45]. Asimismo, RODRÍGUEZ FERNÁNDEZ, establece que "el legislador de 2015 ha tratado de incorporar al ámbito de punición las revelaciones o difusiones de materiales audiovisuales de índole sexual obtenidos a través de las prácticas de "privacidad compartida" que hoy día conocemos como *sexting*".[46]

El problema es que, por el principio de legalidad, la interpretación de un precepto no puede ir más allá de lo que permite su literalidad, bajo riesgo de incurrir en la analogía prohibida.[47] Por ello, se entiende que la redacción del artículo merece ser revisada y modificada a fin de aclarar la intención del legislador y los actos subsumibles en este delito.

- Lugar de la obtención: Tanto el domicilio como otro lugar fuera del alcance de la mirada de terceros. Este último término goza de cierta imprecisión pues, no aclara dónde está el límite del alcance de la mirada de terceros. Por ello, se precisaría analizar el contexto en cada caso concreto. Además, se entiende que para que el precepto se aplique, la grabación objeto del delito debe haberse llevado a efecto en un espacio de carácter reservado, lo que remarca el carácter

[45] Preámbulo de la 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.
[46] RODRÍGUEZ FERNÁNDEZ, I., *Tutela penal de la "privacidad compartida". Reflexiones sobre el nuevo tipo de difusión de grabaciones audiovisuales íntimas,* p. 11.
[47] Así se expone en SAP de Barcelona núm. 302/2017 (Sección 6ª), de 24 de abril, FJ 2, en relación con la interpretación del artículo 197.7 CP. En dicha sentencia se debate sobre el alcance de dicho precepto, atendiendo a la intención del legislador de sancionar determinadas conductas. La AP critica cómo, en ocasiones, la legislación pretende regular ciertas situaciones y que, a la hora de representarlas en palabras, no siempre éstas se adecuan a la imagen pretendida mental. De este modo, expone que "el principio de estricta legalidad impide sancionar las conductas que no se encuentren claramente contenidas en la descripción típica, pues de otro modo el tipo no desempeñaría función alguna de garantía".

íntimo de la misma.[48] Sin embargo, a tenor de lo expuesto en el propio artículo y según ya hemos comentado, el lugar fuera del alcance de terceros ¿hace referencia a la grabación de las imágenes? O, por el contrario, ¿se refiere a la obtención por parte del sujeto de dichas imágenes por recibirlas por mensaje u otro medio?

- Autorización del afectado: El único elemento que parece estar claro es que para que la conducta se encuadre dentro del delito tipificado en el artículo 197.7 CP se precisa que el afectado consienta que se tomen las imágenes pero que no autorice, ni tácita ni expresamente, su posterior difusión.

Objeto material: Lo constituyen las imágenes o grabaciones audiovisuales íntimas. Esto excluye del tipo las grabaciones de audio no acompañas de video e incluye las imágenes, tanto con sonido como sin él.

Resultado: Para que haya delito, la conducta debe menoscabar gravemente la intimidad personal de la víctima. Esto implica un resultado de lesión. De acuerdo con otros autores como OTERO GONZÁLEZ y COLÁS TURÉGANO, hay que interpretar esta exigencia de grave menoscabo a la intimidad de una manera restrictiva en base al principio de intervención mínima, de tal manera que se limite la incriminación penal a los ataques al "núcleo duro de la intimidad": ideología, creencias, salud, religión y vida sexual. De lo contrario, cualquier conducta, como una mera comida en el domicilio y su posterior divulgación, podría subsumirse en el tipo penal y esto parecería excesivo.[49]

5. ARTÍCULO 197 BIS CP

> Artículo 197 bis CP: 1. *El que, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.*

[48] Circular 3/2017, *op. cit.*
[49] OTERO GONZÁLEZ, P., "Delitos contra la intimidad, derecho a la propia imagen e inviolabilidad del domicilio" *op. cit.*, p. 378; y COLÁS TURÉGANO, A., "Nuevas conductas delictivas contra la intimidad (arts. 197; 197 bis; 197 ter)" *op. cit.,* p. 666

2. El que, mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

El primer problema que presenta este delito es el de su ubicación sistemática, especialmente atendiendo a que el bien jurídico protegido por los delitos que se encuentran en el mismo Título (Título X: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio) y Capítulo (Capítulo primero: Del descubrimiento y revelación de secretos) se considera que es la intimidad, mientras que el análisis del delito conduce a pensar que lo protegido a través de él es la seguridad informática. Esta cuestión se abordará infra en el apartado 5.2.

La conducta comúnmente conocida como *hacking* constituye el delito de intrusismo informático, un delito cuyo único medio de comisión es la red (delito informático en sentido propio).[50] Este delito fue introducido en el Código Penal por la LO 5/2010, encontrándose entonces en el artículo 197.3, junto con los demás delitos contra la intimidad en él tipificados. Tras la reforma de 2015, la figura pasa a recogerse en otro artículo, el artículo 197 bis CP. Por esta separación se entiende que con la LO 1/2015 el intrusismo informático se ha desligado del delito de descubrimiento y revelación de secretos en cuanto a ataque directo contra la intimidad personal, dándosele un tratamiento sistemático autónomo.[51]

Antes de comenzar con su estudio, hay que aclarar el concepto de *hacking*. Entendemos como *hacking "*la conducta de aquel sujeto que emplea su experiencia y conocimientos informáticos para quebrantar las medidas de seguridad de un sistema de información".[52] El *hacking* puede ser de dos tipos:

[50] SALVADORI, I., "Los nuevos delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5/2010. Perspectiva de derecho comparado" en *Anuario de Derecho Penal y Ciencias Penales,* vol. 64, 2011, p.223.
[51] Circular 3/2017 *op. cit.*
[52] COLÁS TURÉGANO, A., "El delito de intrusismo informático tras la reforma del CP español de 2015" en *Revista Boliviana de Derecho,* nº 21, 2016, p. 214.

- *Hacking* blanco: Cuando el propósito del hacker únicamente es acceder al sistema, sin intención de dañarlo, o bien, a la información que recoge, sin intención de usarla; se trata de la conducta del mero intrusismo[53]. Esta modalidad es la que se estudia en el presente trabajo.
- *Hacking* negro (*cracking*): En este caso el propósito por el que el *hacker* o *cracker* accede al sistema es causar cualquier tipo de daño al sistema, a sus datos o a su titular. Esta modalidad se subsume en el tipo de daños informáticos, previsto en el artículo 264 CP.

Además, existe un tercer tipo de conducta en relación con las anteriores, que se concreta en ataques a los sistemas informáticos, que se conoce como *data breaches* o violación de datos. Consiste en cualquier forma de destrucción, modificación o acceso a datos de particulares o empresas. Normalmente, esta violación de datos se realiza como método de espionaje informático. Dicha conducta se encuentra igualmente tipificada en el artículo 264 CP.

La respuesta penal antes de 2010 era la de no penalizar de una manera específica el *hacking* blanco, de tal manera que únicamente se castigaba el intrusismo informático si éste suponía un ataque contra la intimidad.[54] Para la consumación del delito se requería que el sujeto activo tuviera intención de descubrir los secretos o vulnerar la intimidad ajena. Así pues, la mera conducta de acceso y/o permanencia no autorizados a sistemas informáticos sólo era punible cuando había intención de interceptar telecomunicaciones, por la vía del artículo 197.1 CP, o cuando se llevaba a cabo por modificación, uso o

[53] SAP de Madrid núm. 329/2015 (Sección 2ª), de 27 de abril, FJ 3.

[54] Véase en el Auto de la AP de Barcelona (Sección 3ª) núm. 231/2009, de 6 abril, FJ 1, en relación con la conducta del acusado consistente en "acceder al lugar desde donde la denunciante recibía y enviaba sus correos electrónicos" para después enviar el denunciado otros mensajes. Dicho Auto establece que "su conducta podría encontrarse incardinada en el ámbito propio del art. 197.2 in fine del Código Penal" afirmando que "el simple acceso a datos reservados de carácter personal que se hallan registrados en ficheros o soportes informáticos, electrónicos o telemáticos ya es constitutivo de delito, aun cuando el sujeto activo no los altere o utilice". Con esto, concluía que "el art. 197.2 del Código Penal castiga el acceso a datos personales de otra persona que se encuentren registrados en ficheros o soportes informáticos, electrónicos o telemáticos, sin necesidad de que concurra ningún otro requisito adicional y es claro que la conducta denunciada por Eva presupone que alguien (el denunciado u otra persona todavía no identificada) ha tenido que acceder a su correo electrónico y ha tenido acceso al contenido de todos los correos que aquella tuviera guardados (tanto los enviados como los recibidos), por lo que, en este momento procesal no cabe afirmar de forma concluyente que los hechos denunciados no son constitutivos de delito, toda vez que podrían ser calificados como un delito de descubrimiento y revelación de secretos".

apoderamiento de datos de carácter personal o familiar, por la vía del artículo 197.2 CP.[55]

Posteriormente, siguiendo a COLÁS TURÉGANO[56], con la reforma de 2010 se tipifica el acceso ilegal a los sistemas de información protegidos por barreras de seguridad, cumpliendo con los compromisos internacionales contraídos por España para proteger a la sociedad frente a la ciberdelincuencia. Así, el artículo 197.3 CP, conforme a la redacción dada al mismo por la LO 5/2010, castigaba el acceso o mantenimiento "sin autorización" "vulnerando las medidas de seguridad" "a datos o programas informáticos contenidos en un sistema informático". De acuerdo con la mayoría de la doctrina, que pone en relación este tipo penal con el de allanamiento de morada, la conducta consistente en mantenerse en el sistema abarca los supuestos en los que el acceso ha sido lícito y la conducta se vuelve ilícita tras el requerimiento de abandono del sistema.

Finalmente, con la reforma de 2015, que incorporaba las nuevas exigencias de la Directiva 2013/40/UE, se producen una serie de cambios en relación con este delito, conformándolo tal y como lo encontramos hoy en día. Se mantienen los requisitos típicos de actuar "sin autorización" y "vulnerando las medidas de seguridad". También, se mantienen las conductas típicas de acceder y mantener, pero se incorpora una nueva conducta típica que hace referencia a los actos de colaboración, pues se tipifican aquellos supuestos en los que se facilite el acceso al sistema a un tercero.

Otro cambio relevante frente a la anterior redacción que exigía el acceso efectivo a datos o programas contenidos dentro del sistema informático[57], consiste en que, con la nueva redacción, únicamente se exige el acceso al sistema informático, sin necesidad de acceder a la información personal recogida en datos o programas concretos. Es decir, las conductas típicas pueden proyectarse sobre el conjunto o parte de un sistema de información, en lugar de proyectarse sobre datos o programas contenidos en el mismo.

[55] SÁNCHEZ BERCEDO, M., *El delito de intrusismo informático o Hacking. Artículo 197.3 CP*, p. 5
[56] COLÁS TURÉGANO, A., "Nuevas conductas delictivas contra la intimidad (arts. 197; 197 bis; 197 ter)" *op. cit.*, p. 671-678.
[57] La redacción tras la reforma de 2010 del art. 197.3 CP hablaba de "datos o programas informáticos contenidos en un sistema informático o en parte del mismo".

En relación con esta cuestión, consideramos que hay dos conceptos que es importante diferenciar a fin de analizar en profundidad el delito. Se trata de los conceptos "sistemas de información" y "datos informáticos":

- Sistema de información: "Todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automatizado de datos informáticos, así como los datos informáticos almacenados, tratados o recuperados o trasmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento".[58]
- Datos informáticos: "Toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice su función".[59]

5.1. Elementos del delito

5.1.1. Artículo 197 Bis 1 CP

Sujeto activo: Se trata de un delito común, por cuanto lo puede cometer cualquier persona, "sujeto activo genérico"[60]; no obstante, lo más probable será que se trate de personas con conocimientos informáticos.

Sujeto pasivo: El titular del sistema informático.

Conducta típica: La propia literalidad del artículo se refiere expresamente a tres conductas típicas: acceder, facilitar a otro el acceso y mantenerse en el sistema informático, bajo los requisitos de actuar sin autorización y vulnerando las medidas de seguridad que impiden el acceso a terceros.

Siguiendo a COLÁS TURÉGANO[61], desde un primer momento, la doctrina, por lo general, ha interpretado que el acceso a sistemas no protegidos es un caso atípico, por requerirse

[58] Directiva 2013/40/UE art.2.a
[59] Directiva 2013/40/UE art.2.b
[60] STS núm. 230/2017 (Sala de lo Penal, Sección 1ª), de 4 abril, FJ 6.

en el tipo la "vulneración" de las medidas de seguridad y no ser necesario en estos casos. Sin embargo, hubo mayor controversia en relación con la conducta típica de mantenerse en el sistema, sobre si era necesario o no que el acceso hubiera sido lícito en esos casos. La cuestión que se debate es si la exigencia de que la conducta se lleve a cabo sin autorización y vulnerando las medidas del sistema se refiere únicamente a las dos primeras conductas típicas – acceso y facilitación de acceso- o también a la tercera –mantenimiento en el sistema-. Como ya se ha adelantado, la mayoría de la doctrina defiende que los supuestos que se recogen son aquellos en los que se accede lícitamente, volviéndose la conducta ilícita cuando se requiere al sujeto que abandone el sistema y este no lo hace.[62] Parece lógico que se sostenga esta idea de que para el mantenimiento no es necesario un acceso ilícito mediante vulneración de medidas de seguridad, sino el mantenimiento en contra de la voluntad del titular del legítimo derecho a excluirlo. De este modo, el precepto parece establecer distintos requisitos para las dos primeras conductas típicas, por un lado, y para la tercera, por otro.

Por otro lado, la tipificación de la facilitación del acceso constituye una de las novedades introducidas por la LO 1/2015, como se ha mencionado anteriormente. De este modo, todo aquel que posibilite o ayude a un tercero a acceder a un sistema informático estaría cometiendo el delito, algo que para numerosos autores resulta criticable[63]. En este sentido, se critica la equiparación a nivel punitivo y de autoría de lo que materialmente sería una mera conducta de participación en el delito (cooperación necesaria o, incluso, complicidad) algo que parece ser desproporcionado si se atiende al daño que producen ambos sujetos.[64]

En conclusión, existen tres conductas típicas, acceder al sistema, mantenerse en él y facilitar el acceso, y se exige que se cumplan ciertos requisitos. En el caso de acceso y facilitación a terceros, se exige que se produzca una vulneración de las medidas de seguridad, además de que la acción se produzca sin autorización, mientras que, en el

---

[61]COLÁS TURÉGANO, A., "El delito de intrusismo informático tras la reforma del CP español de 2015" *op. cit.,* p.218.

[62]En este sentido, se aprecian similitudes con la conducta típica del delito de allanamiento de morada.

[63] Véase JORGE BARREIRO, A., "Delitos contra la intimidad, derecho a la propia imagen e inviolabilidad del domicilio" *op. cit*., p. 1041, y COLÁS TURÉGANO, A., "El delito de intrusismo informático tras la reforma del CP español de 2015" *op. cit.,* p. 219.

[64] JORGE BARREIRO, A., "Delitos contra la intimidad, derecho a la propia imagen e inviolabilidad del domicilio" *op. cit.,* p. 1040.

caso de mantenimiento, parece lógico entender que no es necesario un acceso ilícito vulnerando las medidas de seguridad, sino que basta que el mantenimiento se haga en contra de la voluntad del titular del legítimo derecho a excluir el mismo. Hay, por tanto, un requisito común en ambos casos: la falta de autorización por parte del titular del legítimo derecho frente al sistema.

Consecuentemente, se puede afirmar que el mero acceso sin autorización a un sistema informático ajeno constituye una conducta típica, lo que proporciona mayor protección penal para casos en los que antes había que atender a la finalidad o motivo de la conducta.[65] Ahora, el acceso puede estar motivado por numerosas razones, desde un juego o simple curiosidad, a motivaciones con mayor peso como espiar o averiguar información relevante.[66] En contraste con esto, antes de la reforma de 2010, tanto doctrina como jurisprudencia consideraban que las conductas típicas debían ir acompañadas de la finalidad de descubrir secretos o vulnerar la intimidad de otro para que se cometiera tal delito[67].

Asimismo, el delito consiste simplemente en la irrupción en programas y sistemas informáticos protegidos, sin la necesidad de que se usen ilícitamente los datos o la información hallada[68] o se acceda al contenido de los mismos.

Objeto material: Como se exponía anteriormente, se ha producido un cambio respecto al objeto material del delito de intrusismo informático. Tras la nueva redacción, basta con el acceso al sistema informático, sin necesidad de que el mismo se proyecte sobre datos o programas informáticos contenidos en él. Esa modificación es un indicio de que tal vez, el bien jurídico protegido en este delito sea la seguridad jurídica en lugar de la intimidad, como se verá a continuación.

---

[65] Rius Alonso, P., "La nueva regulación penal de los delitos relativos a la intromisión en la intimidad y descubrimiento y revelación de secretos." *Enatic Abogacía Digital, Blog.*

[66] SIEBER, U., *The lnternational Handbook on Computer Crime,* John Wiley and Sons, Chichester, 1986, [non vidi, citado en GUTIERREZ FRANCÉS, M., "El intrusismo informático (Hacking): ¿Represión Penal Autónoma?" *Informática y derecho: Revista iberoamericana de derecho informático*, n.º 12-15, 1996, p. 1165].

[67] Véase como ejemplo de esta situación en STS núm. 358/2007, de 30 abril, FJ 1 "interesa resaltar que el tipo objetivo requiere solamente un acto de apoderamiento, sin necesidad de que el autor llegue a descubrir los secretos o a vulnerar la intimidad en el primer caso, y el mero acceso a los datos protegidos en el segundo. El tipo subjetivo exige, sin embargo, aquella finalidad, junto con el dolo en el acto de apoderamiento o de acceso."

[68] SÁNCHEZ BERCEDO, M., *El delito de intrusismo informático o Hacking. Artículo 197.3 CP*, *op. cit.,* p. 3.

5.1.2. Artículo 197 Bis 2 CP

Hay que señalar las diferencias con el artículo 197.2 CP, donde se castiga la conducta de interceptación de comunicaciones para descubrir los secretos o vulnerar la intimidad del otro. Parece claro que la diferencia que se observar es que en el artículo 197.2 CP se pretende proteger la lesión de la intimidad, mientras que con la conducta que se comenta no se pretende afectar a la intimidad de la persona. Se recogen, por tanto, aquellos casos en los que tiene lugar una intromisión ilícita en una transmisión de datos informáticos, siempre que no se haga en términos de comunicación privada y no se pretenda descubrir secretos o vulnerar la intimidad de otro, puesto que entonces estaríamos ante el supuesto regulado en el artículo 197.2 CP.[69]

Tanto el sujeto activo como el sujeto pasivo son los mismos que en el apartado anterior, por lo que a continuación se expondrá brevemente en qué consiste la conducta típica, a fin de poder tener una visión general de los dos apartados del artículo 197 bis. La conducta que regula este apartado es la de utilización de artificios o instrumentos técnicos para interceptar sin autorización transmisiones no públicas de datos informáticos.

5.2. Bien jurídico protegido: Intimidad Vs. Seguridad Informática

En contra de lo que suele ser habitual, se aborda al final la cuestión del bien jurídico protegido, después del análisis del artículo, porque es ahora cuando nos encontramos en mejor disposición para pronunciarnos sobre la cuestión, máxime teniendo en cuenta que el de la determinación del bien jurídico protegido constituye uno de los aspectos más controvertidos que plantea este delito desde su introducción en el CP. La doctrina se encuentra dividida; hay quienes consideran que principalmente por su ubicación y otros motivos que se comentarán en el presente epígrafe, se trata de un delito que protege la intimidad, mientras que otros autores consideran que la ubicación sistemática del delito es errónea y que lo que tutela el artículo es la seguridad informática.

[69] COLÁS TURÉGANO, A., "Nuevas conductas delictivas contra la intimidad (arts. 197; 197 bis; 197 ter)" *op. cit*., p. 679.

Para analizar el bien jurídico protegido por el artículo 197 bis CP, parece oportuno partir de la base de su ubicación en la Ley. Dicho artículo se encuentra en el Capítulo primero: Del descubrimiento y revelación de secretos, dentro del Título X: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. De su ubicación sistemática cabría entender que se trata de un delito que protege la intimidad, pues es el bien jurídico que se tutela en el mismo Capítulo. Como se exponía anteriormente, la intimidad se entiende y se tutela en un doble sentido. Por un lado, en un sentido negativo se entiende la intimidad como espacio privado y personal, y así se considera en el artículo 197.1 CP. Por otro lado, se interpreta en un sentido positivo, la intimidad recogida en ficheros o archivos, entendida como intimidad informática. Esta vertiente hace referencia a la autodeterminación informativa, es decir, el derecho de cada individuo a decidir qué datos personales comparte, cuándo, etc. A la protección de esta vertiente de la intimidad responde el artículo 197.2 CP.

Si se tiene en cuenta que los demás artículos del Capítulo contienen tipos penales destinados a salvaguardar la intimidad, la idea de "domicilio informático", entendido como esfera de privacidad y secretos integrada en un sistema informático protegido, la idea de "morada informática" o lugar íntimo o privado en el ámbito de la informática, permitiría afirmar que en este delito también se está protegiendo la intimidad, y, en consecuencia, permitiría mantener la coherencia del Capítulo y del Título.

En este sentido, autores como MORALES GARCÍA[70] defienden que lo que se busca proteger con este precepto es la información contenida en los espacios informáticos, que hacen el papel de "domicilio informático". Estos espacios constituyen una "reserva de dicho espacio en términos de intimidad", por lo que, para el autor, la tutela en este artículo va dirigida hacia la intimidad informática. También, es partidario de esta postura BOLEA BARDÓN[71], quien opina que se ha producido un adelantamiento de las barreras protectoras del derecho a la intimidad, porque la intromisión en un sistema informático pone en peligro la privacidad del titular del mismo. Para el autor, el

[70] MORALES GARCÍA, O., "Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas", en *La reforma penal de 2010: análisis y comentarios* (dir. QUINTERO OLIVARES, G.) Aranzadi, Cizur Menor, 2010, p. 185 [*non vidi*, citado en COLÁS TURÉGANO, A., "Nuevas conductas delictivas contra la intimidad (Arts. 197; 197 Bis; 197 Ter), *op. cit.,* p. 672].

[71] Bolea Bardón, C., *Comentarios al código penal. Reforma LO 5/2010* (dir. Cordoy Bidasolo, M., Mir Puig, S.), Tirant lo Blanch, Valencia, 2011, p. 468 [*non vidi*, citado en COLÁS TURÉGANO, A., "Nuevas conductas delictivas contra la intimidad (Arts. 197; 197 Bis; 197 Ter), *op. cit.,* p. 672].

adelantamiento de la barrera supone, aun así, una protección a la intimidad luego es este el bien jurídico protegido mediante esta figura.[72]

En términos similares, pero con cierta conexión con la otra postura doctrinal, podemos citar a MATELLANES RODRÍGUEZ[73], quien considera que en este artículo se tutela la intimidad personal, pero, a su vez, añadiendo que los sistemas informáticos pueden ser de uso exclusivamente personal o particular, de uso público, o de uso no privado pero restringido, entiende que, en el caso de que los datos estén recogidos en sistemas informáticos "no personales", la ubicación resulta desafortunada.

El otro punto de vista, donde se sitúa la mayor parte de la doctrina, defiende que la ubicación sistemática del delito de *hacking* es errónea y, que lo que esta figura trata de proteger es el mero acceso a sistemas informáticos protegidos, tanto si contienen datos de carácter reservado, como si no. Esto es, considera que el bien jurídico protegido mediante esta figura es la seguridad de los sistemas informáticos. Desde esta postura se entiende que si el bien jurídico que se pretende proteger fuese la privacidad en el ámbito de la informática, se excluirían los supuestos en los que se accede ilícitamente a sistemas informáticos públicos, donde los datos o la información recogida no se puede calificar como datos de carácter íntimo. Por ello, este sector de la doctrina afirma que el bien jurídico que se tutela es la seguridad informática en sí misma, y que ésta, indirectamente, integra la protección de la intimidad personal en el ámbito informático.[74] Así lo afirma MORALES PRATS[75], quien entiende que el delito de intrusismo informático tutela la seguridad de los sistemas informáticos pero que, como fin último, lo que pretende es tutelar la intimidad informática (*privacy*) de las personas.

---

[72] Véase SAP de Madrid núm. 895/2017 (Sección 7ª), de 27 de noviembre, FJ 1, que, en línea con este punto de vista, en relación con el bien jurídico tutelado en el artículo 197 bis CP expone que "cabe defender que la incriminación de esta conducta supone un adelantamiento de las barreras de protección de la intimidad que parte de la consideración de que la mera intromisión informática pone en peligro la privacidad del titular del sistema. Esta interpretación además de atender a la ubicación sistemática del precepto y ser respetuosa con el principio de lesividad, viene refrendada por el propio preámbulo de la Ley Orgánica 1/2015 que distingue entre "datos que afectan tan directamente a la intimidad personal" y "otros datos o informaciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal"."

[73] MATELLANES RODRÍGUEZ, N., "Vías para la tipificación del acceso ilegal a los sistemas informáticos (y II)" en *Revista Penal*, n. º 23, 2009, pp. 53-62.

[74] JORGE BARREIRO, A., "Delitos contra la intimidad, derecho a la propia imagen e inviolabilidad del domicilio" *op. cit.,* p. 1043.

[75] Citado en obras como MATELLANES RODRÍGUEZ, N., "Vías para la tipificación del acceso ilegal a los sistemas informáticos (y II)" *op. cit.* p. 61 y COLÁS TURÉGANO, A., "Nuevas conductas delictivas contra la intimidad (Arts. 197; 197 Bis; 197 Ter), *op. cit.,* p. 672.

En esta dirección ANARTE/DOVAL[76], partidarios de que la seguridad de los sistemas informáticos es el bien jurídico protegido por este precepto, consideran que se trata de un objeto al que le falta contenido y que por ello habría que conectarlo con la intimidad, entendiendo que el intrusismo informático se trata de un delito de peligro abstracto para la intimidad.

Sin embargo, cabe destacar cómo, partiendo desde el mismo punto de vista doctrinal, GUTIÉRREZ FRANCÉS[77] exponía en su obra (en 1996) que con todos los avances tecnológicos estaba teniendo lugar el "nacimiento de algún nuevo bien jurídico en este ámbito (…) cuya protección penal es demandada de forma creciente". La autora entendía que accediendo a un sistema informático se puede afectar tanto a la intimidad personal de un individuo, constituyendo entonces una agresión contra el interés del titular particular (protección del titular de la información), como también se puede estar accediendo a sistemas o equipos particularmente relevantes por la información "sensible" que contienen, afectando a un interés, no individual sino colectivo, denominado "seguridad informática". Esta idea la sostiene también RODRÍGUEZ FERNÁNDEZ[78], al considerar que se trata de un bien jurídico nuevo, identificado con la seguridad y fiabilidad de los sistemas informáticos. Apunta que entre las conductas que se pueden enmarcar en el precepto establecido en el artículo 197 bis CP, cabe incluir casos de acceso ilícito que no afectan a la intimidad de las personas, como detectar ondas electromagnéticas de una comunicación electrónica (artículo 197 bis.2 CP).

Por tanto, a pesar de la ubicación sistemática del precepto, Título X del Código Penal, entre los "delitos contra la intimidad, la propia imagen y la inviolabilidad del domicilio y de la intimidad", se puede afirmar que aquel no tutela única y exclusivamente el interés formal del legítimo titular de la privacidad de los datos o programas informáticos contenidos dentro de un sistema, sino que, más bien, "la disposición protege el poder del titular del derecho a excluir a terceros de disponer de manera exclusiva de sus datos

[76] ANARTE BORRALLO, E., DOVAL PAÍS, A., *Derecho penal. Parte especial. Vol. I. La protección penal de los intereses jurídicos personales* (dir. Boix Reig. J.), Iustel, Madrid, 2010, pp. 455-456 [*non vidi,* citados en COLÁS TURÉGANO, A., "El delito de intrusismo informático tras la reforma del CP español de 2015", *op. cit.,* p. 217].
[77] GUTIÉRREZ FRANCÉS, M., "El intrusismo informático (Hacking): ¿represión penal autónoma?" *op. cit.,* pág. 1182-1183.
[78] RODRÍGUEZ FERNÁNDEZ, I., *Tutela penal de la "privacidad compartida". Reflexiones sobre el nuevo tipo de difusión de grabaciones audiovisuales íntimas.* p. 17.

y programas informáticos, independientemente de su contenido (secreto o reservado) o de su valor económico".[79]

En resumen, el primer punto de vista supone aceptar que el bien jurídico protegido mediante el delito de *hacking* es la intimidad, tutelada bien directa, o bien indirectamente. En este último caso se hace referencia a la posibilidad de que el sistema informático al que se accede ilícitamente contiene datos informáticos que forman parte de la intimidad de una persona. Así, castigando esta conducta, se estaría protegiendo indirectamente la intimidad. Este punto de vista lo que supone es entender que, en todo caso, acceder a un sistema informático implica atacar a la intimidad de una persona. Finalmente, el segundo punto de vista defiende que el bien jurídico protegido mediante este delito es la seguridad de los sistemas informáticos, independientemente de la intimidad, de tal manera que se conforma como un delito de peligro abstracto. Así, lo que se protege la seguridad del sistema, independientemente del contenido del mismo, constituyendo el delito tipificado el mero acceso a dicho sistema.

Con todo ello podemos concluir, en primer lugar, que no tendría sentido afirmar que este delito protege la intimidad personal, por no abarcar este bien jurídico todos los supuestos que cabe enmarcar en la conducta tipificada. Más bien, la regulación de esta figura protege la seguridad de los sistemas informáticos, que, con los avances rápidos de las tecnologías de la información y la comunicación, están cobrando cada vez un mayor protagonismo en nuestra sociedad y manejan mayor cantidad de datos informatizados de todo tipo, tanto de carácter reservado como no reservado.

Además, cabe añadir que proteger el ámbito de seguridad de redes y los sistemas informáticos es una exigencia a nivel internacional[80]. Hay que valorar la magnitud o dimensión alcanzada por Internet, que se ha convertido en uno de los grandes protagonistas de nuestra sociedad, la extensión de las redes de datos, en las que los particulares no sólo consumen el contenido que en ellas se encuentra, sino que también

[79] SALVADORI, I., "Los nuevos delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5/2010. Perspectiva de derecho comparado", *op. cit.,* p. 235.

[80] Véase a modo de ejemplo, el Convenio de Budapest sobre Ciberdelincuencia, de 23 de noviembre de 2001, que establece en el preámbulo que "es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos". De aquí se puede deducir, por tanto, que la necesidad es de proteger, no sólo los datos informáticos, sino también los sistemas informáticos y las redes.

lo crean, provocando una masificación de la creación de contenido informático, y el elevado número de personas que participan e interactúan a través de la red. Teniendo en cuenta esto, no parece atrevido defender que el ámbito informático o de Internet merece específica tutela jurídica.

De esta forma, aparecería y se tutelaría el bien jurídico de la seguridad de los sistemas informáticos como un bien jurídico autónomo. Por el carácter abstracto de este bien jurídico, el *hacking*, como mera conducta de acceso a un sistema informático vulnerando las medidas de seguridad y sin autorización alguno, independientemente del contenido que en él se encuentre, se trata de un delito de peligro abstracto.[81]

En conclusión, hay que tener en cuenta, por un lado, la exigencia y necesidad internacional de proteger frente a los atentados contra los sistemas informáticos, cada vez más usuales, tal y como se refleja en los acuerdos y convenios internacionales. Los avances tecnológicos están alcanzando una magnitud que propicia la aparición de este nuevo bien jurídico – la seguridad de los sistemas informático -, por la cantidad de información que manejan. Por otro lado, atendiendo a la distinción entre sistema informático y datos informáticos, existe un amplio abanico de situaciones que cabe enmarcar en la conducta tipificada en el artículo 197 bis CP. Esto es así porque, se puede acceder a sistemas informáticos sin necesidad de acceder a los datos recogidos en los mismos, o bien, accediendo a los datos que se guardan en dichos sistemas, puede resultar que los datos no sean de carácter íntimo o reservado. Es decir, no toda conducta de *hacking* va a resultar un ataque directo o indirecto contra la intimidad.

Mediante el adelantamiento de la barrera de protección penal se tutela la seguridad de los sistemas informáticos, que, en su caso, protege indirectamente los datos que en ellos se recogen y la intimidad. Por ello, cabe afirmar que el bien jurídico protegido con la tipificación del delito de intrusismo informático, *hacking,* es la seguridad de los sistemas informáticos. En consecuencia, hay que concluir que sería recomendable estudiar la conveniencia de introducir en el Código Penal un Título o Capítulo específico destinado a la protección de la seguridad de los sistemas informáticos.

[81] JORGE BARREIRO, A., "Delitos contra la intimidad, derecho a la propia imagen e inviolabilidad del domicilio" *op. cit*., p.1043

6. CONCLUSIONES

El presente trabajo ha pretendido estudiar la protección penal del bien jurídico intimidad, tras los cambios producidos en el Código Penal con la reforma de 2015, haciendo especial referencia a las nuevas tecnologías, por entender que han sido uno de los principales motores de los cambios producidos. En este contexto, se ha dedicado mayor atención a los delitos recogidos en los artículos 197.7 y 197 bis CP, por considerar que se trata de las figuras más novedosas y que plantean mayores problemas interpretativos. Así, mediante el estudio del tema, se ha llegado a las siguientes conclusiones:

El bien jurídico intimidad debe interpretarse en un doble sentido: positivo y negativo. Por un lado, la vertiente negativa del mismo supone el derecho a estar libre de intromisiones ilegítimas de terceros en el ámbito personal. Con esta vertiente lo que se protege es el espacio privado de cada individuo de la intromisión de terceros; cada uno es dueño y libre de elegir a quién hace partícipe de su intimidad, de ese ámbito personal e individual, y a quién no. En definitiva, la intimidad en su sentido negativo consiste en la prohibición de interferencias externas en el ámbito íntimo y personal de las personas, salvo que éstas decidan lo contrario.

Por otro lado, la vertiente positiva de la intimidad supone el derecho a la autodeterminación informativa, lo que implica que cada individuo tiene derecho a decidir qué datos referentes a él, cómo, cuándo, dónde… pueden ser obtenidos y tratados por otros. Esto supone, por tanto, el poder de control de los datos personales de cada uno, el poder de decisión sobre la información personal de cada uno.

De este modo, estas dos vertientes constituyen una completa interpretación del bien jurídico intimidad, en todos sus sentidos. Así se recoge en la Constitución Española, en cuyo artículo 18 apartados 1 y 4 se reconoce el derecho a la intimidad en su sentido negativo y positivo, respectivamente.

El Capítulo I del Título X del Código Penal contiene diferentes tipos penales a través de los cuales se tutela la intimidad en sus dos vertientes. En los apartados 1 y 2 del artículo 197 CP se tutela la intimidad personal (vertiente negativa) y la intimidad informática

(vertiente positiva), respectivamente. El artículo 197 bis constituye el tercer tipo básico de los delitos recogidos en ese Capítulo, tipificando el delito de intrusismo informático. Los demás artículos constituyen los tipos agravados de dichas conductas básicas, salvo el artículo 201, que regula la perseguibilidad de estos delitos.

El desarrollo de las nuevas tecnologías ha supuesto el surgimiento de nuevos ámbitos de riesgo para la intimidad en sus diferentes facetas, lo que ha dado lugar a la introducción de nuevos tipos penales. Entre estos destacan los recogidos en los artículos 197.7 y 197 bis CP, que han generado controversia.

El nuevo apartado 7 del artículo 197 surgió con la pretensión de dar respuesta penal a supuestos en los que las imágenes o grabaciones difundidas ilícitamente de una persona hubieran sido obtenidos por el sujeto activo del delito con consentimiento de la víctima, sirviendo como ejemplo los supuestos de *sexting*, en los que el sujeto activo ha recibido imágenes íntimas de la víctima por mensaje. Sin embargo, a tenor de la literalidad del texto legal, no se puede asegurar que realmente estas conductas se puedan subsumir bajo este tipo. Por el principio de legalidad, no se puede interpretar un precepto más allá de su literalidad. Así pues, a fin de esclarecer la intención del legislador, se propone revisar el precepto y mejorar su redacción.

El artículo 197 bis se encuentra destinado a castigar las conductas de acceso o de facilitación a terceros del acceso a un sistema informático vulnerando las medidas de seguridad, o de mantenimiento en un sistema informático protegido contra la voluntad del legítimo titular del derecho a excluirlo. Se penaliza la mera conducta de acceso o mantenimiento en un sistema informático, independientemente de la voluntad del sujeto activo. Se trata, en definitiva, del delito de intrusismo informático (*hacking)*.

A pesar de su ubicación en el Título referido a los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio resulta discutible que el bien jurídico protegido sea la intimidad. Se puede considerar que el objeto de salvaguarda del delito de *hacking* es la seguridad de los sistemas informáticos, constituyendo así un delito de peligro abstracto.

Hay que tener en cuenta que un sistema informático abarca datos y programas que no necesariamente son personales y por tanto íntimos de una persona en concreto (baste como ejemplo, el sistema informático del Canal de Isabel II). Existe una gran variedad de posibilidades en las que estemos ante un sistema informático protegido mediante medidas de seguridad susceptible de ser vulnerado y no estar, necesariamente, ante un peligro contra la intimidad personal.

Asimismo, no podemos menospreciar la situación actual en la que vivimos, una sociedad de la información en la que, prácticamente todo lo que sucede en nuestro alrededor, está informatizado. Con toda firmeza se puede afirmar que la informática está alcanzando una elevadísima extensión, se está expandiendo a numerosos ámbitos hasta el punto de que se ha convertido en una necesidad internacional el "proteger las redes y los sistemas".

Considerando estos dos factores - el abanico de situaciones enmarcables en la conducta de "acceso a un sistema informático vulnerando las medidas de seguridad y sin autorización" y el gran alcance de las redes y la informática – se puede asegurar que estamos ante el nacimiento de un nuevo bien jurídico, de peligro abstracto, y que, por tanto, es recomendable incorporar un Título o Capítulo específico en el Código Penal destinado a la protección de la seguridad de los sistemas informáticos.

7. BIBLIOGRAFÍA

DOCTRINA

COLÁS TURÉGANO, A. "El delito de intrusismo informático tras la reforma del CP español de 2015" en *Revista Boliviana de Derecho,* nº. 21, 2016, pp.210-229.

COLÁS TURÉGANO, A., "Nuevas conductas delictivas contra la intimidad (arts. 197; 197 bis; 197 ter)" en MATALLIN EVANGELIO, A., y GÓRRIZ ROYO, E. (coord.), GONZÁLEZ CUSSAL, J. (dir.), *Comentarios a la reforma del Código Penal de 2015*, Tirant Lo Blanch Reformas, Valencia, 2015, pp. 663-683.

ELVIRA PERALES, A., "Sinopsis artículo 18" (Disponible en: http://www.congreso.es/consti/constitucion/indice/imprimir/sinopsis_pr.jsp?art=18&tipo=2; última consulta 10/02/2018)

FAYOS GARDÓ, A., *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Dykinson, Madrid, 2015. (Disponible en: https://books.google.es/books?id=hTQkBwAAQBAJ&pg=PA127&lpg=PA127&dq=nucleo+duro+de+la+privacidad+jurisprudencia&source=bl&ots=AUDVEetQ_n&sig=gy9YP5ZzYDBo-q8pOK09dJEghOg&hl=es&sa=X&ved=0ahUKEwicrKPHo_TZAhUDRhQKHbeBCzAQ6AEIVTAG#v=onepage&q=nucleo%20duro%20de%20la%20privacidad%20jurisprudencia&f=false; última consulta: 01/03/2018)

FAYOS GARDÓ, A., *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Dykinson, Madrid, 2015 p. 127.

GUTIÉRREZ FRANCÉS, M., "El intrusismo informático (Hacking): ¿represión penal autónoma?" *Informática y derecho: Revista iberoamericana de derecho informático,* n. º 12-15, 1996, pp. 1163 – 1184.

JORGE BARREIRO, A., "Delitos contra la intimidad, derecho a la propia imagen e inviolabilidad del domicilio" (Actualizado por GUÉREZ TRICARICO, P) en MOLINA

FERNÁNDEZ, F. (coord.), *Memento Práctico Penal*, Francis Lefebvre, Madrid, 2016, p. 1029-1057.

MARTÍNEZ DE PISÓN, J. "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional" en MINISTERIOS DE JUSTICIA, BOLETÍN OFICIAL DEL ESTADO, BOE Y SOCIEDAD ESPAÑOLA DE FILOSOFÍA JURÍDICA Y POLÍTICA (ed.), *Anuario de Filosofía del Derecho*, Ministerio de Justicia y la Agencia Estatal Boletín Oficial del Estado, 2016, pp. 409-430.

MATELLANES RODRÍGUEZ, N., "Vías para la tipificación del acceso ilegal a los sistemas informáticos (y II)" en *Revista Penal*, n. º 23, 2009 pp. 52-72. Disponible en: http://rabida.uhu.es/dspace/bitstream/handle/10272/11936/Vías.pdf?sequence=2; última consulta 20/03/2018)

MORALES PRATS, F., "La reforma de los delitos contra la intimidad artículo 197 CP" en Quintero Olivares, G., (dir.) *Comentario a la reforma penal de 2015*, Thomson Reuters Aranzadi, Madrid, 2015, p.462

OTERO GONZÁLEZ, P., "Delitos contra la intimidad, derecho a la propia imagen e inviolabilidad del domicilio" en ORTIZ DE URBINA GIMENO, I. y AYALA GÓMEZ, I. (coord.), *Memento Práctico. Penal Económico y de la Empresa*, Francis Lefebvre, Madrid, 2016-2017, pp. 357-387.

Rius Alonso, P. "La nueva regulación penal de los delitos relativos a la intromisión en la intimidad y descubrimiento y revelación de secretos." *Enatic Abogacía Digital, Blog.* (Disponible en*:* www.enatic.org/la-nueva-regulacion-penal-de-los-delitos-relativos-a-la-intromision-en-la-intimidad-y-descubrimiento-y-revelacion-de-secretos/; última consulta: 25/03/2018)

RODRÍGUEZ FERNÁNDEZ, I. *Tutela penal de la "privacidad compartida". Reflexiones sobre el nuevo tipo de difusión de grabaciones audiovisuales íntimas*. Disponible en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20escrita%20Rodriguez_Fernandez.pdf?idFile=cbf06fcf-788e-4ff9-a47d-759b4ca71b8e; última consulta: 16/03/2018)

SALVADORI, I., "Los nuevos delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5/2010. Perspectiva de derecho comparado" en *Anuario de Derecho Penal y Ciencias Penales,* vol. 64, 2011. Disponible en: https://www.boe.es/publicaciones/anuarios_derecho/abrir_pdf.php?id=ANU-P-2011-10022100252_ANUARIO_DE_DERECHO_PENAL_Y_CIENCIAS_PENALES_Los_nuevos_delitos_inform%E1ticos_introducidos_en_el_C%F3digo_Penal_espa%F1ol_con_la_Ley_Org%E1nica_5/2010._Perspectiva_de_derecho_comparado; última consulta: 04/04/2018)

SÁNCHEZ BERCEDO, M. *El delito de intrusismo informático o Hacking. Artículo 197.3 CP*.

WARREN, S. Y BRANDEIS, L. "Right to Privacy" *Harvard Law Review*, The Harvard Law Review Association, Vol. 4, No. 5, 1890, pp. 193-220. (Disponible en: http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C; última consulta: 07/02/2018)

LEGISLACIÓN

Circular 3/2017, sobre la reforma del código penal operada por la LO 1/2015 de 30 de marzo en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos.

Constitución Española.

Convenio de Budapest sobre Ciberdelincuencia, de 23 de noviembre de 2001.

Declaración Universal de Derechos Humanos de 1948.

Directiva 2013/40/UE.

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.

Pacto Internacional de Derechos Civiles y Políticos de 1966

JURISPRUDENCIA

Auto de la AP de Barcelona (Sección 3ª) núm. 231/2009, de 6 abril, FJ 1.

Auto de la AP de La Rioja núm. 171/2017 (Sección 1ª), de 19 de mayo, FJ 2.

Auto de la AP de Madrid (Sección 30ª) núm. 286/2017, de 29 marzo, FJ 3.

Auto del TS (Sala de lo Penal, Sección 1ª) núm. 199/2018, de 18 enero, FJ 1.

SAP de Barcelona núm. 302/2017 (Sección 6ª), de 24 de abril, FJ 2.

SAP de Barcelona núm. 742/2017 (Sección 20ª), de 7 de septiembre FJ 8.

SAP de Granada núm. 351/2014 (Sección 1ª), de 5 junio

SAP de Granada núm. 486/2014 (Sección 1ª), de 18 de septiembre, FJ 2.

SAP de Guadalajara núm. 31/2017 (Sección 1ª), de 4 diciembre, FJ 2

SAP de Islas Baleares núm. 197/2017 (Sección 1ª), de 31 julio, FJ 2.

SAP de Las Palmas núm. 22/2011 (Sección 1ª), de 20 de enero, FJ 3.

SAP de Lleida núm. 90/2004, de 25 de febrero de 2004, FJ 1.

SAP de Madrid núm. 329/2015 (Sección 2ª), de 27 de abril, FJ 3.

SAP de Madrid núm. 895/2017 (Sección 7ª), de 27 de noviembre, FJ 1.

SAP de Santa Cruz de Tenerife núm. 419/2015 (Sección 2ª), FJ 3.

STS núm. 176/2013 (Sala 2ª), de 21 de octubre, FJ 7.

STS núm. 230/2017 (Sala de lo Penal, Sección 1ª), de 4 abril, FJ 6.

STS núm. 358/2007, de 30 abril, FJ 1.

STS núm. 358/2007, de 30 abril, FJ 1.

STS núm. 532/2015 (Sala de lo Penal, Sección 1ª), de 23 septiembre, FJ 5.

STS núm. 586/2016 (Sala de lo Penal, Sección1ª), de 4 julio, FJ 4.

STS núm. 803/2017 (Sala de lo Penal, Sección1ª), de 11 diciembre, FJ 4.