Universidad de Alcalá

Delito de descubrimiento y revelación de secretos

Crime of discovery and disclosure of secrets

Máster Universitario en Acceso a la Profesión de Abogado

Autora: Dª VALENTINA NITOIU SOTO

Tutor: D. ANTONIO BARBERO DÍAZ

Co-tutora: Dra. Dª RAQUEL ROSO CAÑADILLAS

Alcalá de Henares, 5 de febrero de 2018.

Tabla de contenido

I. ABREVIATURAS 1
II. RESUMEN Y PALABRAS CLAVE 3
III. INTRODUCCIÓN. 4
IV. DELITO DE DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS. 8
1. Regulación. 8
2. Bien jurídico protegido: El derecho fundamental a la intimidad personal y familiar. 11
2.1. Regulación constitucional e internacional de la intimidad. 11
2.2. Concepto y contenido. 14
2.3. Titularidad. 16
3. Tipos básicos (art. 197.1 y 2) 19
3.1. Delito de descubrimiento de secretos documentales (art. 197.1, primer inciso). 19
3.1.1. Tipo objetivo. 20
i. Sujetos activo y pasivo. 20
ii. Conducta típica. 20
iii. Objeto material y bien jurídico protegido. 23
iv. Consentimiento y autorización. 26
3.1.2. Tipo subjetivo. 26
3.2. Delito de interceptación de telecomunicaciones, y utilización de medios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen, o de cualquier otra señal de comunicación (art. 197.1, segundo inciso). 27
3.2.1. Tipo objetivo. 28
i. Sujeto activo y pasivo. 28
ii. Conducta típica. 28
iii. Objeto material y bien jurídico protegido. 31
iv. Consentimiento y autorización. 33
3.2.2. Tipo subjetivo. 35
3.2.3. Causas de justificación. 35
3.3. Delito de descubrimiento de datos reservados de carácter personal o familiar (art. 197.2). 37
3.3.1. Tipo objetivo. 38
i. Sujetos activo y pasivo. 38
ii. Conducta típica. 38
iii. Objeto material. 41
iv. Consentimiento y autorización. 43
3.3.2. Tipo subjetivo. 44
4. Tipos agravados. 46

4.1. Agravación por difusión, revelación o cesión a terceros (art. 197.3). 46
4.2. Agravación por razón del sujeto activo y por suplantación de datos personales (art.197.4). 47
4.3. Agravación por afectación a datos especialmente protegidos y por la especial vulnerabilidad de la víctima (art. 197.5). 49
4.4. Agravación por el especial desvalor de la finalidad perseguida (art 197.6). 51
5. Tipos específicos 52
5.1. Revelación de secretos sin haber sido parte en el descubrimiento (art.197.3, párr. 2). 52
5.2. Revelación de imágenes o grabaciones audiovisuales, obtenidos con anuencia del sujeto pasivo (art. 197.7). 52
6. Nuevas conductas: arts. 197 bis y ter. 59
6.1. Introducción en el CP mediante las Reformas de 2010 y 2015. 59
6.2. Concreción del bien jurídico protegido por las nuevas figuras. 60
6.3. Acceso o mantenimiento ilícito a un sistema de información (art. 197 bis 1). 63
6.3.1. Tipo objetivo. 63
i. Sujetos activo y pasivo. 63
iii. Conducta típica. 64
ii. Objeto material. 65
iv. Realización de la conducta típica por cualquier medio o procedimiento, vulnerando las medidas de seguridad impuestas y sin autorización. 66
6.3.2. Tipo subjetivo. 67
6.4. Interceptación de transmisiones no públicas de datos informáticos (art. 197 bis 2). 68
6.4.1. Distinción con la conducta contenida en el segundo inciso del art. 197.1. 68
6.4.2. Tipo objetivo. 69
i. Sujetos activo y pasivo. 69
ii. Conducta típica. 70
iii. Objeto material. 71
6.4.3. Tipo subjetivo. 73
6.5. Producción, adquisición para su uso, importación o facilitación de instrumentos para la comisión de los delitos contenidos en los arts. 197.1 y 2 y 197 bis (art. 197 ter). 74
6.5.1. Tipo objetivo. 75
i. Conducta típica. 75
ii. Objeto material. 76
6.5.2. Tipo subjetivo. 78
7. Tipos agravados comunes a todas las conductas del Capítulo I del Título X. 79
7.1. Comisión dentro de una organización o grupo criminal (art. 197 quater). 79

7.2. Agravación por cualidad del sujeto activo, cuando el mismo fuere autoridad o funcionario público (art. 198). 80
8. Revelación de secretos laborales o profesionales (art. 199). 83
9. Especial consideración de la persona jurídica (arts. 197 quinquies y art. 200). 86
10. Requisitos procedimentales: art 201. 88
V. CONCLUSIONES 90
VI. BIBLIOGRAFÍA. 94
VII. ANEXO I. LEGISLACIÓN APLICADA. 98
VIII. ANEXO II. JURISPRUDENCIA. 100

I. ABREVIATURAS

AAP	Auto de la Audiencia Provincial
AP	Audiencia Provincial
Art., arts.	Artículo, artículos
ATC	Auto del Tribunal Constitucional
ATS	Auto del Tribunal Supremo
CDFUE	Carta de los Derechos Fundamentales de la Unión Europea (2000/C-364/01)
CE	Constitución Española, de 29 de diciembre de 1978
CEDH	Convenio Europeo para la protección de los derechos humanos y las libertades fundamentales, de 4 de noviembre de 1950
Coord., coords.	Coordinador, coordinadores
CP	Ley orgánica 10/1995, de 23 de noviembre, del Código Penal
DUDH	Declaración Universal de los Derechos Humanos, de 10 de diciembre de 1948
UE	Unión Europea
FJ	Fundamento Jurídico
Lecrim	Ley de Enjuiciamiento Criminal (Real Decreto, de 14 de septiembre de 1882)
LGP	Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria
LO	Ley Orgánica
LO 1/1982	LO 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la propia imagen

LO 5/2010	Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal
LO 1/2015	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
LOPD	Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos de Carácter Personal
Núm.	Número
Pág., págs.	Página, páginas
Párr.	Párrafo
RD	Real Decreto
SAP	Sentencia de la Audiencia Provincial
STC	Sentencia del Tribunal Constitucional
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STS	Sentencia del Tribunal Supremo
TC	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
TS	Tribunal Supremo
Vol.	Volumen

II. RESUMEN Y PALABRAS CLAVE

Resumen: En el presente trabajo se realiza un análisis de las figuras contenidas en el Capítulo I del Título X del CP, relativas al descubrimiento y revelación de secretos, con observancia de los tipos básicos, tipos agravados, tipos específicos y las nuevas conductas, incluidas tras la Reforma del CP español en 2015.

Abstract: In the present work is an analysis of the figures contained in Title X, Chapter I, relating to the crime of discovery and disclosure of secrets, with observance of the basic types, aggravated types, specific types and new behaviors including after the reform of the Spanish CP in 2015.

Palabras clave: Delitos contra la intimidad, datos reservados de carácter personal, delitos contra la seguridad informática, Reforma 2015.

Key words: Crimes against privacy, reserved personal data, computer security crimes, Reform 2015.

III. INTRODUCCIÓN.

Mediante la aprobación de la LO 1/2015, se produjo una Reforma total de nuestro CP, la cual fue consecuencia de la necesidad de actualización del sistema penal existente en aquel momento. Concretamente, respecto a la Parte Especial del CP se produce una revisión del articulado, tanto a nivel formal como material, introduciendo cambios destacables en conductas que ya se encontraban reguladas, e incluyendo, además, nuevos comportamientos típicos que con anterioridad a la Reforma no disponían de un correcto encaje legal.

Ante tal escenario, el delito de descubrimiento y revelación de secretos contenido en el Capítulo I del Título X del CP, también es objeto de distintas modificaciones, algunas de las cuales obedecen a demandas sociales (como pudiera ser la tipificación de la conducta de revelación de imágenes obtenidas con anuencia de la víctima), mientras que otras son consecuencia de los compromisos internacionales asumidos por el Estado español (como aquellos contenidos en la Directiva 2013/40/UE, relativa a los ataques contra los sistemas de información). En atención a ello, el presente trabajo ofrece un análisis de las distintas figuras que componen dicho delito, con atención a los cambios introducidos mediante la Reforma de 2015.

La primera parte del trabajo se dedica a la concreción del bien jurídico protegido por este delito, en concreto, el derecho fundamental a la intimidad personal y familiar (art. 18.1 CE), procediendo al análisis de la jurisprudencia constitucional existente en relación al mismo. Para ello, se delimita el ámbito de protección de tal derecho en relación con otros derechos fundamentales, como el derecho al honor o a la propia imagen junto a los cuales se halla reconocido en el art. 18 CE, analizando su conexión con los derechos a la inviolabilidad del domicilio, el secreto de las comunicaciones y la autodeterminación informativa (contenidos en los apartados segundo, tercero y cuarto, respectivamente, del art. 18 CE). Asimismo, se procede al estudio del carácter personalísimo del derecho a la intimidad, planteando la posible conexión del mismo con la persona jurídica, la persona fallecida y la persona con proyección pública.

En la segunda parte del trabajo se exponen los tipos básicos del delito de descubrimiento y revelación de secretos, contenidos en los apartados primero y segundo del art. 197 CP, los cuales no han visto modificada su redacción tras la Reforma de 2015,

pues el legislador opta por el mantenimiento de los mismos. En este sentido, se enuncian los tipos objetivo y subjetivo de cada una de las conductas, con observancia de cada uno de los elementos típicos exigidos.

De conformidad con la configuración del art. 197.1 CP se procede al análisis de la conducta de apoderamiento de papeles, cartas, mensajes de correo electrónico u otros documentos o efectos personales (contenida en el primer inciso), de forma separada a la conducta de interceptación de comunicaciones y utilización de medios técnicos de escucha, transmisión o reproducción de sonido o imagen u otra señal de comunicación (establecida en el segundo inciso). La fundamentación de tal distinción reside en la distinta conducta típica y objeto material sobre el que recae cada una de aquellas figuras.

En atención a la primera figura se examina la redacción empleada y mantenida por el legislador, atendiendo a los pronunciamientos doctrinales y jurisprudenciales existentes en torno al apoderamiento de los correos electrónicos, objeto material que ha suscitado problemas interpretativos, de conformidad con su carácter inmaterial. En virtud de ello, se analiza la posible desmaterialización del objeto material y la espiritualización de la conducta de apoderamiento.

En lo que respecta al segundo tipo básico, contenido en el segundo inciso del art. 197.1, se plantea la relación de las conductas de interceptación de comunicaciones y utilización de medios técnicos de escucha, transmisión o reproducción de sonido o imagen u otra señal de comunicación, con otros bienes jurídicos distintos al derecho a la intimidad personal y familiar, como son el derecho al secreto a las comunicaciones o a la propia imagen, exponiendo en último lugar las posibles causas de justificación de esta figura (que también resultan de aplicación a otras conductas del Capítulo) .

El último de los tipos básicos examinados es el relativo a la conducta de acceso, apoderamiento, utilización, modificación o alteración de los datos reservados de carácter personal o familiar, contenido en el art. 197.2 CP. En relación al mismo, se procede a la concreción del bien jurídico protegido por el delito, esto es, el derecho a la autodeterminación informativa o libertad informática (art. 18.4 CE), de conformidad con el objeto material del tipo, los datos reservados de carácter personal o familiar. Igualmente, se delimitan, en atención a la redacción empleada por el legislador, las distintas conductas típicas contenidas en dicha figura.

A continuación, se enumeran los distintos tipos agravados contenidos en los apartados tercero a sexto del art. 197, que son de aplicación a los tipos básicos anteriores. Concretamente, se examinan los siguientes tipos: agravación por revelación, difusión o cesión de los secretos descubiertos, agravación en atención al sujeto activo (persona encargada o responsable del fichero) o por suplantación de datos personales de la víctima (respecto a los cuales se prevé un tipo súper agravado, en atención a si los datos son revelados, difundidos o cedidos), agravación por la especial naturaleza de los datos o de la víctima, y agravación por el especial desvalor de la conducta (realización con fines lucrativos).

Dentro del apartado quinto del trabajo se exponen dos tipos específicos de carácter atenuado, el tipo contenido en el art. 197.3, segundo párrafo, que contiene aquella conducta de difusión, revelación o cesión sin realización de la conducta de descubrimiento, y el nuevo tipo introducido por el legislador, mediante la Reforma de 2015, relativo a la conducta de difusión no autorizada de imágenes obtenidas con anuencia de la víctima, contenido en el art. 197.7. En relación a este último se efectúa un análisis pormenorizado, planteando las causas que motivaron su inclusión en el reformado CP, y con observancia de los precedentes penales existentes. Conjuntamente, se analiza la redacción empleada en el párr. primero del art. 197.7 CP, y los problemas interpretativos que la misma puede plantear, en contraste con la propia finalidad de la norma. Se examina en último lugar el tipo agravado previsto para ésta misma figura, contenido en el párr. segundo, resultando de aplicación si el sujeto activo es cónyuge, o persona unida por análoga relación de afectividad, aun sin convivencia, si la víctima fuere menor de edad o persona necesitada de especial protección, o si los hechos fueren cometidos con finalidades lucrativas; así como los posibles concursos entre este tipo agravado y otras figuras del CP.

Seguidamente, se procede al planteamiento de forma separada a las anteriores figuras, de las nuevas conductas introducidas en los arts. 197 bis y ter, por medio de las cuales, se tipifican los comportamientos de acceso o mantenimiento ilícito en un sistema de información (art 197 bis 1), de interceptación de transmisiones no públicas de datos informáticos producidos desde, hacia o dentro de un sistema de información (art 197 bis 2), y en último lugar, los actos preparatorios de producción, adquisición para su uso, importación o facilitación de herramientas para la comisión de los delitos contenidos en

los arts. 197.1 y 2 y 197 bis (art 197 ter). La inclusión de dichas figuras en el CP, obedece a los compromisos internacionales asumidos por España, mediante la aprobación del Convenio sobre la Ciberdelincuencia, la Decisión Marco 2005/222/JAI y la Directiva 2013/40/UE, cuyo objetivo principal era la creación de una política penal común, tendente a la protección de la sociedad frente a las nuevas formas de delincuencia producidas a través de medios informáticos. En relación a ello, se procede a la interpretación de las figuras, analizando los distintos elementos típicos exigidos. Al mismo tiempo, se concreta el bien jurídico protegido por las mismas, esto es, la seguridad de los sistemas de información y su relación con el derecho a la intimidad, dada la ubicación de las nuevas figuras en el CP.

Con posterioridad, se desarrollan dos tipos agravados comunes al Capítulo I del Título X del CP, cuya cualificación se fundamenta en la realización de la conducta dentro de una organización o grupo criminal, y en la cualidad de autoridad o funcionario público del sujeto activo, contenidos en los arts. 197 quater y 198, respectivamente.

El apartado octavo del presente trabajo se dedica a la especial consideración de la persona jurídica en relación con el delito de descubrimiento y revelación de secretos. De conformidad con el art. 197 quinquies, se analiza la responsabilidad de la persona jurídica por los delitos contenidos en los arts. 197, 197 bis y 197 ter, examinando a continuación y de conformidad con el art. 200, su inclusión como sujeto pasivo de las conductas contenidas en el Capítulo I del Título X CP.

Consecutivamente, se expone la última figura típica del Capítulo contenida en el art. 199, relativa a la revelación de secretos obtenidos por razón de oficio o relación laboral, y de divulgación de secretos con incumplimiento de la obligación, de carácter profesional, de sigilo o reserva. Respecto a ello, son analizados separadamente los distintos elementos típicos de cada una de las conductas.

En el último apartado del trabajo se exponen los requisitos de procedibilidad contenidos en el art. 201. En este sentido, y de conformidad con el carácter semipúblico del delito, se plantea la necesidad de interposición de denuncia para la perseguibilidad de los tipos expuestos, con la salvedad de la conducta contenida en el art. 198 y aquellas que afecten a intereses generales o a una pluralidad de personas. Asimismo, se analiza la extinción de la acción penal, en caso de que medie el perdón del ofendido.

IV. DELITO DE DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS.

1. Regulación.

El tema principal del presente trabajo es el delito de descubrimiento y revelación de secretos, el cual se encuentra tipificado por nuestro CP en los arts. 197 a 201, hallándose insertos en el Capítulo I (*Del descubrimiento y revelación de secretos*), del Título X (*Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del Domicilio*).

Antes de exponer dicho delito, es importante señalar que no todas las figuras que afectan a la intimidad se encuentran en el Título X del CP, por ejemplo, encontraríamos separadamente los delitos de infidelidad en la custodia de documentos y de violación de secretos[1], o los cometidos por funcionario público contra la inviolabilidad domiciliaria y demás garantías de la intimidad[2]. Asimismo, podemos observar una misma dinámica delictiva, tendente a conocer o apoderarse de información reservada, entre el delito de descubrimiento y revelación de secretos (del Título X), y el delito de difusión, revelación o cesión de un secreto de empresa[3]. En tales casos, el bien jurídico protegido no sería únicamente el derecho fundamental a la intimidad, sino que éste guardaría relación con otros derechos (carácter pluriofensivo), que conlleva a su configuración separada[4]. En el presente trabajo, no obstante, no haremos referencia a dichos delitos, centrando el estudio de manera única en los delitos de descubrimiento y revelación de secretos contenidos en el Capítulo I del Título X del CP.

Tras la Reforma del CP, mediante la LO 1/2015, la nueva redacción del delito de descubrimiento y revelación de secretos, puede esquematizarse del siguiente modo:

- Tipos básicos.
  - Art. 197.1: apoderamiento de papeles, cartas, mensajes de correo electrónico u otros documentos o efectos personales; interceptación de las comunicaciones o

[1] Capítulo IV, arts. 413 a 418, del Título XIX *Delitos contra la Administración Pública.*
[2] Sección 2ª, arts. 534 a 536, del Capítulo V, *De los delitos cometidos por los funcionarios públicos contra las garantías constitucionales*, Título XXI, *Delitos contra la Constitución.*
[3] Art. 279, Sección 3ª, *De los delitos relativos al mercado y a los consumidores*, del Capítulo XI *De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores*, del Título XIII *Delitos contra el patrimonio y contra el orden socioeconómico.*
[4]ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, pág. 254.

utilización de medios técnicos de escucha, transmisión o reproducción de imagen o sonido u otra señal de la comunicación.

- Art. 197.2: acceso, apoderamiento, utilización, modificación o alteración de datos reservados de carácter personal o familiar.

- Tipos agravados.
  - Art. 197.3, párr. 1: difusión, revelación o cesión de los secretos descubiertos.
  - Art. 197.4: por la cualidad del sujeto activo (persona encargado responsable del fichero) o por suplantación de datos personales.
  - Art. 197.5: por la especial naturaleza de los datos o de la víctima.
  - Art. 197.6: por el especial desvalor de la conducta (fin lucrativo).
- Tipos autónomos:
  - Art. 197.3, párr. 2: difusión, revelación o cesión de los secretos sin haber realizado la conducta de descubrimiento.
  - Art. 197.7: revelación no autorizada de imágenes obtenidas con anuencia de la víctima.
- Nuevos delitos:
  - Art. 197 bis 1: acceso o mantenimiento ilícito en un sistema de información.
  - Art. 197 bis 2: interceptación de transmisiones no públicas de datos entre sistemas.
  - Art. 197 ter: producción, adquisición para su uso, importación o facilitación de herramientas con la finalidad de cometer los delitos contenidos en los arts. 197.1 y 2 ó 197 bis.
- Tipos agravados comunes a todas las conductas anteriores:
  - Art. 197 quater: comisión en el seno de una organización o grupo criminal.
  - Art. 198: comisión por autoridad o funcionario público.
- Especial referencia a la persona jurídica arts. 197 quinquies y 200.
- Revelación de secretos obtenidos por razón de oficio o relación laboral e incumplimiento del deber de reserva o sigilo respecto al secreto profesional: art. 199.
- Requisitos procedimentales: art. 201.

Del anterior esquema, pueden observarse los grandes cambios operados con respecto al delito de descubrimiento y revelación de secretos a través de la Reforma de 2015, cambios que no solamente se han producido a nivel formal sino también sobre su contenido. En primer lugar, se ha producido una reorganización del articulado, por ejemplo, en la ubicación de los apartados del art. 197, o en la incorporación de nuevos

artículos (arts. 197 bis, ter, quater, quinquies). Por otra parte, en cuanto a los aspectos materiales, el legislador ha optado por incluir nuevas figuras típicas como la revelación de imágenes obtenidas con anuencia de la víctima (art 197.7) o el intrusismo informático (art. 197 bis 1), modificando, además, algunos tipos agravados ya existentes.

En este sentido, es conveniente reseñar que algunas de las modificaciones plasmadas en nuestro CP derivan de la incorporación al ordenamiento jurídico español de normas internacionales, tendentes a la persecución penal efectiva de ciertas conductas criminales, y surgidas como consecuencia de la evolución tecnológica. Ello ha conducido a la adaptación de figuras delictivas que ya se encontraban tipificadas y cuyas formas comisivas (ya sean de planificación o de ejecución) han encontrado una herramienta útil en el desarrollo de las nuevas tecnologías.

El delito de descubrimiento y revelación de secretos ha sufrido distintas modificaciones desde su inclusión en el CP de 1995, no obstante, la Reforma operada en 2015 resulta claramente significativa. Concretamente, los últimos cambios introducidos son principalmente consecuencia de la transposición de la Directiva 2013/40/UE. No obstante, la nueva regulación de este delito no responde única y exclusivamente a objetivos europeos, pues también surge como consecuencia de las demandas que la doctrina venía formulando, así como de las propuestas emitidas por el Consejo General del Poder Judicial[5].

Ante tal escenario, algunos autores han criticado las modificaciones operadas en el delito objeto del presente trabajo, en virtud de que el legislador ha optado por mantener la redacción de ciertos artículos cuyos términos resultan difusos e indeterminados, incorporando, en contraposición, figuras que exceden los principios de mínima intervención y *ultima ratio* del Derecho Penal[6]. No obstante, tales consideraciones, serán referidas ulteriormente.

[5] GONZÁLEZ COLLANTES, en: Revista de Derecho Penal y Criminología, núm.13, 2015, pág. 54.
[6] ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, pág. 254.

2. Bien jurídico protegido: El derecho fundamental a la intimidad personal y familiar.

Como precisamos anteriormente, el delito de descubrimiento y revelación de secretos se encuentra regulado por nuestro CP en el Título X bajo la rúbrica de "*Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*", insertándose esta modalidad delictual dentro del Capítulo I (arts. 197 a 201), junto al delito de allanamiento de morada, domicilio de personas jurídicas y establecimientos abiertos al público (Capítulo II, arts. 202 a 204). En relación a ello, Muñoz Conde entiende que: "*bajo la rúbrica "Del descubrimiento y revelación de secretos", se tipifican varios delitos que tienen como nota en común el que en ellos se protege la voluntad de una persona de que no sean conocidos determinados hechos que solo son conocidos por ella o por un circulo reducido de personas, es decir, que pueden ser calificados de secretos, y también el derecho de la persona a controlar cualquier información o hecho que afecte a su vida privada y, por tanto, a su intimidad. El descubrimiento y/o revelación de esos secretos y de hechos relativos a la intimidad constituyen, pues el núcleo de estos tipos delictivos"*[7].

Como consecuencia, podemos afirmar que el bien jurídico protegido por el delito es la intimidad personal y familiar, no obstante, y como se analizará posteriormente, también se protegen otro tipo de expresiones de este derecho fundamental, como la autodeterminación informativa sobre los datos personales o el secreto de las comunicaciones. En virtud de ello, deviene necesario hacer una breve exposición del contenido y alcance del derecho a la intimidad personal y familiar.

2.1. Regulación constitucional e internacional de la intimidad.

En primer lugar, el derecho a la intimidad personal y familiar se encuentra reconocido por nuestro texto constitucional en el art. 18, dentro del Título I (*De los derechos y deberes fundamentales),* Capítulo II (*Derechos y libertades*), Sección 1ª (*De los derechos fundamentales y de las libertas públicas)*. Mediante esta configuración se dota al mismo de carácter fundamental, reconociéndole las máximas garantías dentro de nuestro ordenamiento jurídico, permitiendo que el mismo pueda ser invocado a través del

[7] MUÑOZ CONDE, en: *Derecho Penal. Parte Especial*, 2015, pág. 233.

recurso de amparo ante el TC, y gozando además de especial protección ante los tribunales ordinarios.

En el plano internacional, el derecho a la intimidad personal y familiar también goza de la condición de derecho fundamental (aunque su contenido no es coincidente con el proporcionado por la CE), encontrándose reconocido en distintas cartas de derechos fundamentales, entre las que cabe destacar las siguientes:

- La DUDH, reconoce en su art. 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".*
- El CEDH, art. 8: "*Derecho al respeto a la vida privada y familiar. 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".*
- La CDFUE, dispone el art. 7: "*Respeto de la vida privada y familiar. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones"*.

Volviendo al ámbito nacional, el art. 18 CE, dispone lo siguiente:

"1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
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".

Debido a la redacción conjunta por la que optó el legislador en el primer apartado (honor, intimidad personal y familiar, y propia imagen), se han suscitado distintos debates en torno a si los mismos conforman un único derecho o si, por el contrario, se encuentran delimitados, siendo derechos independientes entre sí. En este sentido, el Alto Tribunal[8] se pronunció indicando que el honor, la intimidad y la propia imagen, son derechos que derivan de la dignidad humana y que por tanto son derechos de la personalidad destinados a proteger la dimensión moral de las personas; no obstante, si bien pueden existir supuestos en que dichos derechos puedan hallarse interrelacionados, existe una clara distinción entre el contenido de los mismos, disponiendo cada uno de autonomía propia, así como de un ámbito de protección diferenciado.

Al hilo de lo anterior, algunos autores[9] han considerado que esta configuración responde al objetivo en común que los tres derechos poseen, concretado en la protección de la vida privada de la persona, en tanto que su configuración emana directamente del derecho a la dignidad y libre desarrollo de la personalidad reconocidos en el art. 10.1 CE. Asimismo, la estrecha vinculación entre los mismos puede conllevar a la superposición, llegando a alegarse los tres en un mismo recurso de amparo[10].

En segundo lugar, conviene dilucidar la relación existente entre los derechos reconocidos en el art. 18.1 CE y la inviolabilidad del domicilio, el secreto de las comunicaciones y la autodeterminación informativa o libertad informática, concretados en los apartados segundo, tercero y cuarto (respectivamente) del art. 18 CE. Si bien de la propia redacción constitucional pudiera inferirse que estos últimos son derechos que gozan de autonomía propia, al igual que el derecho al honor, a la intimidad y a la propia imagen, la jurisprudencia y doctrina[11] han señalado que los apartados segundo a cuarto del art. 18 CE son expresiones concretas del derecho a la intimidad personal y familiar, disponiendo no obstante, de un contenido propio, específico y distinto del derecho a la intimidad.

Si bien, con respecto al delito de descubrimiento y revelación de secretos el bien jurídico protegido es el derecho a la intimidad, algunas de las nuevas figuras introducidas

[8] STC 81/2001, de 26 de marzo, FJ 2º.
[9] FERNÁNDEZ ESTEBAN, en.: *Nuevas tecnologías, Internet y Derechos Fundamentales*, 1998 pág. 116.
[10] MARTÍNEZ DE PISÓN, en: Anuario de Filosofía del Derecho (XXXII), 2016, pág. 417.
[11] FRIGOLS I BRINES, en BOIX REIG (Dir.), JAREÑO LEAL (Coord.), *La protección jurídica de la intimidad*, 2010, págs. 40-45.

en el mismo Capítulo I del Título X del CP, exigirán un análisis pormenorizado de su posible desconexión con este derecho fundamental.

2.2. Concepto y contenido.

Desde la consagración del derecho a la intimidad, y al no existir en la CE, un concepto concreto del mismo, su definición, así como la delimitación del ámbito de protección, ha resultado una tarea compleja. Ante tal panorama, el TC ha desempeñado una labor loable en lo que respecta a la concreción del contenido esencial de los derechos contenidos en el art. 18 CE. En este sentido indica, Martínez de Pisón que: "*Una de las piezas de este sistema han sido los derechos del art. 18 CE. De hecho, el Tribunal Constitucional se pronunció muy prontamente sobre los mismos y sobre las cuestiones antes relatadas. La doctrina constitucional sobre el derecho al honor, a la intimidad personal y familiar y a la propia imagen quedó prácticamente fijada en las primeras sentencias emitidas ya en los años 80s del siglo xx, aunque no, por ello, el Tribunal Constitucional ha dejado de pronunciarse o matizar, si ha sido el caso, durante las décadas transcurridas"*[12].

En virtud de ello, la jurisprudencia constitucional en uno de sus primeros intentos por fijar el alcance de este derecho, se pronunció otorgando una noción amplia del mismo: "*…la intimidad es un ámbito o reducto en el que se veda que otros penetren y que no guarda por sí solo relación directa con la libertad de relacionarse con otras personas o derecho a tener amistades*"[13]. De este modo, se configura la intimidad, como aquel ámbito perteneciente a la propia persona, el cual se encuentra vetado a la injerencia de terceros.

Con posterioridad a aquella, el TC determinó que: *"…el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de*

[12] MARTÍNEZ DE PISÓN, en: Anuario de Filosofía del Derecho (XXXII), 2016, pág. 417.
[13] STC 73/1982, de 2 de diciembre, FJ 5º.

vida. No siempre es fácil, sin embargo, acotar con nitidez el contenido de la intimidad"[14]. En este sentido, podemos observar como el derecho a la intimidad abarca una multitud de escenarios que no pueden hallarse circunscritos únicamente a las manifestaciones contenidas en el art. 18 CE, pues protege un ámbito mucho más extenso, que es aquel espacio reservado y perteneciente a la vida de la persona, el cual se halla vetado al conocimiento o injerencia de terceros (incluidos los poderes públicos). En consecuencia, la definición del derecho a la intimidad resulta compleja, en virtud de que la misma no se limita a la protección de espacios físicos en los que pueda desarrollarse la vida privada (como es el domicilio), sino que, además de ellos, la intimidad abarca espacios inmateriales en los que la persona se desenvuelve (como podrían ser por medio de los ordenadores).

Con fundamentación en lo anterior, la inviolabilidad del domicilio y de las comunicaciones han sido consideradas manifestaciones tradicionales de la intimidad, que garantizan el respeto a un ámbito concreto y material de la vida privada personal y familiar, excluyendo a terceros de su conocimiento o intromisión. Resultando, el derecho a la autodeterminación informativa o libertad informática, una manifestación más reciente de la intimidad que es consecuencia del avance de la tecnología, el cual ha provocado un cambio en el concepto de intimidad, ampliando su ámbito de protección[15].

Por otra parte, es importante destacar el siguiente pronunciamiento del TC: "*Intimidad y honor son realidades intangibles cuya extensión viene determinada en cada sociedad y en cada momento histórico, cuyo núcleo esencial en sociedades pluralistas ideológicamente heterogéneas deben determinar los órganos del Poder Judicial"*[16]. En atención al mismo, podemos observar que el concepto de intimidad no ha de entenderse de manera absoluta, sino que éste variará en función de cada momento y sociedad en que nos hallemos, correspondiendo al Poder Judicial fijar su contenido, con la observancia de aquellos criterios existentes en la cultura de la sociedad que se trate[17]. Es por ello que el derecho a la intimidad, dada su amplitud conceptual, plantea un reto en cuanto a su concreción.

[14] STC 110/1984, de 26 de noviembre, FJ 3º.
[15] *Ibidem*, FJ 3º.
[16] STC 171/1990, de 12 de noviembre, FJ 4º.
[17] STC 37/1989, de 15 de febrero, FJ 7º.

En relación con los principios de mínima intervención y *ultima ratio* del Derecho Penal, es preciso indicar que éste habrá de conocer únicamente aquellas conductas que dispongan de una mayor trascendencia sobre el derecho a la intimidad, o que resulten más graves, pues existen otras vías (como son la vía civil o la administrativa) a través de las cuales, la persona puede salvaguardar este derecho fundamental sin necesidad de recurrir al cauce penal.

2.3. Titularidad.

El derecho a la intimidad personal y familiar es un derecho que se encuentra claramente ligado a la dignidad de la persona y al libre desarrollo de su personalidad (art. 10 CE)[18]. Siendo consecuencia del mismo y hallando en este último su fundamentación, la intimidad se define como un derecho fundamental de carácter personalísimo ligado a la existencia del propio individuo. En virtud de ello, cabe concluir que la titularidad del derecho a la intimidad personal y familiar pertenece a las personas físicas, ya sean españoles o extranjeros.

A tal respecto, se ha planteado la posibilidad de que las personas jurídicas puedan ser titulares de este derecho fundamental. En torno a este debate, el TC se pronunció, en un principio, negando tal posibilidad, en base a que: "*El derecho a la intimidad que reconoce el art. 18.1 de la CE por su propio contenido y naturaleza, se refiere a la vida privada de las personas individuales, en la que nadie puede inmiscuirse sin estar debidamente autorizado, y sin que en principio las personas jurídicas, como las Sociedades mercantiles, puedan ser titulares del mismo, ya que la reserva acerca de las actividades de estas Entidades, quedarán, en su caso, protegidas por la correspondiente regulación legal, al margen de la intimidad personal y subjetiva"*[19].

Pese a ello, la jurisprudencia constitucional ha estimado, con posterioridad, que la persona jurídica puede ser titular de las manifestaciones concretas del derecho fundamental a la intimidad, como son la inviolabilidad del domicilio (art. 18.2 CE) o la autodeterminación informativa respecto a aquellos datos que la correspondan (art. 18.4 CE), gozando, no obstante, de una protección o tutela menor que aquella que se predica de la persona física. Tal menor protección, se fundamenta en la falta de vinculación entre

[18] MIERES MIERES, en: *Intimidad Personal y Familiar. Prontuario de Jurisprudencia Constitucional*, 2002, pág. 24.
[19] ATC 257/1985, de 17 de abril, FJ 2º.

el domicilio o los datos de la persona jurídica y la intimidad (entendida ésta en su sentido estricto u originario)[20] y [21]. Asimismo, la jurisprudencia ha reconocido que la persona jurídica puede ser titular de otros derechos fundamentales como el derecho al honor.[22]

En atención a ello, el TC ha precisado que puede reconocerse, a la persona jurídica, la titularidad de aquellos derechos fundamentales que necesariamente necesite en la consecución de aquellos fines para los que fue creada, debiendo analizarse previamente la naturaleza de tal derecho (pues resultaría difícil reconocer el derecho a la vida o integridad física a una persona jurídica): "…*puede sostenerse que, desde un punto de vista constitucional, existe un reconocimiento, en ocasiones expreso y en ocasiones implícito, de la titularidad de las personas jurídicas a determinados derechos fundamentales. Ahora bien, esta capacidad, reconocida en abstracto, necesita evidentemente ser delimitada y concretada a la vista de cada derecho fundamental. Es decir, no sólo son los fines de una persona jurídica los que condicionan su titularidad de derechos fundamentales, sino también la naturaleza concreta del derecho fundamental considerado, en el sentido de que la misma permita su titularidad a una persona moral y su ejercicio por ésta*"[23].

Por lo que respecta al ámbito penal, la persona jurídica puede ser víctima de todas las figuras contenidas en el Capítulo I del Título X del CP, de conformidad con el art. 200 CP, no obstante, sobre ello habremos de referirnos con posterioridad.

Por otro lado, cabe analizar si el derecho a la intimidad personal y familiar puede ser reconocido a personas fallecidas, es decir, si sus derechos pueden ser defendidos por los herederos o aquellas personas a las que se reconozca legitimación procesal suficiente.

---

[20] STC 69/1999, de 26 de abril, FJ 2º: "*Por tanto, cabe entender que el núcleo esencial del domicilio constitucionalmente protegido es el domicilio en cuanto morada de las personas físicas y reducto último de su intimidad personal y familiar. Si bien existen otros ámbitos que gozan de una intensidad menor de protección, como ocurre en el caso de las personas jurídicas, precisamente por faltar esa estrecha vinculación con un ámbito de intimidad en su sentido originario; esto es, el referido a la vida personal y familiar, sólo predicable de las personas físicas".*

[21] STC 54/2015, 16 de marzo de 2015, FJ 5º: "*De suerte que ha de entenderse que en este ámbito la protección constitucional del domicilio de las personas jurídicas y, en lo que aquí importa, de las sociedades mercantiles, sólo se extiende a los espacios físicos que son indispensables para que puedan desarrollar su actividad sin intromisiones ajenas, por constituir el centro de dirección de la sociedad o de un establecimiento dependiente de la misma o servir a la custodia de los documentos u otros soportes de la vida diaria de la sociedad o de su establecimiento que quedan reservados al conocimiento de terceros"*.

[22] Cabe señalar que, en la reciente STS 408/2016, Sala 1º, de 15 junio, se ha establecido que las personas jurídicas de Derecho Público no son titulares del derecho al honor garantizado por el art. 18.1 CE.

[23] STC 139/1995, de 26 de septiembre, FJ 5º.

En este sentido, el TC[24] ha determinado que la personalidad jurídica se extingue con la muerte de la persona, por lo que no puede reconocerse el derecho fundamental a la intimidad a una persona fallecida. Sin embargo, es importante concretar el contenido del derecho a la intimidad familiar, entendido como aquel ámbito reservado del que disponen los propios integrantes de la familia y que se halla protegido frente a la injerencia de terceros ajenos.

Además de ello, TC estima que el derecho a la intimidad familiar *"se extiende, no sólo a aspectos de la vida propia y personal, sino también a determinados aspectos de la vida de otras personas con las que se guarde una especial y estrecha vinculación, como es la familiar; aspectos que, por la relación o vínculo existente con ellas, inciden en la propia esfera de la personalidad del individuo que los derechos del art. 18 de la C.E. protegen"*[25]. Como consecuencia, mientras el derecho a la intimidad personal se extingue con la muerte, el derecho a la intimidad familiar permanece para aquellos que conforman la familia. En este sentido, el TC concreta que la intimidad no solo es propia de aquel que pudiera verse afectado directamente por una conducta, sino que, atendiendo a su repercusión moral, supone también un derecho para sus familiares[26].

En lo relativo al ámbito penal, es importante hacer referencia a la perseguibilidad del delito, pues si bien la acción penal corresponde a la persona agraviada por el delito conforme al art. 201 CP, tal derecho se transmitirá a los herederos con el fallecimiento de aquella[27].

En último lugar, conviene hacer referencia, de forma breve, al derecho a la intimidad personal y familiar de las personas que, dada su profesión o repercusión social, dispongan de cierta fama en la sociedad. En este sentido, la STC 7/2014, dispone que: "*La proyección pública y social, como consecuencia de la actividad profesional desempeñada, no puede ser utilizada como argumento para negar a la persona que la ostente una esfera reservada de protección constitucional en el ámbito de sus relaciones afectivas, derivada del contenido del derecho a la intimidad personal, reduciéndola hasta su práctica desaparición. Si bien los personajes con notoriedad pública inevitablemente*

[24] ATC 149/1999, de 14 de junio, FJ 3º.
[25] STC 231/1988, de 2 de diciembre, FJ 4º (la cual ha sido confirmada por la STC 197/1991, de 17 de octubre, FJ 3º).
[26] *Ibidem*, FJ 4º.
[27] STS 437/2010, 16 de abril de 2010, FJ 2º.

ven reducida su esfera de intimidad, no es menos cierto que, más allá de esa esfera abierta al conocimiento de los demás su intimidad permanece y, por tanto, el derecho constitucional que la protege no se ve minorado en el ámbito que el sujeto se ha reservado…"[28]. Como consecuencia, podemos considerar que la esfera de intimidad dependerá de cada persona, puesto que su titular dispone de la facultad de hacer públicos cuantos aspectos de su vida desee. En relación con el delito de descubrimiento y revelación de secretos, ello puede resultar importante para determinar si existe o no un consentimiento (en ocasiones tácito) sobre la conducta típica[29].

3. Tipos básicos (art. 197.1 y 2).

Conociendo cual es el bien jurídico que protege el delito de descubrimiento y revelación de secretos, hemos de analizar las distintas conductas que dentro del mismo se tipifican, comenzando por concretar cuáles son los tipos básicos.

El art. 197 contiene en sus apartados 1 y 2 las modalidades básicas del delito de descubrimiento y revelación de secretos, manteniendo tanto su ubicación como su redacción anterior. En primer lugar, dentro del apartado primero encontraríamos dos modalidades: el apoderamiento de documentos o efectos personales (primer inciso), y la interceptación de comunicaciones (segundo inciso). En segundo lugar, en el apartado segundo, se situaría la conducta de acceso, apoderamiento, utilización, modificación o alteración de los datos reservados de carácter personal o familiar. Es importante concretar que todas las modalidades básicas, disponen de las mismas consecuencias penológicas, estableciéndose una pena de prisión de 1 a 4 años y multa de 12 a 24 meses.

3.1. Delito de descubrimiento de secretos documentales (art. 197.1, primer inciso).

"1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales…"

Comenzando por el primer tipo básico del delito (art. 197.1 primer inciso), se castiga aquella conducta de apoderamiento de papeles, cartas o mensajes de correo

[28] STC 7/2014, de 27 de enero, FJ 4º.
[29] STS 437/2010, de 16 de abril, FJ 2º.

electrónico, u otros documentos o efectos personales, con el objetivo de revelar los secretos o invadir la intimidad de otra persona.

3.1.1. Tipo objetivo.

i. Sujetos activo y pasivo.

En primer lugar, hemos de hacer referencia, dentro de los elementos objetivos del tipo, al sujeto activo de esta modalidad, el cual podrá ser cualquier persona física o jurídica (ello de conformidad con el art. 197 quinquies).

Respecto al sujeto pasivo, será aquella persona titular del bien jurídico protegido (el derecho a la intimidad), que además habrá de corresponder con el objeto material del delito[30]; es decir, será aquella persona (física o jurídica) titular de los papeles, cartas, mensajes de correo electrónico, u otros documentos o efectos personales que fuesen objeto de apoderamiento, a través de los cuales el sujeto activo pretenda vulnerar su intimidad o descubrir sus secretos.

ii. Conducta típica.

En cuanto a la acción típica, consistirá en el apoderamiento de aquellos documentos o efectos personales, con el objeto de descubrir los secretos o vulnerar la intimidad de la víctima.

Tal y como se indicó anteriormente, este tipo básico no ha visto modificada su redacción tras la Reforma del CP en 2015, lo cual puede resultar criticable en cierta medida, puesto que el legislador ha optado por mantener el término "apoderamiento". Es importante hacer referencia a tal término, ya que su interpretación ha suscitado numerosos pronunciamientos doctrinales[31].

En este sentido, se cuestionaba tal término, en virtud de que tradicionalmente era interpretado como aquella conducta de traslación física del objeto al ámbito de control

[30] En este sentido:
- GÓNZALEZ CUSSAC, en: GÓNZALEZ CUSSAC (Coord.), *Derecho Penal Parte Especial*, 2016, pág. 278.
- JORGE BARREIRO, en: Revista jurídica Universidad Autónoma de Madrid, núm. 6, 2002, pág. 101.

[31] GÓNZALEZ CUSSAC, en: GÓNZALEZ CUSSAC (Coord.), *Derecho Penal Parte Especial*, 2016, págs. 54-55.
También, ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016 pág. 257.

del sujeto activo (dado su empleo en las figuras delictivas patrimoniales); en atención a ello, resultaba difícil incluir los correos electrónicos entre los objetos susceptibles de apoderamiento. No obstante, la doctrina ha admitido que el significado de apoderamiento se ha espiritualizado, en base a que la materialidad de los objetos susceptibles de ser apoderados se ha visto reducida[32]. Como consecuencia, resultan típicas aquellas conductas que, sin producirse un apoderamiento material del soporte sobre el que se hallen ciertos documentos o efectos personales, se acceda a su contenido, causando una lesión a la intimidad o produciéndose el descubrimiento de algún secreto. Dicho en otras palabras, no solo el apoderamiento material resultará punible, sino que también lo serán las conductas en que se produzca una captación intelectual del contenido de determinado soporte, incluyendo las copias o reproducciones que sobre los mismos se realicen. De este modo, se evitan incoherencias en la valoración de determinados hechos que pudieran suscitar dudas[33].

La espiritualización del apoderamiento también ha sido aceptada por la jurisprudencia. En este sentido, podemos observar un pronunciamiento reciente en la SAP Cádiz[34], "*La conducta de apoderamiento del primer inciso tiene necesariamente que referirse tanto al apoderamiento físico (impreso en papel o mediante copia en cualquier soporte) como al virtual (visualización). Ciertamente, si viniera referido únicamente a mensajes de correo electrónico cuando están impresos en papel, no tendría sentido la referencia a apoderamiento de papeles que también aparece en el tipo. Para Morant Vidal la captación intelectual del contenido del soporte puede subsumirse en el concepto de apoderamiento, si bien es necesaria la remoción previa de algún obstáculo por parte del autor, excluyendo la mera visualización sin maniobras de este tipo".*

En consecuencia, el reconocimiento generalizado tanto por la doctrina como por la jurisprudencia, de la espiritualización, puede ser uno de los motivos que haya conducido al legislador a mantener la redacción anterior de este precepto. Sin embargo, los límites de la espiritualización exigen ser concretados, puesto que, lo contrario, podría

[32] CASTIÑEIRA PALOU / ESTRADA I CUADRAS, en: SILVA SANCHEZ (Dir.), RAGUÉS I VALLÈS (Coord.), *Lecciones de Derecho Penal. Parte Especial*, 2015, pág. 155.
[33] *Ibidem*, pág. 155.
[34] SAP Cádiz 191/2017, de 1 de septiembre de 2017, FJ 5º.

conducir a extremos ilógicos[35]. En virtud de ello, es preciso exponer algunos supuestos en que el grado de espiritualización del apoderamiento exige ser mayor o menor en función de las circunstancias en que la conducta se desarrolle.

En primer lugar, hemos de hacer referencia a la tipicidad de aquellas conductas en que se produzca la aprehensión de un documento o efecto personal recibido por error, por ejemplo, la retención de una carta por parte de aquel que no fuere su destinatario. En estos casos si bien, el sujeto activo no realiza la traslación física de la cosa, la conducta habría de ser considerada típica siempre que realizare una conducta positiva, tendente a retener aquello recibido por error bajo su dominio[36]. No obstante, cabe la exclusión del dolo si la apertura y la consiguiente aprehensión, se ha producido por error, lo cual sería aplicable tanto a comunicaciones postales como telemáticas[37]. En este sentido, Romeo Casabona[38] estima que no sería típica la comisión por omisión.

En segundo lugar, deben precisarse aquellos supuestos en que el sujeto activo acceda al contenido de un papel, carta, correo electrónico, documento o efecto personal, sin realizar una conducta de apoderamiento sobre el soporte en el que tales se hallen. Esta conducta diferirá en función de si el sujeto activo, para acceder al contenido, ha debido realizar una acción tendente a remover algún obstáculo o ninguno. Tales obstáculos podrían consistir, por ejemplo, en extraer de un sobre abierto una carta para volver a dejarlo dentro del mismo, o incluso, encender la pantalla de un ordenador para acceder a los correos electrónicos, y apagarla tras leer los mismos. Ante tales hechos, se considera que el ámbito de la espiritualización se amplía, resultando típicos aquellos supuestos en que el sujeto activo realiza una conducta tendente a remover determinado impedimento

[35] ROMEO CASABONA, en: Derecho y conocimiento, vol. 2, 2002, pág. 131: "*uno de los problemas más importantes radica en decidir hasta qué grado es admisible tal espiritualización sin que suponga un desvío no permitido del principio de legalidad de los delitos (analogía in malam partem*)".
[36] GÓNZALEZ CUSSAC, en: GÓNZALEZ CUSSAC (Coord.), *Derecho Penal Parte Especial*, 2016, pág. 276: "*Se consuma el delito con el mero apoderamiento para descubrir, y por tal ha entendido la jurisprudencia la aprehensión u obtención ilícita, así como también la retención de lo recibido por error. Es indiferente el fin último perseguido por el autor, incluido su voluntad de presentarlo en un juicio*".
[37] STS 358/2007, de 30 de abril de 2007.
[38] ROMEO CASABONA, en: Derecho y conocimiento, vol. 2, 2002, pág. 132.

para acceder al contenido[39] y [40]. En función de ello, habrá de analizarse si el sujeto pasivo dispuso de alguna medida, sobre sus efectos, que impidiera el conocimiento a terceros.

Distintas serían aquellas conductas en que el sujeto activo no ha realizado acción alguna tendente a eliminar obstáculos[41], accediendo directamente al contenido como, por ejemplo, mediante la visualización o aprehensión intelectual del contenido de un documento depositado sobre una mesa o que se encontrase en la misma pantalla de un ordenador encendido. En virtud de ello, la determinación de tipicidad precisaría una espiritualización mayor sobre la conducta, pudiendo provocar una desmaterialización del tipo excesiva[42].

iii. Objeto material y bien jurídico protegido.

El siguiente elemento del tipo objetivo que debemos analizar, es el objeto material del delito, entendido éste como la persona o cosa sobre la que recae la conducta del sujeto activo. En este caso el art. 197.1, en su primer inciso, incluye los papeles, cartas, mensajes de correo electrónico, así como también otros documentos o efectos personales. De este modo, el legislador realiza una enumeración de los posibles objetos de apoderamiento, incluyendo una clausula general, en la que puede incluirse cualquier clase de objeto.

El significado de algunos de estos objetos materiales, han sido precisados por la doctrina. En primer lugar, dentro del término carta se incluirá cualquier comunicación escrita, que se encuentre cerrada y disponga de un destinatario concreto y determinado, disponiendo además de un contenido personal, que transmita ideas, sentimientos, propósitos o noticias[43]. En lo que respecta a los papeles, estos han de entenderse en sentido amplio, sin la exigencia de ningún requisito específico. Por otra parte, en cuanto a los correos electrónicos Romeo Casabona otorga una definición que, a efectos penales,

[39] *Ibidem,* pág. 132: "*La jurisprudencia ha matizado, respecto a los supuestos de cartas remitidas a un destinatario equivocado por correo postal, que no basta con la simple inactividad o pasividad respecto a la retención, pues en coherencia con el sentido de la palabra apoderamiento es necesaria una acción positiva por parte de quien recibe la cosa para que ésta quede bajo su dominio"*.
[40] En sentido contrario: MUÑOZ CONDE, en: *Derecho Penal. Parte Especial*, 2015, pág. 235 "*difícilmente pueden incluirse en este apartado la simple lectura de mensajes electrónicos o SMS, dándole a la tecla correspondiente".*
[41] Un ejemplo de ello, sería la STS 487/2011, de 30 de mayo, en la cual se absuelve a un hombre que obtiene una escritura perteneciente a su mujer (en procedimiento de divorcio), de la notaria en la que se hallaba dicho documento, sin remover obstáculo alguno.
[42] ROMEO CASABONA, en: Derecho y conocimiento, vol. 2, 2002, pág. 134.
[43] GÓNZALEZ CUSSAC, en: GÓNZALEZ CUSSAC (Coord.), *Derecho Penal Parte Especial*, 2016, pág. 277.

ha de entenderse como "*modalidad de comunicación, por lo general de carácter personal, que incorpora texto, voz, sonido o imagen y que se sirve de las redes telemáticas como tecnología de transmisión y de los sistemas informáticos (ordenadores y el software o sistema lógico correspondiente) como instrumentos de remisión y de recepción entre dos o más comunicantes y, en su caso, de almacenamiento de los mensajes*"[44].

En atención a la redacción empleada por el legislador, resulta complejo establecer los límites a la expresión "*cualesquiera otros documentos o efectos personales*". En primer lugar, la definición de documento la otorga el propio CP, en su art. 26, entendiendo por tal: "*…todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica"*, ello permite una mejor comprensión y delimitación de dicho objeto material. Sin embargo, la concreción de los efectos personales plantea mayores dificultades, entendiendo algunos autores que abarcará cualquier objeto de uso personal, cuyo apoderamiento permita identificar al titular de la intimidad[45].

En atención a la variabilidad del que pudiera ser objeto material del presente delito, se exige que, con independencia del soporte en que se hallen, su contenido afecte a un hecho secreto o a la intimidad de la víctima[46]. Sin embargo, no es imprescindible que la información disponga de un contenido secreto, y ello en virtud de que lo secreto no dispone de autonomía con respecto a la intimidad, que es el bien jurídico protegido[47].

En este sentido, la jurisprudencia señala que este tipo básico protege el derecho fundamental a la intimidad personal (art. 18.1 CE), y de forma aún más específica, el derecho al secreto de las comunicaciones (art 18.3 CE). El TS establece que: "*el art.*

[44] ROMEO CASABONA, en: Derecho y conocimiento, vol. 2, 2002, pág. 129.
[45] En este sentido:
- JORGE BARREIRO, en: Revista jurídica de la Universidad Autónoma de Madrid, núm. 6, 2002, pág. 103.
- GÓNZALEZ CUSSAC, en: GÓNZALEZ CUSSAC (Coord.), *Derecho Penal Parte Especial*, 2016, pág. 277: "*Por ejemplo el equipaje (STS 20 de octubre de 1997); carta de la Seguridad Social (STS 23 de octubre de 2000); agenda y documentos de un abogado (STS 14 de septiembre de 2000)".*

[46] ROMEO CASABONA, en: Derecho y conocimiento, vol. 2, 2002, pág. 128: *"Todos estos objetos se caracterizan por consistir en soportes físicos con capacidad para recoger, incorporar o reproducir hechos, datos, manifestaciones de voluntad, etc. que constituyan un secreto para alguien y afecten a su intimidad o que sin ser secreto involucre a dicha intimidad*".
[47] ANARTE BORRALLO / DOVAL PAIS, en: BOIX REIG (Dir.), *Derecho Penal. Parte Especial*, 2010, pág. 448, "*…los papeles, cartas, mensajes de correo electrónico, documentos o efectos personales de los que el sujeto activo se apodere, deben estar en condiciones de incorporar elementos vinculados (o, al menos vinculables), con la intimidad".*

197.1, tutela dos distintos bienes que son objeto de la protección jurídico penal: la salvaguarda de los secretos propiamente dichos y, aparte, la intimidad de las personas (…) en el caso presente, la conducta típica no se proyecta sobre ningún "secreto" de la víctima, toda vez que la información que contenía la carta de que se apoderó la acusada no es susceptible de ser calificada como tal, en cuanto el secreto supone el conocimiento de ciertos datos relativos a un objeto concreto, por un número limitado de personas y que, por diversas razones, no es conveniente que se amplíe el círculo de quienes poseen tales conocimientos, pero sí opera sobre la otra alternativa sancionada penalmente cual es la agresión a la intimidad mediante la invasión del ámbito de la privacidad representada por la correspondencia personal de la que se apodera el sujeto activo del delito, tomando ilícito conocimiento y posesión de informaciones de naturaleza económica de interés dirigidas a otra persona y posteriormente utilizadas en beneficio y utilidad propios, lo que, sin duda alguna, constituye la segunda de las acciones típicas sancionadas por el legislador"[48].

No obstante, atendiendo a pronunciamientos más recientes, podemos observar que lo secreto, es entendido como un aspecto que forma parte de la intimidad, pues: *"la idea de secreto en el art. 197, 1º CP resulta conceptualmente indisociable de la de intimidad: ese «ámbito propio y reservado frente a la acción y el conocimiento de los demás» (SSTC 73/1982 y 57/1994 entre muchas)"*[49]. En igual sentido, se ha precisado que, "*El bien jurídico protegido es la intimidad individual. Aunque la idea de secreto puede ser más amplia, como conocimientos solo al alcance de unos pocos, en realidad deben estar vinculados precisamente a la intimidad pues esa es la finalidad protectora del tipo"*[50]. Estos pronunciamientos devienen lógicos, en cuanto que la figura no exige que el objeto material afecte a una comunicación (la cual entraría en el contenido del derecho al secreto de las comunicaciones), ya que los mismos pueden recaer sobre papeles que contengan pensamientos del sujeto pasivo, como sería un diario, en los cuales no existiría una comunicación propiamente dicha.

[48] STS 1641/2000, de 23 de octubre, FJ 2º.
[49] STS 666/2006, de 19 de junio, FJ 4º.
[50] STS 358/2007, 30 de abril, FJ 1º.

iv. Consentimiento y autorización.

La propia redacción excluye la tipicidad de aquellas conductas en que, produciéndose un apoderamiento, exista consentimiento por parte del sujeto pasivo.

En este punto, hemos de remitirnos al apartado relativo al bien jurídico protegido por el delito, concretamente el referente a la titularidad del derecho fundamental a la intimidad. Como indicamos, la intimidad personal y familiar abarca no solo aspectos de la vida de la persona sino, además, aquellos aspectos de la vida con otras personas respecto a las cuales exista una especial vinculación (como en su caso, sería la familia). Hacer referencia a ello resulta importante, puesto que la existencia de una dimensión familiar de la intimidad no puede ser considerada como autorización para que se produzca una lesión sobre el derecho fundamental a la intimidad. Este es un derecho personalísimo que, en atención a la jurisprudencia del TS[51], no es susceptible de ser compartido, y que por tanto no puede considerarse renunciado en aquellos casos en que exista una especial vinculación o vida en común (como serían las relaciones paterno-filiales, matrimoniales, convivencia, contractuales, etc.).

Asimismo, con respecto a las personas de relevancia pública, habríamos de remitirnos al mismo apartado mencionado, en el cual se precisó que la proyección pública de una persona no implica una autorización que permita atentar contra su derecho fundamental a la intimidad.

3.1.2. Tipo subjetivo.

Con respecto al tipo subjetivo de la presente figura, éste se encuentra integrado por el dolo, el cual ha de comprender todos los elementos objetivos del tipo que anteriormente hemos enumerado. Además de ello, es exigible que, junto al dolo de apoderarse de los documentos o efectos personales de la víctima (debiendo en algunos casos realizarse una interpretación espiritualizada), concurra además un elemento subjetivo de lo injusto, que consistirá en el ánimo del sujeto activo en descubrir determinado secreto o vulnerar la intimidad de la víctima, resultando éste un elemento esencial del presente tipo del delito.

[51] SSTS 872/2001, de 14 de mayo, 694/2003, de 20 de junio, y 1219/2004, de 10 de diciembre.

A tal respecto, conviene indicar que, no resulta imprescindible para determinar la tipicidad del delito, que efectivamente se produzca el resultado, que se desposea a la víctima de los documentos o efectos personales, o que se produzca una revelación de la información obtenida (esta última modalidad dispone de su propia regulación en el art. 197.3, que estudiaremos con posterioridad). En virtud de tal estructura, este delito se hallaría inserto entre los delitos mutilados en dos actos[52], que a su vez pertenece a la categoría de los delitos de intención, ello quiere decir que la consumación del delito se produce con la simple conducta de apoderamiento, dirigida al conocimiento de un secreto o a la lesión de la intimidad, sin necesidad de que se materialicen las consecuencias. En este sentido, se pronuncia el TS[53], disponiendo que: "*Respecto al "iter criminis", es una figura delictiva que se integra en la categoría de los delitos de intención, y en la modalidad de delito mutilado de dos actos, uno de apoderamiento, interceptación o utilización de artificios técnicos, unido a un elemento subjetivo adicional al dolo, consistente en el ánimo de realizar un acto posterior, descubrir el secreto, o vulnerar la intimidad de otro, sin necesidad de que éste llegue a producirse"*.

3.2. Delito de interceptación de telecomunicaciones, y utilización de medios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen, o de cualquier otra señal de comunicación (art. 197.1, segundo inciso).

"…intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses".

En la actualidad, podemos observar como la multiplicidad de instrumentos a través de los cuales las personas pueden comunicarse (teléfono, fax, mensajería instantánea, redes sociales), conlleva el surgimiento de nuevas formas de ataque sobre el derecho a la intimidad. Ello, podemos considerar que ha conllevado al legislador a optar por mantener las figuras básicas contenidas en el segundo inciso del art. 197.1, el cual establece la tipicidad de aquellos comportamientos de interceptación de las comunicaciones y de utilización de medios técnicos de escucha, transmisión, grabación o

[52] GÓNZALEZ CUSSAC, en: GÓNZALEZ CUSSAC (Coord.), *Derecho Penal Parte Especial*, 2016, pág. 276.
[53] STS 1219/2004, de 10 de diciembre, FJ 7º.

reproducción del sonido o de la imagen, así como cualquier otra señal de comunicación, que se lleven a cabo con la finalidad de descubrir los secretos o vulnerar la intimidad de otra persona.

Es preciso señalar que esta figura dispone de las mismas penas que el tipo penal anterior, no obstante, tal equiparación ha sido criticada por algunos autores en función de la mayor gravedad objetiva que supone la conducta descrita en el segundo inciso del art. 197.1, considerando que el uso de medios técnicos plantea una mayor peligrosidad sobre el derecho fundamental a la intimidad, pues reduce las posibilidades de que la víctima se percate[54].

3.2.1. Tipo objetivo.

i. Sujeto activo y pasivo.

Respecto a los sujetos activo y pasivo del presente tipo hemos de precisar que éstos coinciden con los concernientes a la modalidad delictiva anterior, por lo que no volveremos a reiterarlos.

ii. Conducta típica.

En cuanto a la acción típica, se regula en primer lugar, aquella conducta de interceptación de las comunicaciones de un tercero. En este sentido, la acción de interceptación, como indica Romeo Casabona[55], implica interferir en la telecomunicación de otro, entendida ésta como una forma de comunicación a distancia, que puede ser realizada a través de cualquier medio (teléfono, telefax, red, etc.), no resultando precisa su obstaculización; dicho en otras palabras, supone la captación de cualquier transmisión, emisión o recepción de signos, señales, imágenes, sonidos o información sea cual fuere su naturaleza, con independencia del medio a través del cual se efectúen. En relación a ello, González Cussac[56] matiza que la telecomunicación ha de realizarse a través de un canal cerrado.

[54] GONZÁLEZ COLLANTES, en: Revista de Derecho Penal y Criminología Universidad Nacional de Educación a Distancia, núm. 13, 2015, pág. 52.
[55] ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, pág. 259.
[56] GÓNZALEZ CUSSAC, en: GÓNZALEZ CUSSAC (Coord.), *Derecho Penal Parte Especial*, 2016, pág. 278.

Por otra parte, respecto a la conducta de empleo de medios técnicos han de entenderse excluidos los medios naturales que componen los sentidos de la persona, resultando atípica la conducta de aquel que, pese a hallarse oculto, no emplee ningún medio técnico para escuchar la conversación mantenida por un tercero. Los medios empleados en esta conducta han de ser susceptibles de facilitar la escucha, o permitir la transmisión, grabación o reproducción del sonido (con independencia de si son conversaciones descifrables, o si por ejemplo se hallaren encriptadas) o de la imagen, o de otra señal de la comunicación. Es importante señalar, que el mantenimiento en la redacción de "cualquier otra señal de la comunicación", como precisaron algunos autores[57] con anterioridad a la Reforma de 2015, se debe a que el legislador pretende abarcar aquellas innovaciones tecnológicas que pudieran producirse, subsanando de este modo las posibles lagunas de punibilidad, consecuencia del desarrollo en la tecnología.

Po otra parte, si bien, la interceptación de las comunicaciones y la utilización de medios técnicos resultan conductas diferenciadas, en determinados supuestos ha de apreciarse que únicamente concurre un único delito, con independencia de los diversos comportamientos que el sujeto activo realice, un ejemplo de ello sería la captación de una conversación mantenida por un tercero, a través de un artificio técnico que permita la escucha o grabación. En este sentido, es preciso que exista una misma unidad de acto, y que la conducta afecte a la misma persona[58].

Con respecto a la consumación de este tipo básico, el TSestima que: "*El artículo 197 del Código Penal, contiene varias conductas en una compleja redacción. (…) Se trata de conductas distintas que no precisan que el autor llegue a alcanzar la finalidad perseguida. En los dos primeros casos requiere sin embargo un acto de apoderamiento o de interceptación efectivos, mientras que en el supuesto de utilización de artificios basta con la creación del peligro que supone su empleo con las finalidades expresadas para la consumación de la infracción penal*." [59]. De lo anterior, podemos observar la clara distinción entre la conducta de interceptación de las comunicaciones, cuya consumación

[57] En este sentido:
- JORGE BARREIRO, en: Revista jurídica de la Universidad Autónoma de Madrid, núm. 6, 2002, pág. 105.
- BARRIO ANDRÉS, en: *Ciberdelitos: Amenazas criminales del ciberespacio*, 2017, pág. 63.

[58] ANARTE BORRALLO / DOVAL PAIS, en: BOIX REIG (Dir.), *Derecho Penal. Parte Especial*, 2010, pág. 451.

[59] STS 358/2007, 30 de abril., FJ 1º.

exige que se produzca una efectiva captación de la comunicación perteneciente a un tercero, y la conducta de utilización de artificios técnicos, que por su parte se consuma con el empleo de los mismos. Sin embargo, no se concreta en dicha Sentencia que ha de entenderse por "empleo" de los medios técnicos.

En relación a ello, la doctrina se encuentra dividida respecto a qué circunstancias supondrían la consumación de la conducta de utilización de instrumentos técnicos. En este sentido, se ha precisado que la mera instalación de los medios o artíficos técnicos no produce la consumación, sino que se requiere la realización de alguna actuación adicional, no existiendo unanimidad respecto a qué hechos (añadidos a la instalación) comportan su consumación. En primer lugar, un sector de la doctrina[60] exige que, junto a la instalación de los medios técnicos, se produzca una efectiva captación (aún mínima) de sonido, imagen o cualquier otra señal de comunicación. Por otra parte, otros autores[61] estiman que, junto a la instalación de los instrumentos técnicos, han de activarse o poner en disposición técnica los mismos, no siendo preciso la captación de algún sonido o imagen.

El TS se ha pronunciado al respecto, determinando que: "*Lo relevante es que se trata de un delito en cualquiera de sus versiones que no precisa para su consumación el efectivo descubrimiento del secreto o en el presente caso de la intimidad del sujeto pasivo, pues basta la utilización del sistema de grabación o reproducción del sonido o de la imagen (elemento objetivo) junto con la finalidad señalada en el precepto de descubrir los secretos o vulnerar la intimidad (elemento subjetivo), es decir, en el presente caso el tipo básico se consuma por el sólo hecho de la captación de las imágenes del denunciante con la finalidad de vulnerar su intimidad. Por ello se le ha calificado como delito intencional de resultado cortado cuyo agotamiento tendría lugar, lo que da lugar a un tipo compuesto, si dichas imágenes se difunden, revelan o ceden a terceros, supuesto agravado previsto en el apartado 3º.1 del mismo precepto, lo que conlleva la realización previa del tipo básico.*" [62].

[60] MUÑOZ CONDE, en: *Derecho Penal. Parte Especial*, 2015, pág. 236.
CASTIÑEIRA PALOU / ESTRADA I CUADRAS, en: SILVA SANCHEZ (Dir.), RAGUÉS I VALLÈS (Coord.), *Lecciones de Derecho Penal. Parte Especial*, 2015, pág. 156-157.
[61] ANARTE BORRALLO / DOVAL PAIS, en: BOIX REIG (Dir.), *Derecho Penal. Parte Especial*, 2010, pág. 450.
[62] STS 1045/2011, 14 de octubre, FJ 9º.

En virtud de lo expuesto, podemos concluir que la consumación de este tipo básico se produce con la efectiva utilización de los artificios técnicos, es decir, no basta la puesta en marcha de los dispositivos, sino que se requiere además una efectiva escucha, transmisión, grabación o reproducción de sonido o imagen, o cualquier otra señal de la comunicación. Por tanto, la imposibilidad en la grabación podrá suponer una tentativa de delito. Además de ello, conviene precisar que, en principio, resultarían penalmente irrelevantes aquellas conductas de grabación clandestina de imágenes producidas en lugares públicos, las cuales podrán resolverse a través de la vía civil[63].

Por otra parte, al igual que el tipo básico anterior, esta figura se halla entre los delitos mutilados en dos actos que, como indicamos, su consumación no exige la producción de una efectiva vulneración de la intimidad o descubrimiento de secretos.

iii. Objeto material y bien jurídico protegido.

En primer lugar, respecto a la conducta de interceptación de comunicaciones, el objeto material de la conducta recaerá sobre las telecomunicaciones de un tercero, entendidas como "*Toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos"*[64]. En virtud de ello, el objeto material se encuentra constituido por comunicaciones a distancia, con independencia del medio a través del cual se realicen, pues podrán ser medios que dispongan de cable (teléfono fijo), o que por el contrario sean inalámbricos (teléfono móvil, radio), que se produzcan por medio de ondas radioeléctricas o por vía satélite. Asimismo, las comunicaciones podrán ser de diversa índole, pudiendo ser orales, por signos, escritas, incluso hallarse encriptadas, resultando indiferente que las mismas se produzcan de forma diferida o simultánea[65], resultando preciso, por el contrario, que se realicen por un canal cerrado.

En lo que respecta a la conducta de empleo de artificios técnicos de escucha, transmisión, grabación o reproducción, el objeto material del tipo recae sobre los sonidos, imágenes u otras señales de la comunicación que se obtengan por medio de aquellos.

---

[63] JORGE BARREIRO, en: Revista jurídica de la Universidad Autónoma de Madrid, núm. 6, 2002, pág. 105.
[64] Definición otorgada por la Constitución de la Unión Internacional de Telecomunicaciones, núm. 1012 del Anexo.
[65] ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, pág. 259.

En este punto, hemos de precisar el bien jurídico protegido, en relación a la interceptación de las comunicaciones, es el secreto de las comunicaciones (art. 18.3 CE), entendido éste como una expresión concreta del derecho a la intimidad personal y familiar, disponiendo, no obstante, de un carácter fundamental y autónomo. El derecho al secreto de las comunicaciones protege no solo la libertad de las comunicaciones y su reserva, sino aspectos como la identidad de los interlocutores. Además de ello, el término "secreto" dispone de un carácter formal, lo cual quiere decir que se predica de lo comunicado, con independencia de si el contenido afecta o no a un ámbito íntimo de la persona[66].

Por otra parte, la conducta de utilización de artificios técnicos tutela un ámbito más amplio, que es el derecho a la intimidad (art. 18.1 CE), ya que la acción típica no exige que el objeto material recaiga estrictamente sobre las comunicaciones.

Es preciso indicar que, si bien el empleo de medios técnicos pudiera afectar a imágenes, el bien jurídico protegido no sería el derecho a la propia imagen, sino el derecho a la intimidad personal y familiar. Tal y como indicamos con anterioridad en este trabajo, ambos son derechos fundamentales que gozan de carácter autónomo, disponiendo de un contenido diferenciado que en ocasiones podrá hallarse interrelacionado. En este sentido, el TC, dispone que: "*No cabe desconocer que mediante la captación y publicación de la imagen de una persona puede vulnerarse tanto su derecho al honor como su derecho a la intimidad. Sin embargo, lo específico del derecho a la propia imagen es la protección frente a las reproducciones de la misma que, afectando a la esfera personal de su titular, no lesionan su buen nombre ni dan a conocer su vida íntima. El derecho a la propia imagen pretende salvaguardar un ámbito propio y reservado, aunque no íntimo, frente a la acción y conocimiento de los demás; (…) Ese bien jurídico se salvaguarda reconociendo la facultad para evitar la difusión incondicionada de su aspecto físico, ya que constituye el primer elemento configurador de la esfera personal de todo individuo, en cuanto instrumento básico de identificación y proyección exterior y factor imprescindible para su propio reconocimiento como sujeto individual (SSTC 231/1988, de 2 de diciembre, FJ 3, y 99/1994, de 11 de abril, FJ 5)*" [67].

[66] SSTC 34/1996, de 11 de marzo, FJ 4º; 114/1984, de 29 de noviembre, FJ 7º; 123/2002, de 20 de mayo FJ 4º.
[67] STC 81/2001, de 26 de marzo, FJ 2º.

En relación a lo anterior, hemos de precisar, que el presente tipo exige que la conducta del sujeto activo se halle encaminada a descubrir un secreto o vulnerar la intimidad de un tercero; por tanto, esta conexión con el ámbito de la intimidad, impide que el derecho fundamental a la propia imagen sea el bien jurídico protegido por este delito. En virtud de ello, la conducta de transmisión, grabación o reproducción que, recayendo sobre la imagen de una persona, no afectare a la intimidad, no resultaría encajable en el presente tipo.

iv. Consentimiento y autorización.

La propia redacción de la presente figura exige para determinar la tipicidad de la acción, que no medie consentimiento de aquel sobre el que recaiga la conducta. Al recogerse tal elemento en la propia formulación del tipo, en caso de mediar error sobre el consentimiento, éste será un error de tipo que habrá de resolverse a través del art. 14 CP[68] (lo cual también resultará de aplicación al tipo básico anterior).

En atención a ello, es preciso destacar un pronunciamiento del TC en el cual estableció que: "*No hay «secreto» para aquél a quien la comunicación se dirige, ni implica contravención de lo dispuesto en el art. 18.3 de la Constitución la retención, por cualquier medio, del contenido del mensaje. (…). Y es que tal imposición absoluta e indiferenciada del «secreto» no puede valer, siempre y en todo caso, para los comunicantes, de modo que pudieran considerarse actos previos a su contravención (previos al quebrantamiento de dicho secreto) los encaminados a la retención del mensaje. Sobre los comunicantes no pesa tal deber, sino, en todo caso, y ya en virtud de norma distinta a la recogida en el art. 18.3 de la Constitución, un posible «deber de reserva» que -de existir- tendría un contenido estrictamente material, en razón del cual fuese el contenido mismo de lo comunicado (un deber que derivaría, así del derecho a la intimidad reconocido en el art. 18.1 de la Norma fundamental).*" [69]. De conformidad con ello, puede inferirse que la perpetuación de lo comunicado por parte de uno de los partícipes (por ejemplo, mediante la grabación de una conversación mantenida, o guardando una conversación de WhatsApp), no resulta en sí misma ilegitima, aun cuando

[68] JORGE BARREIRO, en: Revista jurídica de la Universidad Autónoma de Madrid, núm. 6, 2002, pág. 106.
[69] STC 114/1984, 29 de noviembre, FJ 7º.

no exista consentimiento por parte del otro interlocutor, puesto que su obtención carece de los elementos que determinan la tipicidad de la conducta[70].

Además de ello, tampoco supondría una vulneración del secreto de las comunicaciones, aquella conducta en que un tercero interceptara la comunicación (de forma autorizada por alguno de los interlocutores), alcanzando a conocer el contenido de la misma[71]; sin embargo, si lo comunicado afectase a la esfera de intimidad del interlocutor (contenido material de la comunicación), la conducta podría constituir una violación del derecho a la intimidad personal y familiar (art. 18.1 CE). En atención a ello, un sector de la doctrina[72], estima que, tanto la conducta del participe en la conversación, como la del tercero que actúa de modo subrepticio, disponen de relevancia penal.

Distintas se plantean aquellas situaciones en que se produzca una captación de la imagen de un tercero, por parte de alguna persona que también forme parte de dicha escena. Como indicábamos con anterioridad, en estos casos se protege la intimidad en sentido estricto. Si bien pudiera parecer que el esquema lógico de esta conducta es coincidente con el expuesto, es importante señalar las diferencias entre uno y otro. En primer lugar, la tipicidad de la conducta de captación de la imagen exige que esta se realice por el sujeto activo sin autorización y con la finalidad de vulnerar la intimidad o descubrir los secretos de otro. En este sentido, la voluntad de transmitir un secreto (como en el anterior supuesto) o de mantener una relación íntima con otro, son conductas que plantean inherentemente el riesgo (que es asumido por la propia persona) de que tales hechos sean comunicados a terceros. No obstante, la grabación no autorizada de imágenes de carácter íntimo por uno de los intervinientes[73], no es una conducta que plantee en sí misma un riesgo asumible por aquel que es filmado de modo subrepticio; la perpetuidad y veracidad que otorga una imagen, plantea una indefensión y un peligro sobre el derecho a la intimidad superior al que plantearía la divulgación verbal del hecho.

[70] CASTIÑEIRA PALOU / ESTRADA I CUADRAS, en: SILVA SANCHEZ (Dir.), RAGUÉS I VALLÈS (Coord.), *Lecciones de Derecho Penal. Parte Especial*, 2015, pág. 157.
[71] STC 114/1984, 29 de noviembre, FJ 7º: "*quien entrega a otro la carta recibida o quien emplea durante su conversación telefónica un aparato amplificador de la voz que permite captar aquella conversación a otras personas presentes no está violando el secreto de las comunicaciones*"
[72] JUANATEY DORADO en: BOIX REIG (Dir.), JAREÑO LEAL (Coord.), *La protección jurídica de la intimidad*, 2010, pág. 142.
[73] En este sentido, SAP Cáceres, 227/2011, de 20 de junio, en ella se condena a un hombre por grabar una relación sexual de la cual es parte.

3.2.2. Tipo subjetivo.

Al igual que en el anterior tipo básico de descubrimiento de secretos documentales, se exige que el sujeto activo actué con dolo, de forma voluntaria y consciente, debiendo concurrir además el tipo subjetivo, que implica la voluntad de vulnerar la intimidad o conocer un secreto de la víctima.

3.2.3. Causas de justificación.

La ubicación de este apartado en el presente trabajo, no es aleatoria, si bien pudieron ser referidas en el anterior tipo básico, éstas adquieren una mayor relevancia en relación a la presente conducta.

Respecto a las conductas contenidas en el art. 197.1 CP, resultan complejas las causas de justificación, como son aquellas en que el sujeto activo obre en deber o en ejercicio legítimo de un derecho, oficio o cargo, de conformidad con el art. 20.7 CP.

Dentro del ámbito penal, algunas causas de justificación que en primer lugar hemos de referir son las contenidas en los arts. 579 y ss. Lecrim, relativas a la intervención mediante autorización judicial de la correspondencia privada, postal o telegráfica, y las comunicaciones telefónicas o telemáticas[74].

En relación a ello, resulta destacable la reciente STEDH[75], en el asunto Trabajo Rueda c. España. En ella se analizó la conducta policial de acceso al contenido de un ordenador realizada, ante la posible comisión de un delito, sin autorización judicial. Si bien, el Gobierno español fundamentó tal conducta en motivos de urgencia y necesidad, dado el riesgo eventual que suponía la desaparición de los ficheros de contenido pedófilo y pornográfico hallados en el ordenador, el TEDH concluyó negando que existiera riesgo alguno de desaparición, en virtud de que el ordenador se hallaba intervenido y retenido por la policía, no disponiendo el mismo de conexión a Internet. En consecuencia, se resolvió declarando tal intervención policial como una violación del art. 8 del CEDH. Este pronunciamiento es importante, puesto que, se observa como el derecho a la

[74] En idéntico sentido se plantean las medidas establecidas en el art. 51.5 de la LGP, que facultan al Director del establecimiento penitenciario a suspender o intervenir las comunicaciones orales o escritas previstas en el mismo artículo, de forma motivada y dando cuenta a la autoridad judicial competente.
[75] STEDH de 30 de mayo, asunto Trabajo Rueda c. España.

intimidad únicamente habrá de ceder ante razones que se hallen suficientemente motivadas, para lo cual es preciso realizar un juicio de proporcionalidad.

Otra de las posibles causas de justificación que se plantea en relación a este tipo, y que ha motivado grandes debates, sería el ejercicio legítimo del derecho fundamental a comunicar o recibir libremente información veraz a través de cualquier medio de difusión (art. 20.1 d) CE). En atención a la colisión de tal derecho con el derecho a la intimidad familiar y personal, se ha desarrollado una reiterada doctrina por parte del TC[76], que ha optado por otorgar una posición preferente de la libertad de información frente al derecho a la intimidad, en base a que aquella es garantía de la opinión pública libre y del principio de legitimidad democrática[77]. Concretamente la STC 173/1995[78], afirmó que "*únicamente aquellas sociedades que pueden recibir informaciones veraces y opiniones diversas de cuanto constituyen los aspectos más importantes de la vida comunitaria, están en condiciones de ejercitar, después, sus derechos y cumplir sus deberes como ciudadanas, partiendo del principio esencial de que la soberanía nacional reside en el pueblo, del que emanan los poderes del Estado*". En consecuencia, si bien existe una posición preferente del derecho a comunicar o recibir libremente información veraz, frente a los derechos de la personalidad (como son el honor, la intimidad o la propia imagen), el sacrificio de éstos atenderá a la trascendencia y el interés público que tal información comporte para la sociedad, entendiendo que la misma es garantía de una sociedad democrática y libre.

En último lugar, y brevemente, hemos de hacer referencia a las causas de justificación de aquellas conductas de los padres o tutores, respecto de los hijos menores a su cargo. En este sentido, se considerarán justificados, aquellos comportamientos llevados a cabo con la finalidad de educar o formar a los menores, pues en tales casos se entiende que se actúa en atención a su interés y no con intención de vulnerar su intimidad (ello de conformidad con los arts. 154 y 268 C.c.)[79].

[76] SSTC 171/1990, 12 de noviembre.; 172/1990, de 12 de noviembre; 197/1991, 17 de octubre.
[77] JORGE BARREIRO, en: Revista jurídica de la Universidad Autónoma de Madrid, núm. 6, 2002, pág. 109.
[78] STC 173/1995, de 21 de noviembre, FJ 2º.
[79] El reciente AAP de Pontevedra 893/2017, de 25 de octubre, se ha pronunciado respecto a este tema.

3.3. Delito de descubrimiento de datos reservados de carácter personal o familiar (art. 197.2).

"2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero".

El art. 197.2 contiene el tercer tipo básico, el cual, al igual que los dos tipos anteriormente expuestos, no ha visto modificada su redacción tras la Reforma del CP. En relación al mismo, cabe señalar que dispone de un distinto bien jurídico protegido no siendo ya la intimidad personal y familiar, sino el derecho a la autodeterminación informativa o libertad informática reconocido en el art. 18.4 CE.

En cuanto a la redacción empleada por el legislador, conviene indicar que ésta ha sido objeto de numerosas críticas tanto por la doctrina[80] como por la jurisprudencia[81], dada la complejidad que plantea su interpretación, y la reiteración en los términos empleados (concretamente, en el primer inciso se emplean los verbos "apoderar", "utilizar", y "modificar", mientras que en el segundo se utilizan "acceder", "alterar" y "utilizar", que resultan similares e incluso idénticos a los anteriores). Además de ello, el esquema utilizado para cada una de las conductas genera aún mayores complejidades, puesto que el primer inciso exige que se actúe "en perjuicio de tercero", planteándose en el segundo inciso dos conductas alternativas, esto es, el sujeto activo podrá actuar "en perjuicio del titular de los datos" o "de un tercero".

De otra parte, también se ha cuestionado este tipo básico en virtud de la tutela civil y administrativa existente en relación a los datos de carácter personal y familiar, y en atención a los principios de mínima intervención y *ultima ratio* del Derecho Penal. Como

[80] ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, págs. 261 y ss.
JORGE BARREIRO, en: Revista jurídica de la Universidad Autónoma de Madrid, núm. 6, 2002, pág. 117.
GONZÁLEZ COLLANTES, en: Revista de Derecho Penal y Criminología Universidad Nacional de Educación a Distancia, núm. 13, 2015, pág. 60.
[81] STS 234/1999, 18 de febrero de 1999, SSAP Madrid 115/1999, de 15 de abril; 269/1999, de 19 de junio; Zaragoza 106/2000, de 10 de marzo.

consecuencia de ello, han surgido dificultades en cuanto a la delimitación de los ilícitos penales y los hechos sancionables administrativamente[82].

3.3.1. Tipo objetivo.

i. Sujetos activo y pasivo.

El sujeto activo del presente tipo, podrá ser cualquier persona física o jurídica que, careciendo de autorización, realice cualquiera de las conductas descritas en el art. 197.2 CP.

En lo referente al sujeto pasivo, será aquel titular de los datos reservados de carácter personal o familiar; asimismo, de conformidad con el art. 200 CP, las personas jurídicas también podrán resultar ofendidas por el presente tipo.

En este punto, y en atención a la redacción empleada por el art. 197.2 CP, resulta conveniente señalar la distinción entre el sujeto pasivo, que es aquella persona sobre la que recae la conducta típica del sujeto activo, provocando una lesión o puesta en peligro de sus bienes jurídicos, y la persona perjudicada por el delito, que es aquella que sufre un daño derivado del delito, entendido éste no como un mal ínsito en el propio delito, sino como mera consecuencia de la conducta ilícita.

ii. Conducta típica.

En lo que respecta a la acción típica del presente tipo básico hemos de distinguir las conductas contenidas en el mismo: en primer lugar, se situaría la conducta no autorizada y en perjuicio de tercero, de apoderamiento, utilización o modificación de los datos personales de carácter personal o familiar de otro, registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en otro tipo de archivo o registro público o privado; en el segundo inciso se castigaría, el acceso no autorizado y por cualquier medio a los mismos (no concretándose si la referencia es respecto a los datos reservados o respecto a los ficheros o soportes, tema sobre el que trataremos a continuación); tipificando en último lugar la alteración o utilización en perjuicio del titular de los datos o de un tercero.

[82] BARRIO ANDRÉS, en: *Ciberdelitos: Amenazas criminales del ciberespacio*, 2017, pág. 79.

El primer problema que se plantea, en torno esta regulación, es la delimitación y diferenciación de las conductas en ella contenidas, dado el empleo de términos similares para la descripción del tipo. Como consecuencia de ello, existen en la doctrina posturas dispares respecto a su interpretación. En un principio, un sector[83] consideró que la diferencia entre ambos incisos radicaba en el distinto objeto material sobre el que habían de recaer las acciones típicas, entendiendo que las conductas contenidas en el primer inciso afectaban a los datos reservados, mientras que las conductas del segundo inciso venían referidas a los ficheros informáticos.

No obstante, la doctrina mayoritaria se ha decantado por considerar que el objeto material de ambas conductas es idéntico (los datos reservados de carácter personal), pues el bien jurídico protegido por este precepto es el derecho a la intimidad personal y familiar, y de forma más concreta, la libertad informática, considerando que la integridad de los ficheros automatizados no precisa de tal protección penal[84]. Asimismo, el TS ha precisado, que: "*El bien jurídico específico de este delito son los datos de carácter personal. Debe añadirse ahora que las conductas de "apoderarse" y "utilizar", así como las de "acceder" y "utilizar", que delimitan las acciones típicas en los tipos delictivos, suponen un atentado a los datos de carácter personal del sujeto pasivo, con independencia de que tengan o no carácter íntimo*". [85 y 86]

No obstante, tutelando ambos incisos un mismo objeto material, resulta complejo establecer una distinción entre las conductas contenidas. En virtud de ello, Romeo Casabona[87], considera que la diferencia viene determinada por la conducta de "acceso". Concretamente, estima que, al no incluirse en el primer inciso el acceso entre las conductas típicas (pues el tipo exige el apoderamiento, utilización o modificación), el sujeto activo actúa disponiendo de legitimación en el propio acceso a los datos reservados contenidos en el fichero (por ejemplo, siendo empleado del propio fichero). Esta

[83] GONZÁLEZ COLLANTES, en: Revista de Derecho Penal y Criminología Universidad Nacional de Educación a Distancia, núm. 13, 2015, pág. 60: "*Así lo entendieron Carbonell Mateu y González Cussac, y coincidieron con ellos Castiñeira Palou y también Polaino Navarrete. Éste último llegó a afirmar que de no ser así la alteración y la utilización se estarían tipificando dos veces y nos encontraríamos entonces ante una reiteración superflua de las conductas descritas en la enumeración recogida en el primer inciso".*
[84] GÓNZALEZ CUSSAC, en: GÓNZALEZ CUSSAC (Coord.), *Derecho Penal Parte Especial*, 2016, pág. 282.
[85] ATS 1945/2014, de 27 de noviembre, FJ 2º.
[86]En idéntico sentido: STS 525/2014, de 17 de junio; SAP Barcelona 219/2006, de 10 de marzo; SAP Madrid 115/1999, 15 de abril; SAP Madrid 269/1999,19 de junio.
[87] ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, págs. 262-263.

legitimación no concurriría, sin embargo, en el segundo inciso, que califica como típica la conducta de acceso, realizada sin autorización y con independencia del medio a través del cual se realice (pudiendo realizarse, por ejemplo, venciendo el sistema de seguridad o algún mecanismo lógico, etc.).

Asimismo, es preciso analizar cada una de las conductas típicas contenidas en este tipo. En primer lugar, el apoderamiento, como indicamos anteriormente, es aquella conducta de aprehensión o desplazamiento material a través del cual el sujeto activo pone bajo su poder o control el objeto material que, en este caso, son los datos reservados. Si entendemos que el sujeto activo que se apodera de los datos dispone de legitimación para acceder al fichero en que estos pudieran hallarse[88], la conducta de apoderamiento exigiría una aprehensión material de aquellos, mediante reproducción o copia, no bastando su captación intelectual, ya que la mera visualización podría realizarse mediante el acceso que, como indicamos, no constituye una conducta típica, al disponer el sujeto activo de legitimación.

Por otra parte, se considera que los términos modificación o alteración, empleados en el primer y segundo inciso respectivamente, albergan una conducta similar, entendiendo por tales, aquel cambio realizado sobre la realidad que reflejen aquellos datos reservados, provocando que los mismos dejen de resultar útiles u operativos para el fin al que se dirigiesen (pudiendo producirse un vaciamiento del contenido).

Respecto a la conducta de acceso[89], ésta implica la introducción no autorizada, del sujeto activo en el fichero o soporte informático, electrónico o telemático, o cualquier otro registro público o privado, en que se hallen contenidos los datos reservados. Como señalábamos anteriormente, el acceso podrá realizarse a través de cualquier medio, lo cual exige que se produzca el vencimiento de aquellas medidas de seguridad que disponga el sistema en que se hallen los datos reservados, debiendo el sujeto activo actuar sin mediación de otras personas (por ejemplo, a través de un tercero que le ceda tales datos, pues esta figura dispone de una regulación distinta a la expuesta en este apartado).

[88] *Ibidem*, pág. 263.
[89] *Ibidem*, pág. 263.

Por último, la conducta de utilización (empleada en ambos incisos) supone el uso de los datos reservados para una finalidad propia del sujeto activo, es decir implica un aprovechamiento de los mismos por parte del autor.

iii. Objeto material.

Como señalamos en el anterior apartado, las conductas típicas contenidas en esta modalidad han de recaer sobre los datos reservados de carácter personal y familiar, constituyendo éstos el objeto material del presente tipo y no, los ficheros o soportes en que se hallen. En relación a ello, hemos de precisar que el presente tipo exige que los datos sean reservados, de carácter personal o familiar, debiendo hallarse registrados en algún fichero o soporte informático, electrónico o telemático, o cualquier otro archivo o registro público o privado.

Respecto a la cualidad de "reservados", la doctrina[90] considera que tal término, ha de interpretarse como no susceptible de ser conocido o accesible a cualquiera, es decir, se excluye a los terceros ajenos al propio fichero en que se hallen los datos. En virtud de este sector, dicha cualidad resulta superflua e innecesaria, pues el precepto ya exige que la conducta típica se realice sin autorización, por lo que todo dato registrado en un fichero que exija autorización dispone ya de dicha cualidad de reservado.

En idéntico sentido se ha pronunciado el TS, enunciando que: "*el entendimiento más adecuado del carácter reservado de los datos es considerar que son tales los que no son susceptibles de ser conocidos por cualquiera. El precepto insiste en ello al aclarar por partida doble que el delito lo comete el que accede a los datos o los utiliza "sin estar autorizado", evidencia de que no son datos al alcance de cualquiera*" [91 y 92]. Por tanto, el término "reservado" implica que los datos sean de acceso o conocimiento limitado para aquellas personas ajenas al fichero en que aquellos se hallen registrados. En consecuencia, al no poder hallarse los datos al alcance de terceros, se hayan excluidas las fuentes accesibles al público u otros ficheros, archivos o registros, que no requieran autorización del interesado[93]. Por ende, dicha cualidad dispone de un contenido formal, en relación a

[90] GÓMEZ NAVAJAS, en: Revista jurídica de Castilla y León, núm. 16, 2008, pág. 340 y ss.
GÓNZALEZ CUSSAC, en: GÓNZALEZ CUSSAC (Coord.), *Derecho Penal Parte Especial*, 2016, págs. 280-281.
[91] STS 1328/2009, de 30 de diciembre, FJ 6º.
[92] En idéntico sentido: SSTS 1461/2001, de 11 de julio, 666/2006, 19 de junio, 358/2007, de 30 de abril.
[93] LOPD, art 3 j) Son fuentes accesibles al público*:" aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono*

la accesibilidad de los datos, y no material, ya que la vulnerabilidad de los datos o la afectación que sobre la intimidad pudieran provocar, no son elementos que precisen ser analizados en el presente tipo básico, pues éstos supuestos disponen de regulación propia (agravación contenida en el art. 197.5 CP).

Además de ello, se exige que los datos sean de "carácter personal o familiar". Para la determinación de su contenido es preciso acudir a la LOPD que, en su art. 3 a), dispone que son datos de carácter personal: "*cualquier información concerniente a personas físicas identificadas o identificables*". Si bien, tal regulación no otorga una definición de datos de carácter familiar habrá de entenderse como aquellos relacionados con la intimidad familiar. Por otra parte, respecto a las personas jurídicas, es preciso remitirnos a lo concretado respecto a la titularidad del derecho a la intimidad por parte de las mismas, debiendo añadir, que el propio legislador penal, por medio del art. 200 CP, establece que las personas jurídicas podrán ser sujeto pasivo de esta conducta.

Asimismo, es preciso concretar que los datos de carácter personal pueden ser de diversa índole, en este sentido, tendrán tal consideración los siguientes ejemplos: el lugar de trabajo o domicilio de la empresa, el número de afiliación de la Seguridad Social, domicilio, situación laboral, empleadora, domicilio social, u otros datos que permitan la identificación del trabajador o de sus ingresos en archivos de la Seguridad Social, antecedentes policiales, datos de los miembros de una asociación, datos relativos al domicilio, aun cuando éste resulte ser un hotel, aquellos cuyo contenido económico dispongan de trascendencia tributaria, o las hojas del Padrón Municipal de Habitantes.[94]

Conjuntamente, el tipo exige que los datos se hallen "*registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado*". Ello supone que los datos deban estar contenidos, recogidos o anotados en cualquier conjunto organizado, que se regirá a través de un sistema informático, electrónico o telemático, incluyéndose una clausula residual que permite que los datos se encuentren en otro tipo de archivo o registro público o privado. En relación

de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.".

[94] GÓMEZ NAVAJAS, en: Revista jurídica de Castilla y León, núm. 16, 2008, pág. 341.

a ello, es conveniente acudir nuevamente a la LOPD, para concretar el significado de "fichero", disponiendo el art. 3 b) que será: "*todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".* Además, y como señalamos anteriormente, se exige que el fichero, en virtud del carácter reservado de los datos, disponga de acceso o utilización limitado a personas concretas (como pueden ser los empleados), resultando indiferente la naturaleza de los mismos (económica, personal, medica, laboral, etc.).

En atención al objeto material, resulta conveniente determinar el bien jurídico protegido por el tipo básico analizado. Si bien, como indicamos al comienzo del trabajo, el bien jurídico protegido por el delito de descubrimiento y revelación de secretos es el derecho a la intimidad personal y familiar, derecho fundamental reconocido a través del art. 18.1 CE, el presente tipo básico dispone de la particularidad de recaer sobre un objeto concreto que son los datos reservados de carácter personal y familiar. Por tanto, el presente tipo otorga una protección específica sobre el derecho a la autodeterminación informativa o libertad informática (reconocido en el art. 18.4 CE)[95].

Como ya señalamos, la libertad informática es una expresión del derecho fundamental a la intimidad, disponiendo de un contenido distinto y autónomo que es la facultad de la persona de controlar aquellos datos personales o familiares que le pertenezcan. En este sentido, se estima que la libertad informática excede el ámbito del derecho a la intimidad, puesto que otorga a su titular un poder de control sobre sus datos personales, con respecto al uso y destino de los mismos, disponiendo además de una facultad negativa de impedir su conocimiento a terceros[96]. En función del bien jurídico protegido, resulta lógico que el presente tipo, no exija que los datos personales hayan de afectar a algún contenido de la intimidad, entendida en su sentido estricto, así como tampoco es preciso que la conducta típica recaiga sobre datos especialmente protegidos.

iv. Consentimiento y autorización.

El último de los elementos del tipo objetivo exigido, es la no concurrencia de autorización en la realización de las conductas descritas. Al igual que en los tipos básicos expuestos anteriormente, en los cuales se requería que la conducta típica se realizare sin

[95] STS 1328/2009, 30 de diciembre.
[96] MONTSERRAT SÁNCHEZ-ESCRIBANO en: Anuario Iberoamericano de Justicia Constitucional, núm. 19, 2015, págs. 326 y ss.

el consentimiento del sujeto pasivo, este tipo incluye una característica del tipo formulada de forma negativa, que es la ausencia de autorización. Ello implica que, si en la conducta de apoderamiento, utilización, acceso o modificación concurre autorización, tal hecho resultaría atípico por no reunir todos los elementos del tipo.

En este aspecto, González Cussac[97] califican tal exigencia como una causa de justificación y no como un elemento del tipo, en virtud de que la protección de la intimidad, no habría de cesar sino ante un interés de mayor entidad que justificase la lesión y eximiese de la responsabilidad penal. No obstante, doctrina y jurisprudencia[98] se decantan por considerar la ausencia de autorización como un elemento del tipo. Asimismo, conviene indicar que en aquellos casos en que el sujeto disponiendo de autorización para acceder, apoderarse, utilizar, modificar o alterar los datos reservados, exceda la misma, tales conductas habrán de ser calificadas como típicas, en la medida en que no se hallen cubiertas por los fines que fundamentaron la autorización.

Es importante señalar, que la autorización es el consentimiento otorgado por el titular de los datos reservados de carácter personal o familiar, concretamente y de conformidad con el art. 3 h) LOPD (coincidente con el art. 5.1 d) RD 1720/2007), el consentimiento del titular será "*Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen"*. Asimismo, la autorización también podrá ser otorgada por la persona encargada del fichero, tal y como establece el art. 5.2 a) RD 1720/2007, que define el acceso autorizado como "*autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad*".

3.3.2. Tipo subjetivo.

Al igual que los anteriores tipos básicos, la presente modalidad requiere que la conducta del sujeto activo sea dolosa. No obstante, la redacción empleada por el

[97] GÓNZALEZ CUSSAC, en: GÓNZALEZ CUSSAC (Coord.), *Derecho Penal Parte Especial*, 2016, pág. 281.
[98] SAP Madrid 115/1999 de 15 de abril, "*Los razonamientos que se acaban de referir nos llevan, obviamente, a declarar atípica la conducta de los acusados sin necesidad de llegar a analizar ya la posible exclusión de la antijuridicidad, es decir, la concurrencia o no de una causa de justificación que difuminara la posible tipicidad indiciaria de la actuación de los imputados*". En idéntico sentido: SSTS 234/1999, de 18 de febrero, FJ 1º, 525/2014, de 17 de junio., FJ 4º.

legislador, exige que la conducta se realice "en perjuicio de", fórmula respecto a la cual se haya dividida la doctrina, en función de si tal expresión ha de entenderse como un elemento subjetivo de lo injusto, o como un resultado típico de la lesión.

De aceptar la primera interpretación, pese a anticipar el momento de la intervención penal, ya que la consumación del delito no exigiría la efectiva producción de resultado alguno, plantearía el inconveniente de restringir el ámbito de lo punible, pues la ausencia del elemento subjetivo determinaría la atipicidad de la conducta[99]. En cuanto a la segunda acepción, supondría un añadido respecto a la lesión del bien jurídico protegido[100]. En atención a tal debate, la doctrina[101] se ha decantado, de conformidad con las penas previstas para el presente tipo básico, por la interpretación restrictiva, considerando tal expresión como un elemento subjetivo de lo injusto, considerando, además, que tal interpretación ofrecería una coherencia sistemática en relación al tipo subjetivo del art. 197.1 CP.

Por otra parte, hemos de señalar la distinta redacción empleada en el primer inciso del art. 197.2 CP, que exige que la conducta se realice "en perjuicio de tercero", de la dispuesta en el segundo inciso, que establece que ésta se ejecute "en perjuicio del titular de los datos o de un tercero". La configuración de este precepto, el cual ha sido mantenido por el legislador tras la Reforma de 2015, ha planteado numerosos pronunciamientos por parte de la doctrina.

Concretamente, se ha criticado la redacción empleada en el primer inciso, en la cual el legislador parece excluir del concepto de perjudicado, al titular de los datos reservados de carácter personal o familiar. Pese a ello, se estima que tal interpretación carece de fundamentación alguna, pues no es lógico excluir del concepto de tercero perjudicado al propio titular de los datos; en virtud de ello, se ha optado[102] por entender la fórmula del primer inciso, como una cláusula genérica en la cual habría de integrarse cualquier persona (incluida el titular de los datos) distinta del sujeto activo.

---

[99] SSTS 1461/2001, de 11 de julio, y 1084/2010, de 9 de diciembre.
[100] SSTS 234/1999, de 18 de febrero, 1328/2009, de 30 de diciembre, 525/2014, de 17 de junio.
[101] ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, págs. 262-263.
CASTIÑEIRA PALOU / ESTRADA I CUADRAS, en: SILVA SANCHEZ (Dir.), RAGUÉS I VALLÈS (Coord.), *Lecciones de Derecho Penal. Parte Especial*, 2015, pág. 161.
[102] GONZÁLEZ COLLANTES, en: Revista de Derecho Penal y Criminología Universidad Nacional de Educación a Distancia, núm. 13, 2015, págs. 59 y ss.

4. Tipos agravados.

4.1. Agravación por difusión, revelación o cesión de secretos a terceros (art. 197.3).

"3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior".

El primer inciso del art. 197.3, contiene el primero de los tipos agravados de este delito, el cual, tras la Reforma de 2015, ha mantenido su contenido, pero no su ubicación dentro del CP. Este tipo cualificado establece una pena de prisión de 2 a 5 años para aquella persona que, realizando cualquiera de los tipos básicos expuestos anteriormente, proceda a la difusión, revelación o cesión a terceros, de aquellos datos o hechos descubiertos, o imágenes captadas. Esta agravación se fundamenta en el mayor daño o injusto que supone tal conducta sobre el bien jurídico protegido.

La apreciación de la agravación exige que el sujeto activo haya realizado previamente alguna de las conductas tipificadas en los apartados 1 y 2 del art. 197 CP, esto es: apoderamiento de secretos documentales, interceptación de las comunicaciones, utilización de algún artificio técnico de escucha, transmisión o reproducción del sonido o imagen, o el apoderamiento, acceso, utilización o modificación de datos reservados de carácter personal o familiar. No obstante, como indicamos con anterioridad, la consumación del art. 197.1 CP no exige que efectivamente se descubra secreto alguno o se vulnere la intimidad de la víctima; por lo tanto, en atención a la redacción empleada por el presente tipo agravado ("datos o hechos descubiertos o las imágenes captadas"), será exigible que, para su apreciación, el sujeto activo agote el tipo básico[103].

Respecto a las conductas exigidas hemos de precisar sus diferencias. En primer lugar, "difusión" ha de entenderse como la comunicación a una o varias personas de aquello descubierto, con independencia de si existe interés por parte de tales personas en

[103] ANARTE BORRALLO / DOVAL PAIS, en: BOIX REIG (Dir.), *Derecho Penal. Parte Especial*, 2010, pág. 458.

su conocimiento. La conducta de "revelación" dispone de un significado similar al anterior, estableciendo su distinción en el mayor alcance que implica la difusión[104]. Por último, "cesión", supone la transferencia de información a otro.

Con respecto al segundo párrafo del art. 197.3, en atención a la menor pena prevista, será analizado posteriormente en el presente trabajo como un tipo autónomo de carácter atenuado.

4.2. Agravación por razón del sujeto activo y por suplantación de datos personales (art.197.4).

"4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:
a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o
b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.
Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior".

El art. 197.4 contiene el segundo tipo cualificado, estableciendo una pena de prisión de 3 a 5 años para las conductas que expondremos a continuación.

La primera modalidad, contenida en el apartado a), ha mantenido su redacción anterior, resultando de aplicación cuando las conductas tipificadas en los apartados 1 y 2 del art. 197, sean cometidas por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros.

El fundamento de este tipo, se basa en la condición del sujeto activo y en la especial posición de garante de la intimidad que pesa sobre el mismo con respecto al fichero, soporte, archivo o registro[105]. La exigencia de tal condición dispone de naturaleza normativa que limita el ámbito de aplicación de este tipo cualificado, pues únicamente podrá aplicarse a aquellos sujetos que sean encargados o responsables del fichero, excluyéndose, por ejemplo, aquellos que obren por mero encargo, o que dispongan de

[104] STS 1219/2004, de 10 de diciembre.
[105] GÓMEZ NAVAJAS, en: Revista jurídica de Castilla y León, núm.16, 2008, pág. 348.

una responsabilidad de hecho. En virtud de ello, este tipo ha sido calificado como "delito especial impropio"[106].

En este sentido, resulta destacable que el legislador no haya optado por la inhabilitación del sujeto activo, dado el riesgo que puede plantear que el autor pueda volver a disponer de aquellas facultades de las cuales se valió para realizar la conducta ilícita[107].

Respecto a los términos empleados por el presente tipo hemos de concretar el significado de "personas encargadas o responsables del fichero". En primer lugar, dispone el art. 3 g) LOPD, que será encargado del tratamiento "*la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento*"; mientras que el art. 3 d), define al responsable del fichero o tratamiento como "*persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento"*. En atención a ello, hemos de señalar las discrepancias en cuanto a los términos empleados por la norma penal en contraste con a la norma administrativa, puesto que, mientras aquel se refiere a "personas encargadas o responsables del fichero", la norma administrativa menciona al "encargado del tratamiento" y al "responsable del fichero o tratamiento". Pese a tales distinciones, es conveniente equiparar "encargado del tratamiento" (término empleado por la LOPD), a las "personas encargadas del fichero" (exigidas por el presente tipo agravado).

En lo referente a las conductas exigidas, resulta difícil, en la práctica, encuadrar la aplicación del presente tipo agravado a aquellas contenidas en el primer apartado del art. 197, que son las referentes al apoderamiento de secretos documentales, interceptación de comunicaciones o empleo de medios técnicos de escucha, transmisión o reproducción de sonido o imagen; resultando ser un tipo agravado más acorde con las conductas establecidas en el segundo apartado del art. 197, relativas al acceso, apoderamiento, utilización, alteración o modificación de datos reservados de carácter personal.

Por otra parte, el legislador ha optado por incorporar, junto al anterior, un nuevo tipo cualificado en el apartado b) del art. 197.4, elevando las penas cuando las conductas

[106] *Ibidem*, pág. 349.
[107] ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, pág. 265.

establecidas en los apartados 1 y 2 del art. 197, se lleven a cabo utilizando de forma no autorizada los datos personales de la víctima. La fundamentación del presente tipo agravado, reside en la mayor vulnerabilidad de la víctima, pues permite al sujeto activo asegurar la lesión e imposibilitar la defensa por parte de aquella. Algunos autores califican esta conducta como una suplantación de la personalidad[108].

Respecto a qué debe entenderse por "datos personales de la víctima", la Circular de la Fiscalía General del Estado 3/2017[109] ha precisado lo siguiente: "*habrían de entenderse no solo los datos de identidad oficial, en sentido estricto, sino cualesquiera otros, propios de una persona o utilizados por ella, que le identifiquen o hagan posible su identificación frente a terceros tanto en un entorno físico como virtual. Tienen tal consideración no solo el nombre y apellidos, sino también, entre otros, los números de identificación personal como el correspondiente al DNI, el de afiliación a la Seguridad Social o a cualquier institución u organismo público o privado, el número de teléfono asociado a un concreto titular, la dirección postal, el apartado de correos, la dirección de correo electrónico, la dirección IP, la contraseña/usuario de carácter personal, la matrícula del propio vehículo, las imágenes de una persona obtenidas por videovigilancia, los datos biométricos y datos de ADN, los seudónimos y en general cualquier dato identificativo que el afectado utilice habitualmente y por el que sea conocido*".

En último lugar, el apartado 4 del art. 197 establece un tipo "hiper agravado" o "súper agravado" aplicable a los tipos anteriores, por el cual se elevan las penas en su mitad superior, en aquellos casos en que los datos reservados sean difundidos, cedidos o revelados a terceros. Esta agravación, es similar a la contenida en el art. 197.3.

4.3. Agravación por afectación a datos especialmente protegidos y por la especial vulnerabilidad de la víctima (art. 197.5).

"5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad

[108] GONZÁLEZ COLLANTES, en: Revista de Derecho Penal y Criminología Universidad Nacional de Educación a Distancia, núm. 13, 2015, pág. 66.
[109] FISCALÍA GENERAL DEL ESTADO, *Circular 3/2017, 6 de julio de 2017*, págs. 14 y ss.

necesitada de especial protección, se impondrán las penas previstas en su mitad superior".

El apartado quinto del art. 197, dispone de 2 tipos agravados que imponen las penas en su mitad superior y que serán aplicables a los tipos anteriormente descritos. Respecto al mismo, conveniente precisar, que no ha visto alterado su contenido, salvo en la referencia a la "persona con discapacidad necesitada de especial protección", cuyo término empleado con anterioridad a la Reforma era "incapaz".

El primer inciso establece una agravación cuando las conductas anteriormente descritas, es decir, las contenidas en los apartados 1 a 4 del art. 197, afecten a datos de carácter personal, que permitan revelar la ideología, religión, creencias, salud, origen racial o vida sexual de su titular. Tales datos, han sido calificados como "datos sensibles", entendidos como aquellos que pertenecen al "núcleo duro" de la intimidad[110] que, gozan de una protección especial en nuestro ordenamiento jurídico. Por tanto, la fundamentación de este tipo agravado se basa en el mayor injusto de la conducta típica, cuando esta recae sobre tales datos, pues supone una vulneración del derecho a la intimidad personal y familiar en sus aspectos más básicos y esenciales. (art. 16.2 CE, 7.2 y 3 LOPD).

El segundo inciso, dispone una agravación cuando las conductas descritas en los apartados anteriores del art. 197 tengan por víctima a un menor de edad o una persona con discapacidad necesitada de especial protección. La fundamentación, en este caso reside en la especial situación de vulnerabilidad y desvalimiento en la que se halla el sujeto pasivo.

En primer lugar, el significado "menor de edad" habrá de entenderse de acuerdo con la legislación civil, que establece la menoría de edad hasta los 18 años. Por otra parte, como señalábamos, el presente tipo no utiliza ya el término "incapaz", sino "persona con discapacidad necesitada de especial protección", esta modificación es consecuencia de la Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad. Respecto a su significado viene expresado en el propio CP, mediante el art. 25, párr. 2, que dispone: "*Asimismo a los*

[110] ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, pág. 266.

efectos de este Código, se entenderá por persona con discapacidad necesitada de especial protección a aquella persona con discapacidad que, tenga o no judicialmente modificada su capacidad de obrar, requiera de asistencia o apoyo para el ejercicio de su capacidad jurídica y para la toma de decisiones respecto de su persona, de sus derechos o intereses a causa de sus deficiencias intelectuales o mentales de carácter permanente".

4.4. Agravación por el especial desvalor de la finalidad perseguida (art 197.6).

"6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años".

El apartado 6 del art. 197, no ha visto modificado su contenido tras la Reforma, incluyendo dos circunstancias agravatorias. El primer inciso, del art. 197.6, dispone una elevación de las penas, previstas en los apartados 1 a 4 del mismo artículo, en su mitad superior, cuando las conductas se lleven a cabo con fines lucrativos. Mientras que el segundo inciso, establece una pena de prisión de 4 a 7 años cuando además de lo anterior, la conducta afecte a los datos mencionados en el art. 197.5, es decir, a los datos especialmente protegidos.

La cualificación de la pena se fundamenta en el mayor desvalor que supone la realización de cualquiera de las conductas anteriores con la finalidad de lucrarse. Asimismo, tal agravación es reflejo de la lucha contra el tráfico ilícito de datos, que es una práctica criminológica cada vez más habitual en nuestra sociedad. Dispone de un fundamento político-criminal, tendente a prevenir la comercialización de los aspectos íntimos de la persona[111].

El presente tipo exige que el sujeto activo actúe con ánimo de lucro, lo cual supone un elemento subjetivo de lo injusto añadido al dolo[112]. En este sentido, la intencionalidad del autor es suficiente para entender consumado el presente tipo, sin ser necesario que efectivamente haya obtenido lucro alguno, por tanto, es un delito de resultado cortado.

[111] *Ibidem*, pág. 266.
[112] *Ibidem*, pág. 266.

Por último, la agravación es mayor cuando los fines lucrativos afecten a datos especialmente protegidos que, como señala el anterior precepto, son aquellos que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, puesto que, como previamente indicamos, la afectación de la intimidad producida en estos casos es mayor.

5. Tipos específicos.

5.1. Revelación de secretos sin haber sido parte en el descubrimiento (art.197.3, párr. 2).

El segundo inciso del art. 197.3 CP establece un tipo que ha sido calificado como "tipo atenuado"[113], el cual tipifica la conducta realizada por aquella persona que, conociendo el origen ilícito y sin ser parte en el descubrimiento, realizare la conducta de difusión, revelación o cesión a un tercero. El castigo previsto para ésta es pena de prisión de 1 a 3 años más multa de 12 a 24 meses, respectivamente.

Como la propia redacción establece, se exige que el sujeto activo conozca el origen ilícito de los hechos, datos o imágenes, que pretenda difundir, pues de lo contrario la conducta seria atípica. En consecuencia, podrá crearse una cadena de sujetos responsables por esta conducta, no obstante, el límite a la misma se establecería cuando la información dejare de ser secreta[114].

5.2. Revelación de imágenes o grabaciones audiovisuales, obtenidas con anuencia del sujeto pasivo (art. 197.7).

"7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla 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

[113] GÓNZALEZ CUSSAC, en: GÓNZALEZ CUSSAC (Coord.), *Derecho Penal Parte Especial*, 2016, pág. 283.
[114] *Ibidem*, pág. 283.

discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa".

El art. 197.7 castiga con pena de prisión de 3 meses a 1 año, o multa de 6 a 12 meses, a aquel que, sin autorización de la persona afectada, difunda, revele o ceda a terceros, imágenes o grabaciones audiovisuales de aquella, obtenidas con su anuencia en un domicilio o lugar fuera del alcance de terceros, en el caso de que tal divulgación implique un menoscabo grave sobre su intimidad personal. Además de ello, el segundo párrafo, establece una agravación en su mitad superior, en 3 casos distintos: primero, que el sujeto activo fuere el cónyuge o persona que esté o haya estado unida por análoga relación de afectividad, aun cuando no existiese convivencia; segundo, que la víctima fuere menor de edad o persona con discapacidad necesitada de especial atención; y en último lugar, que la conducta se hubiere cometido con fines lucrativos.

Este precepto exige un análisis pormenorizado, en virtud de que el mismo contiene una de las nuevas figuras introducidas por el legislador tras la Reforma de 2015, la cual ha sido objeto de numerosos pronunciamientos por parte de la doctrina.

La inclusión de esta figura nace ante un contexto de desarrollo de nuevas tecnologías y del uso generalizado de Internet, el cual ha permitido a la sociedad una comunicación instantánea, facilitando además la difusión de contenidos a través de las distintas redes existentes. Si bien, tales avances plantean numerosas ventajas, surgen, al mismo tiempo, graves consecuencias sobre los derechos fundamentales de la persona, y especialmente sobre su derecho a la intimidad personal y familiar.

Con anterioridad a la Reforma del CP, la divulgación de imágenes o contenidos audiovisuales de carácter íntimo, obtenidas con consentimiento de la víctima, no disponía de un correcto encaje legal. En la práctica, tales conductas conllevaban sentencias absolutorias, ya que el hecho de no mediar autorización determinaba la atipicidad de las mismas[115]. En ocasiones, su difícil encaje dentro de los delitos contra la intimidad

[115] SAP Granada 351/2014, de 5 de junio, SAP Madrid 240/2014, de 15 de abril; SAP Almería 242/2005, de 2 de noviembre, plantea una excepción a tal parecer judicial, pues se condena a una persona que reveló unas fotos intimas que obtuvo con anuencia de la víctima.

conllevó a los juzgados a considerar tales conductas como vulneradoras del derecho al honor, siendo calificadas como delitos de injurias[116].

Ante la proliferación de tales comportamientos, el legislador optó por introducir esta nueva figura, siendo consecuencia de una decisión político-criminal tendente a la salvaguarda del derecho a la intimidad[117]. No obstante, pese a que su redacción se estima acertada, en tanto que permite superar la situación de indefensión en que anteriormente se hallaba la víctima, algunos autores[118] estiman que el alcance del tipo no se agota en este fenómeno, ni puede afirmarse que castigue atentados a la intimidad relacionados con este tipo de prácticas, pues aún existen supuestos que no encontrarían amparo en esta nueva figura.

Esta nueva figura, ha sido calificada como un "tipo mixto alternativo"[119], pues la conducta se consumaría con la realización de una de las conductas descritas, esto es, con la difusión, la revelación o la cesión de imágenes o contenidos audiovisuales. Respecto al significado de tales conductas, hemos de remitirnos al tipo agravado por difusión del art. 197.3, en el cual las mismas fueron ya descritas. Asimismo, es considerado un tipo de carácter autónomo o especifico[120] en base a que, protege el mismo bien jurídico que los tipos básicos (esto es, el derecho a la intimidad personal y familiar), aunque no guarda relación con los demás tipos agravados, entre los cuales se halla ubicado dentro del Capítulo I del Título X del CP.

En cuanto al contenido del mismo, hemos de describir en primer lugar, la acción típica contenida en el primer párrafo del art. 197.7. La acción consta de dos partes diferenciadas: una parte instrumental, que implica la obtención por parte del sujeto activo de imágenes o grabaciones audiovisuales, con el consentimiento de la víctima, en un domicilio o lugar fuera del alcance de terceros (que no constituiría un ilícito penal); y una segunda parte, que exige la difusión, revelación o cesión a terceros de aquellas imágenes

[116] SAP Lleida 90/2004, de 25 de febrero, SAP Cádiz 75/2005, de 22 de abril.
[117] Tal decisión, se vio claramente influida por el caso mediático de la edil socialista Dña. Olvido Hormigo, en el cual resultó absuelto aquel que difundió masivamente un video de carácter erótico protagonizado por ella.
[118] CASTIÑEIRA PALOU / ESTRADA I CUADRAS, en: SILVA SANCHEZ (Dir.), RAGUÉS I VALLÈS (Coord.), *Lecciones de Derecho Penal. Parte Especial*, 2015, pág. 162.
[119] DÍAZ TORREJÓN, en: Revista del Ministerio Fiscal, Fiscalía General del Estado, número 1, 2016, pág. 14.
[120] ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, pág. 268.

o grabaciones, sin consentimiento de la víctima, produciendo un grave menoscabo sobre su intimidad personal.

En virtud de ello, conviene analizar los elementos o requisitos típicos de la acción. En primer lugar, es preciso que el sujeto activo disponga del consentimiento de la víctima en la obtención de las imágenes o contenidos audiovisuales, y que, por el contrario, carezca del mismo en cuanto a la difusión de éstos. Por tanto, se estima que la autorización se plasma únicamente sobre el acceso a un ámbito o reducto privado de la intimidad, que no puede considerarse extensible a aquellas conductas posteriores de exhibición del material obtenido[121]. De este modo, el legislador establece una clara distinción entre el consentimiento para la obtención de imágenes y el consentimiento para la difusión, superando aquellas circunstancias de desprotección en que se hallaba la víctima y reforzando la dimensión subjetiva del derecho a la intimidad, entendido, como facultad de control y exclusión a terceros.

En cuanto a las imágenes o grabaciones audiovisuales, la propia redacción exige que éstas hayan sido obtenidas en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros. Es preciso recalcar que aquellos contenidos que disponiendo de sonido o audio, carezcan de imagen, quedan excluidos del presente tipo. Tampoco es preciso que las imágenes dispongan de un contenido sexual (aun cuando su redacción se haya visto claramente influida por esta clase de comportamientos), podrán ser objeto del presente tipo cualesquiera imágenes o grabaciones audiovisuales que afecten al núcleo duro de la intimidad.

Respecto a la obtención de dichas imágenes o vídeos, el tipo dispone que tal acción haya sido ejecutada por el propio autor de la revelación, es decir, se configura como un delito especial de propia mano[122]. Es importante subrayar este aspecto, puesto que durante el trámite parlamentario de la LO 1/2015, el Grupo Socialista planteó una enmienda solicitando la inclusión dentro del precepto, de aquellas imágenes o grabaciones audiovisuales que fueren realizadas directamente por la persona afectada, no obstante, la misma fue rechazada. Como consecuencia de ello, la doctrina se encuentra dividida, pues mientras un sector[123] estima que el propio tipo excluye aquellos contenidos captados por

[121] MUÑOZ CONDE, en: *Derecho Penal. Parte Especial*, 2015, pág. 239.
[122] GONZÁLEZ COLLANTES, en: Revista de Derecho Penal y Criminología Universidad Nacional de Educación a Distancia, núm. 13, 2015, pág. 69.
[123] En este sentido:

la propia persona afectada, distintos autores[124] admiten que dentro del tipo han de considerarse incluidas éstas, realizando una interpretación integradora y acorde con el espíritu de la Reforma (concretado en el Preámbulo de la LO 1/2015).Tampoco existe un claro posicionamiento en la jurisprudencia[125], aunque en distintas ocasiones se ha admitido la tipicidad de la conducta cuando es la víctima la que capta y cede voluntariamente las imágenes que, con posterioridad, son reveladas por el sujeto activo. En este sentido, resulta más correcta la interpretación integradora acorde con la propia motivación de la norma, sin embargo, será preciso acudir a la jurisprudencia que sobre este tema se desarrolle.

Por otra parte, el tipo exige que las imágenes o grabaciones audiovisuales sean obtenidas en un "domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros". La conducta de "obtención" habrá de equipararse a la de captación y no a la de recepción, pues es independiente la forma en que tales imágenes o grabaciones sean recibidas por el sujeto activo, exigiéndose, contrariamente, que éstas se hallan realizado, captado o grabado en los lugares señalados por el precepto. Además de ello, se ha criticado[126] el empleo de un concepto netamente jurídico, como es el de "domicilio", en confrontación con uno extrajurídico, "lugar fuera del alcance de la mirada de terceros". Especialmente, se ha cuestionado esta última referencia, en tanto que se plantea ambigua e indeterminada. Pese a ello, habrá de entenderse por tal, cualquier lugar (aún público) que en el momento en que se obtengan las imágenes o grabaciones no resulte accesible al campo visual de terceros, es decir, que disponga de garantías suficientes de privacidad. En base a lo anterior, puede deducirse la intención del legislador, de que las imágenes o grabaciones sean obtenidas en un contexto de reserva o íntimo, con independencia de si el mismo es un lugar privado o no.

- CASTIÑEIRA PALOU / ESTRADA I CUADRAS, en: SILVA SANCHEZ (Dir.), RAGUÉS I VALLÈS (Coord.), *Lecciones de Derecho Penal. Parte Especial*, 2015, pág. 162.
- ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, pág. 269.
- MUÑOZ CONDE, en: *Derecho Penal. Parte Especial*, 2015, pág. 239 y ss.

[124] DÍAZ TORREJÓN, en: Revista del Ministerio Fiscal, Fiscalía General del Estado, número 1, 2016, pág. 13.

[125] SSAP Valladolid 290/2017, de 6 de octubre, Valencia 488/2016, de 25 de noviembre, Burgos 360/2016, de 8 de noviembre. En sentido contrario, SAP Barcelona 302/2017, de 24 de abril.

[126] DÍAZ TORREJÓN, en: Revista del Ministerio Fiscal, Fiscalía General del Estado, número 1, 2016, pág. 10.

En último lugar, la conducta exige que "la divulgación menoscabe gravemente la intimidad personal de esa persona", configurándose como un delito de resultado[127]. Este elemento normativo plantea diversos problemas, ya que, no se ha establecido ningún parámetro que permita su valoración. Como indicábamos con anterioridad en el presente trabajo, la intimidad dispone de un carácter voluble, pues su contenido variará en función de cada sociedad y momento histórico, lo cual puede plantear pronunciamientos relativamente subjetivos. Sin embargo, una delimitación demasiado estricta del derecho a la intimidad personal y familiar podría, a su vez, excluir de su ámbito aspectos que surgiesen como consecuencia de las nuevas realidades. En consecuencia, corresponde al juez, conforme a su leal saber, determinar el grado de afectación sobre la intimidad, señalando si la conducta dispone de entidad suficiente como para ser merecedora de reproche penal o si, por el contrario, habrá de ser reconducida otras vías (como la civil)[128]. En atención a ello, pueden plantearse problemas de seguridad jurídica, pues una regulación formulada en términos tan amplios, conllevaría a que la efectividad de la norma dependiera de la decisión del juzgador.

En cuanto al tipo subjetivo, es preciso que el sujeto activo actúe de forma dolosa. En relación a ello, conviene reseñar algunas situaciones paradigmáticas. En primer lugar, hemos de analizar la posible responsabilidad de aquellos que, no siendo autores de la conducta contenida en el art. 197.7, procedan a la divulgación o reenvío de las imágenes o grabaciones obtenidas por aquel que si lo fuere. Ante tales circunstancias, la doctrina mayoritaria considera que dichas personas se hallan excluidas del presente tipo, limitando la responsabilidad penal a aquel que hubiere obtenido previamente las imágenes con anuencia de la víctima, pues lo contrario, rebasaría las posibilidades del proceso penal[129]. En segundo lugar, se plantean aquellos supuestos en que la persona envíe por error imágenes o grabaciones de contenido íntimo, que luego fueren difundidas por el receptor de las mismas. En este caso, se ha entendido que el error en el envío queda excluido del ámbito de la anuencia y, por ende, de la aplicabilidad del presente tipo[130]. Pese a ello, en

[127] *Ibidem*, pág. 11.
[128] Algunos ejemplos de ello, podrían ser los siguientes:
- SAP Madrid 372/2017, de 21 de junio, absolución por revelación de torso desnudo, no afecta a la intimidad, no se llega a mostrar detalles que permitan la identificación de la persona.
- SAP Madrid 461/2016, de 29 de junio, absolución por la publicación de fotos de carácter artístico, la denunciante posa voluntariamente como modelo, y las fotos no divulgan su rostro ni sus zonas íntimas.

[129] FISCALÍA GENERAL DEL ESTADO, *Circular 3/2017, 6 de julio de 2017,* págs. 14 y ss.
[130] GÓNZALEZ CUSSAC, en: GÓNZALEZ CUSSAC (Coord.), *Derecho Penal Parte Especial*, 2016, pág. 286.

ambos supuestos cabe la posibilidad de exigir responsabilidad civil de conformidad con la LO 1/1982, o en su caso, exigir responsabilidad por un delito contra el honor o la integridad moral de la víctima. Asimismo, en el primer caso, se plantea la posibilidad de que los terceros que procedan a la difusión, sean responsables del delito a título de partícipes o cómplices.

Con respecto al castigo impuesto por este tipo, se establece una pena de prisión de 3 meses a 1 año, o multa de 6 a 12 meses. Si bien la conducta típica de este nuevo tipo es similar a la contenida en el segundo inciso del art. 197.1, que contemplaba una pena de prisión de 1 a 4 años y multa de 12 a 24 meses, aquella se fundamenta en la menor afectación de la conducta sobre la intimidad, pues el sujeto activo dispone del consentimiento en la obtención de aquellas imágenes o grabaciones audiovisuales.

Por otra parte, como indicamos anteriormente, este tipo establece en su segundo párrafo una elevación, en su mitad superior, de las penas previstas cuando los hechos fueren cometidos por el cónyuge de la víctima o persona unida a la misma por relación análoga de afectividad (aun sin convivencia), la víctima fuere menor de edad o persona con discapacidad necesitada de especial protección, o los hechos fueren cometidos con finalidad lucrativa. Si bien tales circunstancias ya fueron analizadas con anterioridad en el presente trabajo, es conveniente realizar algunas puntualizaciones respecto a la redacción empleada por el legislador.

En primer lugar, algunos autores estiman que el legislador ha obviado hacer referencia al "ex cónyuge", obligando a una interpretación forzada del precepto, debiendo entender incluido al mismo.

Por otra parte, respecto a la obtención de imágenes o grabaciones con anuencia de la víctima cuando ésta es menor o persona con discapacidad necesitada de especial protección, algunos autores cuestionan si en tales supuestos, la víctima dispone de capacidad suficiente como para consentir de forma valida. Además de ello, puesto que nos hallamos ante una conducta que con frecuencia tiene por objeto material imágenes o grabaciones de contenido sexual, la elaboración de los mismos cuando la víctima es menor de edad o persona con discapacidad puede resultar constitutiva de otros delitos

como, por ejemplo, de pornografía infantil regulado en el art. 189 CP[131]. En este sentido, si la norma penal limita la validez en el consentimiento de menores o discapacitados en la elaboración de aquel material, resulta contradictorio que el presente tipo considere válido el consentimiento otorgado por dichas víctimas. Como consecuencia de ello, conviene analizar tal requisito, a fin de que no suponga un obstáculo para la aplicación de este tipo agravado, pudiendo plantearse casos en que exista una situación de concurso entre tales figuras.

6. Nuevas conductas: arts. 197 bis y ter.

6.1. Introducción en el CP mediante las Reformas de 2010 y 2015.

Como señalamos anteriormente, el avance de la tecnología ha planteado nuevos riesgos que afectan a los derechos pertenecientes, ya no solo a personas físicas, sino también a personas jurídicas (como pudieran ser empresas, instituciones, o incluso infraestructuras públicas). La delincuencia ha hallado un nuevo espacio en el que desarrollarse, esto es, el ciberespacio, el cual ha favorecido tanto el anonimato de los sujetos activos, como la facilidad en la comisión de delitos. Esta situación plantea un gran reto para el Derecho penal, pues se enfrenta a conductas cada vez más técnicas y profesionalizadas que no hallan un correcto encaje en las tradicionales formas de delinquir contempladas en el ordenamiento jurídico.

En atención a dichos comportamientos, se han aprobado distintos convenios, así como resoluciones por parte de organismos supranacionales (de los cuales España es parte), tendentes a la elaboración de una política penal común. Como consecuencia de ello, el Consejo de Europa aprobó el Convenio sobre la Ciberdelincuencia, cuyo fundamento principal era la consecución de una política penal común enfocada a la protección de la sociedad frente a la ciberdelincuencia; sin embargo, su entrada en vigor en España resultó tardía, pues no se produjo hasta el 1 de octubre de 2010[132].

Con posterioridad a dicho Convenio, se publicó la Decisión Marco 2005/222/JAI, que dio lugar a la Reforma del Código Penal en el año 2010 (por medio de la LO 5/2010). En lo que respecta al tema en que nos hallamos, esta Reforma introdujo dentro del Título

[131] DÍAZ TORREJÓN, en: Revista del Ministerio Fiscal, Fiscalía General del Estado, número 1, 2016, pág. 16.
[132] Mediante el Instrumento de Ratificación publicado en el BOE el 17 de septiembre de 2010.

X, perteneciente a los delitos contra la intimidad, derecho a la propia imagen e inviolabilidad del domicilio, concretamente por medio del apartado 3 del art. 197 CP, una nueva figura que tipificaba las conductas de acceso, no autorizado, a los datos o programas informáticos contenidos en un sistema informático o en parte del mismo, así como el mantenimiento dentro del mismo en contra de la voluntad de aquel que tuviera el legítimo derecho a excluirlo.

La Decisión Marco 2005/222/JAI fue sustituida por la Directiva 2013/40/UE, la cual fue introducida en el ordenamiento jurídico español por medio de la LO 1/2015, que, como es bien sabido, supuso una reforma total del sistema penal español.

Tal y como indica la LO 1/2015 en su Preámbulo (XIII), las modificaciones operadas en el CP tienen por objetivo la superación de aquellas limitaciones que la anterior legislación planteaba, ofreciendo una respuesta a la delincuencia informática acorde con la normativa europea. De este modo, se produce una reorganización del articulado del Capítulo I del Título X del CP, introduciendo una separación nítida entre los supuestos de revelación de secretos que afectan a la intimidad personal, y el acceso a otros datos o informaciones que, afectando a la privacidad, no se hallen referidos directamente a la intimidad. Como resultado de ello, el legislador procede a la revisión del delito de acceso, no autorizado, a un sistema informático, reubicándolo en el nuevo art. 197 bis, en su apartado primero. Asimismo, se introduce una nueva conducta típica, por medio del apartado segundo del art. 197 bis, consistente en la interceptación de transmisiones entre sistemas. En último lugar, se tipifica a través del art. 197 ter la facilitación o producción de programas informáticos o equipos, específicamente diseñados o adaptados para la comisión de los anteriores delitos.

6.2. Concreción del bien jurídico protegido por las nuevas figuras.

La introducción de las nuevas conductas contenidas en los arts. 197 bis y ter, relativas al acceso ilícito a un sistema de información, interceptación de transmisiones de datos informáticos, y de facilitación o producción de programas informáticos o códigos de acceso para la comisión de las anteriores conductas, ha planteado numerosos problemas en cuanto a su interpretación. Como hemos señalado, la tipificación de estas modalidades delictivas se fundamenta en la necesidad de cumplir con aquellos compromisos internacionales asumidos por el Estado español. No obstante, el legislador

penal, lejos de llevar a cabo una armonización jurídica acorde con nuestro ordenamiento, ha realizado una transposición casi literal de la normativa supranacional, produciendo un claro menoscabo sobre la seguridad jurídica[133].

En un primer momento, la inclusión por medio del art. 197.3 de la conducta de acceso ilícito a los sistemas informáticos (a través de la Reforma del CP en 2010), provocó una división de la doctrina, respecto a cuál pudiera ser el bien jurídico protegido. Un sector doctrinal, consideró que el objeto tutelado por dicha figura era el derecho fundamental a la intimidad, ello de conformidad con la ubicación de esta nueva conducta y en atención al paralelismo existente entre esta figura y el allanamiento de morada, entendiendo que la misma pretendía tutelar un ámbito de privacidad, concretado en el denominado "domicilio informático"[134]. En contraposición a tales argumentos, otro sector optó por considerar que el bien objeto de tutela, era la seguridad de los sistemas informáticos, señalando las claras dificultades de interpretación y delimitación, que planteaba su ubicación entre los delitos contra la intimidad[135].

En líneas generales, la mayor parte de la doctrina se decantó por esta segunda argumentación, considerando que el legislador había incorporado una figura con una estructura típica de peligro abstracto para la intimidad[136]. De este modo, se pretendía superar la falta de contenido del objeto protegido, conectando la seguridad de los sistemas de información con el derecho a la intimidad. Tales planteamientos, conllevaron a que algunos autores cuestionaran tanto la necesidad técnica, como la idoneidad política-criminal[137] , de introducir dicha figura en el sistema penal, de conformidad con la carencia de un sustrato material propio y el injusto de mero peligro que planteaba.

Actualmente, mediante la Reforma llevada a cabo a través de la LO 1/2015, el legislador ha pretendido superar tal debate, procediendo a revisar la configuración de esta figura mejorando tanto su redacción como su ubicación dentro del CP. En virtud de ello,

---

[133] VALDÉS-SOLÍS IGLESIAS, en.: *Los delitos contra los sistemas informáticos: arts. 197 bis y 197 ter del código penal*, 2017, pág. 5.
[134] COLÁS TURÉGANO, en: Revista Boliviana de Derecho núm.21, 2016, pág. 216: "*Desde dicha postura MORALES consideró que lo que se pretende tutelar es "la información vital que se sitúa en estos espacios…reserva de dicho espacio en términos de intimidad*"".
[135] ANARTE BORRALLO / DOVAL PAIS, en: BOIX REIG (Dir.), *Derecho Penal. Parte Especial*, 2010, pág. 455-456.
[136] COLÁS TURÉGANO, en: Revista Boliviana de Derecho núm.21, 2016, pág. 216 y ss.
[137] ANARTE BORRALLO / DOVAL PAIS, en: BOIX REIG (Dir.), *Derecho Penal. Parte Especial*, 2010, pág. 455-456.

mediante una reorganización del articulado estableció una separación entre aquellas conductas afectantes a la intimidad (contenidas en el art. 197), y aquellas cuya afectación se produjera sobre la privacidad y no directamente sobre la intimidad (arts. 197 bis y ter).

De conformidad con los principios internacionales que inspiraron estas nuevas conductas, puede afirmarse que el bien jurídico protegido por las mismas es la seguridad de los sistemas de información, esto es, su integridad e indemnidad. No obstante, continúan existiendo claras dificultades en cuanto a su interpretación y delimitación en el sistema penal español, dada su permanencia dentro del Capítulo I del Título X, relativo a los delitos contra la intimidad, propia imagen e inviolabilidad del domicilio. Si bien el Preámbulo de la LO 1/2015, establece que estas conductas, afectan a la privacidad sin hallarse referidas directamente a la intimidad, no excluye que las mismas dispongan de una naturaleza de peligro sobre tal derecho fundamental.

En consecuencia, la inclusión de dichas figuras ha provocado una anticipación de la intervención penal, ello quiere decir que, al protegerse la seguridad de los sistemas de información, se produce un adelantamiento en la protección del derecho a la intimidad, no exigiéndose que, en tales casos, se actúe con la voluntad de descubrir los secretos o vulnerar la intimidad (elemento subjetivo de lo injusto, que por el contrario exigen los tipos básicos). Tal consideración, se fundamenta en la necesidad de una tutela especifica de la seguridad de los sistemas de información, en atención a la importancia de los mismos en el actual desarrollo de nuestra sociedad y en el riesgo que éstos pueden plantear sobre la intimidad.

En atención a lo expuesto, cabe señalar que este tema no se halla exento de debate, pues si bien el legislador ha realizado una labor meritoria en cuanto a la delimitación de estas nuevas figuras con los tipos básicos de descubrimiento y revelación de secretos, no se han solucionado aquellas cuestiones planteadas con la introducción en el año 2010 del delito de acceso ilícito a un sistema de información, entre los delitos contra la intimidad. Por tanto, será preciso un desarrollo jurisprudencial, que permita al intérprete concretar el bien jurídico protegido por estas nuevas conductas.

Visto lo anterior, conviene analizar dichas conductas de forma concreta.

6.3. Acceso o mantenimiento ilícito en un sistema de información (art. 197 bis 1).

"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".

El apartado primero del art. 197 bis castiga con pena de prisión de 6 meses a 2 años a aquel que, por cualquier medio o procedimiento, vulnerando aquellas medidas de seguridad establecidas y sin autorización, acceda, o facilite a un tercero el acceso, al conjunto o parte de un sistema de información, o se mantenga en el mismo en contra de la voluntad de aquella persona que disponga legítimo derecho a excluirlo. Algunos autores han calificado esta figura como "allanamiento informático"[138], "intrusismo informático"[139] o "espionaje informático"[140]. Esta modalidad, como indicamos con anterioridad, no es nueva en nuestro CP, no obstante, se han producido claras modificaciones en su redacción tras la Reforma de 2015.

6.3.1. Tipo objetivo.

i. Sujetos activo y pasivo.

En primer lugar, al tratarse de un delito común, el sujeto activo podrá ser cualquier persona, no exigiendo el tipo que el mismo disponga de ninguna cualidad específica, ni que tenga conocimientos técnicos sobre informática. En este sentido, y de conformidad con el art. 197 quinquies, se podrá exigir a la persona jurídica la responsabilidad por este delito, no obstante, sobre ello habremos de extendernos más adelante. Por otra parte, el sujeto pasivo será aquella persona (física o jurídica) titular del sistema de información, o aquella que disponga de legítimo derecho para excluir del sistema a aquel que se niegue a abandonarlo.

---

[138] VALDÉS-SOLÍS IGLESIAS, en.: *Los delitos contra los sistemas informáticos: arts. 197 bis y 197 ter del código penal*, 2017, pág. 5.
[139] COLÁS TURÉGANO, en: Revista Boliviana de Derecho núm. 21, 2016, pág. 214.
ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, pág. 269.
[140] VALDÉS-SOLÍS IGLESIAS, en.: *Los delitos contra los sistemas informáticos: arts. 197 bis y 197 ter del código penal*, 2017, pág. 6.

ii. Conducta típica.

En cuanto a la conducta típica, se mantienen los comportamientos exigidos anteriormente, esto es, el acceso o mantenimiento en un sistema de información, incluyendo la Reforma una nueva modalidad, consistente en la facilitación a un tercero el acceso a un sistema. El delito se configura como un tipo mixto alternativo, pues la consumación se producirá cuando el sujeto activo realice cualquiera de las conductas referidas. Además de ello, el tipo dispone que tales comportamientos podrán llevarse a cabo por cualquier medio o procedimiento, exigiendo, no obstante, que se produzca vulnerando las medidas de seguridad establecidas para impedir el acceso o mantenimiento, y que no concurra autorización.

La conducta de acceso podrá ser de dos tipos[141]: directo, lo cual implica la introducción en el sistema a través de medios físicos (por ejemplo, accediendo directamente a un ordenador, ingresando en el mismo la contraseña); o remoto, produciéndose el acceso a través de una red pública o privada. En este sentido, si el acceso al sistema de información se produce mediante el empleo de datos personales de la víctima, nos hallaríamos ante la concurrencia de dos figuras distintas (la prevista en el art. 197 bis y la contenida en el apartado b), del art. 197.4), cuya apreciación conjunta provocaría una infracción del principio non bis in ídem, siendo preciso acudir al art. 8.1º CP, que establece la prioridad del precepto especial sobre el general, es decir, habremos de decantarnos por el art. 197.4.

En lo relativo a la conducta de facilitación a un tercero el acceso, se exige la concurrencia de dos personas, un sujeto que disponga de un modo (lícito o no) de acceder a un sistema de información, y otro al que aquel permita o favorezca por medios suficientes el acceso al sistema. La introducción de esta forma ha sido criticada[142], pues amplía de forma desproporcionada el ámbito de lo punible, equiparando la conducta de participación a la de autoría. La consumación, en este caso, requiere que el tercero efectivamente acceda al sistema de información, no siendo relevante penalmente la mera facilitación sin que se produzca el acceso (por ejemplo, señalando las vulnerabilidades de

[141] BARRIO ANDRÉS, en: *Ciberdelitos: Amenazas criminales del ciberespacio*, 2017, pág. 68.
[142] COLÁS TURÉGANO, en: Revista Boliviana de Derecho núm. 21, 2016, pág. 219.

seguridad de un sistema a un tercero), pues ello plantearía problemas en cuanto a la delimitación de esta conducta con aquellas contenidas en el art. 197 ter.

En cuanto al mantenimiento en un sistema de información se trata de una conducta omisiva consistente en el no abandono. La doctrina[143] ha discutido si el acceso, previo al mantenimiento, debía ser lícito o no, determinando, de conformidad con la doctrina surgida para la interpretación del delito de allanamiento de morada (respecto al cual existe una correspondencia evidente en cuanto a la redacción), que la tipicidad de esta figura se producirá en cuanto al mantenimiento y no en cuanto al acceso. Por tanto, resulta lícita la introducción en el sistema, produciéndose la ilicitud cuando se requiere al sujeto el abandono del sistema y éste se niega, manteniéndose en el mismo.

iii. Objeto material.

El objeto material de este delito, de conformidad con la propia redacción, serán los sistemas de información. Si bien, con anterioridad, el tipo exigía que el acceso o mantenimiento se produjera sobre los datos o programas informáticos contenidos en un sistema informático, en la actualidad, basta con que la conducta de acceso o mantenimiento, se realice respecto a un sistema de información (o parte del mismo).

En atención a ello, conviene concretar el significado de "sistema de información", para lo cual hemos de acudir al art. 2 a) de la Directiva 2013/40/UE, en el cual se define como, "*todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento*".

Respecto a dicha definición hemos de realizar una serie de precisiones. En primer lugar, el aparato o grupo de aparatos relacionados entre sí, conformarán el hardware del sistema; mientras que el software, será aquel programa (cadena de instrucciones que el propio sistema ejecuta para un fin concreto) a través del cual, dicho aparato o conjunto de aparatos, realizará el tratamiento automático de datos. En segundo lugar, el tratamiento automático implica la no intervención humana, es decir, tal función será realizada por el

[143] *Ibidem*, págs. 218-219.

propio sistema. Por otra parte, la definición exige que dicho tratamiento recaiga sobre datos informáticos, cuyo significado viene establecido por el mismo artículo de la Directiva, en su apartado b), como: "*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 una función*".

Es preciso recalcar que, al no exigir la nueva redacción que el acceso se produzca sobre los datos o programas informáticos, la consumación de la conducta se producirá con el mero acceso al sistema de información o a una parte del mismo (pudiendo recaer sobre alguno de los elementos que hemos señalado), lo cual supone un claro adelantamiento de la intervención penal.

iv. Realización de la conducta típica por cualquier medio o procedimiento, vulnerando las medidas de seguridad impuestas y sin autorización.

Tal y como establece la propia redacción, el acceso o mantenimiento en el sistema de información podrá realizarse a través de cualquier medio o procedimiento. El establecimiento de esta cláusula abierta supone un acierto por parte del legislador, puesto que, en la actualidad, existe una infinidad de formas por medio de las cuales un sujeto puede acceder a un ordenador, cuya delimitación podría conllevar a considerar atípicos determinados medios de acceso que no cumplieren con los requisitos exigidos por el tipo. En atención a ello, conviene mencionar algunas de las conductas que recientemente son empleadas para acceder de forma ilícita a un sistema: el descifrado de contraseñas (o *password guessing*, entendido como aquel proceso de recuperación de contraseñas almacenadas en un equipo), *phishing* (técnica consistente en la captación de información mediante engaño), la creación de puertas traseras (o *backdoors*, creación de un acceso al sistema, que permite sortear los sistema de seguridad en él establecidos), caballos de Troya o troyano (software malicioso, que se presenta ante el titular del sistema con la apariencia de un programa legítimo o inofensivo), o la utilización de herramientas que permitan el acceso remoto (conducta a la que ya hemos hecho referencia)[144].

Por otro lado, se exige que se establezcan medidas de seguridad sobre el sistema de información que impidan el acceso a terceros. Tal exigencia se configura como un

[144] BARRIO ANDRÉS, en: *Ciberdelitos: Amenazas criminales del ciberespacio*, 2017, pág. 64.

elemento del tipo sin el cual no existiría tipicidad de la acción, por lo tanto, el acceso a un sistema de información que no disponga de barrera de protección alguna, no supondrá un ilícito penal. En este sentido, resulta complejo determinar qué nivel de seguridad será el exigible, no obstante, algunos autores[145] consideran que la protección habrá de ser adecuada a la técnica, usos o costumbres de la propia sociedad. En consecuencia, las medidas podrán consistir, por ejemplo, en el establecimiento de alguna clave o contraseña, en la instalación de antivirus, cortafuegos (*firewall*), o algún sistema de detección de espías o intrusos (*anti-spyware, IDS- intrusion detection system*)[146].

Junto al requisito anterior, se requiere que el sujeto activo no actúe con autorización de aquel que sea el titular del sistema de información o aquel que disponga de legítimo derecho a excluirlo (por ejemplo, un delegado). Asimismo, y como ya hemos señalado, respecto al mantenimiento en un sistema de información, la autorización habrá de recaer sobre la conducta de no abandono y no sobre el acceso.

6.3.2. Tipo subjetivo.

Respecto al tipo subjetivo, bastará la concurrencia del dolo, produciéndose la consumación del delito con el mero acceso o mantenimiento en el sistema de información, no siendo preciso que exista un elemento subjetivo de lo injusto, ni que se produzca un efectivo daño. En el caso de que la conducta de acceso se realice para producir un menoscabo o inutilización de todo o parte del sistema (conducta también conocida como *cracking*), podrá surgir un concurso con el delito de daños regulado en los arts. 264 y ss. CP.

En este punto, resulta relevante reseñar que ciertos autores[147] han analizado la posible atipicidad de aquella conducta conocida como "intrusismo blanco" o "*hackering* blanco", la cual consiste en el acceso a otros equipos con la finalidad de reportar aquellos fallos en el sistema de seguridad y dar aviso de los mismos a sus titulares. No obstante, en atención a la regulación actual, dicha conducta es ilícita, en virtud de que reúne todos los elementos del tipo, resultando irrelevante la finalidad de la misma.

[145] COLÁS TURÉGANO, en: Revista Boliviana de Derecho núm. 21, 2016, pág. 219.
[146] BARRIO ANDRÉS, en: *Ciberdelitos: Amenazas criminales del ciberespacio*, 2017, pág. 65. GÓNZALEZ CUSSAC, en: GÓNZALEZ CUSSAC (Coord.), *Derecho Penal Parte Especial*, 2016, pág. 287.
[147] COLÁS TURÉGANO, en: Revista Boliviana de Derecho núm. 21, 2016, pág. 213.

En último lugar, conviene hacer referencia a la distinta pena prevista para esta modalidad (pena de prisión de 6 meses a 2 años), en contraste con las previstas para los tipos básicos del delito de descubrimiento y revelación de secretos (1 a 4 años y multa de 12 a 24 meses). Esta menor sanción se fundamenta en el distinto bien jurídico protegido que, como señalamos, es la seguridad de los sistemas de información, y no el derecho a la intimidad, aun cuando pueda admitirse la naturaleza de peligro sobre este derecho fundamental.

6.4. Interceptación de transmisiones no públicas de datos informáticos (art. 197 bis 2).

"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".

La interceptación de transmisiones no públicas de datos entre sistemas, contenida en el art. 197 bis 2, es nueva en nuestro ordenamiento jurídico, siendo introducida a través de la LO 1/2015, como consecuencia de las exigencias impuestas por la Directiva 2013/40/UE (art. 6). Como señalamos anteriormente, la inclusión por parte del legislador penal de esta conducta se ha producido de modo casi literal, sin haber realizado una autentica labor de transposición o aproximación legislativa, lo cual además de atentar contra el principio de seguridad jurídica, ha conformado una legislación confusa y oscura.

Esta figura impone una pena de prisión de 3 meses a 2 años, o multa de 3 a 12 meses, a aquel que, sin hallarse debidamente autorizado y utilizando artificios o instrumentos técnicos, proceda a la interceptación de transmisiones no públicas de datos informáticos, producidos desde, hacia o dentro de un sistema de información, incluyéndose las emisiones electromagnéticas de los mismos.

6.4.1. Distinción con el tipo básico contenido en el segundo inciso del art. 197.1.

Como puede observarse, existen claras similitudes entre esta nueva conducta y aquella relativa a la interceptación de las comunicaciones y empleo de artificios técnicos de escucha, transmisión o reproducción del sonido o imagen, u otras señales de la

comunicación (art. 197.1, segundo inciso). En virtud de ello, deviene preciso delimitar el contenido de ambas conductas.

En primer lugar, en atención al análisis llevado a cabo en el presente trabajo, podemos determinar que, mientras el tipo básico del delito de descubrimiento y revelación de secretos contenido en el art. 197.1, tiene por bien jurídico protegido el derecho fundamental a la intimidad, en contraposición el tipo contenido en el art. 197 bis, tutela un bien jurídico distinto, consistente en la seguridad de los sistemas de información.

Es preciso volver a referir que nos hallamos ante un análisis complejo que actualmente no se halla exento de debate, en este sentido, algunos autores estiman que el bien jurídico protegido por esta nueva conducta es la intimidad, estableciendo la diferenciación entre ambas figuras, en el objeto material de la acción, es decir, el tipo contenido en el art. 197 bis 2 habrá de recaer sobre datos de menor entidad que no afecten directamente a la intimidad personal o familiar del sujeto pasivo[148]. No obstante, en caso de decantarnos por esta interpretación, surgirían claras dificultades en la delimitación entre ambas conductas, pues la figura de interceptación de transmisiones no públicas de datos informáticos, resultaría redundante y la misma dispondría ya de encaje legal en el segundo inciso del art. 197.1.

En consecuencia, si bien consideramos que el bien jurídico protegido por la nueva figura es la seguridad de los sistemas, es preciso concretar la naturaleza de peligro sobre la intimidad, lo cual justificaría su ubicación en el Título X, relativo a los delitos contra la intimidad, propia imagen e inviolabilidad del domicilio. De este modo, no es necesario que la conducta afecte directamente a la intimidad (característica exigida por el tipo básico), superando así la ausencia de sustrato material propio del bien jurídico protegido.

6.4.2. Tipo objetivo.

i. Sujetos activo y pasivo.

Respecto al sujeto activo, habremos de remitirnos a lo anteriormente indicado para el tipo anterior, relativo al acceso o mantenimiento ilícito en un sistema de información.

[148] CASTIÑEIRA PALOU / ESTRADA I CUADRAS, en: SILVA SANCHEZ (Dir.), RAGUÉS I VALLÈS (Coord.), *Lecciones de Derecho Penal. Parte Especial*, 2015, pág. 164 y ss.

En cuanto al sujeto pasivo, será aquella persona titular de un sistema de información cuyas transmisiones de datos informáticos (o emisiones electromagnéticas) sean interceptadas.

ii. Conducta típica.

La conducta típica de esta figura consiste en la interceptación, sin la debida autorización y por medio de artificios o instrumentos técnicos, de aquellas transmisiones no públicas de datos informáticos, producidos desde, hacia o dentro de un sistema de información.

El término "interceptación", viene definido por el considerando 9, de la Directiva 2013/40/UE, el cual indica que "*La interceptación abarca, sin limitarse necesariamente a ello, la escucha, el seguimiento y el análisis del contenido de comunicaciones, así como la obtención del contenido de los datos bien directamente, mediante el acceso y recurso a ese sistema de información, o indirectamente, mediante el recurso a sistemas de escucha y grabación electrónicos por medios técnicos"*. Es decir, al igual que en el tipo básico de interceptación de las telecomunicaciones, la conducta típica abarca una multitud de comportamientos a través de los cuales el sujeto activo puede captar las transmisiones no públicas de datos informáticos.

De conformidad con la redacción penal, se exige que la interceptación se lleve a cabo mediante la utilización de artificios o instrumentos técnicos, configurándose como un elemento del tipo y no siendo preciso que se produzca mediante la vulneración de medidas de seguridad. De este modo, se restringe la intervención penal, a aquellos supuestos en que la interceptación se realice mediante el uso de algún dispositivo técnico que permita la escucha, seguimiento, o análisis del contenido de las comunicaciones, o la obtención del contenido de los datos, no siendo relevantes las conductas de carácter manual o directo.

Al no ser definidos en el CP tales artificios o instrumentos técnicos, es preciso acudir al Informe explicativo del Convenio sobre la Ciberdelincuencia, el cual establece en su párrafo 53 lo siguiente: "*El término "medios técnicos" incluye los dispositivos técnicos conectados a las líneas de transmisión, así como también los dispositivos utilizados para obtener y grabar las comunicaciones inalámbricas. Pueden incluir el uso de software, contraseñas y códigos"*. En virtud de ello, la interceptación podrá realizarse

a través de un medio técnico que permita la conexión a líneas de transmisión (por ejemplo, la interceptación de la línea telefónica a través de un sistema conectado por cable a un router), o que permita la obtención o grabación de comunicaciones que no se produzcan por medios inalámbricos (por ejemplo, la intercepción de la línea wifi).

Junto a ello, es preciso que el sujeto activo realice la conducta sin estar debidamente autorizado a ello. Respecto a este elemento, se exige que, en su caso, la autorización sea otorgada por aquel que fuere propietario u otro titular del derecho sobre el sistema de información (art. 2 d), Directiva 2013/40/UE).

iii. Objeto material.

En lo relativo al objeto material de la presente conducta, serán las "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". En atención a ello, hemos analizar cada uno de los elementos que componen el mismo.

En primer lugar, es conveniente señalar que la LO 1/2015 establece en su preámbulo que esta nueva figura tipifica la interceptación de transmisiones automáticas –no personales– entre equipos. Su análisis resulta significativo, en virtud de que el legislador opta por no incluir el término "automáticas" en la redacción del art. 197 bis 2. En este sentido, existe una clara diferenciación entre el significado de "automáticas" y "no públicas", no obstante, su inclusión en el preámbulo puede resultar clarificadora, a los efectos de entender y discernir de otras figuras, el objeto material sobre el que ha de recaer esta nueva figura. En consecuencia, hemos de entender que las transmisiones "automáticas" de datos informáticos, que podrán ser interceptadas, serán aquellas que tengan un origen en la previa programación o en el funcionamiento interno del sistema, sin que exista en la propia transmisión un comportamiento humano; por tanto, las comunicaciones interpersonales no se encontrarían dentro del objeto material[149]. Algunos autores[150] consideran que la inclusión de tal término en el art. 197 bis 2 resulta necesaria,

[149] FISCALÍA GENERAL DEL ESTADO, *Circular 3/2017, 6 de julio de 2017*, pág. 23 y ss.
[150] VALDÉS-SOLÍS IGLESIAS, en.: *Los delitos contra los sistemas informáticos: arts. 197 bis y 197 ter del código penal*, 2017, pág. 7 y ss.

no obstante, y pese a su ausencia, es interpretado como un elemento más del objeto material[151].

Por otra parte, la redacción establece que las transmisiones sean "no públicas", lo cual no es equiparable a que las mismas sean privadas. Su significación deviene compleja, puesto que ha de interpretarse en un sentido amplio, como aquellas transmisiones de datos informáticos, que se hallen excluidos del conocimiento de terceros, o que no sean accesibles a los mismos[152]. De conformidad con el Informe explicativo del Convenio de Cibercriminalidad, párrafo 54, el carácter no público, puede desprenderse de datos que, pese a ser accesibles al público, pretendan ser transmitidos de forma confidencial, por ejemplo, en un ámbito comercial, serán datos no públicos aquellos que, aun cuando sean transmitidos mediante una red pública, se hallen restringidos a terceros hasta el efectivo pago del servicio (como ocurriría en el caso de las plataformas de series comercializadas por internet). Por tanto, serán datos no públicos los efectuados por redes privadas o públicas cuando dispongan de un carácter reservado.

Respecto a la definición de "datos informáticos", hemos de remitirnos a la otorgada por la Directiva 2013/40/UE, la cual fue referenciada anteriormente.

Además de ello, establece la redacción que las transmisiones de datos sean producidas desde, hacia o dentro de un sistema informático, ello implica que la interceptación podrá recaer sobre una comunicación que tenga lugar entre dos o más sistemas de información, entre dos o más sistemas conectados a través de una misma red local (por ejemplo, en un centro de trabajo, los ordenadores suelen hallarse interconectados a través de una misma red), en un mismo sistema informático (comunicación entre los distintos componentes, por ejemplo, la CPU y la pantalla), o entre un sistema y una persona (a través del teclado, o ratón)[153].

En último lugar, la conducta de interceptación podrá recaer sobre las "emisiones electromagnéticas", configurado como un objeto material alternativo a las transmisiones

[151] ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, pág. 273: "*esta expresión nos aleja todavía más de la intimidad como objeto de protección en beneficio de la seguridad de los sistemas informáticos (…) De nuevo se refuerza la observancia de lo inadecuado de la ubicación elegida para este delito*".
[152] CASTIÑEIRA PALOU / ESTRADA I CUADRAS, en: SILVA SANCHEZ (Dir.), RAGUÉS I VALLÈS (Coord.), *Lecciones de Derecho Penal. Parte Especial*, 2015, pág. 164 y ss.
[153] Informe explicativo del Convenio de Cibercriminalidad, párr. 55.

de datos informáticos. Si bien, su contenido no viene determinado por la norma penal, habrán de entenderse como aquellas ondas o radiaciones que emiten los dispositivos electrónicos (en este caso, los sistemas de información), a través de las cuales pueden reconstruirse los datos informáticos provenientes de los mismos[154]. En este sentido, Velasco Nuñez las define como "*emisiones o transmisiones entre sistemas, diálogos entre máquinas, no humanas, transmisiones automáticas entre equipos, máquinas, cuyos rastros y datos pueden dar información sobre costumbres privadas de un usuario, por ejemplo, si hay conexión con un router o si se está con un aparato encendido, que pueden dar información locativa o temporal sobre las costumbres de una persona*"[155].

La introducción de las emisiones electromagnéticas como objeto material de la conducta resulta del todo acertada, puesto que, a falta de ella, resultarían atípicos aquellos comportamientos de interceptación de emisiones realizados con la finalidad de reconstruir los datos informáticos de un sistema de información, que alcanzarían un desvalor igual al producido mediante la interceptación de transmisiones de datos informáticos.

6.4.3. Tipo subjetivo.

Será suficiente la concurrencia del dolo, no exigiendo el tipo que el sujeto activo actúe con intención de descubrir los secretos o vulnerar la intimidad de otro, elemento subjetivo de lo injusto que, por el contrario, concurre en el tipo básico del segundo inciso del art. 197.1. En el caso de que la interceptación de transmisiones de datos informáticos se realizare concurriendo tal elemento subjetivo de lo injusto, nos hallaríamos ante un concurso de normas (entre el art. 197.1, segundo inciso, y el art. 197 bis 2), que exige ser resuelto a través del art. 8.3º CP, que establece que, el precepto más amplio o complejo habrá de absorber al que castigue la infracción consumida en aquel, resultando de aplicación, en este supuesto, el art. 197.1.

En base a lo expuesto, puede observarse la distinción entre el objeto material del presente delito de aquel contenido en el segundo inciso del art. 197.1, radicando la principal diferencia en el carácter automatizado de aquel, no exigiendo que el mismo sea una comunicación interpersonal. Ello permite constatar que nos hallamos ante bienes jurídicos distintos, tal y como enunciamos anteriormente, la seguridad de los sistemas y

[154] *Ibidem*, párr. 57.
[155] VALDÉS-SOLÍS IGLESIAS, en.: *Los delitos contra los sistemas informáticos: arts. 197 bis y 197 ter del código penal*, 2017, pág. 13.

el derecho a la intimidad. En consecuencia, deviene complejo establecer una conexión entre la intimidad y la interceptación de transmisiones automáticas al carecer éstas de un componente personal. No obstante, dado el empleo de los sistemas de información en nuestra sociedad actual, ha de considerarse que la interceptación de transmisiones de datos, aun cuando no supongan un atentado directo contra la intimidad, pueden plantear un riesgo sobre determinados ámbitos que se hallan reservados.

Además de ello, el distinto bien jurídico protegido por ambas figuras, justifica el distanciamiento entre las penas impuestas por una y otra figura, pues, mientras el tipo básico contenido en el art. 197.1 castiga con una pena de prisión de 1 a 4 años y multa de 12 a 24 meses, la nueva figura dispone una pena de prisión de 3 meses a 2 años o multa de 3 a 12 meses.

6.5. Producción, adquisición para su uso, importación o facilitación de instrumentos para la comisión de los delitos contenidos en los arts. 197.1 y 2 y 197 bis (art. 197 ter).

"Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:

a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información".

El art. 197 ter, plantea una nueva figura que, al igual que las dos anteriores surge con la Reforma de 2015, como consecuencia de la transposición de la Directiva 2013/40/UE (art. 7). La creación de este nuevo tipo supone un adelantamiento de la barrera de protección[156], pues castiga comportamientos de mero favorecimiento o preparatorios. En concreto, se impone una pena de prisión de 6 meses a 2 años o multa de 3 a 18 meses a aquel, que no hallándose debidamente autorizado, produzca, adquiera

[156] BARRIO ANDRÉS, en: *Ciberdelitos: Amenazas criminales del ciberespacio*, 2017, pág. 70.

para su uso, importe o, de cualquier manera, facilite a terceros, instrumentos o herramientas que tengan por finalidad facilitar la comisión de los delitos contenidos en el art. 197. 1 y 2, o en el art. 197 bis; en concreto dichos instrumentos o herramientas habrán de consistir en: programas informáticos, adaptados para cometer tales delitos, o contraseñas de ordenadores, códigos o datos similares, que permitan acceder a todo o parte de un sistema de información.

La introducción de esta figura, por parte de la Directiva 2013/40/UE, se fundamenta en la preocupación de los ataques a gran escala que pueden producirse en el seno de la UE (tanto para sus infraestructuras, como para las entidades, organismos e instituciones de los Estados miembros). De este modo, la propia Directiva, señala en su considerando 5, que: "*Se comprueba una tendencia hacia ataques de gran escala cada vez más graves y recurrentes contra sistemas de información, que a menudo pueden ser críticos para los Estados miembros o para determinadas funciones del sector público o privado. Esta tendencia coincide con el desarrollo de métodos cada vez más sofisticados, como la creación y utilización de redes infectadas (botnets), que conllevan fases múltiples del acto delictivo, cada una de las cuales puede por sí sola constituir un grave peligro para el interés público*". En virtud de ello, la Directiva aboga por la configuración de una normativa común, en relación a los elementos constitutivos de las infracciones penales (considerando 8), así como por una cooperación entre los Estados, con la finalidad de dar una respuesta adecuada a estas nuevas conductas, que pueden plantear graves perjuicios.

Como puede observarse, la normativa no se limita a la punición de ataques a gran escala, sino que opta por la tipificación de los actos preparatorios sin restringir ni exigir que disponga de consecuencias sobre un ámbito extenso. Por tanto, la inclusión de esta figura se halla encaminada a la prevención de los posibles ataques que, a través de los sistemas de información, puedan producirse sobre la intimidad o seguridad de los sistemas, como bienes jurídicos protegidos por los arts. 197.1 y 2, y 197 bis.

6.5.1. Tipo objetivo.

i. Conducta típica.

En lo relativo a la conducta típica, el tipo incluye en su redacción distintos comportamientos a través de las cuales puede consumarse el tipo como la producción, la adquisición para su uso, la importación o cualquier otra conducta de facilitación a terceros

de los instrumentos o herramientas que faciliten la comisión de los delitos del arts. 197.1 y 2 y 197 bis. No obstante, el legislador opta por no incluir entre los mismos, la mera posesión de tales instrumentos. En este sentido, la Circular de la Fiscalía 3/2017[157] estima que la acción de posesión es alcanzada por medio de las conductas referidas[158]. En igual sentido se expresa Estrada i Cuadras considerando que la mera posesión no resulta punible[159].

Además de ello, la redacción exige que el sujeto activo realice la conducta típica sin disponer de la debida autorización. Tal autorización podrá preverse legalmente o ser encomendada por una persona que disponga de capacidad para ello, en el concreto marco de una actividad (por ejemplo, auditoria de seguridad de un sistema)[160].

ii. Objeto material.

El objeto material del presente delito podrá ser un programa informático que haya sido concebido o adaptado principalmente para la comisión de los delitos indicados (apartado a.) o, por otra parte, una contraseña de un ordenador, un código de acceso o dato similar que permita el acceso a un sistema de información o a parte del mismo (apartado b.).

En primer lugar, el programa informático o software, como señalamos anteriormente en el presente trabajo, es un conjunto o cadena de instrucciones que el sistema ejecuta para un fin o tarea concreta[161]. La presente figura exige que el programa sea creado o modificado con la finalidad de cometer alguno de los delitos contenidos en los arts. 197.1 (descubrir los secretos o vulnerar la intimidad, mediante el apoderamiento de secretos documentales, interceptación de comunicaciones, empleo de medios técnicos de escucha, transmisión o reproducción de sonido o imagen, u otra señal de la comunicación), 197.2 (acceso, apoderamiento, utilización, modificación o alteración de

[157] FISCALÍA GENERAL DEL ESTADO, *Circular 3/2017, 6 de julio de 2017,* pág. 31.
[158] VALDÉS-SOLÍS IGLESIAS, en.*: Los delitos contra los sistemas informáticos: arts. 197 bis y 197 ter del código penal*, 2017, pág. 19: "*Sin embargo, el tipo penal no hace referencia expresa a la posesión del programa o código, haciendo descansar la punición de tal comportamiento en la expresión adquiera para su uso. (…) Además, la adquisición para su uso tiene una connotación de obtención del programa o código a título oneroso. Por tanto, puede plantear problemas de tipicidad la conducta de recepción a título gratuito de dicho material, sin perjuicio de que dicha entrega sí sea típica*"
[159] CASTIÑEIRA PALOU / ESTRADA I CUADRAS, en: SILVA SANCHEZ (Dir.), RAGUÉS I VALLÈS (Coord.), *Lecciones de Derecho Penal. Parte Especial*, 2015, pág. 166.
[160] FISCALÍA GENERAL DEL ESTADO, *Circular 3/2017, 6 de julio de 2017*, pág. 19.
[161] Directiva 2013/40/UE, art. 6 b).

datos personales), 197 bis.1 (acceso o mantenimiento ilícito en un sistema de información) o 197 bis.2 (interceptación de transmisiones no públicas de datos informáticos). Es preciso indicar que será indiferente que tales programas dispongan, además de aquélla, de alguna función distinta[162].

En consecuencia, el programa será diseñado o alterado con la finalidad de infiltrarse u obtener información de la víctima, con independencia de la técnica o vía de entrada que emplee el mismo. En este sentido, un software con tales características puede ser introducido en un sistema de información a través de correo electrónico, páginas web, mensajería instantánea, dispositivos de almacenamiento externos (como serían las memorias USB o los CDs), etc. Algunos ejemplos de tales softwares maliciosos (o *malware*), son los de espionaje (o *spyware*, que permiten el seguimiento de la actividad producida en un sistema de información), o los de registro de teclas (o *keylogger*, que se encargan de registrar las pulsaciones del teclado para adquirir contraseñas o datos de un sistema).

En relación con lo anterior, la propia Directiva en su considerando 16 examina la tipicidad de aquellos instrumentos adecuados (o especialmente adecuados) que, pese a facilitar la comisión de los delitos indicados, fueren creados o comercializados con fines legítimos, como probar la fiabilidad de algún producto tecnológico o la seguridad de un sistema de información. Atendiendo a los mismos, la propia Directiva concluye que, tales supuestos serán atípicos mientras no exista voluntad de facilitar a terceros alguna de las conductas contenidas en los arts. 197. 1 y 2 y 197 bis[163].

En lo referente al segundo objeto material sobre el que puede recaer la conducta, serán las contraseñas de ordenador, códigos o datos similares que permitan el acceso a todo o parte de un sistema de información. La conducta de "producir", contenida en la propia figura, resulta de difícil aplicación a este objeto material, pues el apartado b), viene referido a la disponibilidad de una contraseña, código de acceso o dato similar existente,

[162] GONZÁLEZ COLLANTES, en: Revista de Derecho Penal y Criminología Universidad Nacional de Educación a Distancia, núm. 13, 2015, pág. 76.
[163] VALDÉS-SOLÍS IGLESIAS, en.: *Los delitos contra los sistemas informáticos: arts. 197 bis y 197 ter del código penal*, 2017, pág. 20: "*En mi opinión, es muy complicada la inclusión de tal software dual en el tipo penal por varios motivos: se trata de software de acceso sencillo, cuya aplicación principal es la auditoría de seguridad, de difícil prueba en cuanto a la finalidad delictiva y cuya tenencia se compagina mal con la expresión literal de que se trate de un programa informático adaptado principalmente para la comisión de tales delitos*".

y no a la producción de un nuevo dato que permita el acceso. Es decir, las contraseñas, códigos de acceso o datos similares, habrán sido creadas legítimamente, produciéndose la tipicidad cuando las mismas sean adquiridas para su uso, importadas o de cualquier modo facilitadas a terceros, a fin de cometer los delitos señalados[164].

6.5.2. Tipo subjetivo.

Esta figura, exige que el sujeto activo actúe con dolo, precisando que junto al mismo concurra un elemento subjetivo específico, consistente en la intención de facilitar la comisión de los delitos contenidos en los arts. 197.1 y 2 y 197 bis. Respecto a este elemento, cabe indicar que no bastará la mera presunción, sino que habrá de ser acreditado mediante pruebas o indicios que corroboren tal afirmación[165]. Se configura como un elemento más del tipo, sin el cual la conducta no dispondría de relevancia penal.

En atención a lo expuesto, conviene precisar que, pese a que el legislador eleva a la categoría de autoría los actos preparatorios, la presente figura impone una pena significativamente menor a la impuesta para los tipos básicos del art. 197.1 y 2, concretamente establece una pena de prisión de 6 meses a 2 años y una pena de multa, configurada de forma alternativa a la anterior, de 3 a 18 meses. Sin embargo, las penas son equivalentes a las previstas para el art. 197 bis 1 y 2, lo cual puede justificarse en el mayor peligro que puede plantear esta figura sobre la intimidad.

Finalmente, conviene delimitar esta figura respecto a aquella contenida en el art. 197 bis 1, concretamente respecto a la conducta de facilitación a un tercero el acceso a un sistema de información o parte del mismo. En virtud de lo anterior, algunos autores estiman que se produce un solapamiento inadecuado entre ambas conductas[166], produciendo un concurso de normas, que exige ser resuelto por el principio de absorción establecido en el art. 8.3 CP. En este sentido, al hallarnos ante una figura que tipifica un

[164] FISCALÍA GENERAL DEL ESTADO, *Circular 3/2017, 6 de julio de 2017*, pág. 34.
[165] GÓNZALEZ CUSSAC, en: GÓNZALEZ CUSSAC (Coord.), *Derecho Penal Parte Especial*, 2016, pág. 288.
[166] COLÁS TURÉGANO, en: Revista Boliviana de Derecho núm. 21, 2016, pág. 222.
ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, pág. 273: "*El posible solapamiento de este delito con el del art. 197 bis (facilitar el acceso ilegal a un sistema informático a un tercero es más teórico que real, pues en relación con este último no se exige ninguna intención específica".*

acto preparatorio, ésta será absorbida por la conducta de acceso del art. 197 bis 1, cuya consumación exige el efectivo acceso al sistema de información[167].

7. Tipos agravados comunes a todas las conductas del Capítulo I del Título X.

7.1. Comisión del delito dentro de una organización o grupo criminal (art. 197 quater).

"Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado".

El art. 197 quater, establece un tipo cualificado que prevé aplicar las penas superiores en grado cuando las conductas del Capítulo I del Título X, sean cometidas en el seno de una organización o grupo criminal.

La inclusión de este tipo agravado en nuestro CP se produjo en el año 2010 como consecuencia de la Decisión Marco 2005/222/JAI. Si bien esta norma limitaba la aplicación del presente tipo a aquellas conductas de acceso ilícito a un sistema de información, el legislador español optó por ampliar tal ámbito, resultando de aplicación a todas las conductas que se encontraban contenidas en el art. 197 (esto es, el acceso ilícito a un sistema de información, y los tipos básicos del delito de descubrimiento de secretos). Mediante la Reforma de 2015, el legislador ha optado, no solo por mantener tal ámbito de aplicación, sino por extender el mismo a todo el Capítulo I, opción que ha sido criticada por algunos autores[168].

La fundamentación de esta agravación radica en la mayor insidia que plantea la realización de alguna de las conductas contenidas en el Capítulo I en un contexto criminal organizado. En virtud de ello, resulta preciso establecer el significado de organización criminal, para lo cual hemos de acudir al art. 570 bis 1 CP: "*la agrupación formada por más de dos personas con carácter estable o por tiempo indefinido, que de manera concertada y coordinada se repartan diversas tareas o funciones con el fin de cometer delitos*". Encontrando la definición de grupo criminal, en el art. 570 ter 1 CP: "*la unión de más de dos personas que, sin reunir alguna o algunas de las características de la*

[167] COLÁS TURÉGANO, en: Revista Boliviana de Derecho núm. 21, 2016, pág. 219 y ss.
[168] GÓNZALEZ CUSSAC, en: GÓNZALEZ CUSSAC (Coord.), *Derecho Penal Parte Especial*, 2016, pág. 288.
GONZÁLEZ COLLANTES, en: Revista de Derecho Penal y Criminología Universidad Nacional de Educación a Distancia, núm. 13, 2015, págs. 77 y ss.

organización criminal definida en el artículo anterior, tenga por finalidad o por objeto la perpetración concertada de delitos".

7.2. Agravación por cualidad del sujeto activo, cuando el mismo fuere autoridad o funcionario público (art. 198).

"La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años".

El art. 198 dispone un tipo agravado que eleva las penas en su mitad superior y establece una inhabilitación absoluta de 6 a 12 años, cuando el sujeto activo que, disponiendo de la condición de autoridad o funcionario público, fuera de los casos permitidos por la ley, sin existir causa legal, y prevaliéndose de tal cargo, llevare a cabo alguna de las conductas contenidas en el artículo anterior.

En primer lugar, es preciso reseñar la deficiente y precipitada adaptación de este tipo agravado por parte del legislador, pues dispone que la agravación será aplicable a "las conductas descritas en el artículo anterior", cuya interpretación literal resulta compleja e incongruente, en virtud de que el artículo anterior existente en el actual CP es el art. 197 quinquies, que hace referencia a la responsabilidad de la persona jurídica[169]. En atención a ello, se plantean problemas de difícil solución que exigirán un desarrollo jurisprudencial.

Concretamente y atendiendo a la configuración de tal tipo agravado, el intérprete no puede discernir si resulta de aplicación al art. 197, 197 bis, 197 ter, o a la totalidad de conductas contenidas en el Capítulo I. Asimismo, la doctrina se halla dividida, pues existen pronunciamientos dispares, en relación a ello Romeo Casabona estima que: "*No cabe duda de que se remite al art. 197, aunque ya no sea el "anterior" en sentido estricto, pero no está claro si también lo hace a los demás delitos que figuran previamente y a*

[169] En este sentido se expresan:
- ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, págs. 265 y ss.
- VALDÉS-SOLÍS IGLESIAS, en.: *Los delitos contra los sistemas informáticos: arts. 197 bis y 197 ter del código penal*, 2017, pág. 23 y ss.

cuáles, en su caso. Puesto que son delitos heterogéneos, aquí la duda debe resolverse a favor del acusado, por respeto de la prohibición de la analogía in malam partem y no aplicar esta agravación en los demás delitos, pudiendo acudir directamente a ellos si resultan cometidos"[170] Pese a que, autores como Muñoz Conde[171] y Estrada i Cuadras[172], se pronuncian en igual sentido que Romeo Casabona, tal concepción plantea inconvenientes en relación a la conducta de acceso ilícito a un sistema de información que, con anterioridad a la Reforma del CP de 2015, se situaba en el apartado tercero del art. 197, ello de conformidad con su nueva ubicación en el art. 197 bis junto a las figuras de interceptación de transmisiones no públicas de datos informáticos (art. 197 bis 2) y de producción de herramientas para cometer delitos (art. 197 ter). Por otra parte, Colás Turégano se decanta por considerar que este tipo es de aplicación a todas las figuras delictivas del Capítulo I del Título X del CP[173].

En lo relativo a la condición de "autoridad" y "funcionario público", hemos de acudir al art. 24 CP que establece que: *"1. A los efectos penales se reputará autoridad al que por sí solo o como miembro de alguna corporación, tribunal u órgano colegiado tenga mando o ejerza jurisdicción propia. En todo caso, tendrán la consideración de autoridad los miembros del Congreso de los Diputados, del Senado, de las Asambleas Legislativas de las Comunidades Autónomas y del Parlamento Europeo. Se reputará también autoridad a los funcionarios del Ministerio Fiscal. 2. Se considerará funcionario público todo el que por disposición inmediata de la Ley o por elección o por nombramiento de autoridad competente participe en el ejercicio de funciones públicas"*. La exigencia de que el sujeto activo disponga de tal condición, configura esta figura como un delito especial impropio[174].

Además de ello, el presente tipo exige que el sujeto activo realice la conducta "fuera de los casos permitidos por la Ley", "sin mediar causa legal por delito"[175] y

[170] ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, págs. 266.
[171] MUÑOZ CONDE, en: *Derecho Penal. Parte Especial*, 2015, pág. 242.
[172] CASTIÑEIRA PALOU / ESTRADA I CUADRAS, en: SILVA SANCHEZ (Dir.), RAGUÉS I VALLÈS (Coord.), *Lecciones de Derecho Penal. Parte Especial*, 2015, pág. 167.
[173] COLÁS TURÉGANO, en: Revista Boliviana de Derecho núm. 21, 2016, pág. 226. En idéntico sentido: VALDÉS-SOLÍS IGLESIAS, en.: *Los delitos contra los sistemas informáticos: arts. 197 bis y 197 ter del código penal*, 2017, págs. 23 y ss.
[174] GÓNZALEZ CUSSAC, en: GÓNZALEZ CUSSAC (Coord.), *Derecho Penal Parte Especial*, 2016, pág. 289-
[175] Estas fórmulas son empleadas por otros preceptos del CP, como el art. 167, relativo a las detenciones ilegales o secuestros cometidos por autoridad o funcionario público.

"prevaliéndose de su cargo". En atención a tales exigencias, es preciso indicar que esta no es una conducta pluriofensiva, pues el bien jurídico protegido es la intimidad, no siendo objeto de tutela el correcto ejercicio de la función pública.

En virtud de lo anterior, es importante delimitar el ámbito de aplicación de esta figura de aquellas contenidas en los arts. 534 a 536 (delitos cometidos por funcionarios públicos contra la inviolabilidad domiciliaria y demás garantías de la intimidad), las cuales no protegen directamente la intimidad, sino las garantías constitucionales y legales de la misma[176]. En el supuesto de que se realice la conducta mediando causa legal por delito habremos de acudir a éstas últimas figuras; resultando de aplicación el presente tipo agravado, cuando la autoridad o funcionario actúe prevaliéndose de su cargo, de conformidad con el "dominio social típico" [177] que estas figuras representan.

Asimismo, es preciso plantear las diferencias entre el presente tipo agravado, y aquella conducta contenida en el art. 417, que castiga a aquel que, siendo autoridad o funcionario público, revelare los secretos o informaciones de los que tuviera conocimiento por razón de su cargo u oficio. En este sentido, el TS indicó que: "*La diferencia esencial entre las conductas contempladas en los artículos 197 y 198 y el 417, cometidas por un funcionario o autoridad, se centra en la legalidad del acceso a la información reservada a la que se refieren dichos preceptos. El artículo 197 parte de la exigencia de que el autor no esté autorizado para el acceso, el apoderamiento, la utilización o la modificación en relación a los datos reservados de carácter personal o familiar, castigándose en el artículo 198 a la autoridad o funcionario público que, fuera de los casos permitidos por la ley, sin mediar causa legal por delito y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior. Mientras que el artículo 417 castiga la revelación de secretos o informaciones que no deban ser divulgados, y de los que la autoridad o funcionario público haya tenido conocimiento por razón de su oficio o cargo"* [178].

[176] GÓNZALEZ CUSSAC, en: GÓNZALEZ CUSSAC (Coord.), *Derecho Penal Parte Especial*, 2016, pág. 290.
[177] ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, pág. 266.
[178] STS 377/2013, de 3 de mayo.

8. Revelación de secretos laborales o profesionales (art. 199).

"1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años".

El art. 199 incluye una figura que es situada dentro del Capítulo I, de forma separada a los tipos básicos y a las nuevas conductas, contenidas en los arts. 197 bis y ter. En este tipo, al contrario que en los anteriores (en los que, por lo general, el sujeto activo accedía a un contenido secreto de una forma ilícita), el sujeto activo conoce el secreto lícitamente, resultando típica la conducta de revelación o divulgación. Esta figura ha sido calificada como un "delito especial" o "delito de indiscreción"[179], cuyo reconocimiento como ilícito penal, señala Romeo Casabona, "*se justifica porque en el caso del secreto laboral se produce una mayor facilidad de acceso a hechos o informaciones confidenciales que propicia el desempeño de su actividad en relación con el empleador, los demás trabajadores, los clientes y otras personas relacionada con aquella*" [180].

En primer lugar, se castiga a aquel que revele secretos conocidos por razón de su oficio o relación laboral, imponiendo una pena de prisión de 1 a 3 años y multa de 6 a 12 meses. Seguidamente, en el apartado segundo, se castiga a aquel sujeto profesional que, incumpliendo su obligación de sigilo, divulgue secretos ajenos, con una pena de prisión de 1 a 4 años, multa de 12 a 24 e inhabilitación especial para dicha profesión de 2 a 6 años.

Respecto a la primera figura conviene definir los términos "oficio" o "relación laboral" contenidos en el mismo, en este sentido Estrada i Cuadras considera que: "*la primera expresión es muy amplia y permite incluir todo tipo de relaciones mercantiles o laborales que impliquen una prestación de servicio, aunque, dadas las características*

[179] MUÑOZ CONDE, en: *Derecho Penal. Parte Especial*, 2015, pág.244.
[180] ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, pág. 275.

del delito, habrá de tratarse de relaciones que supongan contacto de las partes contractuales con la vida privada o intima de una de ellas. En cuanto a la segunda cuestión, el Código no precisa qué parte contractual está obligada a guardar secreto: así, si bien normalmente será el empleado quien conozca secretos de su empleador, no hay que descartar la situación contraria."[181]. Por tanto, el sujeto activo será aquel que ejerza un oficio o mantenga una relación laboral (resultando indiferente si la relación laboral es por cuenta propia o ajena). Mientras que el sujeto pasivo será aquella persona titular de los datos o informaciones de contenido secreto, pudiendo ser un compañero de trabajo, el empleador, el propio trabajador, etc.

En relación al objeto material de esta figura, recaerá sobre un secreto ajeno que haya sido conocido por el sujeto activo por razón de su oficio o relación laboral, resultando indiferente el contenido del secreto, pues no es preciso que guarde relación con tal oficio o relación laboral. Esta figura protege una dimensión de la intimidad concretada en una información secreta. Es importante delimitar el concepto de "secreto", en relación a las conductas referidas, pues es preciso que el mismo se encuentre proyectado sobre la intimidad de terceras personas, no guardando relación con otros intereses (como, por ejemplo, un secreto de empresa, o el deber de secreto, de las autoridades o funcionarios, respecto a los intereses de la seguridad nacional, cuya regulación se efectúa por medio de figuras distintas a la aquí expuesta)[182].

La acción típica de este tipo viene determinada por la propia redacción, consistiendo en la revelación de aquel secreto ajeno. En virtud de ello, Romeo Casabona considera que "*El deber de secreto no está sujeto a límite temporal alguno, pues la obligación de reserva persiste en el tiempo mientras la revelación del secreto pueda comportar un riesgo para la intimidad; es decir, la obligación de secreto perdura más allá de la relación laboral o de la prestación realizada"*[183]. Por tanto, la consumación de la conducta podrá producirse aun cuando se halle extinta la relación laboral, no resultando típica (pese a no configurarlo la propia redacción) aquella conducta de revelación consentida o autorizada por el titular del secreto.

[181] CASTIÑEIRA PALOU / ESTRADA I CUADRAS, en: SILVA SANCHEZ (Dir.), RAGUÉS I VALLÈS (Coord.), *Lecciones de Derecho Penal. Parte Especial*, 2015, pág. 168.
[182] ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, pág. 275.
[183] *Ibidem*, pág. 277.

En cuanto a la segunda figura contenida en el art. 199.2, se establece una mayor pena, en comparación con la anterior, en atención a que la presente exige un deber de sigilo mayor que es consecuencia del carácter profesional del sujeto activo. El desarrollo de una actividad profesional, en principio, requerirá estar en posesión de un título académico u oficial que habilite para la práctica de una profesión (ello de conformidad con el art. 403 CP[184], que regula el delito de intrusismo), y tal y como indica Muñoz Conde, la misma podrá disponer de "*un Código deontológico y una normativa especial, de carácter disciplinario o colegial, que regula los deberes específicos de sigilo que incumben a la respectiva profesión"* [185]. Por tanto, el sujeto activo de la conducta, será aquella persona que, encontrándose en posesión de un título habilitante, desempeñe una actividad profesional sobre la cual pese una obligación de sigilo o reserva; siendo el sujeto pasivo de la conducta, el titular de los secretos.

Por otro lado, el objeto material del delito serán aquellos secretos (datos o informaciones) sobre los que exista la obligación de sigilo o reserva. En relación a dicha obligación, hemos de indicar que nos hallamos ante una norma penal en blanco que exige ser completada mediante la reglamentación especifica de la concreta profesión. En este sentido, algunas de las profesiones afectadas por tal deber serán las siguientes: abogados y procuradores, médicos y personal sanitario, detectives privados, profesionales del periodismo[186].

En lo que respecta a la acción típica, supone la divulgación de aquellos secretos, con incumplimiento de la obligación profesional de sigilo o reserva. Bastará para consumar la conducta que la información sea revelada a una única persona, excluyéndose la tipicidad, al igual que en la figura anterior, la conducta realizada con consentimiento del titular de los secretos.

[184] Art. 403: "*1. El que ejerciere actos propios de una profesión sin poseer el correspondiente título académico expedido o reconocido en España de acuerdo con la legislación vigente, incurrirá en la pena de multa de doce a veinticuatro meses. Si la actividad profesional desarrollada exigiere un título oficial que acredite la capacitación necesaria y habilite legalmente para su ejercicio, y no se estuviere en posesión de dicho título, se impondrá la pena de multa de seis a doce meses"*.
[185] MUÑOZ CONDE, en: *Derecho Penal. Parte Especial*, 2015, pág. 244.
[186] Hemos de indicar que esta es una actividad discutida, pues si bien la confidencialidad de las fuentes de la información periodística viene garantizada por el art. 20.1 d), no existe, sin embargo, una normativa específica que regule el secreto profesional de dicha profesión.

En último lugar, en atención al elemento subjetivo, ambas conductas exigen la concurrencia del dolo. Por lo que será preciso, que el sujeto activo conozca la naturaleza del secreto, es decir, su carácter reservado.

9. Especial consideración de la persona jurídica (arts. 197 quinquies y 200).

Art. 197 quinquies. "Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33".

Art. 200. "Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código".

El art. 197 quinquies, establece una regulación específica aplicable a aquellos supuestos en que la persona jurídica fuere responsable de los delitos contenidos en los arts. 197, 197 bis y 197 ter. En virtud de ello, se establecen unas penas distintas consistentes en la pena de multa de 6 meses a 2 años. Además de ello, y con carácter discrecional, la norma faculta a los jueces y tribunales, la aplicación de alguna de las penas establecidas en el art. 33.7, apartados b) a g)[187], ello de conformidad con el art. 66 bis.

Tal y como expone la propia redacción, es preciso acudir al art. 31 bis, para determinar si efectivamente la persona jurídica es responsable o no de las conductas

[187] Dispone el art. 33 CP: "7. *Las penas aplicables a las personas jurídicas, que tienen todas la consideración de graves, son las siguientes: a) Multa por cuotas o proporcional. b) Disolución de la persona jurídica. La disolución producirá la pérdida definitiva de su personalidad jurídica, así como la de su capacidad de actuar de cualquier modo en el tráfico jurídico, o llevar a cabo cualquier clase de actividad, aunque sea lícita. c) Suspensión de sus actividades por un plazo que no podrá exceder de cinco años. d) Clausura de sus locales y establecimientos por un plazo que no podrá exceder de cinco años. e) Prohibición de realizar en el futuro las actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito. Esta prohibición podrá ser temporal o definitiva. Si fuere temporal, el plazo no podrá exceder de quince años. f) Inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector público y para gozar de beneficios e incentivos fiscales o de la Seguridad Social, por un plazo que no podrá exceder de quince años. g) Intervención judicial para salvaguardar los derechos de los trabajadores o de los acreedores por el tiempo que se estime necesario, que no podrá exceder de cinco años".*

contenidas en los arts. 197, 197 bis y 197 ter, lo cual exigirá un análisis pormenorizado del caso concreto, dadas las posibilidades que ofrece aquel artículo.

Esta previsión no es nueva, pues la misma fue introducida en nuestro CP mediante la Reforma de 2010 (como consecuencia de la Decisión Marco 2005/222/JAI), en el párrafo segundo, del apartado tercero del art. 197, junto a la conducta de acceso ilícito a un sistema de información. No obstante, a través de la Reforma de 2015, este tipo es reubicado de forma separada, en el actual art. 197 quinquies, resultando de aplicación tanto a los tipos básicos como a las nuevas conductas contenidas en los arts. 197 bis y ter.

Por otra parte, el art. 200, establece expresamente que lo dispuesto en el Capítulo I del Título X, será aplicable cuando el sujeto activo descubra, revele o ceda datos reservados pertenecientes a una persona jurídica, realizando tal conducta sin que medie el consentimiento de sus representantes.

En relación a ello, es preciso remitirnos al análisis efectuado con anterioridad en el presente trabajo, respecto al reconocimiento de la persona jurídica como titular de derechos fundamentales y en concreto, como titular de los derechos a la intimidad, a la inviolabilidad del domicilio y a la autodeterminación informativa o libertad informática. En dicho análisis, se determinó que la persona jurídica puede ser titular de aquellos derechos de carácter fundamental, que precise para la consecución de los fines para los que fuere creada, por tanto, resulta lógico que la misma pueda ser considerada sujeto pasivo de los delitos de descubrimiento y revelación de secretos.

Asimismo, la redacción establece que "lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas", lo cual plantea un problema interpretativo, en virtud de que el legislador no ha adaptado dichas conductas a las nuevas figuras tipificadas en los arts. 197 bis y 197 ter. Pese a tal falta, hemos de afirmar que las personas jurídicas podrán ser sujetos pasivos de las nuevas conductas, de conformidad con la fórmula empleada por el propio precepto "lo dispuesto en ese capítulo será aplicable"[188].

[188] Así lo entienden: VALDÉS-SOLÍS IGLESIAS, en.: *Los delitos contra los sistemas informáticos: arts. 197 bis y 197 ter del código penal*, 2017, pág. 23. Y ROMEO CASABONA, en: ROMEO CASABONA, SOLA RECHE y BOLDOVA PASAMAR (Coords.), *Derecho Penal. Parte especial*, 2016, pág. 274.

10. Requisitos procedimentales: art. 201.

"1. Para proceder por los delitos previstos en este Capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, persona con discapacidad necesitada de especial protección o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

2. No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3. El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal sin perjuicio de lo dispuesto en el segundo párrafo del número 5º del apartado 1 del artículo 130".

Por último, el art. 201 plantea los requisitos de procedibilidad para las conductas contenidas en el Capítulo I del Título X.

En primer lugar, se exige que la persona agraviada por alguno de los delitos expuestos o su representante legal presente denuncia, estableciendo que, si la misma es menor de edad, persona necesitada de especial protección o desvalida, la denuncia podrá ser presentada también por el Ministerio Fiscal. En este sentido, Boix estima que: "*el requisito de perseguibilidad se debe, además de la naturaleza eminentemente personal del bien jurídico, a que, dada la configuración de la intimidad, el proceso penal puede convertirse precisamente en un instrumento que amplifique el daño a la misma, de forma que al restringirla del modo indicado se ofrece al agraviado la posibilidad de calibrar si le interesa desde esa perspectiva abrir o no el proceso penal*"[189].

En segundo lugar, dispone el precepto, que no se exigirá denuncia respecto de las conductas contenidas en el art. 198, ni cuando la comisión del delito comprometa el interés general o afecte a una pluralidad de personas.

En base a lo expuesto, surgen dificultades en relación a la exigencia de denuncia por la persona agraviada, respecto a aquellos actos meramente preparatorios, contenidos en el art. 197 ter, en los cuales resulta complejo identificar quien es el agraviado por los

[189] ANARTE BORRALLO / DOVAL PAIS, en: BOIX REIG (Dir.), *Derecho Penal. Parte Especial*, 2010, pág. 465.

mismos. Pese a ello, hemos de considerar que, en tales casos, no será precisa la interposición de denuncia, de conformidad con el art. 201.2[190].

En último lugar, señala el precepto que, se extinguirá la acción legal con el perdón del ofendido o de su representante legal, no obstante el perdón podrá ser rechazado de conformidad con el art. 130.1, 5º, párr. 2: "*En los delitos contra menores o personas con discapacidad necesitadas de especial protección, los jueces o tribunales, oído el Ministerio Fiscal, podrán rechazar la eficacia del perdón otorgado por los representantes de aquéllos, ordenando la continuación del procedimiento, con intervención del Ministerio Fiscal, o el cumplimiento de la condena"*.

Por tanto, el delito de descubrimiento y revelación de secretos, se configura como un delito de carácter semipúblico.

[190] FISCALÍA GENERAL DEL ESTADO, *Circular 3/2017, 6 de julio de 2017*, págs. 40 y ss.

V. CONCLUSIONES

De todo lo anteriormente expuesto, puede apreciarse la clara complejidad que plantea el delito de descubrimiento y revelación de secretos, en atención a los distintos comportamientos que la propia redacción incluye. En este sentido, resulta patente la variabilidad de conductas que el presente delito comprende, pues no solo protege la intimidad, sino que, además, tutela de forma específica, aspectos como el secreto de las comunicaciones, la autodeterminación informativa respecto a los datos personales, la seguridad de los sistemas de información o incluso los secretos obtenidos como consecuencia de un oficio, actividad laboral o ejercicio profesional.

Tal y como se ha expuesto, este delito no es nuevo en nuestro ordenamiento jurídico, no obstante, se configura como un delito novedoso, en atención a las distintas figuras que el legislador integra mediante la Reforma de 2015. De este modo, se incluyen conductas que son un fiel reflejo de aquellos comportamientos existentes en la sociedad que, suponiendo un claro atentado para el derecho a la intimidad, no disponían de un claro encaje legal.

Por otra parte, si bien, son varias las modificaciones operadas por el legislador, su enumeración resulta innecesaria, pues respecto a ello acabamos de referirnos en las páginas anteriores del presente trabajo. No obstante, existen determinados aspectos que exigen ser reseñados.

En primer lugar, el legislador ha optado por mantener la redacción empleada con anterioridad respecto a los tipos básicos, elección que resulta acertada en virtud de los precedentes jurisprudenciales y doctrinales existentes. Pese a ello, deviene criticable que haya conservado aquellos términos que, con anterioridad a la Reforma de 2015, planteaban ya una redacción oscura y difusa. Concretamente, y tal y como hemos referido, una de las figuras básicas que ha generado mayores problemas interpretativos es la contenida en el art. 197.2 CP (relativa al acceso, apoderamiento, utilización, modificación o alteración de datos reservados de carácter personal o familiar), ya que el empleo de términos similares e incluso idénticos en la propia redacción, impiden establecer una distinción clara entre las conductas típicas.

Por otra parte, respecto a la nueva figura introducida en el art. 197.7 CP, consideramos que la misma supone un acierto en virtud de que tipifica aquella conducta

no autorizada de revelación, difusión o cesión de imágenes que fueran obtenidas con anuencia de la víctima, respecto a la cual, el sistema penal, no otorgaba una correcta respuesta dada su difícil encaje legal entre los delitos contra la intimidad. No obstante, en atención a la redacción empleada por el legislador, surgen determinadas lagunas de punición, cuya solución exige una interpretación forzada de la norma. En concreto, nos referimos a que la propia figura exige que la obtención de las imágenes se realice por el sujeto activo con anuencia de la víctima, en un domicilio o lugar fuera del alcance de la mirada de terceros, quedando fuera del ámbito de punibilidad (en virtud de tal esquema), aquellos supuestos en que es la propia víctima la que elabora y cede a un tercero el material, que será objeto de una posterior difusión. Tal configuración, genera una clara contradicción con el espíritu de la propia norma, cuya determinación aún no resulta clara pues, en la actualidad no existe un desarrollo jurisprudencial suficiente que permita aclarar esta cuestión.

Asimismo, otro de los aspectos reprochables es la configuración de un tipo agravado, de aplicación a la anterior figura, cuando la víctima fuere menor de edad o persona con discapacidad necesitada de especial protección. Respecto a la inclusión de este tipo, hemos de concluir que el mismo atenta contra la seguridad jurídica, pues la conducta exige que la propia víctima preste su anuencia para la obtención de aquellas imágenes o grabaciones audiovisuales, que posteriormente son objeto de difusión no autorizada. En virtud de que la norma no otorga parámetro alguno que permita concluir cuando es válido, en dichos supuestos, el consentimiento otorgado por un menor (como pudiera ser, que tuviera más de dieciséis años y un grado de desarrollo o madurez suficientes), resulta necesario que tal deficiencia en la redacción sea solventada, pues la misma puede generar problemas en relación con los delitos de pornografía infantil.

Por otra parte, en lo referente a los delitos relacionados con los sistemas de información (los cuales son consecuencia de la transposición de distintas normas internacionales), el legislador ha optado por la delimitación de los tipos básicos que afectan a la intimidad (contenidos en el art. 197), de aquellos que, afectando a la privacidad, no afecten directamente a la intimidad, mediante la creación de los arts. 197 bis y ter. A tal respecto conviene indicar que la conducta de acceso o mantenimiento ilícito en un sistema de información planteó, con anterioridad a la Reforma de 2015, divisiones en la doctrina en cuanto a la concreción del bien jurídico protegido por el

delito, no determinándose si el mismo afectaba a la seguridad de los sistemas de información o a la intimidad. En este sentido, entendemos que tales problemas interpretativos no han sido solventados por la mera ubicación separada de tales conductas, pues el legislador no concreta si el bien jurídico es la seguridad de los sistemas, así como tampoco, determina si existe una relación entre este bien y el derecho a la intimidad, dada la permanencia de tales figuras entre los delitos contra la intimidad. Ello plantea complicaciones no solo en cuanto a la determinación de qué conductas han de considerarse típicas, sino también en cuanto a la posible introducción en el CP de una conducta de peligro carente de sustrato material suficiente, esto es, la seguridad de los sistemas.

En relación a lo anterior, hemos de indicar que la conducta de interceptación de transmisiones no públicas de datos informáticos (art. 197 bis 2) resulta una figura novedosa que plantea un claro adelantamiento de la intervención penal. Sin embargo, deviene importante delimitar cuál es el objeto material y el bien jurídico protegido por la misma pues, en atención a la redacción empleada, puede plantear un concurso de normas con el tipo básico de interceptación de las comunicaciones o utilización de medios técnicos de escucha, transmisión o reproducción del sonido o de la imagen u otra señal de la comunicación (segundo inciso, art. 197.1).

En cuanto a la figura contenida en el art. 197 ter, por la cual se tipifica la producción, adquisición para su uso, importación, o facilitación a terceros de herramientas para la comisión de los delitos contenidos en los arts. 197.1 y 2 ó 197 bis, ha de considerarse que su introducción implica un rebasamiento de la intervención penal, en virtud de que se castigan los actos meramente preparatorios. En este sentido, pese a que el legislador justifica tal introducción en los compromisos asumidos internacionalmente, ha de cuestionarse si la vía penal es la idónea para castigar esta clase de conductas.

Conforme a ello, hemos de señalar que la inclusión en el CP de las nuevas figuras contenidas en los arts. 197 bis y 197 ter resultan cuestionables tanto en su contenido como en cuanto a su ubicación entre los delitos de descubrimiento y revelación de secretos. La introducción de tales figuras se ha llevado a cabo mediante una transposición literal de normas internacionales, no realizando el legislador una armonización jurídica entre aquellas y los principios existentes en nuestro sistema penal, lo cual ha provocado una

clara superación de los principios básicos de mínima intervención y *ultima ratio*, existentes en el Derecho Penal.

Para finalizar el presente trabajo y a modo de reflexión, es preciso reseñar que nos hallamos en una época en la cual las nuevas tecnologías han avanzado de un modo tal que resultan imprescindibles en nuestro día a día, de manera que los cambios sobre nuestros derechos fundamentales han devenido ineludibles. En virtud de ello, el derecho a la intimidad personal y familiar ha sufrido una ampliación en cuanto a su contenido, abarcando escenarios que hace algunos años resultaban inimaginables. Sin embargo, al tiempo que se ha producido dicha ampliación, el derecho a la intimidad ha sufrido un vaciamiento de conformidad con la tendencia generalizada de la persona de hacer públicos aquellos ámbitos personales que con anterioridad pertenecían a la esfera privada. Concretamente, ello es resultado del avance en los medios de comunicación y de difusión de contenidos (como son las redes sociales), los cuales se plantean como un arma de doble filo para el derecho a la intimidad.

Como consecuencia de ello, y como el presente trabajo ha pretendido exponer, en los últimos años se han multiplicado los cauces penales a través de los cuales la persona puede salvaguardar su derecho fundamental, no obstante, cada vez resulta más frecuente y fácil que la propia persona sacrifique por sí misma su derecho a la intimidad. Tal planteamiento permite concluir que, si bien resulta importante adaptar a las nuevas realidades, tanto el contenido del derecho a la intimidad, como las vías a través de las cuales tal derecho ha de ser protegido, también es trascendental que la sociedad disponga de información suficiente respecto a sus derechos, para poder disfrutar de los mismos plenamente. En esencia, la persona ha de ser la primera garantía para la protección de los derechos fundamentales que le pertenecen, habiendo de intervenir el Derecho Penal lo mínimo posible y de forma subsidiaria, en atención a su carácter de *ultima ratio*.

VI. BIBLIOGRAFÍA (*).

ANARTE BORRALLO, E. y DOVAL PAIS, A.: "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (1). Delitos contra la intimidad y los datos personales", en AA.VV.: *Derecho Penal. Parte Especial*, Vol. I, BOIX REIG. J (Dir.), Madrid, Iustel, 2010, págs. 441-468.

BARRIO ANDRÉS, M.: "Delitos contra la confidencialidad, integridad y disponibilidad de datos o sistemas informáticos", en *Ciberdelitos: Amenazas criminales del ciberespacio*, Madrid, Reus, 2017, págs. 61-81.

CASTIÑEIRA PALOU, M. T. y ESTRADA I CUADRAS, A.: "Tema 7: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en AA.VV.: *Lecciones de Derecho Penal. Parte Especial*, SILVA SANCHEZ, J. M. (Dir.), RAGUÉS I VALLÈS, R. (Coord.), Barcelona, Atelier, 2015, págs. 153- 171.

COLÁS TURÉGANO, A.: *El delito de intrusismo informático tras la Reforma del Código Penal español de 2015*, Revista Boliviana de Derecho núm. 21, ISSN: 2070-8157, enero 2016, págs. 210-229. Disponible en web: http://idibe.org/wp-content/uploads/2013/09/9._Asunci%C3%B3n_Col%C3%A1s.pdf

DÍAZ TORREJÓN, P.: "Tratamiento penal del sexting", en AA.VV.: *La Reforma de la parte especial del código penal derivada de la Ley Orgánica 1/2015*, MORENO VERDEJO, J. (Dir. de este número), Madrid, Consejo de Redacción de la Revista del Ministerio Fiscal, Fiscalía General del Estado, número 1, 2016, págs. 71-104. Disponible en web: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Comunicaci%C3%B3n%20D%C3%ADaz%20Torrej%C3%B3n,%20Pedro.pdf?idFile=43d70b3a-e3fe-48a1-b222-65c18579552d

FERNÁNDEZ ESTEBAN, M.L.: "Capítulo IV: Protección constitucional de la vida privada. El artículo 18 de la Constitución", en.: *Nuevas tecnologías, Internet y Derechos Fundamentales*, Madrid, McGraw Hill, 1998, págs. 115-127.

[*] Las palabras subrayadas son las que se han utilizado en las citas a pie de página.

FISCALÍA GENERAL DEL ESTADO, *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*, 6 de julio de 2017. Disponible en web: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Circular_3-2017.pdf?idFile=5b2dd5f5-5a18-4732-bc75-7e5a63a9075c

FRIGOLS I BRINES, E.: "La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías", en AAVV.: *La protección jurídica de la intimidad*, BOIX REIG (Dir.), JAREÑO LEAL (Coord.), Madrid, Iustel, 2010, págs. 37-90.

JUANATEY DORADO, C.: "Límites de la protección penal de la intimidad frente a la grabación de conversaciones o imágenes", en AAVV.: *La protección jurídica de la intimidad*, BOIX REIG (Dir.), JAREÑO LEAL (Coord.), Madrid, Iustel, 2010, págs.127-164.

GÓMEZ NAVAJAS, J., *La protección de los datos personales en el Código Penal español*, Revista jurídica de Castilla y León, núm. 16, ISSN 1696-6759, septiembre 2008, págs. 325-372. Disponible en web: https://www.uv.es/limprot/boletin6/gomeznavajas.pdf

GONZÁLEZ COLLANTES, T., *Los delitos contra la intimidad tras la Reforma de 2015: Luces y sombras*, Revista de Derecho Penal y Criminología Universidad Nacional de Educación a Distancia, 3ª época, núm. 13, enero de 2015, págs. 51-84. Disponible en web: http://e-spacio.uned.es/fez/eserv/bibliuned:revistaDerechoPenalyCriminologia-2015-13-7010/pag_51.pdf

GÓNZALEZ CUSSAC, J. L., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en AA.VV.: *Derecho Penal Parte Especial*, GÓNZALEZ CUSSAC, J. L. (Coord.), Valencia, Tirant Lo Blanch, 2016, págs. 274- 291.

JORGE BARREIRO, A: "El delito del descubrimiento y la revelación de secretos en el Código Penal de 1995: Un análisis del artículo 197 del CP", Revista jurídica Universidad

Autónoma de Madrid, ISSN 1575-720X, núm. 6, 2002, págs. 99-131. Disponible en web: https://dialnet.unirioja.es/servlet/articulo?codigo=2867843

MARTÍNEZ DE PISÓN, J.: *El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional*. Anuario de Filosofía del Derecho, (XXXII), 2016, ISSN: 0518-0872, págs. 409-430. Disponible en web: https://www.boe.es/publicaciones/anuarios_derecho/abrir_pdf.php?id=ANU-F-2016-10040900430_ANUARIO_DE_FILOSOF%26%23833%3B_DEL_DERECHO_El_derecho_a_la_intimidad:_de_la_configuraci%F3n_inicial_a_los_%FAltimos_desarrollos_en_la_jurisprudencia_constitucional

MIERES MIERES, L. J.: *Intimidad Personal y Familiar. Prontuario de Jurisprudencia Constitucional*, Navarra, Aranzadi, 2002.

MONTSERRAT SÁNCHEZ-ESCRIBANO, M.I., *Libertad informática y protección de datos: desarrollo en la jurisprudencia del tribunal constitucional y tutela penal en el delito de descubrimiento y revelación de secretos*, Anuario Iberoamericano de Justicia Constitucional, núm. 19, Madrid, ISSN-L: 1138-4824, 2015, págs. 323-363. Disponible en web: https://dialnet.unirioja.es/servlet/articulo?codigo=5273641

MUÑOZ CONDE, F., "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Capítulo X: Descubrimiento y revelación de secretos. Especial consideración del quebrantamiento del secreto profesional. Allanamiento de morada", *Derecho Penal. Parte Especial*, Valencia, Tirant Lo Blanch, 2015, págs. 233-249.

ROMEO CASABONA, C. M.: "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en AA.VV.: *Derecho Penal. Parte especial. Conforme a las LO 1 y 2/2015, de 30 de marzo*, ROMEO CASABONA, C. M., SOLA RECHE, E. y BOLDOVA PASAMAR, M. A. (Coord.), Granada, Comares, 2016, págs. 253-281.

ROMEO CASABONA, C. M.: "La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de internet", Derecho y conocimiento, vol. 2, Facultad de Derecho, Universidad de Huelva, ISSN 1578-8202, 2002, págs. 123-149. Disponible en web: https://www.unifr.ch/ddp1/derechopenal/obrasportales/op_20080612_17.pdf

VALDÉS-SOLÍS IGLESIAS, E.: *Los delitos contra los sistemas informáticos: arts. 197 bis y 197 ter del código penal*, Ponencias "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Novedades tras la Reforma operada por LO 1/2015", julio de 2017, disponible en web: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Vald%C3%A9s-Sol%C3%ADs%20Iglesias,%20Enrique.pdf?idFile=7fa46cba-15ec-482b-a2dc-2f7a02f29e5b

VII. ANEXO I. LEGISLACIÓN APLICADA.

Carta de los Derechos Fundamentales de la Unión Europea (2000/C-364/01)

Constitución española, de 29 de diciembre de 1978

Constitución de la Unión Internacional de Telecomunicaciones (Ginebra, 1992)

Convenio sobre la Ciberdelincuencia, hecho en Budapest 23 de noviembre de 2001

Convenio para la protección de los derechos humanos y de las libertades fundamentales, hecho en Roma el 4 de noviembre de 1950

Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información

Declaración Universal de los Derechos Humanos, de 10 de diciembre de 1948

Directiva 2013/40/UE, del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques a los sistemas de información

Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria

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

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos de Carácter Personal

Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

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

Real Decreto, de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

VIII. ANEXO II. JURISPRUDENCIA.

TEDH:

STEDH, de 30 de mayo de 2017, asunto Trabajo Rueda c. España

Tribunal Constitucional:

STC 73/1982, de 2 de diciembre

STC 110/1984, de 26 de noviembre

STC 114/1984, de 29 de noviembre

ATC 257/1985, de 17 de abril.

STC 231/1988, de 2 de diciembre

STC 37/1989, de 15 de febrero

STC 171/1990, de 12 de noviembre

STC 172/1990, de 12 de noviembre

STC 197/1991, de 17 de octubre

STC 139/1995, de 26 de septiembre

STC 173/1995, de 21 de noviembre

STC 34/1996, de 11 de marzo

STC 69/1999, de 26 de abril

STC 149/1999, de 14 de junio

STC 234/1999, de 18 de febrero

STC 81/2001, de 26 de marzo

STC 123/2002, de 20 de mayo

STC 81/2001, de 26 de marzo

STC 7/2014, de 27 de enero

STC 54/2015, de 16 de marzo

Tribunal Supremo (Sala de lo Penal):

STS 1641/2000, de 23 de octubre

STS 872/2001, de 14 de mayo

STS 1461/2001, de 11 de julio

STS 694/2003, de 20 de junio

STS 1219/2004, de 10 de diciembre

STS 666/2006, de 19 de junio

STS 358/2007, de 30 de abril

STS 1328/2009, de 30 de diciembre

STS 437/2010, de 16 de abril

STS 1084/2010, de 9 diciembre

STS 487/2011, de 30 de mayo

STS 1045/2011, de 14 de octubre

STS 525/2014, de 17 de junio

ATS 1945/2014, de 27 de noviembre

Tribunal Supremo (Sala de lo Civil):

STS 408/2016, de 15 junio

Audiencias Provinciales:

SAP Madrid 115/1999, de 15 de abril

SAP Madrid 269/1999, de 19 de junio

SAP Zaragoza 106/2000, de 10 de marzo

SAP Lleida 90/2004, de 25 de febrero

SAP Cádiz 75/2005, de 22 de abril

SAP Almería 242/2005, 2 de noviembre

SAP Barcelona 219/2006, de 10 de marzo

SAP Cáceres, 227/2011, de 20 de junio

SAP Madrid 240/2014, de 15 de abril

SAP Granada 351/2014, de 5 de junio

SAP Madrid 461/2016, de 29 de junio

SAP Burgos 360/2016, de 8 de noviembre

SAP Valencia 488/2016, de 25 de noviembre

SAP Barcelona 302/2017, de 24 de abril

SAP Madrid 372/2017, de 21 de junio

SAP Cádiz, 191/2017, de 1 de septiembre

SAP Valladolid 290/2017, de 6 de octubre

AAP Pontevedra 893/2017, de 25 de octubre