

Grado en Derecho

Facultad de Derecho

Universidad de León

Curso 2016/2017

# **EL   DESCUBRIMIENTO   Y   LA REVELACIÓN DE SECRETOS**

Discovery and disclosure of secrets

**Realizado por la alumna: Dña. Noelia Menéndez Pérez**

**Tutorizado por la Profesora: Dra. Isabel Durán Seco**

# ÍNDICE

ÍNDICE DE ABREVIATURAS .....	4
RESUMEN Y ABSTRACT .....	6
OBJETO DEL TRABAJO.....	8
METODOLOGÍA UTILIZADA .....	9
<b>I. ORIGEN DEL RECONOCIMIENTO DEL DERECHO A LA INTIMIDAD Y A LA PROPIA IMAGEN EN ESPAÑA .....</b>	<b>11</b>
<b>II. RELACIÓN DEL DERECHO A LA PROPIA IMAGEN CON EL SECRETO DE LAS COMUNICACIONES Y LA PROTECCIÓN FRENTE A LA INFORMÁTICA .....</b>	<b>14</b>
<b>III. TIPIFICACIÓN DE LOS DELITOS CONTRA LA INTIMIDAD Y EL DERECHO A LA PROPIA IMAGEN EN EL CÓDIGO PENAL DE 1995.....</b>	<b>18</b>
<b>1. EL BIEN JURÍDICO PROTEGIDO EN EL DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS (ARTS. 197 A 201 CP) .....</b>	<b>23</b>
<b>1.1. La protección reguladora de la libertad informática .....</b>	<b>28</b>
<b>2. CAMBIOS PRODUCIDOS POR LA REFORMA DE LA LO 1/2015 EN EL CÓDIGO PENAL .....</b>	<b>32</b>
<b>3. MODALIDADES DELICTIVAS.....</b>	<b>36</b>
<b>3.1 Apoderamiento de documentos o efectos e intromisión en ámbitos reservados (art. 197.1 CP).....</b>	<b>36</b>
<b>3.2. Manipulación de los datos reservados registrados en ficheros o soportes informáticos (art. 197.2 CP) .....</b>	<b>41</b>
<b>3.3. Revelación de secretos (Art. 197.3 CP) .....</b>	<b>44</b>
<b>3.4. Subtipos agravados (Arts. 197.3, 197.4, 197.5, 197.6, 197 quáter y 198 CP) .....</b>	<b>46</b>
<b>3.5. Difusión no consentida de captaciones íntimas de la imagen (art. 197.7 CP) .....</b>	<b>51</b>
<b>3.6. Intromisión informática (art. 197 bis y 197 ter CP) .....</b>	<b>57</b>

3.7. Manejo de instrumentos idóneos con el fin del espionaje informático (Art. 197 ter CP) .....	63
3.8. Responsabilidad penal de las personas jurídicas (Art. 197 quinquies CP) .....	67
3.9. Revelación de secretos laborales o profesionales (Art. 199 CP).....	69
3.10. Disposiciones comunes (Art. 200 y 201 CP) .....	74
<b>IV. CAUSAS DE JUSTIFICACIÓN EN LOS DELITOS CONTRA LA INTIMIDAD.....</b>	<b>78</b>
<b>V. CONCLUSIONES.....</b>	<b>82</b>
<b>VI. BIBLIOGRAFÍA .....</b>	<b>88</b>
<b>VII. JURISPRUDENCIA CITADA .....</b>	<b>95</b>
1. SENTENCIAS DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS.....	95
2. SENTENCIAS DEL TRIBUNAL CONSTITUCIONAL .....	95
3. SENTENCIAS DEL TRIBUNAL SUPREMO.....	95
4. SENTENCIAS DE LAS AUDIENCIAS PROVINCIALES.....	96
5. OTRAS RESOLUCIONES JUDICIALES .....	97

## ÍNDICE DE ABREVIATURAS

- **AEPD** ..... Agencia Española de Protección de Datos
- **Art.** ..... Artículo
- **AP** ..... Audiencia Provincial
- **BOCG** ..... Boletín Oficial de las Cortes Generales
- **Cap.** ..... Capítulo
- **CC** ..... Código Civil
- **Cdo.** ..... Considerando
- **CE** ..... Constitución Española
- **CEDH** ..... Convenio Europeo de Derechos Humanos
- **Coord. / Coords.** ..... Coordinador / Coordinadores
- **CP** ..... LO 10/1995, de 23 de noviembre del Código Penal
- **Dir. / Dirs.** ..... Director / Directores
- **GPS** ..... Global Positioning System
- **IP** ..... Internet Protocol
- **LECrim** ..... RD de 14 de septiembre de 1882, aprobatorio de la Ley de Enjuiciamiento Criminal, con posteriores modificaciones
- **LO** ..... Ley Orgánica
- **LOPDCP** ..... LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
- **LORTAD** ..... LO 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal
- **Núm.** ..... Número
- **Pág.** ..... Página
- **RD** ..... Real Decreto
- **RDLOPDCP** ..... RD 1720/2007, de 21 de diciembre, aprobatorio del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
- **RP** ..... RD 190/1996, de 9 de febrero, aprobatorio del Reglamento Penitenciario
- **SAP** ..... Sentencia de la Audiencia Provincial

- **SITEL** ..... Sistema de Interceptación de Telecomunicaciones
- **Ss.** ..... Siguietes
- **STC** ..... Sentencia del Tribunal Constitucional
- **STS** ..... Sentencia del Tribunal Supremo
- **TC** ..... Tribunal Constitucional
- **TEDH** ..... Tribunal Europeo de Derechos Humanos
- **Tít.** ..... Título
- **TOR** ..... The Onion Router
- **TS** ..... Tribunal Supremo
- **UE** ..... Unión Europea
- **WIFI** ..... Wireless Fidelity

## **RESUMEN Y ABSTRACT**

### **RESUMEN DEL TRABAJO:**

La sociedad actual, tal y como la conocemos, ha sufrido grandes cambios debido a los avances tecnológicos y al mayor uso de las redes sociales. Ello acarrea ciertos problemas al existir la incipiente posibilidad de que se vulneren diversos derechos fundamentales regulados tanto en nuestra Constitución Española de 1978, como en multitud de tratados internacionales y europeos. Algunos de los derechos más afectados por el descubrimiento y revelación de secretos son, entre otros, la intimidad, la propia imagen y la libertad informática.

Por ello, se reforman a través de la LO 1/2015, de 30 de marzo, los delitos de descubrimiento y revelación de secretos en el Código Penal, con el fin de dotar de mayor protección dichos derechos fundamentales. No obstante, la reforma no solventa todos los conflictos sociales y normativos sobre este tema.

De esta forma, en este trabajo se ha pretendido elaborar un análisis exhaustivo, sobre la reforma de los delitos de descubrimiento y revelación de secretos, con el fin de discernir sobre las ventajas y los inconvenientes de dicha reforma.

**PALABRAS CLAVE:** descubrimiento y revelación de secretos, intimidad, libertad informática, habeas data, sexting, interceptación de las telecomunicaciones, cibercriminalidad, hacking, espionaje informático.

### **ABSTRACT:**

Nowadays, our society, such as we know it, has suffered from a lot of changes due to technological advances and the major use of social networks. This situation brings up some problems since there is a real possibility of some fundamental rights being vulnered, which are ruled both for our Spanish Constitution of 1978 and for multiple international european treaties. Among some of the rights affected by the discovery and disclosure of secrets we have, privacy, self-image and computer freedom.

For this reason, discovery crimes and disclosure of secrets have been reformed in the Criminal Code through OL 1/2015, on 30 March, in order to provide prety much protection for these fundamental rights. However, the reform does not solve all social and normative conflicts regarding this particular issue.

Taking all these things into account, this work has tried to elaborate a thorough analysis, concerning the reform of crimes of discovery and disclosure of secrets, in order to distinguish between the advantages and disadvantages of such reform.

**KEYWORDS:** discovery and disclosure of secrets, privacy, computer freedom, habeas data, sexting, telecommunications interception, cybercrime, hacking, computer spying.

## **OBJETO DEL TRABAJO**

El principal objeto de este trabajo subyace en determinar si la reforma de los delitos de descubrimiento y revelación de secretos es o no suficiente para poder proteger a cualquier persona frente a la posible vulneración de cualquier derecho, fundamental o no. Para lograr alcanzar una conclusión jurídica sobre ello, es necesario cumplir varios objetivos más explícitos, como:

1. Explicar la evolución teleológica y cronológica de los delitos contra la intimidad en España, y a su vez en el ámbito internacional, para comprender el cómo y el porqué se comienzan a regular estos delitos.
2. Analizar la protección que garantiza la Constitución Española y el resto de la normativa jurídica en nuestro país a los derechos fundamentales de la intimidad, de la propia imagen y de la libertad informática, para llegar a comprender si está justificada o no la protección que se da a los delitos contra la intimidad, en concreto, a los delitos de descubrimiento y revelación de secretos, en nuestro Código Penal.
3. Mostrar las distintas teorías doctrinales acerca de los bienes jurídicos protegidos por los delitos contra la intimidad y extraer las reflexiones de los autores más relevantes en la materia, sobre los beneficios o desventajas de la reforma realizada por la Ley Orgánica 1/2015, de 30 de marzo.
4. Desplegar diversos criterios jurisprudenciales dictados por el TEDH, el TS y el TC y exponer, de modo ejemplificativo, algunas sentencias de las AP para ver cómo resuelven, los distintos órganos jurisdiccionales, los conflictos existentes sobre delitos de descubrimiento y revelación de secretos. También, exponer la interpretación jurisprudencial de las normas referentes a la intimidad, desde los años 70 hasta el presente.
5. Por último, estudiar separadamente las distintas modalidades delictivas de los delitos de descubrimiento y revelación de secretos para comprobar, en qué consiste la conducta delictiva de cada delito y el por qué se decide introducir o modificar dicho delito, por la reforma anteriormente mencionada, en el Código Penal.



## **METODOLOGÍA UTILIZADA**

En el presente trabajo se pretende alcanzar, como ya se ha dicho, una conclusión lo más clara y verídica posible, sobre si nuestra regulación actual es suficiente y puede solucionar cualquier tipo de conflicto acerca de los delitos de descubrimiento y revelación de secretos o, por el contrario, está parcialmente obsoleta y necesita cambios más drásticos en algunas cuestiones y en cambio, en otros supuestos, no necesitaría ninguna modificación legislativa.

Para poder llegar a dicha conclusión, he seguido una investigación jurídica.

La metodología de la investigación jurídica se basa en el estudio y la aplicación de métodos y técnicas jurídicas que ayudan a alcanzar una solución frente a una cuestión no resuelta vigente en la sociedad actual. Hay un amplio abanico de métodos de investigación jurídica, en este caso se utilizan:

El método jurídico- descriptivo, que se basa en la aplicación del método analítico a un tema jurídico, explicando de manera sistematizada las principales características de un tema jurídico y el funcionamiento de las normas; el método jurídico- exploratorio, consistente en dar pasos preliminares sobre cuestiones jurídicas que abren camino a investigaciones más profundas; finalmente, el método jurídico- propositivo, que analiza los posibles errores de las normas, para llegar a alcanzar las posibles soluciones.

Cabe destacar a su vez que la investigación jurídica posee tres elementos esenciales que han de estudiarse: la facticidad, que se refiere a aquellos hechos que dan lugar a la creación de las normas jurídicas y que, en consecuencia, van a regularse por el Derecho; la normatividad, referente al ordenamiento jurídico, sin importar su vigencia; y por último, la axiología, la cual se refiere a la valoración de nuestro entorno social sobre si las normas jurídicas son o no justas y por ello puedan ser modificadas, creadas o derogadas.

Para poder exponer los resultados alcanzados mediante la realización del trabajo, efectuando la investigación jurídica mencionada, se han ido estableciendo las siguientes etapas:

1. Elección del tema y creación del índice provisional: con la colaboración del Área de conocimiento de la tutora de este trabajo, se muestra a la misma un tema relacionado

con la materia, tras ponderar el grado de relevancia e interés que puede suscitar dicho tema, siendo programado el inicio de su desarrollo, ofreciendo, la tutora y el área de Derecho Penal, reuniones explicativas para saber cómo y dónde buscar la información relativa al trabajo de investigación y cómo elaborarlo.

Después de eso, se comienza a elaborar el índice provisional sobre los hechos más reseñables a tratar en la investigación.

2. Recopilación de información y fuentes informativas existentes: se empieza a buscar y a recopilar las fuentes de información para el análisis del tema a exponer y la posterior realización del trabajo. Entre las diversas fuentes utilizadas, se pueden mencionar los criterios jurisprudenciales de los diversos órganos jurisdiccionales, la normativa, tanto la vigente como la derogada, diferentes monografías y artículos doctrinales en revistas jurídicas, tesis, manuales de derecho penal, parte especial, desde los más antiguos hasta los más actuales, con el fin de aportar una gran variedad de opiniones y razonamientos doctrinales sobre la materia.

3. Análisis crítico y sintético del material: tras leer los diversos materiales obtenidos que permiten configurar una base científica sobre la materia, se procede a su análisis y resumen. Se plantean las cuestiones más problemáticas a tratar en la investigación, creando un pensamiento crítico al respecto.

4. Redacción y corrección del trabajo: finalmente, se establece en el presente trabajo todo lo investigado, intentando aportar una información lo más sencilla y precisa posible sobre los objetivos. A su vez, se pretende esclarecer un tema tan sumamente importante, actual y futurista, como son los delitos de descubrimiento y revelación de secretos, sobretodo en el ámbito informático. Asimismo, se ha ido entregando a la tutora, periódicamente, partes del trabajo que fueron siendo modificadas con sus posteriores correcciones para lograr una versión definitiva del mismo.

## **I. ORIGEN DEL RECONOCIMIENTO DEL DERECHO A LA INTIMIDAD Y A LA PROPIA IMAGEN EN ESPAÑA**

Como bien dice OLMO FERNÁNDEZ – DELGADO: “*la intimidad no es una realidad natural que venga dada desde el origen de los tiempos, sino más bien una realidad histórica construida de manera diferente por determinadas sociedades*”.<sup>1</sup>

En el caso de España, el artículo 18.1 CE de 1978 introduce el derecho a la propia imagen. No había antes de esa fecha ninguna referencia al derecho al honor o a la intimidad en Constituciones anteriores.

El precedente que nos sirvió para regular estos derechos lo encontramos en el Derecho comparado: la Constitución portuguesa de 1976. Esta Constitución, en su art. 26.1, bajo la rúbrica “*Outros direitos pessoais*”, reconoce los derechos a la identidad personal, a la capacidad civil, a la ciudadanía, al buen nombre y reputación, a la imagen, a la palabra y a la reserva de la intimidad de la vida privada y familiar.

Dicha Constitución recoge en su art. 35, tras ciertas reformas en 1982 y 1989, regulación sobre la utilización de los ficheros y registros que contengan datos personales, con referencias a la utilización de la informática.

El legislador constitucional español también incorporó, de una forma más escueta, el uso de la informática a partir de la legislación portuguesa.

Por otro lado, en virtud del art. 10.2 de nuestra Constitución, es necesario acudir a Tratados y Acuerdos internacionales sobre derechos fundamentales para entender el reconocimiento del derecho a la propia imagen.

A este respecto, conviene referirse a la *Declaración Universal de los Derechos Humanos de 1948* que, aunque no se refiere de forma expresa a este derecho, está redactado de una manera lo suficientemente amplia, en opinión de ALEGRE MARTÍNEZ, como para considerarlo implícito.<sup>2</sup>

También se refieren al derecho a la propia imagen, el *Pacto Internacional de Derechos Civiles y Políticos de 1966*, firmado por España en 1976 y la *Convención Europea para*

---

<sup>1</sup> OLMO FERNÁNDEZ - DELGADO, *El descubrimiento y revelación de secretos documentales y de las telecomunicaciones. Estudio del art. 197.1º del Código Penal*, 2009, pág. 24.

<sup>2</sup> ALEGRE MARTÍNEZ. *El derecho a la propia imagen*, 1997, pág. 30- 36.

*la protección de los Derechos del hombre y las Libertades Fundamentales de 1950*, suscrito por nuestro país en 1977.

Por otra parte, a nivel de la Unión Europea, también deben considerarse reconocidos el derecho a la intimidad y a la propia imagen.

Así, la doctrina del Tribunal de Justicia comunitario había mantenido reiteradamente estos derechos en el Tratado de la Unión Europea, también conocido como Tratado de Maastricht, vigente hasta la entrada en vigor en 1997 del Tratado de Amsterdam.

Este último Tratado establece en sus Disposiciones Generales, que: *“La Unión respetará los derechos fundamentales tal y como se garantizan en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales firmado en Roma en 1950, y tal y como resultan de las tradiciones constitucionales comunes a los Estados miembros como principios generales del Derecho comunitario”*.

Respecto al *iter* constituyente para implantar este derecho fundamental en la CE, fueron pocos los pasos que se siguieron para elaborar una redacción definitiva.

El art. 18. 1 del Anteproyecto constitucional (BOCG 5 de enero 1978) establecía: *“Se garantiza el honor y la intimidad personal y familiar”*<sup>3</sup>. A ese texto, se presentaron tres enmiendas en el Congreso. Una de ellas, de Alianza Popular, proponía suprimir los párrafos 1 y 4 del art. 18, porque alegaba que su contenido ya se hallaba recogido en otro artículo.

Otra enmienda, cuyo firmante era diputado de Unión de Centro Democrático, consideraba que debía añadirse en el epígrafe 1 la garantía del derecho a la propia imagen, en relación con el art. 20.6, actual 20.4 CE.

Finalmente, la redacción definitiva fue: *“Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen”* permaneciendo inalterado en el

---

<sup>3</sup> Sesión núm. 13 de la Comisión de Asuntos Constitucionales y Libertades Públicas de 1978. Consultado en la *Constitución española. Trabajos parlamentarios, I, Cortes Generales, Servicio de Estudios y publicaciones*, 1980, pág. 1216.

Pleno del Congreso y del Senado a pesar de la contraposición del senador de la Agrupación independentista, Camilo José Cela.<sup>4</sup>

Por último, cabe citar la LO 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Dicha ley que aún sigue en vigencia, desarrolla el art. 18.1 CE.

La LO 1/1982 condiciona prácticamente en total medida las decisiones de los Tribunales ordinarios y del TS, el cual realiza según NAVAS SÁNCHEZ: *“Una interpretación y aplicación en la que lo que prima es la indagación y la argumentación relativa a la concurrencia o no de las circunstancias previstas en la ley para determinar, en consecuencia, si se excluye o no la protección del derecho a la propia imagen.”*<sup>5</sup>

Así las cosas, la LO 1/ 1982 determina los derechos referentes a la personalidad como el honor o la intimidad en el ámbito civil. Pretende proteger esos derechos subjetivos con el fin de reforzar los bienes esenciales e inmateriales de la persona.

Aun así, en relación al derecho de la intimidad, CLAVERÍA GOSALBEZ indica que: *“la falta de tipificación legal no privaría al derecho a la intimidad de su calificación como derecho subjetivo, pues para que se dé un derecho subjetivo no es necesario el reconocimiento del ordenamiento jurídico. Basta su mención y el establecimiento de medidas protectoras generales, sin que sea imprescindible una descripción pormenorizada de poderes concretos, etc”*.<sup>6</sup>

Cabe decir que dicha ley no sólo protege frente a sanciones administrativas, delitos u obligaciones de responsabilidad civil extracontractual, sino que permite en su art. 9.2 LO 1/1982 que se adopten medidas cautelares para intentar acabar con las intromisiones ilegítimas, prevenirlas o aminorarlas.<sup>7</sup>

---

<sup>4</sup> A tal efecto véase, ALEGRE MARTÍNEZ. *El derecho a la propia imagen*, 1997, pág. 30- 36.

<sup>5</sup> NAVAS SÁNCHEZ, *El uso informativo de la imagen*, Indret: Revista para el análisis del derecho, 2017, pág. 20-22.

<sup>6</sup> CLAVERÍA GOSALBEZ, *Notas para la construcción jurídica de los llamados derechos de la personalidad*, 1984, pág. 109.

<sup>7</sup> El art. 9.2 de la LO 1/1982 establece que: *“La tutela judicial comprenderá la adopción de todas las medidas necesarias para poner fin a la intromisión ilegítima de que se trate y, en particular, las necesarias para: a) El restablecimiento del perjudicado en el pleno disfrute de sus derechos, con la*

Antes de esta ley, los daños que atentaban contra el honor, la intimidad y la propia imagen se regulaban en el art. 1902 del CC, que sólo protegía frente a los daños ya causados.<sup>8</sup>

---

## II. RELACIÓN DEL DERECHO A LA PROPIA IMAGEN CON EL SECRETO DE LAS COMUNICACIONES Y LA PROTECCIÓN FRENTE A LA INFORMÁTICA

El art. 18 CE recoge en los párrafos 2, 3 y 4 derechos instrumentales que garantizan la eficacia del derecho a la intimidad y la propia imagen del artículo 18.1 CE.

Un sector de la doctrina considera a tenor de lo establecido en el art. 18.4 CE, que el derecho fundamental que se protege aquí es la autodeterminación informativa o la libertad informática.<sup>9</sup>

El fundamento de este derecho es el peligro que puede acarrear la acumulación informática de datos sobre las personas y su vida privada.<sup>10</sup>

Uno de los derechos instrumentales que garantizan la intimidad y la propia imagen es el secreto de las comunicaciones, objeto de desarrollo legislativo en la Ley Orgánica 7/1984, de 15 de octubre, sobre tipificación penal de la colocación ilegal de escuchas telefónicas.<sup>11</sup>

A nivel mundial, no se hizo referencia al secreto de las comunicaciones en ninguna declaración o carta de derechos humanos. Fue en la Declaración de Derechos del Hombre y del Ciudadano de la Revolución Francesa, concretamente en la Asamblea

---

*declaración de la intromisión sufrida, el cese inmediato de la misma y la reposición del estado anterior. En caso de intromisión en el derecho al honor, el restablecimiento del derecho violado incluirá, sin perjuicio del derecho de réplica por el procedimiento legalmente previsto, la publicación total o parcial de la sentencia condenatoria a costa del condenado con al menos la misma difusión pública que tuvo la intromisión sufrida.b) Prevenir intromisiones inminentes o ulteriores.c) La indemnización de los daños y perjuicios causados.d) La apropiación por el perjudicado del lucro obtenido con la intromisión ilegítima en sus derechos. Estas medidas se entenderán sin perjuicio de la tutela cautelar necesaria para asegurar su efectividad.”*

<sup>8</sup> En este sentido véase, OLMO FERNÁNDEZ – DELGADO, *El descubrimiento y revelación de secretos documentales*, 2009, pág. 47- 51.

<sup>9</sup> En este sentido, por ejemplo, ROMEO CASABONA, *Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías*, Revista Poder Judicial, 1993, pág. 170.

<sup>10</sup> Sobre ello véase, ESPÍN, *Derecho Constitucional*, Vol. I, 6ª edición, 2003, pág. 242.

<sup>11</sup> Sobre ello puede verse, RODRÍGUEZ MARIN, *Los delitos de escuchas ilegales y el derecho a la intimidad*, Anuario de derecho penal y ciencias penales, Tomo 43, Fasc. 1, 1990, pág. 197 - 240; CASTILLO JIMENEZ, *Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información*, Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento, núm. 1, 2001, pág. 35- 48.

Nacional de 1790, donde se sometió, por lo menos a debate, la importancia del secreto en la correspondencia escrita.<sup>12</sup>

Era comprensible esta falta de regulación debido a la poca preocupación de la correspondencia privada en ese tiempo. En España, fueron las Ordenanzas Generales de Correos o las Instrucciones Reales las que comenzaron a garantizar parcialmente la protección del correo postal. Así, se empezó a garantizar la confidencialidad frente a las comunicaciones en la Instrucción Real de 1762; o en la Ordenanza General de Correos y Postas de 8 de julio de 1794, que quiso asegurar medidas que garantizaran la protección del correo postal frente a pérdidas, sustracciones o manipulaciones.<sup>13</sup>

Ya se reconoce en ese momento la autoridad y la competencia de los órganos administrativos o jurisdiccionales para ordenar abrir o sustraer el correo, siempre que estuviese justificado y fuese necesario. Es a partir de estos hechos, según RODRÍGUEZ LAINZ, donde empieza a formarse lo que es la comunicación protegida por el secreto: *“la intermediación de un tercero en quien confiamos su tránsito y buen fin, y la existencia de un fuerte vínculo de confidencialidad que trasciende en la garantía de que aquello que se transmite no llegará al conocimiento ajeno mientras se encuentre bajo la custodia de este tercero”*.<sup>14</sup>

La regulación sobre el derecho a las comunicaciones telefónicas o telecomunicaciones tiene su origen, en opinión de RODRÍGUEZ LAINZ, en los periodos de posguerra de la I y la II Guerra Mundial.<sup>15</sup> Es en este momento cuando hay una necesidad de legislar sobre esta materia, debido al espionaje y al gran uso de los medios de comunicación. Así, tras la Constitución de Weimar de 1919, Alemania comienza a garantizar el derecho sobre las comunicaciones. Unas décadas más tarde, la Constitución de la República Italiana de 1947 y la Ley Fundamental de Bonn de 1949 reconocerían de forma expresa el secreto postal y el secreto a las comunicaciones telefónicas.

---

<sup>12</sup>En este sentido véase, RODRÍGUEZ LAINZ, *El secreto de las telecomunicaciones y su interceptación legal*, 2016, pág. 21 y 22.

<sup>13</sup> Sobre ello véase, RODRÍGUEZ LAINZ, *El secreto de las telecomunicaciones y su interceptación legal*, 2016, pág. 22 y 23.

<sup>14</sup> RODRÍGUEZ LAINZ, *El secreto de las telecomunicaciones y su interceptación legal*, 2016, pág. 23.

<sup>15</sup> RODRÍGUEZ LAINZ, *El secreto de las telecomunicaciones y su interceptación legal*, 2016, pág. 25.

Respecto a la labor jurisprudencial en las telecomunicaciones, fue el TEDH el que empezó a dictar sentencias sobre este derecho, asentando una mayor protección frente a las comunicaciones postales, telefónicas y electrónicas.<sup>16</sup>

Actualmente en nuestro Código Penal, los delitos relativos a los secretos de las comunicaciones se castigan en los arts. 197 y ss. del CP de 1995, en el Cap. I “*del descubrimiento y revelación de secretos*”.

Aunque en un principio se consideraba que el bien jurídico aquí protegido era solamente la intimidad, hoy en día no se sostiene este pensamiento. Así, GONZÁLEZ PORRAS considera que: “*la actual tutela del derecho al secreto de las comunicaciones es autónoma y no depende del derecho a la intimidad para su protección, pues las comunicaciones son protegidas con independencia del contenido de éstas.*”<sup>17</sup>

Aun así, también se protege en el derecho a las comunicaciones la intimidad y la propia imagen, pues el Cap. I del Tít. X, del Libro II del CP, también engloba las conductas delictivas referentes a los delitos informáticos. Según RUEDA MARTÍN, el bien jurídico protegido en las conductas tipificadas en los arts. 197 y ss. CP, donde también se incluyen los delitos contra la libertad informática, es “*la intimidad personal y familiar, en la que debemos destacar por un lado, el ámbito personal donde cada uno, preservado del mundo exterior, encuentra las posibilidades de desarrollo y fomento de su personalidad y, por otro lado, como un control sobre la publicidad de la información relativa a la persona y a su familia*”.<sup>18</sup>

Respecto a la interpretación que de estos derechos hizo el Tribunal Constitucional, fundada en la sentencia núm. 114/1984, de 29 de noviembre, señala como bien jurídico protegido “*la libertad de las comunicaciones, a través de la imposición a todos del secreto*”. Añade dicha sentencia que “*el derecho puede conculcarse tanto por la interceptación en sentido estricto (que suponga la aprehensión física del soporte del mensaje o captación, de otra forma del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, por ejemplo)*”.

---

<sup>16</sup> Véanse las sentencias del TEDH: de 6 de septiembre de 1978 (caso Klass versus Alemania, asunto 5029/1971) y de 4 de agosto de 1984 (caso Malone versus Reino Unido, asunto 8691/1979).

<sup>17</sup> GONZÁLEZ PORRAS, *Los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica. La vigilancia masiva*, 2016, pág. 191- 198.

<sup>18</sup> RUEDA MARTÍN, *Protección penal de la intimidad personal e informática*, 2004, pág. 30 y 31.



En conclusión, según el TC no se vulnera el art. 18.3 CE ni existe el derecho a guardar secreto en el caso de que el receptor de una información guarde el contenido de dicha información que se dirigía a él.

Como bien plantea GONZÁLEZ MONTES, la STC núm. 114/1984, de 29 de noviembre: *“Introduce en nuestro sistema la prohibición de utilizar pruebas que, en el momento de su obtención, hubieran vulnerado derechos fundamentales, alterando de forma notable el panorama de la admisibilidad probatoria en el ámbito del proceso”*.<sup>19</sup>

Por otro lado, también se refiere la citada sentencia a la relación medial que existe entre el derecho a la intimidad y a la propia imagen del art. 18.1 CE y el derecho al secreto de las comunicaciones del art. 18.3 CE. Esa relación medial implica que el daño realizado al secreto de las comunicaciones puede dañar a su vez el derecho a la intimidad, y viceversa.<sup>20</sup>

Un ejemplo sobre cómo se puede dañar el derecho a la intimidad y a la propia imagen (art. 18.1 CE) y el derecho al secreto de las comunicaciones (art. 18.3 CE) simultáneamente se aprecia en el art. 7.6 de la LO 1/1982, donde se dice que: *“La apertura de la correspondencia ajena del destinatario puede conllevar el descubrimiento de fotografías enviadas por correo, en las que aparezca remitente, destinatario o cualquier otra persona y esas imágenes se utilicen para fines publicitarios, comerciales o de análoga naturaleza”*.

Así, sobre el derecho a la propia imagen cree ALEGRE MARTÍNEZ que *“no se sabría exactamente si calificarlo como un derecho autónomo o derivado de otros derechos. La propia imagen en un ámbito público, no surgiría del derecho a la intimidad, mas que se difundiera o publicase la propia imagen dependería del consentimiento del titular”*.<sup>21</sup>

Tras la regulación del derecho a las comunicaciones y a la protección de la informática, en el art. 18.4 CE, la doctrina constitucionalista puso en cuestión el posible daño que suponen los avances informáticos para la intimidad de las personas. Así, se comenzó a desarrollar la legislación sobre este derecho para proteger los datos personales, que

---

<sup>19</sup> GONZÁLEZ MONTES, *La prueba ilícita (STC 114/1984, de 29 de noviembre)*, Persona y derecho: Revista de fundamentación de las Instituciones Jurídicas y de Derechos Humanos, Núm. 56, 2006, pág. 363.

<sup>20</sup> Sobre ello véase, ALEGRE MARTÍNEZ, *El derecho a la propia imagen*, 1997, pág. 71- 91.

<sup>21</sup> ALEGRE MARTÍNEZ, *La dignidad de la persona como fundamento del ordenamiento español*, 1996, pág. 105-106.

según VILLAVERDE MENÉNDEZ son “*indispensables para precisar jurídicamente el respeto a la autonomía y libertad individuales, en último término a la dignidad individual, tan maltrecha en estos tiempos donde la verdad parece concebirse en el interior de las máquinas*”.<sup>22</sup>

La protección de los datos personales se basa fundamentalmente en la autodeterminación informativa y el *habeas data*, que es el derecho que tenemos todas las personas a poder saber qué datos figuran en los programas informáticos sobre nosotros.

A través del fundamento del *habeas data*, la doctrina constitucionalista consideró que al darse una garantía constitucional que también protege frente a la vulneración de la dignidad y los derechos de la persona, como el honor y la intimidad, contra el mal uso de lo que la CE denomina “*informática*”, surgió un derecho instrumental en el art. 18.4 CE. Así, el art. 18.4 dicta: “*La ley limitará el uso de la informática para garantizar...*”.

La protección de la CE para garantizar dichos derechos a la propia imagen y a la intimidad, se desarrolló a través de la derogada LO 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos de carácter personal y en la LO 4/1997, de 4 de agosto, que regula la utilización de videocámaras por Fuerzas y Cuerpos de Seguridad en lugares públicos, vigente en la actualidad.<sup>23</sup>

La LO 5/1992 se reemplazó por la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y por el RD 1720/2007, de 21 de diciembre, de desarrollo de la Ley Orgánica de Protección de Datos, que determina las medidas de seguridad que deben aplicarse en los sistemas de información.

Por último, también es importante citar al respecto el RD 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

### **III. TIPIFICACIÓN DE LOS DELITOS CONTRA LA INTIMIDAD Y EL DERECHO A LA PROPIA IMAGEN EN EL CÓDIGO PENAL DE 1995**

La tutela penal de la intimidad en el Código penal se halla en los arts. 197 a 204, dentro del Libro II, en el Título X, que se divide en dos Capítulos: el I, referido al

---

<sup>22</sup> VILLAVERDE MENÉNDEZ, *Protección de datos personales. Derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993, Revista de Derecho Constitucional*, núm. 41, 1994, pág. 224.

<sup>23</sup> Sobre ello véase, ALEGRE MARTÍNEZ. *El derecho a la propia imagen*, 1997, pág. 61- 71.

“*Descubrimiento y revelación de secretos*” (arts 197 a 201 del CP), el cual analizo en este trabajo, y el II, relativo al “*Allanamiento de morada, domicilio de las personas jurídicas y establecimientos abiertos al público*” (arts 202 al 204 CP).<sup>24</sup>

No sólo se protege la intimidad en el Título X, hay otros artículos a lo largo del CP que coadyuvan a su tutela.

Así, en el art. 171.2 CP se castigan las amenazas consistentes en revelar hechos referentes a la vida privada (chantaje). Este tipo delictivo se basa en pedir a la víctima una cantidad de dinero o recompensa, amenazándola con divulgar o revelar datos referidos a su intimidad que desconozcan terceros o familiares y creen en dicha persona un perjuicio social, moral, económico o de otra clase.<sup>25</sup>

La STS 49/2001, de 26 de enero, condenó bajo la aplicación del art. 171.2 CP, a una prostituta que chantajeaba a sus clientes con revelar las relaciones sexuales que mantenía con éstos a sus familias si no le pagaban ciertas cantidades de dinero.

Por otro lado, en los arts. 278 -280 CP se castigan los secretos de empresa, que no han sido modificados por la reforma de 2015, y en los arts. 284 y 285 CP la revelación de información privilegiada o infracción relevante.

Si concretamente, lo que se revela es una patente secreta de un objeto, también se debe tener en cuenta el art. 277 CP.

En el ámbito europeo, es la Directiva 2016/943/UE la que regula la protección de los conocimientos técnicos y la información empresarial, que se transpondrá el 9 de junio de 2018.

Los secretos de empresa (arts. 278- 280 CP) formarían parte del término conocido como *Know-how* (saber cómo hacer). El know-how engloba los datos e informaciones relevantes que las empresas utilizan para desarrollar sus actividades.<sup>26</sup>

En conclusión, los secretos de empresa según LÓPEZ BARJA DE QUIROGA, “*son todo aquello que no debe ser divulgado, pues el mantenimiento en secreto le confiere*

---

<sup>24</sup> A tal efecto basta ver el Código Penal.

<sup>25</sup> Sobre ello véase, RAGUÉS I VALLÉS, *Delitos contra la libertad*, en: SILVA SÁNCHEZ (Dir.)/ RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 107.

<sup>26</sup> Sobre ello véase, LÓPEZ BARJA DE QUIROGA, *Los secretos de empresa*, *Revista Aranzadi de Derecho y Proceso Penal*. núm. 44. Octubre- Diciembre 2016, pág. 106-112.

*una posición de exclusividad en el mercado y, ello le otorga un claro interés económico. Esto implica que un dato esencial es que el secreto sea tratado por la empresa como confidencial y restrinja el acceso a su conocimiento a pocas personas y siempre vinculados con contratos de confidencialidad”.*<sup>27</sup>

A veces no queda claro si los listados de clientes o proveedores son o no secretos de empresa. Teniendo en cuenta la sentencia del TS núm. 864/2008, de 16 de diciembre, sí se trata de un secreto de empresa siempre y cuando se den los requisitos exigidos en el tipo penal, como el deber de confidencialidad.

En cambio, los arts. 278-280 CP no castigarían aquellos secretos que sean ilícitos, por ejemplo, que se revelase el uso de alguna sustancia para crear una droga. De esta manera, queda claro que para que se considere a algún dato empresarial como secreto de empresa debe, además de ser lícito, ser secreto; otorgar una posición de exclusividad a la empresa; y aportarle un beneficio económico.

Es importante tener en cuenta que el legislador con total falta de precisión, desde el punto de vista de LÓPEZ BARJA DE QUIROGA, regula actuaciones muy similares en otros tipos penales. Por ejemplo, en los arts. 199 y 200 CP se castigan la revelación de secretos en medio de una relación laboral, el deber de sigilo y los secretos cedidos, descubiertos o revelados de una persona jurídica sin su consentimiento.<sup>28</sup>

Respecto a los funcionarios públicos, además de castigarse en el art. 198 CP que éstos revelen o descubran secretos prevaliéndose de su cargo, en el 535 CP se tipifica la conducta consistente en la violación de la correspondencia privada y en el art. 536 CP la interceptación de las comunicaciones personales.<sup>29</sup> Ambas conductas se castigan en esos artículos cuando son realizados por dicha autoridad o funcionario público y se extralimitan en sus funciones, cometiendo hechos delictivos político-policiales, también castigados en el art. 534.1.2º CP.

Estos tipos penales (534 a 536 CP) regulan los “*delitos cometidos por funcionarios públicos contra la inviolabilidad domiciliaria y demás garantías de la intimidad*”. Se

---

<sup>27</sup> LÓPEZ BARJA DE QUIROGA, *Los secretos de empresa*, Revista Aranzadi de Derecho y Proceso Penal, núm. 44, Octubre- Diciembre 2016, pág. 112-114.

<sup>28</sup> LÓPEZ BARJA DE QUIROGA, *Los secretos de empresa*, Revista Aranzadi de Derecho y Proceso Penal, núm. 44, Octubre- Diciembre 2016, pág. 114- 123.

<sup>29</sup> Sobre ello véase, CASTIÑEIRA PALOU/ ESTRADA i CUADRAS, *Delitos contra la intimidad*, en: SILVA SÁNCHEZ (Dir.)/ RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 167- 168.

aplican cuando el funcionario o autoridad actúa mediando causa por delito y vulnerando las garantías constitucionales o legales.

Por otra parte, en los arts. 414- 418 CP se tipifican las conductas delictivas cometidas por una autoridad o funcionario público cuando destruya o impida el acceso a documentos de acceso restringido (art. 414 CP). También se aplica este tipo penal cuando consienta ese hecho aunque él mismo no fuese el que impidiera el acceso al documento.

El art. 415 CP castiga al funcionario que accede o permite acceder a terceros a documentos secretos sin estar debidamente autorizado. En el art. 416 CP se castiga esta misma conducta pero cuando se trate de un particular encargado de custodiar esos documentos secretos.

Cuando la conducta consiste en revelar secretos o informaciones que el funcionario o autoridad pública conoce por razón de su cargo y está prohibida su divulgación resulta de aplicación el art. 417 CP. Se agrava la pena del art. 417 CP cuando esos secretos o informaciones que revelase fuesen de grave peligro para el interés público o un particular.<sup>30</sup>

Cabe destacar que según el TS, en la sentencia núm. 424/2014, de 28 de mayo, se entiende por información en estos casos: *“aquel hecho conocido en atención al cargo u oficio aunque no hayan recibido la calificación formal de secretos, ya que por su propia naturaleza el funcionario está obligado a no revelar”*.

La última modalidad delictiva referente al descubrimiento y revelación de secretos por los funcionarios públicos en el capítulo IV “de la infidelidad en la custodia de documentos y de violación de secretos”, se encuentra en el art. 418 CP. Este tipo penal castiga la conducta llevada a cabo por un particular que consigue a través de un funcionario o autoridad pública, el secreto o la información privilegiada.<sup>31</sup>

En referencia a la administración de la justicia, el art. 466 CP castiga al que revele las actuaciones procesales que hayan sido declaradas secretas. No se comete este delito si

---

<sup>30</sup> En este sentido véase, ORTIZ DE URBINA GIMENO, *Delitos contra la Administración Pública*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 376- 380.

<sup>31</sup> Sobre ello véase, ORTIZ DE URBINA GIMENO, *Delitos contra la Administración Pública*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 380- 381.

no fueron declaradas secretas, expresamente y con anterioridad al proceso, las actuaciones que se revelan (art. 302 LECrim). Esa declaración de secreto puede hacerse a través de un auto que decrete de manera expresa el secreto de sumario.

La pena del art. 466 CP se agrava cuando es el Juez, el representante del Ministerio Fiscal, un miembro del tribunal o cualquier funcionario de la Administración de la Justicia quien comete el delito. Y en cambio, se atenúa si es un particular el que revela dicho secreto.<sup>32</sup>

Desde una perspectiva sistemática, el descubrimiento y revelación de secretos del Capítulo I, denota una vertiente instrumental del bien jurídico intimidad personal y familiar a través del secreto.

El secreto, pues, se entiende en los arts. 197 a 201 CP, como concerniente a la intimidad, sin poder confundirlo con el secreto que protege otros intereses, como por ejemplo el secreto de Estado.

Por otro lado, la introducción del Tít. X del Código Penal, ofrece una protección más coherente y sistemática agrupando figuras delictivas que se hallaban dispersas en el anterior CP.

Así, se separa la tutela de las informaciones íntimas del Tít. X, de las informaciones económico-empresariales, que se ubican en el Título XIII del actual CP.

No obstante, puede producir confusión, sobre esta separación sistemática, el art. 200 CP, que dota de protección a las personas jurídicas y no se ubica en el Cap. XIII, sino en el Cap. X del CP.

El Cap. X comienza por el tipo básico del art. 197 CP, el cual configura las conductas típicas contra la intimidad personal y familiar, y de los arts. 198 y 199 CP, en los que se hallan los delitos especiales.

Este capítulo establece hasta seis modalidades delictivas diferentes: 1) apoderamiento de documentos o efectos y la intromisión en ámbitos reservados (art. 197.1 CP); 2) manipulación de datos de carácter personal o familiar en ficheros o soportes

---

<sup>32</sup> Sobre ello véase, BENLLOCH PETIT, *Obstrucción a la justicia y deslealtad profesional*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 407 y 408.

informáticos (art. 197.2 CP); 3) la difusión no consentida de captaciones íntimas de la imagen, conocido como *sexting* (art. 197.7 CP); 4) la intromisión informática (197 bis CP); 5) el espionaje informático (art. 197 ter CP); y 6) la revelación de datos previamente descubiertos (arts. 197.3 y 199 CP).<sup>33</sup>

Cuando el sujeto activo sea autoridad o funcionario público, se castiga esa conducta delictiva en el art. 198 CP. En el art. 199 CP en su primer párrafo, si el hecho delictivo proviene de una relación laboral, y si la relación es profesional, se tipifica esa conducta en el párrafo segundo del art. 199 CP.

El art. 200 CP regula una cláusula de ampliación del sujeto pasivo, bastante problemática al querer dotar de protección frente a la intimidad a las personas jurídicas. Cierta parte de la jurisprudencia entiende que no debe darse la misma protección de las personas físicas a las personas jurídicas. Así, la AP sentencia que: *“No resulta posible admitir que las personas jurídicas puedan ser titulares del derecho a la intimidad personal stricto sensu, máxime cuando el art. 18.4 de la CE (RCL 1978, 2836) habla de la intimidad personal “de los ciudadanos”. Cosa distinta es que a través de la protección de la persona jurídica se tutele la intimidad personal de las personas físicas que la integran, por ejemplo, conductas tales como la revelación de la lista de asociados de una entidad con unas connotaciones y objetivos muy vinculados a la intimidad de sus componentes”*.<sup>34</sup>

Y por último, el art 201 CP regula la condición de perseguibilidad en su primer párrafo, para poder proceder a castigar estos delitos, y otorga en el 201.3 CP el perdón del ofendido para extinguir la acción penal.<sup>35</sup>

## **1. EL BIEN JURÍDICO PROTEGIDO EN EL DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS (ARTS. 197 A 201 CP)**

La intimidad personal es conferida, por primera vez como bien jurídico protegido del descubrimiento y revelación de secretos, en el Código Penal de 1995.

---

<sup>33</sup>A tal efecto véase, CASTIÑEIRA PALOU/ ESTRADA i CUADRAS, *Delitos contra la intimidad*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 154.

<sup>34</sup> Véase la SAP de Cuenca, núm. 8/2015, de 13 de enero.

<sup>35</sup> A tal efecto véase, DOVAL PAIS / ANARTE BORRALLA, *delitos de descubrimiento y revelación de secretos*, en: BOIX REIG (Coord.), *Derecho Penal, Parte especial*, Vol. I, 2016, pág. 493- 546.

La intimidad personal se consagra, en nuestro país, en el art. 18 de la CE y en el ámbito civil en la LO 1/1982.

Se trata de un bien jurídico referido al derecho de la personalidad, que presenta dificultades para establecer su contenido.

Una de las definiciones más adecuadas acerca de la intimidad protegida por los delitos de descubrimiento y revelación de secretos la establece ROMEO CASABONA. Para este autor la Intimidad es: “ *La manifestación de la personalidad individual o familiar cuyo conocimiento o desarrollo queda reservado a su titular o sobre la que ejerce alguna forma de control cuando se ven implicados terceros, debiendo resaltar que se incluye no sólo el conocimiento, sino también el desenvolvimiento en sí mismo* ”.<sup>36</sup>

Por otro lado, según BAJO FERNÁNDEZ la Intimidad se trata “*del ámbito personal donde cada uno, preservado del mundo exterior, encuentra las posibilidades de desarrollo y fomento de la personalidad. Es un ámbito personal, reservado a la curiosidad pública, absolutamente necesario para el desarrollo humano y donde enraiza la personalidad*”.<sup>37</sup> Conforme a su criterio, la intimidad está formada por tres clases de protección penal. Primeramente, como defensa de la manifestación de la personalidad en la vida privada. En segundo lugar, como manifestación de confidencialidad compartida; y por último, como protección frente al procesamiento y comunicación de datos en las tecnologías de la información y de la comunicación.

No obstante, es muy difícil elaborar una definición de intimidad debido a los grandes cambios que ha sufrido su concepción a lo largo del tiempo.

Es a partir del Siglo XVIII cuando se empieza realmente a distinguir entre la esfera pública y privada de las personas, otorgando a cada individuo su derecho a la intimidad.

Así, los juristas norteamericanos WARREN y BRANDEIS en su obra “*The Right to Privacy*” publicada en 1890, entendían la intimidad como “*el derecho a estar solo*”, es decir, como una libertad de exclusión de terceros<sup>38</sup>. Es aquí donde se empieza a ver el

---

<sup>36</sup> ROMEO CASABONA, *Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías*, Revista Poder Judicial, núm. 31, 1993, pág. 164.

<sup>37</sup> BAJO FERNÁNDEZ, *El secreto profesional en el Proyecto del Código Penal*, Anuario de Derecho Penal y Ciencias Penales, 1980, pág. 599.

<sup>38</sup> WARREN/ BRANDEIS, *El derecho a la intimidad*, traducido por Benigno Pendás y Pilar Baselga, 1995, pág. 45.



derecho a la intimidad como el derecho a impedir la injerencia de terceros o el derecho a no ser molestado.<sup>39</sup>

A medida que transcurre el Siglo XX y principios del XXI, se crea una concepción de la intimidad en su vertiente positiva. Esto se debe al aumento de mayores peligros con el desarrollo de la informática. Es por ello que se amplía el contenido del derecho a la intimidad, para proteger “*nuevas realidades sociales y tecnológicas*”.<sup>40</sup>

De esta forma, la jurisprudencia va definiendo la intimidad como un poder sobre la información de una persona y su familia. La STC núm. 134/1999, de 15 de julio, considera que “*el art. 18.1 CE no garantiza una intimidad determinada, sino el derecho a poseerla, a tener vida privada, disponiendo de un poder de control sobre la publicidad de la información relativa a la persona y su familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público*”.

Debido a esa justificada ampliación del derecho a la intimidad, según LONDOÑO TORO, se empieza a proteger y a enlazar, aún más, la protección de la dignidad y de la libertad con otros derechos y libertades secundarios como: la libertad de residencia, de circulación, el secreto de la correspondencia etc.<sup>41</sup>

Para saber el alcance de este bien jurídico, debemos tener en cuenta las teorías formuladas por la doctrina. Así por ejemplo, LONDOÑO TORO considera que la intimidad alcanza a “*mantener fuera del conocimiento ajeno hechos o actos que pertenecen a la vida privada de una persona, en su sentido positivo*”.<sup>42</sup>

Se superan la teoría de las esferas, promulgada por la doctrina alemana, que dividía la vida íntima o no de las personas según esferas.<sup>43</sup> También, las disputas doctrinales entre

---

<sup>39</sup> A tal efecto véase, LONDOÑO TORO, *El derecho a la intimidad, el honor y la propia imagen enfrentado a las nuevas tecnologías informáticas*, Revista Facultad de Derecho y Ciencias Políticas, núm. 77, 1987, pág. 107- 108; OLMO FERNÁNDEZ – DELGADO, *El descubrimiento y revelación de secretos documentales y de las telecomunicaciones*, 2009, pág. 24-28; ÁLVAREZ CARO, *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la Era digital*, 2015, pág. 47-48.

<sup>40</sup> OLMO FERNÁNDEZ – DELGADO, *El descubrimiento y revelación de secretos documentales y de las telecomunicaciones*, Estudio del art. 197.1º del Código Penal, 2009, pág. 28.

<sup>41</sup> LONDOÑO TORO, *El derecho a la intimidad, el honor y la propia imagen enfrentado a las nuevas tecnologías informáticas*, Revista Facultad de Derecho y Ciencias Políticas, núm. 77, 1987, pág. 108-109.

<sup>42</sup> LONDOÑO TORO, *El derecho a la intimidad, el honor y la propia imagen enfrentado a las nuevas tecnologías informáticas*, Revista Facultad de Derecho y Ciencias Políticas, núm. 77, 1987, pág. 113.

<sup>43</sup> Sobre ello véase, ÁLVAREZ CARO, *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la Era digital*, 2015, pág. 44- 45.

la teoría de la voluntad y la teoría del interés, pues es la voluntad la que transforma cualquier comunicación en secreto.<sup>44</sup>

Por una parte, hay que tener en cuenta que la intimidad se protege también, como bien dice VILLANUEVA TURNES, operando como límite.<sup>45</sup> El art. 20.4 CE limita los derechos y libertades fundamentales del art. 20 CE.

Así, por ejemplo, un periodista tiene derecho a comunicar y recibir información por cualquier medio de difusión (art. 20.1. d. CE) pero siempre y cuando respete el honor, la intimidad y la propia imagen de las personas (art. 20.4 CE).

Por otra parte, cabe a su vez decir que la intimidad abarca y garantiza otros derechos.

Uno de ellos es la dignidad de la persona del art. 10.1 CE la cual, dice el TC, está rigurosamente unida a la intimidad personal y familiar del art. 18.1 CE. Esto se debe a que el TC en su sentencia núm. 231/1988, de 2 de diciembre, señala que: *“Los derechos a la imagen y a la intimidad personal y familiar aparecen como derechos estrictamente vinculados a la propia personalidad, derivados sin duda de la dignidad de la persona, que reconoce el art. 10 CE, y que implican la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario para mantener una calidad mínima de la vida humana”*.

El precepto que recoge el art. 10.1 CE sobre la dignidad supone, según el constitucionalista ALEGRE MARTÍNEZ: *“El reconocimiento de un status especial de la persona, que se sitúa por encima de los demás seres en virtud de su racionalidad, que a su vez determina su sociabilidad, libertad, responsabilidad y dimensión trascendente”*.<sup>46</sup>

---

<sup>44</sup> Sobre ello véase, GALLARDO ORTIZ, *Problemas morales de las intrusiones, grabaciones y escuchas: Hacia una ética del descubrimiento y la revelación de secretos*, 2015, pág. 28-30.

<sup>45</sup> VILLANUEVA TURNES, *El derecho al honor, a la intimidad y a la propia imagen, y su choque con el derecho a la libertad de expresión y de información en el ordenamiento jurídico español*, *Revista Díkaion*, Vol. 25, núm. 2, 2016, pág. 204.

<sup>46</sup> ALEGRE MARTÍNEZ, *La dignidad de la persona como fundamento del ordenamiento constitucional español*, 1996, pág. 17.

Conforme a esa condición de ser racional de cualquier ser humano que vive en un entorno que posibilita su desarrollo a nivel individual y colectivo, se justifica también que la dignidad esté relacionada con los derechos de libertad e igualdad.<sup>47</sup>

Así, el art. 18 CE reconoce expresamente la intimidad personal y familiar (art. 18.1), la inviolabilidad del domicilio (art. 18.2), la confidencialidad de las comunicaciones privadas (art. 18.3) y la libertad informática (art. 18.4), siendo éstos aspectos concretos de la vida privada.<sup>48</sup>

Según el TC (Sala Primera) en la sentencia núm. 7/2014, de 27 de enero, el derecho a esa intimidad personal del art. 18.1 CE *“tiene por objeto garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona (art. 10.1 CE), frente a la acción y conocimiento de terceros, sean éstos poderes públicos o simples particulares, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana”*.

En su dimensión familiar, la intimidad, como aclara la sala de lo penal en la STS 569/2013, de 26 de junio, en relación con la vida en pareja: *“...no supone para los implicados la desaparición de todo espacio íntimo, aunque la decisión de dos personas de compartir su existencia y el hecho de vivir juntos, conlleve una transferencia recíproca o recíproco acceso de cada uno a algunos aspectos de la intimidad del otro que antes le pertenecían en exclusiva.”*<sup>49</sup>

No obstante, a pesar de todo lo dicho anteriormente, no toda la doctrina considera que la protección realizada por la CE sobre el derecho a la intimidad y a la dignidad es inagotable. En este sentido, VILLAVERDE MENÉNDEZ se opone a esa idea y considera que *“el art. 18.1 CE no garantiza un remedo de derecho de autonomía personal que garantice a la persona la toma de decisiones sobre su vida y forma de vivirla. Como tampoco garantiza el derecho a tener una vida privada o a vivirla como*

---

<sup>47</sup> Sobre ello véase, ALEGRE MARTÍNEZ, *La dignidad de la persona como fundamento del ordenamiento constitucional español*, 1996, pág. 102- 106.

<sup>48</sup> A tal efecto véase, JORGE BARREIRO, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*, en: COBO DEL ROSAL (Dir.), *Comentarios al Código Penal*, Tomo VII, 1999, pág. 84-90; RUEDA MARTÍN, *protección penal de la intimidad personal e informática*, 2004, pág. 19 y 20.

<sup>49</sup>A tal efecto véase, CASTIÑEIRA PALOU/ ESTRADA i CUADRAS, *Delitos contra la intimidad*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal*, Parte especial, 4ª edición, 2015, pág. 153-154.

*cada cual estime conveniente. En la CE se garantiza la intimidad, no entendida como lo íntimo, sino la decisión sobre qué queda reservado a la mirada ajena”.*<sup>50</sup>

También cabe aclarar al respecto que, la intimidad se conciba como un derecho personalísimo vinculado al ser humano, no significa que las personas jurídicas no puedan gozar de ella, pues quedan protegidas penalmente por el art. 200 CP.<sup>51</sup>

Ello se considera mayoritariamente un acierto, pues según algunos penalistas como LONDOÑO TORO “*tales organismos manejan información de vital importancia que al igual que los demás desean y necesitan conservar y que el derecho debe proteger con un criterio más amplio*”.<sup>52</sup>

Como vemos es complicado precisar todo lo que protege la intimidad, pues en su aspecto negativo excluye a las demás personas de ciertos aspectos de la vida privada, que se calificasen como secretos. Y en su aspecto positivo, se concibe como un derecho de control sobre la información y los datos de la persona, para que solamente puedan ser usados esos datos con el consentimiento de su titular.<sup>53</sup>

Por ello, destaca el aspecto positivo, porque puede fundamentar la sanción de la revelación de datos almacenados a través de aparatos tecnológicos y de ciertos datos de la vida privada que se hayan adquirido de manera legítima, pero que no pueden revelarse sin la previa autorización de su titular.

Esta protección de la intimidad, en su esfera positiva, se ha incrementado gracias a la reforma de 2015.<sup>54</sup>

### **1.1. La protección reguladora de la libertad informática**

Dentro de la vertiente negativa de la intimidad (derecho a no ser molestado por terceros), se da un contenido positivo para controlar el uso que hagan esos terceros de los datos personales de una persona mediante medios tecnológicos.

---

<sup>50</sup> VILLAVERDE MENÉNDEZ, *La intimidad, ese “terrible derecho” en la era de la confusa publicidad virtual*, Revista Espaço jurídico, núm. 3, Vol. 14, 2013, pág. 59- 64.

<sup>51</sup> A tal efecto véase, RUIZ MARCO, *El bien jurídico protegido: La intimidad*, en: COBO DEL ROSAL (Dir.), *Comentarios al Código Penal*, Tomo VII, 1999, pág. 146-148.

<sup>52</sup> LONDOÑO TORO, *El derecho a la intimidad, el honor y la propia imagen enfrentado a las nuevas tecnologías informáticas*, Revista Facultad de Derecho y Ciencias Políticas, núm. 77, 1987, pág. 114.

<sup>53</sup> Sobre ello véase, RUEDA MARTÍN, *Protección penal de la intimidad personal e informática*, 2004, pág. 19 - 25.

<sup>54</sup> A tal efecto véase MUÑOZ CONDE, *Derecho penal parte especial*. 20ª edición, 2015, pág. 233-234.

Es a partir de la doctrina anglosajona cuando se empiezan a ver, los datos y la información sobre una persona en el ámbito tecnológico, como un bien jurídico que merece especial protección.

Esta clase de sociedad tecnológica en la que vivimos, conocida como *sociedad de riesgos*, conlleva según JAÉN VALLEJO: “*A un abuso de modernos instrumentos de la vida económica, como es el caso de las nuevas tecnologías*”.<sup>55</sup> Esto supone un riesgo no sólo frente a la intimidad, sino también frente al ejercicio de la libertad, ya que cada vez es más frecuente el uso de la informática para sabotear o piratear programas con el fin de atracar un banco por ejemplo, o revelar información secreta en cualquier ámbito.<sup>56</sup>

El art. 18.4 CE limita el uso de la informática y reconoce facultades de control sobre los datos relativos a la persona con el fin de proteger ese posible daño a la intimidad y la libertad informática<sup>57</sup>.

Tampoco se debe olvidar la protección que garantiza el art. 20.1 CE, el cual reconoce el derecho a recibir o comunicar información por los diversos medios de difusión.<sup>58</sup> No obstante, el art. 20 CE no protege cualquier información, sino, como bien dice CONTRERAS NAVIDAD “*para que el ejercicio del derecho a la información que realizan los medios de comunicación sea conforme a la Constitución debe reunir los requisitos de veracidad, interés y relevancia y, por último el de la corrección de formas*”.<sup>59</sup>

Por otra parte, mucho antes de que se controlase y protegiese la libertad informática en los arts. 18.3 y 18.4 CE, ya se reconocía el derecho a la inviolabilidad de la correspondencia en la *Gloriosa* Constitución de 1869. Dicho derecho fue redactado de la misma forma en el Proyecto de Constitución Federal de la República Española de 1873 y, de manera similar, en la Constitución de la Monarquía Española de 1876.

---

<sup>55</sup> JAÉN VALLEJO, *Delitos informáticos*, en: JAÉN VALLEJO / PERRINO PÉREZ (Dir.), La reforma penal de 2015, 2015, pág. 99.

<sup>56</sup> Sobre ello véase, JAÉN VALLEJO, *Delitos informáticos*, en: JAÉN VALLEJO / PERRINO PÉREZ (Dir.), La reforma penal de 2015, 2015, pág. 98 y 99.

<sup>57</sup> A tal efecto véase, RUIZ MARCO, *Intimidad, poder informático y Estado policial*, en: COBO DEL ROSAL (Dir.), Comentarios al Código Penal, Tomo VII, 1999, pág. 97-100.

<sup>58</sup> Sobre ello véase, CONTRERAS NAVIDAD, *La protección del honor, la intimidad y la propia imagen en Internet*, 2012, pág. 29-34.

<sup>59</sup> CONTRERAS NAVIDAD, *La protección del honor, la intimidad y la propia imagen en Internet*, 2012, pág. 31.

No obstante, fue la Constitución Republicana de 1931 la que amplió el precepto sobre la protección a las comunicaciones y quiso proteger también las comunicaciones telefónicas.<sup>60</sup>

Respecto a la legislación anterior a la actual sobre el control de la información, cabe decir que la LECrim de 1881 ya contemplaba, en los arts. 579 y ss, la posibilidad de que las Fuerzas y Cuerpos de Seguridad del Estado accediesen a la correspondencia privada de una persona en el curso de una investigación.<sup>61</sup>

Por último, sería en la Constitución de 1978 donde se protegerían de forma íntegra todas las comunicaciones tecnológicas en el art. 18.3 CE, artículo “*claramente inspirado*”, en opinión de RODRÍGUEZ LAINZ, por la Constitución portuguesa de 1976, como ya quedó señalado.<sup>62</sup>

Sobre la norma constitucional del art. 18.4 CE, se trata de un presupuesto para el ejercicio de otros derechos fundamentales, como puede ser la dignidad de la persona (art. 10.1 CE).

El TC, que previó el mal uso que también podría hacer el Poder Ejecutivo de los avances informáticos, declaró que el art. 18.4 CE: “*...no sólo entraña un específico instrumento de protección de los derechos frente al uso torticero de la tecnología informática, sino que consagra un derecho fundamental autónomo a controlar el flujo de las informaciones que conciernen a cada persona, pertenezcan o no al ámbito más estricto de la intimidad*”.<sup>63</sup>

A pesar de ello, fue la normativa comunitaria la que originó su protección en España. Cabe destacar: *El Convenio 108 del Consejo de Europa* de protección de las personas frente al tratamiento automatizado de datos personales, de 28 de enero de 1981; *la Directiva 95/46 del Parlamento Europeo y del Consejo*, de 24 de octubre de 1995, relativa a la protección de las personas físicas respecto al tratamiento de los datos personales y a la libre circulación de esos datos; el art. 8 del *Convenio Europeo de*

---

<sup>60</sup> El art. 32 CE de 1931 establece que: “*Queda garantizada la inviolabilidad de la correspondencia en todas sus formas, a no ser que se dicte auto judicial en contrario*”.

<sup>61</sup> A tal efecto véase, RODRÍGUEZ LAINZ, *El secreto de las telecomunicaciones y su interceptación legal*, 2016, pág. 25 y 26.

<sup>62</sup> RODRÍGUEZ LAINZ, *El secreto de las telecomunicaciones y su interceptación legal*, 2016, pág. 26.

<sup>63</sup> Sobre ello véase la STC núm. 104/1998, de 18 de mayo.

*Derechos Humanos (Convenio de Roma de 1950)*<sup>64</sup>; *el Reglamento 45/2001*, relativo al tratamiento de datos personales por las instituciones y los organismos comunitarios; y la *Directiva 2006/24/CE*.<sup>65</sup>

Estos textos normativos fueron desarrollados en nuestro país mediante la doctrina, jurisprudencia y leyes como la *LO 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD)*, derogada por la *LO 15/1999, de 13 de diciembre, de Protección de datos de carácter personal*, y la *LO 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la intimidad personal y a la propia imagen*. La *LO 5/1992 (LORTAD)* había sido recreada, según *GACITÚA ESPÓSITO*, a partir del Convenio 108 y de la Directiva 95/46, que todavía no había entrado en vigor en ese momento.<sup>66</sup>

Estas dos leyes orgánicas confieren una protección extrapenal, al ser dos normas civiles.

Por otro lado, la protección penal se halla en el Tít. X del libro II del Código Penal de 1995. En concreto, es el art. 197.2 CP, el que recoge el tipo básico de los delitos contra la libertad informática o habeas data.

El Derecho penal, mediante el Tít. X del CP de 1995, pretende proteger el ámbito de la vida privada frente a los ataques derivados del uso de las nuevas tecnologías conforme a las exigencias del art. 18 CE.<sup>67</sup>

Cabe decir que el anteriormente citado art. 197.2 CP, tiene en cuenta las exigencias normativas europeas antes descritas, para poder interpretar el alcance del bien jurídico protegido en cada caso.<sup>68</sup>

---

<sup>64</sup> El art. 8 del CEDH establece: “1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencias de la autoridad pública en el ejercicio de este derecho sino en tanto esta injerencia esté prevista por 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 del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás”.

<sup>65</sup> Sobre ello véase, *GACITÚA ESPÓSITO, El derecho fundamental a la protección de datos personales en el ámbito de la prevención y represión penal europea, (En busca del equilibrio entre la libertad y la seguridad)*, 2014, pág. 124 – 141.

<sup>66</sup> *GACITÚA ESPÓSITO, El derecho fundamental a la protección de datos personales en el ámbito de la prevención y represión penal europea, (En busca del equilibrio entre la libertad y la seguridad)*, 2014, pág. 77 y 78.

<sup>67</sup> Sobre ello véase, *JORGE BARREIRO, Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*, en: *COBO DEL ROSAL (Dir.)*, Comentarios al Código Penal, Tomo VII, 1999, pág. 88-90.

Toda esta protección, que nos aporta el ordenamiento, es lo que se conoce, según el Derecho, como *habeas data o privacy*. Se trata de un derecho de autodeterminación informativa, que nos permite impedir o controlar el acceso de los demás a nuestros datos personales.

Se requiere, según la jurisprudencia constitucionalista, el previo consentimiento del titular de los datos para que puedan usarse. También tendrá derecho a saber y ser informado sobre el destino y el uso de esos datos, además de poder rectificar, acceder y cancelarlos.

Fue, como se puede apreciar, la jurisprudencia constitucional, la que dotó de cierta autonomía a este derecho respecto del de la intimidad.<sup>69</sup>

Así, se afirma en la STC núm. 290/2000, de 30 de noviembre, que el *habeas data* del art. 18.4 CE “es una garantía del derecho a la intimidad y al honor del art. 18.1 CE pero también un derecho en sí mismo”.

Mediante esta elaboración jurisprudencial, el TC, en la sentencia núm. 254/1993, de 20 de julio, empieza a definir el bien jurídico de la libertad informática. El TC declara aquí que “la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es también derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*)”.

## **2. CAMBIOS PRODUCIDOS POR LA REFORMA DE LA LO 1/2015 EN EL CÓDIGO PENAL**

A través de la reforma de la LO 1/2015, de 30 de marzo, el legislador introduce por un lado, nuevas conductas delictivas contra la libertad informática y la intimidad. Y por otro lado, modifica algunas modalidades delictivas ya existentes reordenándolas. Este gran cambio hace cuestionarse a parte de la doctrina, como a COLÁS TURÉGANO “si

---

<sup>68</sup> Sobre ello véase, JORGE BARREIRO, *Del descubrimiento y revelación de secretos*, en: COBO DEL ROSAL (Dir.), *Comentarios al Código Penal*, Tomo VII, 1999, pág. 125-128.

<sup>69</sup> A tal efecto véase, RUIZ MARCO, *El concepto emergente. La libertad informática*, en: COBO DEL ROSAL (Dir.), *Comentarios al Código Penal*, Tomo VII, 1999, pág. 149- 152.



*tal vez debería haberse reflexionado sobre la oportunidad de crear un título específico en el que agrupar los atentados contra este bien jurídico (la libertad informática)”.<sup>70</sup>*

A veces, las reformas que se producen en el Código se originan por las repercusiones mediáticas. Así, el precepto del art. 197.7 CP, fue la respuesta del legislador a la polémica que suscitó el “*Caso Hormigos*”, que se comentará más tarde. Este precepto es el que más debate ha suscitado con su introducción tras la reforma.<sup>71</sup>

La respuesta punitiva a los supuestos del art. 197.7 CP ha sido y es muy criticada por la doctrina. El desacuerdo con este tipo penal se debe a que la víctima del hecho remite de forma voluntaria esa grabación o imagen a un destinatario. Al haber esa voluntariedad, parte de la doctrina considera que esta conducta debería ser castigada por el derecho civil, en la LO 1/1982, de 5 de mayo, de Protección del Honor, la Intimidad y la propia imagen y no por el Código Penal.<sup>72</sup>

Es principalmente esa cuestión la que hace que esa parte de la doctrina se muestre disconforme a la reforma del Código, tachándola de caer en el populismo punitivo y de convertir a todas las personas en confidentes necesarios de imágenes o grabaciones que reciban.<sup>73</sup>

Por otro lado, se atenta contra la seguridad jurídica y el principio de ofensividad con la introducción del art. 197 *ter* CP. Este nuevo artículo castiga los meros actos preparatorios y delimita la esfera de desvalor de forma incierta.

---

<sup>70</sup> COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/ MATA LLÍN EVANGELIO (Coords.), *Comentarios a la reforma penal de 2015*, 2ª edición, 2015, pág. 663.

<sup>71</sup> Sobre ello véase, MENDO ESTRELLA, *Delitos de descubrimiento y revelación de secretos: acerca de su aplicación al sexting entre adultos*, *Revista electrónica de ciencia penal y criminología*, núm. 18, 2016, pág. 11.

<sup>72</sup> Así, entre otros, MORALES PRATS, *La reforma del Código Penal de 2015 relativa a los delitos contra la intimidad*, en: QUINTERO OLIVARES (Dir.), *Comentarios a la reforma penal de 2015*, 2015, pág. 459.

<sup>73</sup> Sobre ello véase, JUANATEY DORADO / DOVAL PAIS, *Límites de la protección penal de la intimidad frente a la grabación de conversaciones e imágenes*, en: BOIX REIG (Dir.) / JAREÑO LEAL (Coord.), *La protección jurídica de la intimidad*, 2010, pág. 163-165; COMES RAGA, *La protección penal de la intimidad a través de la difusión inconsciente de sexting ajeno*, *La ley penal: Revista de derecho procesal, penal y penitenciario*, núm. 105, 2013, pág. 2.

Según MORALES PRATS, el legislador ha desaprovechado la oportunidad de mejorar técnicamente en materia de delitos contra la intimidad y, no ha revisado desde una perspectiva lógica y político-criminal, los tipos agravados del art. 197 CP.<sup>74</sup>

No obstante, también hay otros sectores que consideran que la reforma ha sido un acierto. Así, el Consejo General del Poder Judicial y el Parlamento han creído que la reforma ha sido más que necesaria debido a los graves daños que hoy en día se cometen contra la intimidad, al haber un mayor uso de las redes sociales y las nuevas tecnologías.<sup>75</sup>

Desde mi punto de vista, la reforma ha supuesto una gran mejora respecto a la regulación de los delitos informáticos y el habeas data. No obstante, no estoy totalmente de acuerdo con la modificación o introducción de ciertas modalidades delictivas, como expongo detalladamente en las conclusiones.

Por otro lado, cabría hacer mención a la LO 13/2015, de 5 de octubre, la cual también ha ayudado a reformar los delitos de descubrimiento y revelación de secretos. Dicha ley ha establecido, según RODRÍGUEZ LAINZ, un fortalecimiento de las garantías procesales y una nueva regulación de las medidas de investigación tecnológicas en la LECrim (arts. 579 y ss. LECrim).<sup>76</sup> Esta modificación ha supuesto un cambio sobre la delimitación del derecho al secreto de las comunicaciones (art. 18.3 CE).

El legislador, presionado, en opinión de RODRÍGUEZ LAINZ, por la resolución de la STC 145/2014, de 22 de septiembre, sobre el derecho fundamental al secreto de las comunicaciones, ha querido remendar las dificultades técnico - jurídicas sobre el acceso a información transmitida o compartida por prestadores de servicios de la sociedad de la información. También ha querido regular más detalladamente la introspección sobre las redes que usan estrategias para impedir la trazabilidad de las comunicaciones de sus

---

<sup>74</sup> MORALES PRATS, *El art. 197.7 y la alteración de los postulados de partida de la intervención penal en la tutela de la intimidad*, en: QUINTERO OLIVARES (Dir.), *Comentarios a la reforma penal de 2015*, 2015, pág. 460.

<sup>75</sup> Sobre ello véase, COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/ MATALLÍN EVANGELIO (Coord.), *Comentarios a la reforma penal de 2015*, 2ª edición, 2015, pág. 663- 665.

<sup>76</sup> RODRÍGUEZ LAINZ, *El secreto de las telecomunicaciones y su interceptación legal*, 2016, pág. 50-52.

usuarios (redes TOR), o que no eran protegidas por la protección formal de los preceptos constitucionales (art. 18.3 y 18.4 CE).<sup>77</sup>

De esta manera, el legislador ha regulado de forma más restrictiva las medidas de tecnovigilancia que puedan ser utilizadas en una investigación criminal (art. 588 bis. a) 1 LECrim).<sup>78</sup> Uno de los grandes motivos que hicieron que el legislador decidiera regular de forma más nítida las medidas de tecnovigilancia, fueron los criterios jurisprudenciales que se señalaron en la STC núm. 115/2013, de 9 de mayo, y la STS núm. 786/2015, de 4 de diciembre. Estas sentencias pretendían paliar los posibles abusos o vulneraciones de derechos que podían cometer los Cuerpos y Fuerzas de Seguridad del Estado al emplear las medidas de tecnovigilancia en sus investigaciones.

Al respecto, el TS en la STS núm. 906/2008, de 19 de diciembre, relativa a un supuesto de utilización de dispositivos de seguimiento con tecnología GPS por iniciativa policial, consideraba que estas medidas eran: *“diligencias de investigación legítimas desde la función constitucional que tiene la policía judicial, sin que en su colocación se interfiera en su derecho fundamental que requeriría la intervención judicial”*. No obstante, el TS reconocía que si la utilización de esos dispositivos se producía por largos períodos de tiempo, llegaría a afectar de forma flagrante la intimidad del investigado.

Para RODRÍGUEZ LAINZ esta reforma de la LO 13/2015 expresa *“un importante logro en aras de la garantía de la tutela judicial en las comunicaciones, cuya posibilidad de introspección quedaba oculta en una densa nebulosa jurídica; sobre todo en aquellos ámbitos, como la información visible de cabeceras IP que circulaba libremente a través de las redes WIFI, en los que podía adentrarse la Policía con solo realizar un barrido de espectro radioeléctrico”*.<sup>79</sup>

---

<sup>77</sup> RODRÍGUEZ LAINZ, *El secreto de las telecomunicaciones y su interceptación legal*, 2016, pág. 59 y 60.

<sup>78</sup> Véase en ese sentido, RODRÍGUEZ LAINZ, *El secreto de las telecomunicaciones y su interceptación legal*, 2016, pág. 60 y 61.

<sup>79</sup> RODRÍGUEZ LAINZ, *El secreto de las telecomunicaciones y su interceptación legal*, 2016, pág. 51.

### 3. MODALIDADES DELICTIVAS

#### **3.1 Apoderamiento de documentos o efectos e intromisión en ámbitos reservados (art. 197.1 CP)**

El precepto del art. 197.1 CP tipifica el delito de descubrimiento de secretos.

El secreto es definido por el Tribunal Supremo, en la STS núm. 1641/2000, de 23 de octubre, como *“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”*.

La técnica reguladora de esta conducta en el actual Código, según OLMO FERNÁNDEZ- DELGADO, *“es más acertada que la del art. 497 CP,<sup>80</sup> donde se tipificaba esta conducta típica en el anterior Código Penal. En el art. 497 CP la norma describía primero el tipo agravado, para después, en el párrafo siguiente, hacer lo propio con el básico”*.<sup>81</sup>

El CP de 1995 surgió, según MORALES PRATS, *“de una sólida base político - criminal en cuanto a la lógica de la incriminación en las modalidades típicas”*. Se basó en la idea de que los tipos básicos contra la intimidad, debían hallarse en alguna modalidad de acceso ilícito a la intimidad ajena. Así, los anteriores tipos básicos del art. 197. 1 CP plasmaban esa idea.<sup>82</sup>

La atipicidad que existía sobre la difusión, revelación o cesión de grabaciones audiovisuales o imágenes que surgían cada vez más por el mayor uso de los medios tecnológicos o de las redes sociales, alentó al legislador para que reformara los principios sistemáticos del tipo básico (art. 197.1 CP).

Debido a esto, el tipo básico fue reformado por el art. 106 de la LO 1/2015, de 30 de marzo.

---

<sup>80</sup> El art. 497 del CP de 1973 establecía: *“El que para descubrir los secretos de otro se apoderase de sus papeles o cartas y divulgare aquéllos será castigado con las penas de arresto mayor y multa de 100.000 a 2.000.000 de pesetas. Si no los divulgare, las penas serán de arresto mayor y multa de 100.000 a 500.000 pesetas”*.

<sup>81</sup> OLMO FERNÁNDEZ - DELGADO, *El descubrimiento y revelación de secretos documentales*, 2009, pág. 71.

<sup>82</sup> MORALES PRATS, *El art. 197.7 y la alteración de los postulados de partida de la intervención penal en la tutela de la intimidad*, en: QUINTERO OLIVARES (Dir.), *Comentarios a la reforma penal de 2015*, 2015, pág. 460- 465.

Desde el punto de vista objetivo, son dos las modalidades de comisión del delito del art. 197.1 CP.<sup>83</sup> Estas dos modalidades hacen que se considere al art. 197. 1 CP como un “*tipo mixto alternativo*”, según OLMO FERNÁNDEZ- DELGADO. Ello se debe a que el tipo prevé diversas acciones: apoderamiento, interceptación y utilización.<sup>84</sup>

La primera modalidad (art. 197.1. CP), se produce cuando el sujeto activo se apodera de papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales de otra persona. Para que se cometa el delito, solamente se necesita ese acto de apoderamiento. No se requiere que se desposea al titular de los papeles o mensajes ni que se descubra algún secreto.

El apoderamiento fue la primera conducta delictiva que tuvo en cuenta el legislador del Código Penal de 1848 para atentar contra la intimidad. Se debe concebir este término, según POLAINO NAVARRETE, “*en el sentido de traslación posesoria cognitiva, que confiere a quien realiza la posibilidad del acceso intelectual al contenido de los documentos o efectos*”.<sup>85</sup>

Por otra parte, la segunda modalidad (art. 197.1. CP), consiste en interceptar las telecomunicaciones o utilizar artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación. Se castiga con la misma pena que la primera modalidad.

A través de este precepto, que establece como intromisión ilegítima la interceptación de las telecomunicaciones por persona ajena, se garantiza el derecho al secreto de las telecomunicaciones del art. 18.3 CE.

El término interceptación posee dos acepciones que se basan en la interferencia de una comunicación. La primera acepción consiste en tomar conocimiento de la telecomunicación y, la segunda en interceptar una comunicación interpersonal a distancia.

---

<sup>83</sup> El art. 197.1 CP establece: “*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, 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.*”

<sup>84</sup> OLMO FERNÁNDEZ – DELGADO, *El descubrimiento y revelación de secretos documentales*, 2009, pág. 72.

<sup>85</sup> POLAINO NAVARRETE, *Descubrimiento y revelación de secretos*, en: COBO DEL ROSAL (Dir.), *Curso de Derecho Penal español, Parte especial*, Vol. I, 1996, pág. 940.

No obstante, como considera OLMO FERNÁNDEZ- DELGADO, estas dos acepciones sobre la interceptación no pueden aplicarse al art. 197 CP. *“La ley exige que la interceptación se realice para descubrir los secretos o la intimidad de otras personas, por lo que no tiene sentido dar aquí cabida a la segunda significación que el concepto tiene, pues el obstaculizar o impedir las comunicaciones no es el medio adecuado para descubrir los secretos o la intimidad de nadie”*.<sup>86</sup>

La conducta del art. 197.1. CP suele basarse en la intervención de teléfonos pero no descarta que el hecho consista en la interceptación de otro medio de comunicación, como los otros descritos en la segunda modalidad.

Dicha modalidad se presenta en el caso resuelto por la STS núm. 224/2004, de 31 de marzo, en el que se hicieron escuchas telefónicas mediante objetos de grabación y reproducción del sonido en una sede de Herri Batasuna.

Nuestro Código Penal sólo considera delito contra la intimidad las acciones que conllevan una intromisión ilegítima en el ámbito de reserva de las personas, no cualquier atentado contra la intimidad. Este hecho posee una gran importancia porque significa que cumple un papel decisivo el titular del derecho vulnerado.

Los ámbitos de reserva de una persona dependen de las barreras de protección concedidas por el ordenamiento jurídico, pero también por las medidas de autoprotección llevadas a cabo por la propia persona, como, por ejemplo, la restricción del acceso a una cuenta de correo electrónico mediante el uso de un código secreto.

Por otra parte, cabe decir que en el caso de que se quiera grabar una conversación y se hayan instalado los medios para interceptarla, RUEDA MARTÍN considera que no hace falta que se haya llegado a grabar dicha conversación para que se haya consumado el delito. Basta la intención de haber querido grabar la conversación y de haber usado los medios idóneos para llevar a cabo ese fin, para que ello suponga un delito de descubrimiento de secretos del art. 197.1 CP y haya una vulneración de la intimidad.<sup>87</sup>

En los casos de la tercera modalidad del art. 197.1 CP (utilizar artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen), se estima

---

<sup>86</sup> OLMO FERNÁNDEZ – DELGADO, *El descubrimiento y revelación de secretos documentales*, 2009, pág. 80 y 81.

<sup>87</sup> RUEDA MARTÍN, *Protección penal de la intimidad personal e informática*, 2004, pág. 62 y 63.

que si la grabación de una conversación se produce por uno de los interlocutores, sin consentimiento del otro, aunque sea de manera clandestina, no va en contra del derecho fundamental al secreto de las comunicaciones (art. 18.3 CE) ni contra la intimidad (art. 18.1 CE).

Por el contrario, MUÑOZ CONDE, sí considera que una grabación puede ser castigada por el tipo penal del art. 197. 1 CP aunque la escucha telefónica sea legal, “*piénsese en una conversación telefónica grabada por uno de los interlocutores, o en la confidencia grabada por el que la escucha o en la grabación de una conversación telefónica captada por casualidad*”.<sup>88</sup>

También al respecto, el TC había considerado, en una de las sentencias pioneras sobre el descubrimiento y revelación de secretos, que una grabación telefónica de ese tipo “*sólo constituiría un ilícito sobre la base del reconocimiento de la protección de la propia voz, que sólo existe en el Derecho Español como concreción del derecho a la intimidad y, por ello mismo, en la medida que se utilice con fines publicitarios, comerciales o de naturaleza análoga, como exige el art. 7.6 de la 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, y no se trate de un mero registro*”.<sup>89</sup>

Cosa distinta es que esa grabación sea empleada como medio de revelación de su contenido. Ahí sí que se está dañando el derecho de la intimidad.

No obstante, si la perpetuación de la conversación se considera legítima, sólo será relevante su revelación a terceros si el autor tenía un deber penal de reservar ese secreto (art. 199 CP).

Sobre ello, la sala primera del TC en la sentencia núm. 12/2012, de 30 de enero, estima que la grabación, con una cámara y micros ocultos, por una periodista que se hace pasar por clienta, de la consulta de una esteticista naturista, vulnera el derecho a la intimidad personal.

También la STS núm. 298/2013, de 13 de marzo, condena a una prostituta por la grabación videográfica clandestina que hizo a un hombre, mientras estaban manteniendo relaciones sexuales, por mandato de un tercero.

---

<sup>88</sup> MUÑOZ CONDE, *Derecho Penal, Parte Especial*, 20ª edición, 2015, pág. 236.

<sup>89</sup> Véase la STC núm. 114/1984, de 29 de noviembre.

Respecto a la perspectiva de la tipicidad subjetiva, nos hallamos ante un delito en el que se exige dolo, pues es totalmente relevante la intención específica del sujeto activo. El autor tiene que realizar el apoderamiento o la intromisión del ámbito reservado para descubrir el secreto o vulnerar la intimidad.<sup>90</sup>

Además de la voluntad de apoderamiento de los documentos o efectos que contengan secretos, el tipo penal requiere que el autor del delito tenga la intención de descubrirlos. El art. 197 CP evidencia este hecho por el uso de la preposición “para”.

Si la intención del hecho delictivo es destruir los documentos, se aplica el art. 263 y ss. CP, no el art. 197 CP.

En conclusión, el sujeto activo puede ser cualquiera. Pero, el sujeto pasivo sólo puede ser el titular de los secretos reflejados en los documentos de los que se apodera el autor del delito.

Sin embargo, la jurisprudencia se presenta ambivalente sobre esto. Así, en la STS núm. 990/2012, de 18 de octubre, se condena a una enfermera que accedió al historial clínico de una paciente del hospital donde trabajaba con la finalidad de proteger a sus sobrinas. La Sala Segunda del TS sentenció que *“los móviles que guían la conducta del autor son irrelevantes en la construcción dogmática del tipo subjetivo”*.

Finalmente, para que se consume el delito, vale con el apoderamiento o la intromisión. No se exige que los datos a los que se tenga acceso sean relevantes. Basta con la intención de descubrir el secreto para consumir el delito, no siendo necesario que al final se descubra.

Sobre la segunda modalidad del art. 197.1 CP, hay una discusión en torno a si la consumación comienza cuando se instalan los artificios o cuando empiezan a funcionar. Es preciso que se capte el sonido o la imagen, con un artificio técnico, para que se consume el delito. Lo que sí está claro es que, en todo caso, no se requiere la efectiva vulneración de la intimidad.<sup>91</sup>

---

<sup>90</sup> A tal efecto véase, MUÑOZ CONDE, *Derecho Penal. Parte Especial*. 20ª edición, 2015, pág. 235-236.

<sup>91</sup> A tal efecto véase, CASTIÑEIRA PALOU/ ESTRADA i CUADRAS, *Delitos contra la intimidad*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 155-159.



Como en la primera modalidad del art. 197.1 CP, se requiere que la conducta delictiva tenga como fin descubrir los secretos de otro o vulnerar su intimidad.

La invasión a la intimidad de alguien, en el ejercicio de ciertos oficios o profesiones, sin autorización expresa del afectado, sólo puede considerarse consentida en lo estrictamente necesario para el desarrollo de su oficio o profesión.

Por esto, el TS condena a un médico, que grababa por videocámara las exploraciones ginecológicas que hacía a sus pacientes, sin justificación y sin los consentimientos de dichas pacientes.<sup>92</sup>

### **3.2. Manipulación de los datos reservados registrados en ficheros o soportes informáticos (art. 197.2 CP)**

El art. 197.2 CP<sup>93</sup> tipifica la modalidad delictiva consistente en manipular datos reservados en ficheros o soportes informáticos. Se trata de un delito contra la libertad informática (habeas data)<sup>94</sup>, reformado por el art. 106 de la LO/2015, de 30 de marzo.

El art. 197.2 CP se refería y se refiere a la incriminación de accesos ilícitos a la intimidad que dañen datos de carácter personal, enumerando el legislador en dicho artículo, los posibles accesos informáticos ilícitos a esos datos.

Este precepto busca proteger la esfera positiva de la intimidad, controlando los datos de carácter personal y familiar recogidos en cualquier tipo de archivo o fichero.<sup>95</sup>

No obstante, se está tendiendo a creer que, en realidad, se pretende proteger un bien jurídico específico, con mayor alcance que el concepto general de intimidad. Así, RUEDA MARTÍN considera que el art. 197.2 CP busca garantizar “*la intimidad personal y familiar referida al control sobre la publicidad de la información relativa a la persona y a su familia*”.<sup>96</sup>

---

<sup>92</sup> A tal efecto véase, la STS núm. 1045/2011, de 14 de octubre.

<sup>93</sup> El art. 197.2 CP establece: “*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*”.

<sup>94</sup> Sobre ello véase, RUEDA MARTÍN, *Protección penal de la intimidad personal e informática*, 2004, pág. 67-92.

<sup>95</sup> A tal efecto véase, la STS núm. 1328/2009, de 30 de diciembre.

<sup>96</sup> RUEDA MARTÍN, *Protección penal de la intimidad personal e informática*, 2004, pág. 68.

Justamente, el TC distingue el derecho fundamental de la intimidad (art. 18.1 CE) y el derecho fundamental a la protección de datos personales (art. 18.4 CE).

Así, en la STC núm. 292/2000, de 30 de noviembre, se afirma que el objeto de la protección de datos *“es más amplio que el del derecho de la intimidad, ya que también extiende su garantía a lo que este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal”*.

La garantía constitucional del art. 18.4 CE, amplía la protección a aquellos datos relevantes en el ejercicio de los derechos de la persona, sean o no constitucionales y se refieran o no al honor, intimidad personal y familiar, o cualquier otro bien amparado por la CE.

Esta amplia interpretación del bien jurídico protegido por la norma, sólo es admisible cuando la afectación al honor, la dignidad u otros bienes de la persona sean de gravedad suficiente como para merecer las penas previstas en el delito del art. 197.2 CP.

De cualquier manera, los datos siempre tienen que ser reservados, no pueden ser conocidos por cualquiera. Han de almacenarse en un fichero o soporte informático, electrónico o telemático, o en un archivo público o privado. Y, finalmente, los datos deben ser ajenos al sujeto que realiza la conducta típica.<sup>97</sup>

Así por ejemplo, en la STS núm. 40/2016, de 3 de febrero, se señala que *“el acceso no autorizado a datos protegidos, como es el historial médico, a los que no puede acceder el titular supone una injerencia al derecho a la intimidad, tipificada en el art. 197.2 CP”*.

La particularidad que encierra el tipo es que los datos estén registrados de manera ordenada, usualmente a través de un mecanismo informático. Por eso, las conductas tipificadas no se limitan al apoderamiento, utilización o modificación de los datos, sino que también incluyen el acceso a los mismos como, por ejemplo, que el sujeto activo utilice un ordenador, una tablet, o un smartphone (medios tecnológicos) para llegar a acceder a dicha información reservada.

---

<sup>97</sup> Sobre ello véase, CASTIÑEIRA PALOU/ ESTRADA i CUADRAS, *Delitos contra la intimidad*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 159- 161.

La Sala Segunda del TS ha definido como dato reservado de carácter personal y familiar, el referido al hotel en el que la exmujer de un acusado se alojaba. Este dato registrado en un fichero de la Policía, fue conocido por el acusado, al tener acceso al fichero por pertenecer al cuerpo de Policía.<sup>98</sup>

El art. 197.2 CP distingue tres modalidades de comisión: a) el apoderamiento, utilización o modificación de datos sin autorización y en perjuicio de terceros; b) el mero acceso a datos, sin autorización; y c) la alteración o utilización de datos en perjuicio de su titular o de un tercero.

Se plantean dudas, en opinión de CASTIÑEIRA PALOU / ESTRADA I CUADRAS, a la hora de interpretar si la modalidad a) es irrelevante penalmente si se ejecuta en perjuicio del titular de los datos.<sup>99</sup>

La jurisprudencia del TS descarta que no tenga importancia ese hecho al declarar que, el primer inciso del art. 197.2 CP, requiere que se actúe “en perjuicio de tercero”. En cambio, el segundo inciso exige una actuación “en perjuicio del titular de los datos o de un tercero”.<sup>100</sup>

Respecto a quién puede cometer este delito, el sujeto activo puede ser cualquier persona. Cabe decir que también se castigará en este artículo, a la persona que tenga autorización para acceder o manipular los datos del fichero o registro, pero que acceda a ellos para fines distintos a los que justifican esa autorización.<sup>101</sup>

Sobre esto, debe aclararse que no se daría por ejemplo, un acceso ilegítimo en el caso de que los órganos jurisdiccionales accedieran a diversos datos personales de un acusado en un proceso judicial. Ello se debe a que la vulneración del derecho a la autodeterminación informativa, que garantiza el art. 18.4 de la CE y castiga el art. 197.2

---

<sup>98</sup> Sobre ello véase, la STS núm. 1945/2014, de 27 de noviembre.

<sup>99</sup> CASTIÑEIRA PALOU/ ESTRADA i CUADRAS, *Delitos contra la intimidad*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 160.

<sup>100</sup> Véase la STS núm. 525/2014, de 17 de junio.

<sup>101</sup> A tal efecto véase, CASTIÑEIRA PALOU/ ESTRADA i CUADRAS, *Delitos contra la intimidad*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 159-161.

CP, en este supuesto está justificada al permitir la ley la cesión de datos en la esfera judicial.<sup>102</sup>

A tal efecto, declara el TS en la sentencia núm. 586/2016, de 4 de julio, que *“la transferencia de datos personales, ya sea con fines jurisdiccionales o no jurisdiccionales, en el ámbito de la actividad judicial no puede tener encaje en el Derecho Penal”*.

Por último, parte de la doctrina como CASTIÑEIRA PALOU / ESTRADA I CUADRAS, cuestionan en este delito si la frase “en perjuicio de” constituye un elemento subjetivo del injusto o no. Interpretar esta fórmula como elemento subjetivo del injusto, le dota de mayor capacidad restrictiva, que si se considerase resultado típico de la lesión. Además, esta interpretación permite relacionar la estructura del tipo subjetivo del delito con la del descubrimiento de secretos del art.197.1 CP.<sup>103</sup>

En conclusión, la expresión “en perjuicio de” indica según MUÑOZ CONDE *“un especial elemento subjetivo del injusto, no siendo necesario para consumar el delito que efectivamente el perjuicio se cause”*.<sup>104</sup>

Cabe decir que según la LO 15/1999, de Protección de Datos de Carácter Personal y el RD 1720/2007, el hecho delictivo queda justificado si hay autorización para realizar esas conductas.<sup>105</sup>

### **3.3. Revelación de secretos (Art. 197.3 CP)**

El art. 197.3 CP<sup>106</sup> recoge la conducta delictiva consistente en la revelación de secretos. Este precepto también ha sido modificado por la LO 1/2015, de 30 de marzo.

---

<sup>102</sup> Sobre ello véase, PÉREZ DE LA OSSA, *Descubrimiento y revelación de secretos*, en Cuaderno jurídico, Práctica Penal, núm. 86, 2017, pág. 71.

<sup>103</sup> CASTIÑEIRA PALOU/ ESTRADA I CUADRAS, *Delitos contra la intimidad*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 161.

<sup>104</sup> MUÑOZ CONDE, *Derecho Penal Parte Especial*. 20ª edición, 2015, pág. 237.

<sup>105</sup> A tal efecto véase, MUÑOZ CONDE, *Derecho Penal Parte Especial*. 20ª edición, 2015, pág. 237.

<sup>106</sup> El art. 197.3 CP establece: *“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”*.

Respecto al cuadro legal que estructuraba las agravaciones a partir de los tipos básicos, se suma la reforma del CP de 2010. Esta reforma crea otra modalidad de acceso ilícito a la intimidad: el intrusismo informático (art. 197.3 CP).

Mediante la regulación de esa nueva figura, España cumple las exigencias del Convenio de Cibercriminalidad de Budapest.<sup>107</sup>

Se trata de un tipo penal cualificado por razón de la divulgación.<sup>108</sup>

Su primer epígrafe recoge el delito de difusión de los secretos o datos que se descubran ilícitamente. Se castiga con una pena superior al tipo básico de apoderamiento o intromisión de secretos.

La agravación del primer apartado del art. 197.3 CP se debe, en opinión de RUEDA MARTÍN, *“a que la difusión, revelación o cesión a terceros de los datos o hechos descubiertos o de las imágenes captadas incrementa el menoscabo al bien jurídico protegido, que se produce cuando los datos o hechos descubiertos o las imágenes captadas son conocidos por varias personas”*.<sup>109</sup>

Por el contrario, la conducta regulada en el segundo apartado del art. 197.3 CP, consistente en revelar datos pero no haber sido quien los descubre, se castiga con una pena menos grave. Por eso, la pena de prisión es de uno a tres años y no de dos a cinco años, como en el art. 197.3.I CP.<sup>110</sup>

Según RUEDA MARTÍN, el hecho por el que se castiga con una pena menos grave el art. 197. 3 CP, se debe a que el precepto recoge conductas de participación, no de autoría. *“Las conductas de participación son difíciles de reconducir a través de las reglas generales de la participación delictiva, ya que en ellas no se acepta la codelincuencia entre la consumación formal y la terminación del delito”*.<sup>111</sup>

---

<sup>107</sup> Sobre ello véase, DÍAZ GÓMEZ, *El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest*, Revista Hologramática, Vol. 5, núm. 14, 2011, pág. 27- 86.

<sup>108</sup> A tal efecto véase, MUÑOZ CONDE, *Derecho Penal Parte Especial*, 20ª edición, 2015, pág. 237-238.

<sup>109</sup> RUEDA MARTÍN, *Protección penal de la intimidad personal e informática*, 2004, pág. 96.

<sup>110</sup> A tal efecto véase, CASTIÑEIRA PALOU/ ESTRADA i CUADRAS, *Delitos contra la intimidad*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 166-167.

<sup>111</sup> RUEDA MARTÍN, *Protección penal de la intimidad personal e informática*, 2004, pág. 115.

El Código Penal exige, para que la conducta se castigue por el segundo apartado del art. 197.3 CP, que quien revele esos datos pero no los haya descubierto, sepa que el origen de esa información revelada es ilícito. No se castigan los supuestos en los que el transmitente no sabe que ese origen no es lícito. Debe haber pues, según RUEDA MARTÍN, “*la conciencia y la voluntad de que los datos, hechos o imágenes captadas se difundan, revelen o cedan a terceros*”.<sup>112</sup>

### **3.4. Subtipos agravados (Arts. 197.3, 197.4, 197.5, 197.6, 197 quáter y 198 CP)**

Las modalidades típicas se agravan según quién es el sujeto activo, cómo son los datos o secretos que se revelan y si hay o no ánimo de lucro.

Dichas agravaciones están, además de en el explicado art. 197. 3 CP, en los arts. 197. 4<sup>113</sup>, 5<sup>114</sup>, 6<sup>115</sup>, quáter<sup>116</sup> y el art. 198 CP<sup>117</sup>.

En los delitos de los arts. 197. 1 y 2 CP se elevará la pena a su mitad superior cuando el sujeto activo sea el encargado o responsable de los ficheros, soportes, registros o archivos (art. 197. 4. a) CP). También, cuando se haya difundido, revelado o cedido el secreto mediante la utilización de datos personales de la víctima (art. 197.4.b) CP).

El apartado segundo del art. 197.4 CP se introdujo con el fin de reordenar los diversos epígrafes de los delitos contra la intimidad en la reforma del CP de 2015. En cambio, el

---

<sup>112</sup> RUEDA MARTÍN, *Protección penal de la intimidad personal e informática*, 2004, pág. 98.

<sup>113</sup> El art. 197.4 CP establece que: “*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*”.

<sup>114</sup> El art. 197.5 CP establece que: “*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 necesitada de especial protección, se impondrán las penas previstas en su mitad superior*”.

<sup>115</sup> El art. 197.6 CP establece que: “*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*”.

<sup>116</sup> El art. 197 quáter CP establece que: “*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*”.

<sup>117</sup> El art. 198 CP establece que: “*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*”.

primer apartado del art 197.4 CP es exactamente igual al art. 197.5 CP antes de la reforma.<sup>118</sup>

El art. 197. 4 CP consta de dos tipos de agravaciones. La primera agravación (art. 197. 4. a) CP) ya estaba en la versión original del CP de 1995 como tipo agravado. Contempla la comisión de los accesos ilícitos a la intimidad (art. 197.1 y 2 CP) por personas encargadas de los ficheros, soportes informáticos, electrónicos o telemáticos.

Se configura esta agravación en razón de la esfera del dominio profesional del sujeto activo. Se refiere a las funciones de los encargados o responsables de los sistemas que prevé el art. 3 de la LOPDP. Es por esto que el art. 197. 4 CP, según RUEDA MARTÍN, “*recoge un delito especial al poder sólo realizarse las acciones típicas por aquellas personas que reúnen una determinada condición para ser autor del delito: ser personas encargadas o responsables de los ficheros o soportes informáticos, electrónicos o telemáticos*”.<sup>119</sup>

Lo que introduce la reforma es una nueva conducta delictiva agravada, que depende de que se den las conductas tipificadas en los arts 197.1 y 197. 2 CP (delitos contra la intimidad y el habeas data).<sup>120</sup>

El segundo apartado del art. 197.4. CP es relativo a que la comisión del acceso ilícito a la intimidad en los términos del art. 197.1 y 2 CP, se realice sin la autorización de datos personales de la víctima. Se trata, en opinión de CASTELLÓ NICÁS, “*de una modalidad del delito de usurpación de estado civil del art. 401 CP, pues la utilización no autorizada de datos personales de la víctima supone, necesariamente, hacerse pasar por ésta*”.<sup>121</sup>

Según COLÁS TURÉGANO, se interpreta el precepto en el sentido de que no es válido el consentimiento presunto para poder obtener la autorización de datos personales de

---

<sup>118</sup> Sobre ello véase, CASTELLÓ NICÁS, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor*, en: MORILLAS CUEVA (Dir.), *Estudios sobre el Código Penal reformado*, 2015, pág. 504.

<sup>119</sup> RUEDA MARTÍN, *Protección penal de la intimidad personal e informática*, 2004, pág. 99.

<sup>120</sup> Sobre ello véase, COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/ MATALLÍN EVANGELIO (Coords.), *Comentarios a la reforma penal de 2015*, 2ª edición, 2015, pág. 675.

<sup>121</sup> CASTELLÓ NICÁS, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor*, en: MORILLAS CUEVA (Dir.), *Estudios sobre el Código Penal reformado*, 2015, pág. 504.

alguien. “Habrá de haber sido otorgado de manera expresa por un sujeto mayor, capaz”.<sup>122</sup>

Así por ejemplo, la AP de Asturias en la sentencia núm. 39/2017, de 15 de febrero, castigó a través del art. 197.4 CP la conducta consistente en la divulgación por vía *whatsapp*, sin sus consentimientos obviamente, de conversaciones sentimentales e íntimas entre una mujer casada y su amante, a terceras personas y familiares con el fin de humillar a ésta última, por parte de su marido al enterarse de la infidelidad.

Respecto al nuevo segundo apartado del art. 197.4 CP, el art. 10 de la LOPDP ya contemplaba obligaciones profesionales con repercusión penal. No se entiende por ello, desde el punto de vista de MORALES PRATS, que se creara esta agravación, pues la legislación ya alcanzaba a entender la posibilidad y los supuestos en los que se trabajaba con datos personales ajenos.<sup>123</sup>

Así las cosas, hay una laguna jurídica, en opinión de MORALES PRATS, en el caso de que una persona opere con datos personales de otro sin su autorización, sin que eso suponga la conducta de acceso ilícito, ya que en esta agravación sólo se tiene en cuenta las conductas básicas del art. 197.1 y 2 CP, en las que el acceso es ilegítimo.<sup>124</sup>

Las causas por las que se agrava la pena en el primer apartado del art. 197.4. CP son entendibles, ya que un encargado o responsable de un fichero o registro de datos tiene la gran responsabilidad de velar por la información que en dichos ficheros o registros se encuentre (art. 9 LO 15/1999, de protección de datos de carácter personal).

En cambio en el apartado segundo del art. 197.4 CP, no está realmente claro por qué se agrava la pena. Sobre ello, MUÑOZ CONDE cree que puede ser por “*la mayor susceptibilidad de la víctima, al tener el autor del delito datos que lesionan la defensa del sujeto pasivo*”.<sup>125</sup>

---

<sup>122</sup> COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/ MATALLÍN EVANGELIO (Coords.), *Comentarios a la reforma penal de 2015*, 2ª edición, 2015, pág. 675.

<sup>123</sup> MORALES PRATS, *La creación del tipo agravado del art. 197.4. b) CP*, en: QUINTERO OLIVARES (Dir.), *Comentarios a la reforma penal de 2015*, 2015, pág. 465.

<sup>124</sup> MORALES PRATS, *La creación del tipo agravado del art. 197.4. b) CP*, en: QUINTERO OLIVARES (Dir.), *Comentarios a la reforma penal de 2015*, 2015, pág. 465.

<sup>125</sup> MUÑOZ CONDE, *Derecho Penal Parte Especial*. 20ª edición, 2015, pág. 237- 238.



La utilización de datos personales de la víctima constituye asimismo, una agravante genérica del art. 22 CP.

Como se aprecia, el art. 197. 4 CP agrava la pena del delito por razón del sujeto activo que realizó el hecho delictivo.

El art. 197.5 CP también forma otro tipo penal agravado. Se aplica a todas las modalidades delictivas dependiendo, en opinión de RUEDA MARTÍN, “*del objeto material del delito sobre el que recaen las acciones delictivas*”.<sup>126</sup>

Se trata de los “*datos sensibles*”. Son aquéllos que revelan la ideología, religión, creencias, salud, origen racial o vida sexual de la víctima. Serán a su vez datos sensibles, los que pertenezcan a un menor de edad o incapaz (Ley 1/1996, de 15 de enero, de Protección Jurídica del Menor).

En estos supuestos, la pena se impone en su mitad superior.

Otro tipo penal agravado se halla en el art. 197.6 CP. Se impone la pena en su mitad superior cuando el delito se realice con un fin lucrativo. Si este hecho afecta a “*datos sensibles*”, la pena es de cuatro a siete años de prisión.

Según RUEDA MARTÍN, el elemento subjetivo que se exige en este tipo penal es diferente al dolo. “*La existencia del elemento subjetivo del injusto determina la concreta lesión o peligro del bien jurídico intimidad personal que se quiere castigar con mayor pena: obtener una ventaja, provecho o goce, incluso de contenido no patrimonial*”.<sup>127</sup>

Así por ejemplo, la STS núm. 201/2017, de 27 de marzo, no castiga a través del art. 197. 6 CP la conducta realizada por un detective privado que accedía a historiales médicos sin ningún tipo de autorización y fraudulentamente, por no existir ese fin lucrativo entre la persona que le conseguía la información sanitaria y dicho detective. De esta forma, el TS casó y sentenció que: “*Los fines de lucro que describe el subtipo agravado del art. 197.6 CP implican algo más: se exige un lucro ligado en concreto a la conducta típica. Que el acusado cobrase por los informes que preparaba para la Aseguradora (no sabemos si esos informes contenían esa información) no es suficiente.*

---

<sup>126</sup> RUEDA MARTÍN, *Protección penal de la intimidad personal e informática*, 2004, pág. 104.

<sup>127</sup> RUEDA MARTÍN, *Protección penal de la intimidad personal e informática*, 2004, pág. 111.

*Sería preciso que existiese un pago concreto determinado o determinable directamente anudado a esa conducta ilícita”.*

Por otro lado, si la conducta delictiva se comete a través de una organización o grupo criminal se impone la pena superior en grado. Este tipo agravado se halla en el art. 197 *quáter* CP. Su redacción es muy similar a la del art. 197. 8 CP antes de la reforma, no obstante, como bien señala CASTELLÓ NICÁS, se produce un gran cambio respecto al ámbito de aplicación. Antes, sólo se aplicaba este tipo agravado a concretos apartados del art. 197 y ahora en cambio, el art. 197 *quáter* CP se aplica a todo el articulado del Cap. X.<sup>128</sup>

De esta forma, mientras que antes de la reforma sólo se agravaban las conductas delictivas relativas al descubrimiento y revelación de secretos que se llevaban a cabo dentro de una organización criminal, en el presente también se aplica la agravación por organización criminal en las conductas delictivas referentes al secreto laboral o profesional.<sup>129</sup>

Por último, cuando es una autoridad o funcionario público el que actúa fuera de los casos permitidos por la ley, sin causa legal y prevaliéndose de su cargo, el art. 198 CP, impone la pena del tipo básico del art. 197 CP en su mitad superior.<sup>130</sup> Además, se le impondrá una pena de inhabilitación absoluta de seis a doce años al tratarse, según RUEDA MARTÍN, *“de un delito especial, pues sólo puede ser realizada la conducta típica aquella persona que reúne una determinada condición para ser autor y que constituye un elemento del tipo objetivo: ser autoridad o funcionario público”*.<sup>131</sup>

Cabe decir que no puede castigarse por el art. 198 CP esas conductas delictivas, en el caso de que no se pruebe de forma sólida o no se esté seguro del medio de acceso o método de aplicación que utilizó dicha autoridad o funcionario público para acceder a

---

<sup>128</sup> CASTELLÓ NICÁS, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor*, en: MORILLAS CUEVA (Dir.), *Estudios sobre el Código Penal reformado*, 2015, pág. 509.

<sup>129</sup> COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/ MATALLÍN EVANGELIO (Coords.), *Comentarios a la reforma penal de 2015*, 2ª edición, 2015, pág. 681.

<sup>130</sup> Sobre ello véase, CASTELLÓ NICÁS, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor*, en: MORILLAS CUEVA (Dir.), *Estudios sobre el Código Penal reformado*, 2015, pág. 510.

<sup>131</sup> RUEDA MARTÍN, *Protección penal de la intimidad personal e informática*, 2004, Pág. 121.

cierta información sin autorización.<sup>132</sup> De esta forma, la STS núm. 407/2016, de 12 de mayo, sentenció que: “*La falta de concreción de la aplicación a la que accedió el agente acusado para obtener los datos de otra persona impide la condena por el delito de descubrimiento y revelación de secretos, no siendo bastantes los indicios*”.<sup>133</sup>

No se debe confundir las conductas castigadas en los arts. 534 a 536 del CP con la del art. 197 CP, que castigan hechos similares.

La diferencia entre estos artículos y el art. 197 CP está, en opinión de RUEDA MARTÍN, en que en los arts. 534 a 536 CP se tipifican las conductas en las que el funcionario sí tiene competencia para actuar pero no respeta las garantías constitucionales.<sup>134</sup>

Cabe también decir que el art. 417 CP regula, de forma expresa, la revelación de secretos por funcionario público.<sup>135</sup>

### **3.5. Difusión no consentida de captaciones íntimas de la imagen (art. 197.7 CP)**

La difusión no consentida de captaciones íntimas de la imagen se tipifica en el art. 197.7 CP<sup>136</sup>.

Este artículo se introdujo con la reforma de la LO 1/2015, de 30 de marzo. El art. 197.7 CP tipifica las conductas consistentes en la difusión, revelación o cesión a terceros de imágenes o grabaciones audiovisuales, realizadas sin la autorización del titular de la imagen o grabación, en un domicilio o fuera del alcance de terceros.

No obstante, la reforma también introdujo el art. 183. ter. 2 CP, el cual “*reputa tantos problemas como el art. 183.ter.1 CP (grooming)*”, en opinión de RAMOS

---

<sup>132</sup> Sobre ello véase, PÉREZ DE LA OSSA, *Descubrimiento y revelación de secretos*, en: GUIMERÁ FERRER-SAMA (Dir.), Cuaderno jurídico, Práctica Penal, núm. 86, 2017, pág. 72.

<sup>133</sup> En este sentido, véase también la STS núm. 509/2016, de 10 de junio.

<sup>134</sup> RUEDA MARTÍN, *Protección penal de la intimidad personal e informática*, 2004, pág. 130.

<sup>135</sup> Sobre ello véase, CASTIÑEIRA PALOU/ ESTRADA i CUADRAS, *Delitos contra la intimidad*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 167- 168.

<sup>136</sup> Art. 197. 7 CP establece: “*Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquella que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona*”.

VÁZQUEZ.<sup>137</sup> Este artículo castiga la transmisión de mensajes con cierto contenido erótico a terceros cuando es un menor quien envía dichos mensajes.

Se decide crear este delito debido a la problemática que suponía el envío voluntario de imágenes propias de contenido sexual a través de mensajes o redes sociales. Este hecho se conoce como *sexting*. Según RAMOS VÁZQUEZ, este término se trata de un “neologismo que deriva de la hibridación de las palabras inglesas “sex” y texting”.<sup>138</sup>

Conforme a la definición que establece MARTÍNEZ OTERO, el *sexting* consiste en “el envío, normalmente a través de Internet o de un dispositivo móvil, de mensajes de contenido sexual producido y protagonizado por el emisor”.<sup>139</sup> Algo similar, aunque más preciso, piensa la AP de Granada, en la sentencia núm. 351/2014, de 5 de junio, que lo define como: “El envío de imágenes estáticas (fotografías) o dinámicas (vídeos) de contenido sexual de mayor o menor carga erótica entre personas que voluntariamente consienten en ello y, que forma parte de su actividad sexual que se desarrolla de manera libre”.

En los últimos tiempos, entre la población adolescente, ha nacido la costumbre de enviar fotos o vídeos de contenido sexual de forma voluntaria, a novios, amantes o amigos, llegando a aparecer en múltiples ocasiones en el espacio público.<sup>140</sup>

Usualmente esas imágenes acaban estando en las redes sociales (facebook, instagram etc.), o acaban enviándose por whatsapp a los conocidos del emisor de la imagen. Estas actuaciones dan lugar a su vez a que el protagonista de la imagen sufra acoso u hostigamiento por esa repercusión perjudicial. Así por ejemplo, un reciente estudio ha comprobado que en Cataluña, un 33,5% de los adolescentes entre los 14 y los 18 años,

---

<sup>137</sup> RAMOS VÁZQUEZ, *Grooming y sexting*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/MATALLÍN EVANGELIO (Coords.), Comentarios a la reforma penal de 2015, 2ª edición, 2015, pág. 623.

<sup>138</sup> RAMOS VÁZQUEZ, *Grooming y sexting*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/MATALLÍN EVANGELIO (Coords.), Comentarios a la reforma penal de 2015, 2ª edición, 2015, pág. 623.

<sup>139</sup> MARTÍNEZ OTERO, *La difusión de sexting sin consentimiento del protagonista: un análisis jurídico*, Revista online especializada en Derecho de la Comunicación (Derecom), núm. 18, 2014, pág.1.

<sup>140</sup> Sobre ello véase, EVANGELINA NARVAJA Y DE PIERO, *Prácticas juveniles íntimas: sexting y vlogging*, Aposta: Revista de ciencias sociales, núm. 69, 2016, pág. 240 y 241.

se han visto envueltos en alguna ocasión en conductas de sexting, sufriendo el 44% de ellos angustia, miedo o vergüenza por ello.<sup>141</sup>

No obstante, MORALES PRATS considera que eso no es motivo suficiente para incriminar esa difusión, grabación o revelación desde un punto de vista político-criminal si el titular de esas acciones lo había consentido.<sup>142</sup>

En mi opinión, dada la gravedad que conlleva este asunto y la frecuencia con que se da hoy en día, me parece totalmente un acierto que el legislador haya decidido regular estas conductas y así intentar paliar los daños que produce en la población más sensible e insegura, como son los adolescentes.

Sobre cuál fue uno de los motivos de peso que hizo que el legislador decidiera introducir esta modalidad delictiva, cabe decir que se debió en gran parte a la polémica social que se originó por la difusión de un vídeo erótico-sexual de la edil Hormigos, tal y como ya se ha señalado en otro lugar de este trabajo. Se llegó a crear en 2013 un anteproyecto de ley del Código Penal.<sup>143</sup>

Este caso se basa en el envío voluntario de un vídeo erótico desde un móvil a un amigo, el cual divulgó esas imágenes de contenido sexual a un tercero, y éste a su vez continuó reenviándolo a más personas por correo electrónico.

Por este hecho, la edil denunció a la persona que había divulgado por primera vez el vídeo. Sin embargo, tras las diligencias de Instrucción, el caso se archivó de manera provisional mediante auto de sobreseimiento, por no castigarse en ese momento ese tipo de conductas en nuestro Código Penal, al haber sido la edil la que envió, de forma voluntaria, dicho contenido sexual.<sup>144</sup>

Como dato curioso, cabe decir que la citada reforma de 2015 de nuestro Código es similar a alguna legislación comparada. En el derecho alemán también se castiga la

---

<sup>141</sup> A tal efecto véase, AGUSTINA SANLLEHÍ Y MONTIEL, *Sexting en adolescentes: nuevos retos médico- legales*, Revista española de medicina legal: órgano de la asociación nacional de médicos forenses, Vol. 43, núm. 1, 2017, pág. 43 y 44.

<sup>142</sup> MORALES PRATS, *El art. 197.7 y la alteración de los postulados de partida de la intervención penal en la tutela de la intimidad*, en: QUINTERO OLIVARES (Dir.), *Comentarios a la reforma penal de 2015*, 2015, pág. 460 - 465.

<sup>143</sup> Sobre ello véase, MORALES PRATS, *La proyectada reforma de los delitos contra la intimidad a propósito del "Caso Hormigos"*, Revista de derecho y proceso penal, núm. 31, 2013, pág. 11 – 13.

<sup>144</sup> Sobre ello véase, MENDO ESTRELLA, *Delitos de descubrimiento y revelación de secretos: acerca de su aplicación al sexting entre adultos*, Revista electrónica de ciencia penal y criminología, núm. 18, 2016, pág. 11 y 12.

lesión de la confidencialidad, a la que se obliga al receptor de la imagen. Este precedente legislativo está trayendo varios problemas interpretativos y prácticos en el país alemán.

Surge una gran problemática sobre este precepto, pues el art. 197.7 CP está alterando el reparto de funciones entre el Derecho Penal y el Derecho civil. Parte de la doctrina, como PUENTE ABA, considera que La LO de Protección Civil 1/1982 ya regula la intromisión ilegítima, la captación, reproducción o publicación de fotos o imágenes que afecten a la intimidad, siempre que no hubiese consentimiento. Y en el caso de que sí hubiese consentimiento estima que *“en estos casos no podemos hablar de la comisión de un delito contra la intimidad”*.<sup>145</sup>

Esto suscita el debate de los límites del consentimiento, donde no deben quedar ausentes las expectativas lógicas de intimidad y los niveles de autotutela del titular de las imágenes. En todo caso, MORALES PRATS cree que *“la vulneración de la confianza como abuso de conocimiento, es un problema jurídico privado donde no cabe el castigo penal”*. Considera que ello supone un peligro al tratarse de un concepto jurídico indeterminado y quedar al albedrío de prejuicios y concepciones subjetivas del juzgador.<sup>146</sup>

Por otro lado hay que mencionar que, lógicamente, el nuevo precepto también es defendido por quienes consideran que el envío consentido de imágenes puede suscitar a veces la revelación de éstas con un fin de venganza, sexista o discriminatorio. Así, COLAS TURÉGANO opina que *“parece oportuna la introducción de esta figura así como el supuesto cualificado basado en la vulnerabilidad del sujeto pasivo cuando los hechos afecten a personas con discapacidad o menores de edad”*.<sup>147</sup>

Sobre el alcance del art. 197.7 CP, cabe decir que no entra dentro del tipo penal una carta en la que se describe una relación afectuosa compartida y se divulga por el que la

---

<sup>145</sup> PUENTE ABA, *Difusión de imágenes ajenas en Internet: ¿ante qué delitos nos encontramos?*, en: GONZÁLEZ CUSSAC/ ORTS BERENGUER/ CARBONELL MATEU / CUERDA ARNAU (Coords.), *Constitución, derechos fundamentales y sistema penal. (Semblanzas y estudios con motivo del setenta aniversario del profesor Tomás Salvador Vives Antón)*, Vol. II, 2009, pág. 1541- 1548.

<sup>146</sup> Así lo considera MORALES PRATS, *El art. 197.7 y la alteración de los postulados de partida de la intervención penal en la tutela de la intimidad*, en: QUINTERO OLIVARES (Dir.), *Comentarios a la reforma penal de 2015*, 2015, pág. 463 – 465.

<sup>147</sup> COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/ MATA LLÍN EVANGELIO (Coords.), *Comentarios a la reforma penal de 2015*, 2ª edición, 2015, pág. 666.

recibe y participa en la relación amorosa. El hecho delictivo tiene que basarse en una grabación audiovisual o una imagen.<sup>148</sup>

Aun así, el tipo penal del art. 197.7 CP no sólo castiga la captación de imágenes no consentida de contenido sexual. También entran dentro del delito, las imágenes referidas a prácticas espirituales, o que contengan datos sensibles de una persona, como los referentes a sus creencias, salud, ideología, origen racial o religión.<sup>149</sup>

Respecto al bien jurídico que se protege en el art. 197.7 CP no sólo es la intimidad, también se protege la dignidad de la persona. Según ALEGRE MARTÍNEZ “*los destinatarios del deber genérico de respeto de los derechos de la persona, derivado de su dignidad, son los poderes públicos y todas las personas*”.<sup>150</sup>

A su vez, MENDO ESTRELLA, cree que los bienes jurídicos que se buscan garantizar en el art. 197.7 CP son el derecho al honor, a la intimidad personal y familiar y a la propia imagen (art. 18.1 CE).<sup>151</sup>

No todas las conductas de sexting se castigan en el CP. Hay algunas que no suponen un delito de descubrimiento y revelación de secretos al haber consentimiento de la víctima. Lo que sí castiga el CP es el caso de que A y B graben un vídeo con el consentimiento de ambos, pero luego B difunda ese vídeo a C, sin consentimiento de A, y se reenvíe a su vez a terceros por C.<sup>152</sup>

En conclusión, el caso Hormigos serviría para comenzar a legislar sobre esta modalidad delictiva, pasando a regularse en el CP el supuesto de la edil. De esta forma, lo que se expresa en el auto dictado por el Juzgado de Primera Instancia de Orgaz, el 15 de marzo de 2013, declarando que: “*la plena voluntariedad y consentimiento de la denunciante en el envío del citado vídeo a través de su teléfono móvil al imputado, quiebra desde el inicio la posible subsunción de los hechos denunciados en un delito contra la intimidad,*

---

<sup>148</sup> A tal efecto véase, MUÑOZ CONDE, *Derecho Penal Parte Especial*. 20ª edición, 2015, pág. 238-240.

<sup>149</sup> Sobre ello véase, COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/ MATALLÍN EVANGELIO (Coords.), *Comentarios a la reforma penal de 2015*, 2ª edición, 2015, pág. 670.

<sup>150</sup> ALEGRE MARTÍNEZ, *La dignidad de la persona como fundamento del ordenamiento constitucional español*, 1996, pág. 133.

<sup>151</sup> MENDO ESTRELLA, *Delitos de descubrimiento y revelación de secretos: acerca de su aplicación al sexting entre adultos*, *Revista electrónica de ciencia penal y criminología*, núm. 18, 2016, pág. 6.

<sup>152</sup> Sobre ello véase, MENDO ESTRELLA, *Delitos de descubrimiento y revelación de secretos: acerca de su aplicación al sexting entre adultos*, *Revista electrónica de ciencia penal y criminología*, núm. 18, 2016, pág. 19 – 21.

y en relación a la redifusión realizada por la tercera persona mencionada, y también acusada, concluye la resolución judicial que no cabe achacar un reproche penal por la conducta realizada”, ya no es válido. Actualmente, sí es punible ese supuesto aunque haya consentimiento en la obtención de la imagen o el vídeo. Ello es así porque lo que el legislador pretende castigar, es la difusión, revelación o cesión a terceros de dicha imagen o vídeo, que es en la que no hay consentimiento de la víctima.

Por otro lado, no vale cualquier lugar para que se cometa el delito. Con la reforma de la LO 1/2015, de 30 de marzo, el lugar en el que tiene que haberse captado la imagen o grabado un vídeo, debe ser un domicilio o cualquier otro sitio fuera del alcance de terceros.<sup>153</sup>

Este hecho restringe el ámbito de aplicación del art. 197.7 CP. No está claro si el contenido del injusto, se basa en la violación del derecho a controlar las imágenes íntimas de cada persona, o en la defraudación de la confianza (vulneración de un compromiso expreso o tácito de reserva).

La defraudación de la confianza respeta más el principio de proporcionalidad y es más restrictiva. La primera opción, en cambio, tiende a justificar la restricción general de la libertad y el peligro de condenar a inocentes por cualquier prohibición penal.

La pena del art. 197.7 CP se agrava en su mitad superior, en su segundo párrafo.

Los supuestos en los que se agrava se dan cuando el autor del hecho delictivo es el cónyuge o persona unida, o que lo haya estado, por análoga relación de afectividad, aun sin convivencia (art. 197.7. 2º CP).<sup>154</sup>

También se impondrá la pena del art. 197.7 CP en su mitad superior, cuando el sujeto pasivo del delito sea un menor de edad o discapacitado necesitado de especial protección, o se hubiese captado imagen con ánimo de lucro (art. 197.7. 2º CP).<sup>155</sup>

---

<sup>153</sup> Sobre ello véase, MENDO ESTRELLA, *Delitos de descubrimiento y revelación de secretos: acerca de su aplicación al sexting entre adultos*, Revista electrónica de ciencia penal y criminología, núm. 18, 2016, pág. 21 y 22.

<sup>154</sup> Sobre ello véase, COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/ MATALLÍN EVANGELIO (Coords.), Comentarios a la reforma penal de 2015, 2ª edición, 2015, pág. 670 y 671.

<sup>155</sup> A tal efecto véase, CASTIÑEIRA PALOU/ ESTRADA i CUADRAS, *Delitos contra la intimidad*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), Lecciones de Derecho Penal, Parte especial, 4ª edición, 2015, pág. 162-163.



Debido a la tipificación de estas dos agravaciones, no puede interpretarse que el art. 197.7 CP se reserve sólo para los casos en los que hubiese una relación de afectividad o análoga que generase una relación de confianza y quedase defraudada con la divulgación de las imágenes. El primer apartado de este tipo penal no está reservado para estos hechos, sino que se agrava en el apartado segundo.

Con lo cual, el tipo penal no se refiere sólo a personas ligadas por una intensa relación de confianza, ni tampoco a los casos en los que la víctima es un menor o un discapacitado necesitado de especial protección.

### **3.6. Intromisión informática (art. 197 bis y 197 ter CP)**

Se regula esta figura delictiva en los arts. 197 *bis*<sup>156</sup> y 197 *ter* CP, el cual explicaré en el presente punto.

A través de estos artículos, el legislador español obedece las exigencias impuestas por la normativa europea sobre la cibercriminalidad y cumple los mandatos de incriminación de los arts. 3,6 y 7 de la Directiva 2013/40/UE, relativa a los ataques contra los sistemas de información.

Ya se había intentado anteriormente regular la cibercriminalidad en la UE en el Convenio Europeo 185, de 23 de noviembre de 2001 (Convenio de Budapest), pero sólo se había llegado a garantizar la retención de los datos de tráfico de comunicaciones electrónicas que surgiesen tras la emisión de una concreta orden de retención. Esto se debió a la oposición de varios Estados pertenecientes al Consejo de Europa y a la presión de los grandes prestadores de servicios de la Red.

Lo que se pretendía en dicho Convenio era establecer una cláusula de conservación de datos relativos a comunicaciones electrónicas, previa a cualquier orden de interceptación o cesión de estos datos.<sup>157</sup>

---

<sup>156</sup> Establece el art. 197 *bis* CP: “1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años. 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”.

<sup>157</sup> A tal efecto véase, RODRÍGUEZ LAINZ, El secreto de las telecomunicaciones y su interceptación legal, 2016, pág. 288 y 289.

Finalmente, se pudo controlar de forma más precisa la cibercriminalidad con la Directiva 2013/40/UE, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, y a la interceptación de datos electrónicos cuando no se trata de una comunicación personal. Conforme a la citada Directiva, se introdujo el delito de intrusismo informático, consistente en las conductas delictivas relacionadas con el espionaje y sabotaje informático. Conforme al criterio de JAÉN VALLEJO Y PERRINO PÉREZ, tras la reforma de la LO 1/2015, de 30 de marzo, el intrusismo informático se regula ahora en los arts. 197 ter, 197 bis, 197 quáter y 197 quinquies CP.<sup>158</sup>

No obstante, el CP ya preveía la incriminación de interceptaciones mediante artificios o instrumentos técnicos, cualquiera que fuese la señal de comunicación y con independencia de su naturaleza, en el art. 197. 1 CP. La pena prevista en este caso era de uno a cuatro años de prisión y multa de doce a veinticuatro meses. El Legislador establece ahora una pena inferior a esa para esta conducta, cifrándose la pena de prisión de tres meses a dos años y multa de tres a doce meses. Es por esto que se considera que el art. 197. 1 CP ya no castiga la interceptación de comunicaciones de datos informáticos. Es el art. 197 bis CP donde se castiga ahora esa conducta tras la reforma, pasando a constituir un delito de menor gravedad.

Como vemos, el legislador de 2015 incrimina la interceptación de transmisiones de datos no públicos, con una pena bastante inferior a la del art. 197.1 CP. De esta forma, no quedan claros, según MORALES PRATS, “*los designios político-criminales del art. 197 bis CP*”.<sup>159</sup>

En la Exposición de Motivos de la LO 1/2015, de 30 de marzo<sup>160</sup>, el legislador intenta justificar la introducción de los arts. 197 bis y 197 ter CP. De esta forma, nos dice que con este precepto se opta por separar los delitos relativos al descubrimiento o revelación

---

<sup>158</sup> JAÉN VALLEJO / PERRINO PÉREZ, *Delitos informáticos*, en: JAÉN VALLEJO / PERRINO PÉREZ (Dir.), *La reforma penal de 2015*, 2015, pág. 101.

<sup>159</sup> MORALES PRATS, *El nuevo art. 197 bis y el nuevo art. 197 ter CP*, en: QUINTERO OLIVARES (Dir.), *Comentarios a la reforma penal de 2015*, 2015, pág. 465- 466.

<sup>160</sup> La Exposición de Motivos de la LO 1/2015 establece: “*De acuerdo con el planteamiento recogido en la Directiva, se introduce una separación nítida entre los supuestos de revelación de datos que afectan directamente a la intimidad personal, y el acceso a otros datos o informaciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal: no es lo mismo el acceso al listado personal de contactos, que recabar datos relativos a la versión de software empleado o a la situación de los puertos de entrada a un sistema. Por ello, se opta por una tipificación separada y diferenciada del mero acceso a los sistemas informáticos*”.

de datos, que afectan de forma directa a la intimidad personal y el acceso a datos o informaciones, que afectan a la privacidad pero no a la intimidad personal.<sup>161</sup>

*“No es de extrañar, según JAÉN VALLEJO Y PERRINO PÉREZ, la especial preocupación que muestra el legislador con la extensa regulación de todas estas hipótesis de ataques contra los sistemas de información, introduciendo nuevas conductas delictivas y reforzando la protección con el aumento considerable de penas, en la necesidad de garantizar la necesaria confianza de la sociedad en la seguridad de los sistemas informáticos”.*<sup>162</sup>

Respecto a la estructura del art. 197 bis CP, dicho precepto se divide en dos apartados. En el apartado primero (art. 197 bis. 1 CP), se regula el acceso o mantenimiento ilegítimo de un sistema de información. A este hecho se le conoce como *hacking*<sup>163</sup>. Este primer apartado sigue manteniendo el tipo penal que introdujo la reforma de 2010.

Lo que modifica aquí la reforma de 2015, en opinión de COLÁS TURÉGANO, es la *“ampliación de la regulación de 2010, incorporando las nuevas exigencias derivadas de la Directiva”*<sup>164</sup>.

Por otra parte, destaca la creación de una alternativa típica al acceso, sin consentimiento, de los sistemas informáticos que aluden a facilitar al autor del delito el acceso a otros datos informáticos.

El segundo apartado del art. 197 bis CP ha partido de cero tras la reforma. Introduce el delito consistente en la utilización de artificios o instrumentos técnicos sin autorización legal, con la verificación de interceptación de transmisiones privadas de datos informáticos que se elaboren desde un sistema de información. En conclusión, el art. 197 bis, segundo apartado CP tipifica la interceptación ilegítima de la transmisión no

---

<sup>161</sup> Sobre ello véase, COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/ MATALLÍN EVANGELIO (Coords.), *Comentarios a la reforma penal de 2015*, 2ª edición, 2015, pág. 677; CASTELLÓ NICÁS, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor*, en: MORILLAS CUEVA (Dir.), *Estudios sobre el Código Penal reformado*, 2015, pág. 505.

<sup>162</sup> JAÉN VALLEJO / PERRINO PÉREZ, *Delitos informáticos*, en: JAÉN VALLEJO / PERRINO PÉREZ (Dir.), *La reforma penal de 2015*, 2015, pág. 106.

<sup>163</sup> Sobre ello véase, SÁNCHEZ RUBIO, *Ciberseguridad y hacking ético*, *Revista Auditoría interna: publicación periódica del Instituto de auditores internos de España*, año 32, núm. 111, 2016, pág. 36 y 37; LÓPEZ VALLEJO, *Hacking ético. Vulnerabilidad de sistemas operativos en el acceso por contraseñas*, *Revista Publicando*, Vol.4, núm. 10, 2017, pág. 31-51.

<sup>164</sup> COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/ MATALLÍN EVANGELIO (Coords.), *Comentarios a la reforma penal de 2015*, 2ª edición, 2015, pág. 674.

pública de un dato informático. Por ello, como bien dicen JAÉN VALLEJO / PERRINO PÉREZ *“será objeto de persecución penal no sólo la interceptación de comunicaciones personales, que ya estaban previstas en el Código, sino también aquellas interceptaciones que se produzcan entre sistemas o equipos”*.<sup>165</sup>

Los fines político-criminales que se castigan mediante estos delitos se explican en los considerandos de la Directiva europea. Se basan en la preocupación por la posibilidad de ataques terroristas o de naturaleza política contra los sistemas de los países comunitarios y de la UE.<sup>166</sup>

El motivo de querer castigar estos hechos del legislador europeo y la ubicación que le ha proporcionado el legislador español, entre los delitos contra la intimidad personal y familiar, suscitan confusión sobre cuál es el verdadero bien jurídico protegido por la norma.

Mientras que algunos, como CASTELLÓ NICÁS<sup>167</sup>, consideran que el bien jurídico protegido es *“la seguridad en el medio informático y la confidencialidad de la información protegida que en él se contiene o que por él se transmite”*, otros como COLÁS TURÉGANO<sup>168</sup>, creen que *“se produce un adelantamiento en la protección del bien jurídico intimidad que se puede ver potencialmente afectado con la realización de las conductas descritas, estableciendo un paralelismo con el delito de allanamiento de morada respecto al que hay una coincidencia en las conductas (entrar y mantenerse) por lo que se afirmaba que en este caso se tutela aquella parcela de la privacidad ligada al domicilio informático”*.

Esto hace que sólo se considere a estas figuras como delitos de peligro, cuando el sistema de información al que se acceda o las transmisiones interceptadas, contengan

---

<sup>165</sup> JAÉN VALLEJO / PERRINO PÉREZ, *Delitos informáticos*, en: JAÉN VALLEJO / PERRINO PÉREZ (Dir.), *La reforma penal de 2015*, 2015, pág. 103.

<sup>166</sup> El Cdo. 3 de la Directiva 2013/40/UE establece que: *“Los ataques contra los sistemas de información y, en particular, los ataques vinculados a la delincuencia organizada, son una amenaza creciente en la Unión y en el resto del mundo, y cada vez preocupa más la posibilidad de ataques terroristas o de naturaleza política contra los sistemas de información que forman parte de las infraestructuras críticas de los Estados miembros y de la Unión. Esta situación pone en peligro la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia y exige, por tanto, una respuesta por parte de la Unión, así como una cooperación y coordinación reforzadas a escala internacional”*.

<sup>167</sup> CASTELLÓ NICÁS, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor*, en: MORILLAS CUEVA (Dir.), *Estudios sobre el Código Penal reformado*, 2015, pág. 505.

<sup>168</sup> COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir) / GÓRRIZ ARROYO/ MATALLÍN EVANGELIO (Coords.), *Comentarios a la reforma penal de 2015*, 2ª edición, 2015, pág. 671- 673.

datos sobre la vida privada de las personas. No es necesario que se llegue a acceder a esos datos.

Desde que la reforma del Código Penal de 2010 incluyó el delito de intromisión informática (*hacking*), se ha castigado por este tipo penal conductas como por ejemplo, un hombre que accedió en la cuenta de Facebook de otra persona, señalándose que no guarda relación lo que se está castigando por este delito, con el ataque a “*infraestructuras críticas para la salud, la seguridad o la estabilidad económica de la Unión Europea o de alguno de sus Estados miembros*”.<sup>169</sup>

Esto hace que, si se considera que el bien jurídico protegido es la intimidad, no sería punible penalmente el acceso a un sistema informático de una central nuclear que permita manipular funciones peligrosas, por ejemplo.

Otra opción interpretativa, según COLÁS TURÉGANO, es que el bien jurídico protegido por el delito de intromisión informática es *la seguridad de los sistemas informáticos*.<sup>170</sup> Esta interpretación sirve para proteger la intimidad y bienes jurídicos de diversa naturaleza, como por ejemplo el patrimonio.

En ese sentido, la AP de Vizcaya apoya esa interpretación afirmando que el delito de intromisión informática “*protege la libertad informática o más exactamente el domicilio informático de una persona, no siendo relevante la naturaleza de los datos contenidos en sistema informático*”.<sup>171</sup>

Respecto al mantenimiento ilegítimo en un sistema de información (primer apartado del art. 197 bis CP), se presupone que el titular del sistema puede revocar en cualquier momento el acceso autorizado. Esto se debe a que el “domicilio informático” es un ámbito de reserva delimitado por la propia víctima.<sup>172</sup>

Es típica esta conducta si se ha hecho a través de la vulneración de medidas de seguridad para impedir el acceso o el mantenimiento en el sistema de información.

---

<sup>169</sup> Véase la SAP- Álava núm. 74/2013, de 7 de marzo.

<sup>170</sup> COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/ MATA LLÍN EVANGELIO (Coords.), *Comentarios a la reforma penal de 2015*, 2ª edición, 2015, pág. 676 y 677.

<sup>171</sup> Véase la sentencia: SAP- Vizcaya núm. 90307/2014, de 23 de julio.

<sup>172</sup> Sobre ello véase, CASTELLÓ NICÁS, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor*, en: MORILLAS CUEVA (Dir.), *Estudios sobre el Código Penal reformado*, 2015, pág. 506 y 507.

Acceder a un sistema de información con una contraseña obtenida mediante engaño (*phising*)<sup>173</sup>, es en opinión de JAÉN VALLEJO / PERRINO PÉREZ, otro medio vulnerador de las medidas de seguridad para evitar el acceso no autorizado.<sup>174</sup> No obstante, no se considera como tal si el engaño no es similar al delito de estafa (art. 248.2 CP).

El objeto material en la intromisión informática según la Directiva 2013/40/UE, tiene que ser un sistema de información.

Por otra parte, el segundo apartado del art. 197 bis CP tipifica la interceptación de transmisiones no públicas de datos informáticos. Desde el punto de vista de CASTELLÓ NICÁS, “*el apartado segundo del art. 197 bis CP castiga el acceso no autorizado en el medio informático, no para interceptar la voz o la imagen (art. 197. 1 CP), sino las transmisiones de datos informáticos que no sean públicas, o sea, privadas*”.<sup>175</sup>

Si por el contrario, se considera que el objeto de transmisión del art. 197 bis 2. CP es la información referida a funciones esenciales de infraestructuras críticas y no a los datos sobre la intimidad personal, sí se entiende, según COLÁS TURÉGANO, la diferencia de gravedad de las penas respecto al tipo básico del art. 197.1 CP.<sup>176</sup>

El objeto material de la interceptación de transmisiones no públicas de datos informáticos (art. 197 bis 2. CP) son los datos en proceso de transmisión, por cable o mediante ondas electromagnéticas, como: *wifi*, ondas de radio, microondas, rayos X etc.<sup>177</sup>

Si el hecho delictivo provoca un daño en el sistema en el que se accede, como introducir un virus, puede darse un concurso con el delito de daños a material informático del art.

---

<sup>173</sup> Sobre ello véase, REY HUIDOBRO, *La estafa informática. Relevancia penal del phising y el pharming*, La ley penal: Revista de derecho penal, procesal y penitenciario, núm. 101, 2013, pág. 2.

<sup>174</sup> JAÉN VALLEJO / PERRINO PÉREZ, *Delitos informáticos*, en JAÉN VALLEJO / PERRINO PÉREZ (Dir.), La reforma penal de 2015, 2015, pág. 100 y 101.

<sup>175</sup> CASTELLÓ NICÁS, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor*, en: MORILLAS CUEVA (Dir.), Estudios sobre el Código Penal reformado, 2015, pág. 507 y 508.

<sup>176</sup> COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/ MATALLÍN EVANGELIO (Coords.), Comentarios a la reforma penal de 2015, 2ª edición, 2015, pág. 678 y 679.

<sup>177</sup> Sobre ello véase, CASTELLÓ NICÁS, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor*, en: MORILLAS CUEVA (Dir.), Estudios sobre el Código Penal reformado, 2015, Pág. 508.

264 CP.<sup>178</sup> Si, por otro lado, el acceso a los datos se hace para cometer alguna clase de fraude, el concurso es ideal medial.<sup>179</sup>

Los datos informáticos que se quieren transmitir no pueden estar disponibles para el público. La conducta no sería típica si los datos informáticos estuviesen al alcance de todo el mundo, tienen que transmitirse en condiciones que excluyan el libre acceso de terceros.

Este requisito hace que sólo se dé la conducta típica cuando se usen artificios técnicos, que vulneren barreras de protección de cierta gravedad. Por ejemplo, que el delito se cometa con instrumentos sofisticados o convencionales, pero usados de manera no convencional.

Esto permite valorar de forma coherente el art. 197 bis 2. CP con las modalidades del primer apartado, donde la vulneración de medidas de seguridad es exigencia explícita del tipo penal.<sup>180</sup>

### **3.7. Manejo de instrumentos idóneos con el fin del espionaje informático (Art. 197 ter CP)**

En el art. 197 ter CP<sup>181</sup> se castigan los actos preparatorios de los delitos de descubrimiento de secretos de la intimidad e intrusismo informático de los arts. 197. 1 y 197.2 y 197 bis CP.

El art. 197 ter CP surge de la reforma de la LO 1/2015, de 30 de marzo, castigando a quienes ayuden o participen en la comisión del delito. Con dicha reforma se comienza, en opinión de JAÉN VALLEJO Y PERRINO PÉREZ, *“a considerar delictiva tanto la producción como la adquisición para su uso, importe o facilitación a terceros, de programas informáticos concedidos o adaptados para cometer delitos informáticos, y*

---

<sup>178</sup> Sobre ello véase, JAÉN VALLEJO / PERRINO PÉREZ, *Delitos informáticos*, en: JAÉN VALLEJO / PERRINO PÉREZ (Dir.), *La reforma penal de 2015*, 2015, pág. 104 – 106.

<sup>179</sup> A tal efecto véase, MUÑOZ CONDE, *Derecho Penal Parte Especial*, 2015, 20ª edición, pág. 240- 241.

<sup>180</sup> A tal efecto véase, CASTIÑEIRA PALOU/ ESTRADA i CUADRAS, *Delitos contra la intimidad*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 163-166.

<sup>181</sup> El art. 197 ter CP establece que: *“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; ob) 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”*.

*también proporcionar contraseñas de ordenador o códigos de acceso que permitan acceder a todo o parte de un sistema de información”*.<sup>182</sup>

El legislador introduce esta nueva modalidad delictiva consistente en la producción, adquisición para su uso, importación o facilitación a terceros de programas informáticos o contraseñas de ordenador, que el autor de estas conductas aplica con la intención de facilitar la comisión de los delitos de los arts. 197.1, 197.2 y 197 bis CP.

La creación de este nuevo art. supone, según COLÁS TURÉGANO, “*un adelantamiento de la línea de defensa de los bienes jurídicos implicados, intimidad y seguridad de los sistemas informáticos*”.<sup>183</sup>

No obstante, el art. 197 ter CP también acarrea ciertos problemas de delimitación respecto a la facilitación del acceso ilegal a terceros del art. 197 bis CP, “*produciéndose un inadecuado solapamiento de ambas figuras*”.<sup>184</sup>

Por otra parte, sorprende ciertamente en opinión de CASTELLÓ NICÁS, “*la reiterativa redacción legal del precepto: facilite a terceros, con la intención de facilitar*”.<sup>185</sup>

Aun así, no se introduce ningún requisito típico nuevo respecto a las contraseñas de ordenador o los códigos de acceso. Lo que sí añade la LO 1/2015 es el elemento subjetivo de intención específica. Este elemento subjetivo se basa en la finalidad de cometer algún delito básico contra la intimidad para que la acción sea punible penalmente. El art. 197 ter CP se trata por lo tanto, de un delito doloso.<sup>186</sup>

---

<sup>182</sup> JAÉN VALLEJO / PERRINO PÉREZ, *Delitos informáticos*, en: JAÉN VALLEJO / PERRINO PÉREZ (Dir.), *La reforma penal de 2015*, 2015, pág. 103.

<sup>183</sup> COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/ MATALLÍN EVANGELIO (Coords.), *Comentarios a la reforma penal de 2015*, 2ª edición, 2015, pág. 680.

<sup>184</sup> COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/ MATALLÍN EVANGELIO (Coords.), *Comentarios a la reforma penal de 2015*, 2ª edición, 2015, pág. 680.

<sup>185</sup> CASTELLÓ NICÁS, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor*, en: MORILLAS CUEVA (Dir.), *Estudios sobre el Código Penal reformado*, 2015, pág. 508.

<sup>186</sup> Sobre ello véase, COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/ MATALLÍN EVANGELIO (Coords.), *Comentarios a la reforma penal de 2015*, 2ª edición, 2015, pág. 680.



Por ese hecho el precepto genera, según MORALES PRATS: “*Una inseguridad interpretativa desde el principio de lesividad*”.<sup>187</sup>

Por otro lado, es complicado interpretar cuáles son los programas informáticos que están concebidos o adaptados para cometer el delito contra la intimidad del art. 197 ter CP y cuáles no, ya que no queda clara la delimitación del concepto.

Respecto a los objetos materiales del delito son: a) las claves de acceso a un sistema de información o datos semejantes, que permitan acceder a la totalidad o parte de un sistema de información ; y b) los programas informáticos concebidos para cometer el descubrimiento de secretos o el intrusismo informático de los artículos antes mencionados.<sup>188</sup>

Aunque el programa informático permita ser utilizado con un fin legítimo, su uso debe ser para cometer delitos de espionaje. Los manuales de instrucciones o los mensajes publicitarios de esos programas, pueden servir como criterio objetivo para señalar su principal utilización.

La adquisición, producción, importación o facilitación de las claves de acceso o del programa informático, debe tener como fin cometer el delito de descubrimiento (art. 197. 1 y 2 CP) o el intrusismo informático (art. 197 bis CP).<sup>189</sup>

No se castiga la simple posesión de ese programa o clave de acceso. Tiene que haber un plan delictivo cierto con sus elementos esenciales (autor, objeto material y víctima). Tiene que demostrarse, en opinión de COLÁS TURÉGANO, “*que la facilitación de tales instrumentos está intencionalmente orientada a la actividad delictiva en concreto*”.<sup>190</sup>

---

<sup>187</sup> MORALES PRATS, *El nuevo art. 197 ter CP*, en: QUINTERO OLIVARES (Dir.), *Comentarios a la reforma penal de 2015*, 2015, pág. 467.

<sup>188</sup> A tal efecto véase, MUÑOZ CONDE, *Derecho Penal Parte Especial*, 2015, 20ª edición, pág. 241-242.

<sup>189</sup> Sobre ello véase, CASTELLÓ NICÁS, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor*, en: MORILLAS CUEVA (Dir.), *Estudios sobre el Código Penal reformado*, 2015, pág. 508 y 509.

<sup>190</sup> COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/ MATALLÍN EVANGELIO (Coords.), *Comentarios a la reforma penal de 2015*, 2ª edición, 2015, pág. 680.

Es cuestionable que la mera obtención de claves de acceso mediante engaño (*phising*), se subsuma en el art. 197 ter CP. Esa obtención de la clave debe facilitarse a terceros con un fin delictivo, si no la conducta es atípica.

Por ese motivo, se excluye del elemento subjetivo especial las conductas con carácter informativo u orientadas a prestar un servicio de auditoría de la seguridad de un sistema de información.<sup>191</sup>

Esta exclusión del elemento subjetivo sobre los servicios de auditoría de la seguridad y las conductas orientadas a un fin informativo, hacen que sea legal el espionaje informático que realizan los Cuerpos y Fuerzas de Seguridad del Estado mediante el sistema de interceptación de telecomunicaciones (SITEL). Este sistema se basa en las técnicas de investigación en soportes digitales, posibilitados por innovadores instrumentos de acceso inmediato, a datos de tráfico y geolocalización para enfrentarse a la delincuencia organizada.<sup>192</sup>

El SITEL es una forma legal de búsqueda o averiguación de delitos y delincuentes. La jurisprudencia del TS se ha encargado de definir fehacientemente este sistema, declarando que se trata de: *“Un método avanzado, y extremadamente invasivo de la intimidad, razón por la cual se considera que la petición policial debía explicar, aunque sea someramente, cuáles eran los objetivos que se pretendía alcanzar y las consecuencias de la puesta en marcha del sistema; contexto en que en cada caso el Juez de Instrucción debía valorar y razonar su decisión. El principio de proporcionalidad, por tanto, abarcará también a aquellos aspectos que van más allá de la simple escucha; en concreto, a datos de tráfico y, especialmente, de geolocalización”*.<sup>193</sup>

La creación de SITEL se debe a las exigencias reglamentarias para controlar la seguridad, ordenado por el RD 1720/2007, de 21 de diciembre. El desarrollo del citado RD 1720/2007 por la Ley de Protección de Datos (RLOPDCP), asegura en opinión de

---

<sup>191</sup> A tal efecto véase, CASTIÑEIRA PALOU/ ESTRADA i CUADRAS, *Delitos contra la intimidad*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 166.

<sup>192</sup> Sobre ello véase, RODRÍGUEZ LAINZ, *SITEL. Nuevas tendencias, nuevos retos*, Diario la Ley. núm. 8082, 2013; RUÍZ DORADO / VIDAL MARÍN, *Análisis de la constitucionalidad del SITEL. Breves consideraciones a partir de la LO 13/2015, de reforma de la Ley de Enjuiciamiento Criminal*, Revista Aranzadi Doctrinal, núm. 9, 2016, pág. 135-162.

<sup>193</sup> Véase a tal efecto, las STS núm. 209/2013, de 6 de marzo; STS núm. 794/2012, de 11 de octubre y la STS núm. 478/2012, de 29 de mayo.

RODRIGUEZ LAINZ, *“un riguroso y eficaz control de los accesos a la información almacenada en los sistemas informáticos”*.<sup>194</sup>

Su funcionamiento se regula en el art. 33 de la Ley General de Telecomunicaciones. La AEPD consiguió asegurar, según RODRÍGUEZ LAINZ, el respeto al principio de legalidad que garantiza SITEL en su funcionamiento a través de un informe de oficio, realizado el 19 de enero de 2010. Este informe pudo justificar las posibles vulneraciones que se hicieron y se hacen al derecho a la intimidad, enseñando en dicho informe el protocolo de seguridad de las bases de datos que lleva a cabo este sistema, la valoración concreta que emplea de las medidas de seguridad y, las garantías de autenticidad y evitación de riesgos de manipulación o accesos ilícitos de datos.<sup>195</sup>

El funcionamiento de SITEL se aclara en la STS núm. 419/2009, de 5 de noviembre: *“Las operadoras de comunicaciones (centros de interceptación), tras recibir la orden, generalmente por mediación de un enlace, el llamado coordinador de centros de recepción, reenvían por un canal seguro la información objeto de interceptación a un servidor central dependiente de la Guardia Civil o de la Policía Nacional (centro de recepción), donde la información va almacenándose en carpetas que se van abriendo por expediente, a las que solamente tendrán acceso los llamados agentes facultados; y que, entre otras medidas de seguridad, contarán con la imposibilidad de modificación de la información a nivel del llamado centro de recepción, y un riguroso registro y control de accesos”*.

### **3.8. Responsabilidad penal de las personas jurídicas (Art. 197 quinquies CP)**

La Directiva 2013/42/UE, de 3 de abril, sobre el embargo y el decomiso de los instrumentos y del producto del delito en la UE, fue el origen, en opinión de JAÉN VALLEJO / PERRINO PÉREZ, de la imposición de sanciones efectivas, proporcionadas y disuasorias a las personas jurídicas.<sup>196</sup> Así, el art. 110 de la LO 1/2015, de 30 de marzo, añade al CP este artículo.

---

<sup>194</sup> RODRÍGUEZ LAINZ, *El secreto de las telecomunicaciones y su interceptación legal*, 2016, pág. 238.

<sup>195</sup> RODRÍGUEZ LAINZ, *El secreto de las telecomunicaciones y su interceptación legal*, 2016, pág. 237-239.

<sup>196</sup> JAÉN VALLEJO / PERRINO PÉREZ, *Delitos informáticos*, en: JAÉN VALLEJO / PERRINO PÉREZ (Dirs.), *La reforma penal de 2015*, 2015, pág. 62 y 63.

No obstante, la responsabilidad penal de las personas jurídicas ya se contemplaba en la reforma del CP, de 22 de junio de 2010, sobre los tipos básicos del art. 197. 1, 197.2 y 197.3 CP.<sup>197</sup>

Al haberse reestructurado el art. 197 CP con la reforma de 2015, se hizo posible una cláusula de responsabilidad penal de las personas jurídicas para las conductas de los arts. 197 bis y 197 ter CP.<sup>198</sup>

Tras la reforma se equiparan penalmente las personas jurídicas a las físicas, para ser también castigadas por todas las modalidades típicas, tanto las básicas como las agravadas, en los delitos contra la intimidad. No obstante, el precepto no introduce cambios respecto lo previsto en la reforma penal de 2010.

Así, COLÁS TURÉGANO, considera que la reforma de 2015 “*no supone ninguna variación respecto a la regulación anterior, más allá de la derivada de la introducción de nuevas figuras delictivas en el ámbito de los delitos contra la intimidad y la seguridad de los sistemas informáticos, a los que también les será de aplicación la cláusula de responsabilidad penal de los entes societarios*”.<sup>199</sup>

El legislador español obliga a sancionar penalmente a las personas jurídicas cuando se den los requisitos del art. 31 bis CP<sup>200</sup>, como: que una empresa cometa un delito de descubrimiento o revelación de secretos (art. 197 CP), un delito de intromisión informática (art. 197 bis CP) o un delito de manejo de instrumentos idóneos para el espionaje informático (art. 197 ter CP).

---

<sup>197</sup> Sobre ello véase, JAÉN VALLEJO / PERRINO PÉREZ, *Delitos informáticos*, en: JAÉN VALLEJO / PERRINO PÉREZ (Dir.), *La reforma penal de 2015*, 2015, pág. 48 y 49.

<sup>198</sup> Sobre ello véase, CASTELLÓ NICÁS, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor*, en: MORILLAS CUEVA (Dir.), *Estudios sobre el Código Penal reformado*, 2015, pág. 510.

<sup>199</sup> COLÁS TURÉGANO, *Nuevas conductas delictivas contra la intimidad*, en: GONZÁLEZ CUSSAC (Dir.) / GÓRRIZ ARROYO/ MATALLÍN EVANGELIO (Coords.), *Comentarios a la reforma penal de 2015*, 2ª edición, 2015, pág. 681.

<sup>200</sup> El art. 31 bis CP establece: “*1. En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables: a) De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma. b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso*”.

Para que se les pueda imponer otro tipo de penas privativas de derechos (art. 33.7 CP), los tribunales deben atender las reglas establecidas en el art. 66 bis del CP.<sup>201</sup>

Finalmente, también cabe decir que al castigarse en el art. 264 ter b) CP “a quien 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 dos arts. anteriores: b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o una parte de un sistema de información”, se crea la problemática de saber si aplicar o no el art. 197 quinquies CP o el art. 264 ter b) CP. En opinión de CASTELLÓ NICÁS, “la disyuntiva habrá de resolverse sobre la base de la finalidad principal de quien obtenga dicha contraseña o código de acceso, que será para causar daños, y no para la comisión de un delito contra la intimidad”.<sup>202</sup>

La sanción penal tipificada en los delitos contra la intimidad, consiste en una multa de seis meses a dos años tipificada en el art. 197 quinquies CP<sup>203</sup>.

### **3.9. Revelación de secretos laborales o profesionales (Art. 199 CP)**

El art. 199 CP<sup>204</sup> contenía una segunda vertiente de tipos penales en el que podía ser también constitutivo de delito el acceso legítimo a la intimidad ajena. Así, se tipificaba la conducta delictiva basada en la revelación o divulgación de algo que se había conocido lícitamente.

El tipo penal se refería a profesiones que requerían un confidente necesario en el ámbito de prestación de servicios sensibles, como abogado, psiquiatra, médico etc.

---

<sup>201</sup> A tal efecto véase, MORALES PRATS, *La responsabilidad penal de las personas jurídicas prevista en el art. 197 quinquies CP*, en: QUINTERO OLIVARES (Dir.), *Comentarios a la reforma penal de 2015*, 2015, pág. 467.

<sup>202</sup> CASTELLÓ NICÁS, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor*, en: MORILLAS CUEVA (Dir.), *Estudios sobre el Código Penal reformado*, 2015, pág. 510.

<sup>203</sup> El art. 197 quinquies CP establece que: “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”.

<sup>204</sup> El art. 199 CP establece que: “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”.

Ya añadía el Código Penal de 1995 de forma poco precisa, la incriminación de la revelación de secretos personales ajenos, conocidos de forma lícita mediante una relación laboral.

Así las cosas, la reforma de 2015 ha cambiado ese sistema de incriminación del art. 199 CP en relación a los términos del delito. Ahora, le es aplicable al art. 199 CP el tipo penal agravado por cometerse un delito en el seno de una organización criminal (art. 197 quáter CP), mientras que antes eso no era posible.

Al contrario que en los otros tipos penales, donde el autor del delito accede ilícitamente al secreto, en este tipo penal el sujeto activo conoce el secreto, como bien dice TOMÁS-VALIENTE LANUZA, de forma lícita. Lo que se castiga en este artículo es que revele dicho secreto.<sup>205</sup>

El art. 199 CP incluye dos modalidades delictivas. La primera se basa en revelar secretos de los que se tenga conocimiento por razón del oficio o de las relaciones laborales, es decir, secretos ajenos.

Aquí se plantea la cuestión de qué se entiende por oficio o relación laboral y a quién afecta la obligación de guardar el secreto.

Por como describe el tipo penal el art. 199 CP, CASTIÑEIRA PALOU / ESTRADA I CUADRAS, consideran que el tipo también engloba las relaciones laborales y mercantiles, siempre que impliquen una prestación de servicios.<sup>206</sup>

Esas relaciones tendrán que hacer que se conozca la vida privada de una de las partes contractuales, dadas las particularidades del delito. Ello supone, según TOMÁS-VALIENTE LANUZA, “*que los datos íntimos cuya revelación dará origen al delito no tienen necesariamente que referirse a aquel con el que se mantiene la relación laboral o profesional*”.<sup>207</sup> Por ejemplo, se castigaría a través del art. 199. 1 CP el supuesto en el que un abogado revela secretos de quien no es su cliente, sino de la otra parte contra la que se da el pleito.

---

<sup>205</sup> TOMÁS-VALIENTE LANUZA, *Del descubrimiento y revelación de secretos*, en: GÓMEZ TOMILLO (Dir.), *Comentarios al Código Penal*, 2ª edición, 2011, pág. 807.

<sup>206</sup> CASTIÑEIRA PALOU/ ESTRADA I CUADRAS, *Delitos contra la intimidad*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal*, Parte especial, 4ª edición, 2015, pág. 169.

<sup>207</sup> TOMÁS-VALIENTE LANUZA, *Del descubrimiento y revelación de secretos*, en: GÓMEZ TOMILLO (Dir.), *Comentarios al Código Penal*, 2ª edición, 2011, pág. 808.

En el tipo penal no se precisa qué parte contractual es la que está obligada a guardar el secreto. Se entiende que será el empleado quien conozca el secreto de su empleador, pero también puede darse la situación al revés.<sup>208</sup>

Es plausible que sea el empleador quien divulgue el secreto. En ese caso, se sanciona la conducta en el art. 8.11 del RD 5/2000, de 4 de agosto, aprobatorio de la ley sobre infracciones y Sanciones en el Orden Social.

El art. 199 CP no indica hasta cuándo podría durar la obligación contractual de guardar secreto.

Esto hace, desde el punto de vista de CASTIÑEIRA PALOU / ESTRADA I CUADRAS, que exista confusión sobre si la obligación persiste cuando ya ha terminado la relación laboral. Si se considera que la obligación de guardar secreto finaliza cuando acaba la relación laboral, basta la resolución del contrato para poder divulgar secretos sin ser castigado.<sup>209</sup>

De otro modo, también resulta incoherente establecer un deber de perpetuidad al respecto. Se han considerado inválidas por parte de la doctrina, como TOMÁS-VALIENTE LANUZA, las cláusulas contractuales que imponen una limitación temporal del deber de guardar secreto.<sup>210</sup>

No obstante, hay que tener en cuenta que la disponibilidad del secreto corresponde a su titular. Con lo cual, es él quien puede decidir sobre el carácter de una determinada información en cualquier momento.

Por otro lado, la segunda modalidad del art. 199 CP trata sobre el secreto profesional. Esta segunda modalidad cifra, desde el punto de vista de TOMÁS-VALIENTE LANUZA, “*el refuerzo jurídico de la obligación de mantener la confidencialidad*”.<sup>211</sup>

---

<sup>208</sup> Sobre ello véase, JORGE BARREIRO, *El delito de revelación de secretos (profesionales y laborales)*, La Ley: Revista jurídica española de doctrina, jurisprudencia, y bibliografía, núm. 3, 1996, pág. 1295-1305.

<sup>209</sup> CASTIÑEIRA PALOU/ ESTRADA I CUADRAS, *Delitos contra la intimidad*, en: SILVA SÁNCHEZ (Dir.) y RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 169- 170.

<sup>210</sup> TOMÁS-VALIENTE LANUZA, *Del descubrimiento y revelación de secretos*, en: GÓMEZ TOMILLO (Dir.), *Comentarios al Código Penal*, 2ª edición, 2011, pág. 808.

<sup>211</sup> TOMÁS-VALIENTE LANUZA, *Del descubrimiento y revelación de secretos*, en: GÓMEZ TOMILLO (Dir.), *Comentarios al Código Penal*, 2ª edición, 2011, pág. 809.

También se refiere a supuestos en los que se ha conocido el secreto lícitamente, pero es punible su revelación como en la modalidad anterior.

Lo que diferencia esta modalidad de la primera, desde el punto de vista de CASTIÑEIRA PALOU / ESTRADA I CUADRAS, es que aquí hay una obligación de sigilo o reserva.<sup>212</sup>

Así, en la STS núm. 574/2001, de 4 de abril, se casa la sentencia de un médico que examinó la historia clínica de una paciente, donde vio que había practicado dos abortos y se lo contó a su madre y ésta a la hermana de la paciente. El TS consideró que se había cometido un delito del art. 199.2 CP: *“El hecho probado es subsumible en el art. 199.2 del Código Penal. Este delito protege la intimidad y la privacidad como manifestaciones del libre desarrollo de la personalidad y de la dignidad de las personas. Se trata de un delito especial propio, con el elemento especial de autoría derivado de la exigencia de que el autor sea profesional, esto es que realice una actividad con carácter público y jurídicamente reglamentada”*.

El autor del delito sólo puede ser alguien que tenga un título académico que habilite la práctica de dedicarse a una profesión reglamentada.

En ese tipo de profesiones reglamentadas debe ser necesario que el cliente cuente la información que desea guardar en secreto, lo que convierte al profesional, según TOMÁS-VALIENTE LANUZA, en “confidente necesario”. Esa conversión del profesional en confidente, fundamenta jurídica y moralmente, la obligación de sigilo y reserva que forma la base del art. 199.2 CP. Esta obligación hace que haya que asistir a la regulación de cada profesión para saber, específicamente, cuáles son los deberes de sigilo y de reserva.<sup>213</sup>

Dependiendo de la profesión que se desempeñe, las leyes que regulan el secreto profesional o el deber de sigilo se hallan:

---

<sup>212</sup> CASTIÑEIRA PALOU/ ESTRADA i CUADRAS, *Delitos contra la intimidad*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 169-170.

<sup>213</sup>TOMÁS-VALIENTE LANUZA, *Del descubrimiento y revelación de secretos*, en: GÓMEZ TOMILLO (Dir.), *Comentarios al Código Penal*, 2ª edición, 2011, pág. 808.



a) Respecto a *procuradores y abogados*, hay que acudir al RD 658/2001, de 22 de junio, y al RD 1281/2002, de 5 de diciembre. En este caso, el secreto profesional se deriva del derecho a la defensa, consagrado en el art. 24 CE como un derecho fundamental.<sup>214</sup>

No impide el deber de reserva, que el abogado sea llamado como testigo si su cliente le da datos sobre la intención de cometer un delito en el futuro, aunque siga ejerciendo su defensa (art. 416. 2º LECrim).

b) Sobre el *secreto periodístico*, surgen los mayores problemas debido a la información que se revela, que suele ser casi siempre secreta.

El art. 20.1.d) CE regula el secreto profesional en el ejercicio de la libertad de la información.

No obstante, tiene sus límites. La mayoría de ellos proceden de las necesidades de la defensa nacional en relación con materias legalmente calificadas (arts. 598 y ss. CP). También, se constituyen límites cuando la información publicada tiene su origen en una vulneración al derecho a la intimidad (segundo apartado del art. 197.3 CP).

Como a los abogados, el art. 262 LECrim permite a los periodistas denunciar un delito público del que tuvieran noticia, lo que es posible con la facultad de no revelar las fuentes de la información.<sup>215</sup>

El sector periodístico carece de una ley que regule de forma específica su obligación de secreto profesional. Esto deja, en opinión de MUÑOZ CONDE, “*un amplio espacio a suposiciones teóricas y a la reflexión sobre los límites de los derechos fundamentales, cuando surge un conflicto entre ellos*”.<sup>216</sup>

En la STS núm. 234/1999, de 18 de febrero, se condenó a una periodista que publicó los nombres de dos presos, enfermos de SIDA, que trabajaban en la cocina de la cárcel, si bien se apreció la eximente incompleta de ejercicio legítimo del derecho a la información.

---

<sup>214</sup> Sobre ello véase, TOMÁS-VALIENTE LANUZA, *Del descubrimiento y revelación de secretos*, en: GÓMEZ TOMILLO (Dir.), *Comentarios al Código Penal*, 2ª edición, 2011, pág. 810.

<sup>215</sup> A tal efecto véase, MUÑOZ CONDE, *Derecho Penal Parte Especial*, 20ª edición, 2015, pág. 243-248.

<sup>216</sup> MUÑOZ CONDE, *Derecho Penal Parte Especial*, 20ª edición, 2015, pág. 247- 248.

c) Sobre el *secreto industrial* o empresarial, no se protege la intimidad en el sector empresarial debido, en opinión de MUÑOZ CONDE, a su dimensión socioeconómica. Esta clase de secreto se protege en los arts. 278 a 280 CP, entre los delitos contra el orden socioeconómico. El bien jurídico que se protege aquí es de índole patrimonial.<sup>217</sup>

Como se puede apreciar, la regulación sobre el secreto profesional está totalmente dispersa. Así, TOMÁS-VALIENTE LANUZA considera que la regulación “*es confusa como consecuencia de no contar con una ley que desarrolle el art. 24.2 CE y sí, en cambio, con una regulación parcial y completamente desfasada del tema en la decimonónica LECrim*”.<sup>218</sup>

### **3.10. Disposiciones comunes (Art. 200 y 201 CP)**

El Código Penal también protege penalmente la intimidad de las personas jurídicas. Así lo expresa el art. 200 CP<sup>219</sup> al señalar que, lo dispuesto en el Capítulo X, también les es aplicable.

Sin embargo, el TC se muestra reticente a reconocerles el derecho a la intimidad (art. 18.1 CP), ya que se trata de un derecho personalísimo.<sup>220</sup>

La mayor parte de la doctrina y de la jurisprudencia menor concibe esta protección como una “*extensión instrumental de la tutela de la intimidad que corresponde al individuo- persona física para los supuestos en que pudiera quedar reflejada en datos reservados de personas jurídicas*”.<sup>221</sup>

En esa misma tesitura se muestra TOMÁS-VALIENTE LANUZA, quien considera que “*produce extrañeza que el legislador parezca extender a las personas jurídicas la tutela de un bien jurídico, a su vez derecho fundamental (la intimidad), que sólo parece poder atribuirse a las personas físicas*”.<sup>222</sup>

---

<sup>217</sup> MUÑOZ CONDE, *Derecho Penal Parte Especial*, 20ª edición, 2015, pág. 248.

<sup>218</sup> TOMÁS-VALIENTE LANUZA, *Del descubrimiento y revelación de secretos*, en: GÓMEZ TOMILLO (Dir.), *Comentarios al Código Penal*, 2ª edición, 2011, pág. 810.

<sup>219</sup> El art. 200 CP establece que: “*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*”.

<sup>220</sup> Sobre ello véase, el Auto núm. 257/1985, de 17 de abril.

<sup>221</sup> Véase la SAP – Pontevedra núm. 314/2011, de 10 de noviembre.

<sup>222</sup> TOMÁS-VALIENTE LANUZA, *Del descubrimiento y revelación de secretos*, en: GÓMEZ TOMILLO (Dir.), *Comentarios al Código Penal*, 2ª edición, 2011, pág. 811.

Respecto a la perseguibilidad de los delitos contra la intimidad, sólo es posible a instancia de parte. Según el art. 201 CP<sup>223</sup>, se necesita la denuncia de la persona agraviada o de su representante legal.<sup>224</sup>

Cabe decir que en opinión de LIBANO BERISTAIN, la persona agraviada en los delitos contra la intimidad es el titular del bien jurídico de la intimidad. Por lo que se interpreta del art. 201 CP, debe ser una persona física la víctima del delito y no una persona jurídica, pues no se halla protegida por el precepto penal.<sup>225</sup>

La perseguibilidad en los delitos contra la intimidad se configuró siempre, salvo en el Código Penal de 1928, a instancia de parte. Es el sujeto pasivo quien decide si debe o no denunciar los hechos delictivos y abrir un proceso.<sup>226</sup>

Así pues, el legislador del Código Penal del 95 considera los delitos contra la intimidad como privados y por ello susceptibles del “ius persecuendi”. De esta forma, se elige una fórmula de equilibrio en estos delitos privados a través de la figura del Ministerio Fiscal, en el art. 201. 1. segundo párrafo CP.<sup>227</sup>

A modo de ejemplo, podemos ver en la SAP de Vizcaya, núm. 43/2016, de 28 de julio, como se absuelve, del delito de descubrimiento y revelación de secretos del art. 197 CP, a una mujer que había accedido e interceptado cartas enviadas a otras personas, al no haber denuncia de los agraviados por el hecho.

Se forma así, según OLMO FERNÁNDEZ- DELGADO: *“Un sistema intermedio de persecución del delito, en el que se faculta al Ministerio Fiscal para querellarse de*

---

<sup>223</sup> El art. 201 CP establece que: *“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”*.

<sup>224</sup> Sobre ello véase, RUEDA MARTÍN, *Protección penal de la intimidad personal e informática*, 2004, pág. 131.

<sup>225</sup> LIBANO BERISTAIN, *Los delitos de descubrimiento y revelación de secretos*, Revista V/Lex España, Información jurídica inteligente, 2017, pág. 218- 231.

<sup>226</sup> Sobre ello véase, LIBANO BERISTAIN, *La perseguibilidad a instancia de parte como proyección de las facultades de la víctima*, en: DE HOYOS SANCHO (Coord.), *La víctima del delito y las últimas reformas procesales penales*, 2017, pág. 121- 134.

<sup>227</sup> Sobre ello véase, RUEDA MARTÍN, *Protección penal de la intimidad personal e informática*, 2004, pág. 132.

*oficio, pero ponderando los intereses en juego, como expresión singular del principio de oportunidad en la prevención del delito”.*<sup>228</sup>

El Ministerio Fiscal puede interponer denuncia o querrela cuando la víctima sea menor, persona con discapacidad necesitada de especial protección o esté desvalida (art. 201.1. segundo párrafo CP).

Respecto a cómo entender a la víctima del delito como menor de edad, sólo debe considerarse a tal efecto al menor de dieciocho años o a lo que establezcan el CC y el CP.<sup>229</sup>

Para entender cuándo una persona tiene una discapacidad necesitada de especial protección, ha de atenderse a lo establecido en el art. 25 CP.<sup>230</sup>

Por otro lado, para considerar a alguien desvalido tiene que tratarse de una persona desamparada, que se encuentre *“imposibilitada para denunciar”*, según JORGE BARREIRO<sup>231</sup> o, como establece OLMO FERNÁNDEZ- DELGADO, que *“en el caso de enfrentarse a un proceso, sea incapaz de entenderlo”*.<sup>232</sup>

En el segundo párrafo del art. 201 CP se establece que no se necesita interponer denuncia cuando se dé un supuesto del art. 198 CP, o el delito afecte a un interés público o a un conjunto de personas. De esta forma, también son perseguibles de oficio los delitos cometidos por autoridad o funcionario público, que realice cualquier hecho

---

<sup>228</sup> OLMO FERNÁNDEZ- DELGADO, *El descubrimiento y revelación de secretos documentales*, 2009, pág. 195.

<sup>229</sup> Sobre ello véase, DOVAL PAIS / ANARTE BORRALLA, *delitos de descubrimiento y revelación de secretos*, en: BOIX REIG (Coord.), *Derecho Penal, Parte especial*, Vol. I, 2016, pág. 540- 546.

<sup>230</sup> El art. 25 CP establece el concepto de Incapacidad: *“A los efectos de este Código se entiende por discapacidad aquella situación en que se encuentra una persona con deficiencias físicas, mentales, intelectuales o sensoriales de carácter permanente que, al interactuar con diversas barreras, puedan limitar o impedir su participación plena y efectiva en la sociedad, en igualdad de condiciones con las demás. Asimismo a los 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”*.

<sup>231</sup> JORGE BARREIRO, *El art. 200 CP*, en: COBO DEL ROSAL (Dir.), *Comentarios al Código Penal*, Tomo VII, 1999, pág. 273.

<sup>232</sup> OLMO FERNÁNDEZ-DELGADO, *El descubrimiento y revelación de secretos documentales*, 2009, pág. 198.

tipificado en el art. 197 CP, fuera de los casos permitidos por la ley y sin mediar justa causa (art. 198 CP).<sup>233</sup>

Finalmente, el art. 201.3 CP<sup>234</sup> recoge el perdón del ofendido. Se extingue la acción penal si la víctima del delito o su representante legal perdonan el hecho delictivo, teniendo en cuenta las características del art. 130. 1. 5º CP.<sup>235</sup>

En opinión de TOMÁS-VALIENTE LANUZA, el art. 201.3 CP, reformado por la LO 5/2010, de 22 de junio, “*elimina la anterior eficacia del perdón del ofendido sobre la pena impuesta, poniendo con ello fin a una obvia contradicción con la regulación general de la figura en el art. 130.1.5º CP (que exigía y sigue exigiendo el otorgamiento de dicho perdón antes de dictarse sentencia)*”.<sup>236</sup>

Tras la LO de 25 de junio de 1983, se limitaron los supuestos en los que tuvo cabida el perdón del ofendido. Así, en el caso de una violación por ejemplo, nunca se extingue la acción penal por el perdón del ofendido. En el anterior Código Penal, la “gracia privada” era posible en todos los delitos perseguibles a instancia de parte.<sup>237</sup>

En el Código Penal vigente, las consecuencias del perdón del ofendido dependen de tres requisitos del art. 130. 5º CP, según lo establecido por la LO 15/2003. Los tres requisitos están formados por: un ámbito material, otro formal y otro temporal.

Primeramente, el requisito de ámbito material quiere decir que el perdón del ofendido sólo se aplica cuando la ley así lo prevea.

El de ámbito formal establece que el perdón tiene que ser expreso. No cabe que se dé de forma tácita, debe ser manifestado expresamente ante el órgano judicial.

---

<sup>233</sup> Sobre ello véase, TOMÁS-VALIENTE LANUZA, *Del descubrimiento y revelación de secretos*, en: GÓMEZ TOMILLO (Dir.), *Comentarios al Código Penal*, 2ª edición, 2011, pág. 812.

<sup>234</sup> El art. 201.3 CP establece que: “*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*”.

<sup>235</sup> Sobre ello véase, RUEDA MARTÍN, *Protección penal de la intimidad personal e informática*, 2004, pág. 135 y 136.

<sup>236</sup> TOMÁS-VALIENTE LANUZA, *Del descubrimiento y revelación de secretos*, en: GÓMEZ TOMILLO (Dir.), *Comentarios al Código Penal*, 2ª edición, 2011, pág. 813.

<sup>237</sup> A tal efecto véase, CASTIÑEIRA PALOU/ ESTRADA i CUADRAS, *Delitos contra la intimidad*, en: SILVA SÁNCHEZ (Dir.) / RAGUÉS I VALLÉS (Coord.), *Lecciones de Derecho Penal, Parte especial*, 4ª edición, 2015, pág. 170-171.

Sobre el ámbito temporal se establece que el perdón tiene que otorgarse antes de que se dicte la sentencia, es decir, antes de que se ordene la ejecución de la pena.<sup>238</sup>

El motivo del requisito temporal se debe, según SERRANO BUTRAGUEÑO “*al consentimiento de la víctima, que se vería sujeta a ciertas presiones si fuera válido, a estos efectos, otorgar el perdón aún después de comenzada la ejecución de la pena*”.<sup>239</sup>

#### **IV. CAUSAS DE JUSTIFICACIÓN EN LOS DELITOS CONTRA LA INTIMIDAD**

Las conductas típicas del art. 197 CP pueden plantear como causa de justificación, el ejercicio legítimo de un derecho. Esta circunstancia supone una eximente al delito (art. 20.7 CP). Para que se aplique dicha eximente del art. 20.7 CP, en opinión de SÁNCHEZ GARCÍA DE PAZ, “*se requiere, además de la concurrencia del presupuesto de hecho de la existencia del deber jurídico, que su ejercicio sea legítimo*”.<sup>240</sup>

Los derechos alegados para justificar la comisión de estos tipos penales causan una gran problemática por la polémica que suscitan. Los que suelen dar lugar a debate son: los del ejercicio del derecho a comunicar o recibir libremente información veraz por cualquier medio de difusión (art. 20.1.d. CE) o la investigación del delito.

Hay otros hechos en cambio, en los que, desde el punto de vista de RODRÍGUEZ LAINZ, queda muy clara la causa de justificación, como en los arts. 579 y ss. de la LECrim, que posibilitan al juez acordar la detención de la correspondencia privada, intervención de las comunicaciones telefónicas del procesado o la observación de las comunicaciones postales, telegráficas o telefónicas de las personas sobre las que existan indicios de responsabilidad criminal.<sup>241</sup>

Otro caso amparado por el ejercicio legítimo de un derecho, según MUÑOZ CONDE, es el de la suspensión o intervención motivada en las comunicaciones orales y escritas

---

<sup>238</sup> En este sentido véase, OLMO FERNÁNDEZ-DELGADO, *El descubrimiento y revelación de secretos documentales*, 2009, pág. 193- 203.

<sup>239</sup> SERRANO BUTRAGUEÑO, *Causas que extinguen la responsabilidad penal*, en: SERRANO BUTRAGUEÑO (Coord.), *Código Penal de 1995, (Comentarios y jurisprudencia)*, 1999, pág. 897.

<sup>240</sup> SÁNCHEZ GARCÍA DE PAZ, *De las causas que eximen de la responsabilidad criminal, Art. 20.7 CP*, en: GÓMEZ TOMILLO (Dir), *Comentarios al Código Penal*, 2ª edición, 2011, pág. 170.

<sup>241</sup> RODRÍGUEZ LAINZ, *El secreto de las telecomunicaciones y su interceptación legal*, 2016, Pág. 73-97.

de los internos con sus familiares, abogado de confianza, amigos etc. (art. 43 y ss. RP).<sup>242</sup>

Cuando exista un conflicto sobre el daño al bien jurídico, los Tribunales establecen el principio de *proporcionalidad* entre los posibles derechos que puedan motivar la conducta delictiva y los derechos perjudicados, dependiendo del supuesto concreto.<sup>243</sup>

El principio de *proporcionalidad*, según SÁNCHEZ GARCÍA DE PAZ, “*se desdobra en dos máximas fundamentales; los principios de necesidad y de proporcionalidad en sentido estricto*”.<sup>244</sup>

En el supuesto de que el hecho se trate del derecho a comunicar o recibir libremente información veraz (art. 20.1.d.CE), se tiene que tener en cuenta que “*tiene su límite en el respeto de los derechos reconocidos en este título, en los preceptos de las leyes que lo desarrollan y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia*” (art. 20.4 CE).<sup>245</sup>

Si la colisión se produce entre la libertad de la información (art. 20.1 CE) y el derecho a la intimidad o al honor (art. 18.1 CE), la doctrina reiterada del TC declara que “*la libertad de información goza por su trascendencia, (dimensión de garantía de la opinión pública libre y del principio de legitimidad democrática), de una posición preferente*”.

Así al respecto, el TC señala en la sentencia núm. 172/1990, de 12 de noviembre, que “*la legitimidad de las intromisiones en el honor e intimidad personal requiere no sólo que la información cumpla con la condición de veracidad, sino también que su contenido se desenvuelva en el marco del interés general del asunto al que se refiere*”.

Por otra parte, un caso discutible sobre el conflicto del derecho a la libertad de información (art. 20.1 CE) y la intimidad o el honor (art. 18.1 CE) fue la postura que adoptó la sala de lo penal del TS en la STS núm. 234/1999, de 18 de febrero.

---

<sup>242</sup> MUÑOZ CONDE, *Derecho Penal Parte Especial*, 20ª edición, 2015, pág. 243.

<sup>243</sup> A tal efecto véase, JORGE BARREIRO, *Del descubrimiento y revelación de secretos*, en: COBO DEL ROSAL (Dir.), *Comentarios al Código Penal*, Tomo VII, 1999, pág. 118-124.

<sup>244</sup> SÁNCHEZ GARCÍA DE PAZ, *De las causas que eximen de la responsabilidad criminal*, Art. 20.7 CP, en: GÓMEZ TOMILLO (Dir.), *Comentarios al Código Penal*, 2ª edición, 2011, pág. 172.

<sup>245</sup> Sobre ello véase, DE CARRERAS SERRA, *Las normas jurídicas de los periodistas: Derecho español de la información*, 2008, pág. 38- 41.

En dicha sentencia, el TS apreció una eximente incompleta del ejercicio legítimo del derecho a informar por un periodista que había realizado un artículo, con datos personales de dos internos en una cárcel enfermos del SIDA, que trabajaban en la cocina.

En este supuesto, el TS destacó que, existe un interés público en conocer esa noticia, aunque también es cierto que el periodista se extralimitó en su ejercicio del derecho a comunicar, al recoger datos reservados (nombre, lugar de nacimiento, estado civil, profesión y antecedentes de su carrera criminal).

Si bien un sector de la doctrina consideró que, la conducta del periodista, puede quedar englobada como una eximente incompleta respecto a la difusión de la noticia, el TS finalmente declaró que, ni siquiera cabría esa eximente incompleta, al divulgar la identidad de los presos y no ceñirse a lo noticiable.

Sobre la interceptación de conversaciones telefónicas en investigaciones por razón de la comisión de un delito, se cuestiona esa justificación respecto del derecho fundamental al secreto de las telecomunicaciones y en concreto, a las postales telegráficas y telefónicas (art. 18.3 CE).

En estos casos, a partir de la STS núm. 234/1999, de 18 de febrero, y la doctrina reiterada del TC, se consideró que deben concurrir cuatro requisitos para que la medida judicial sea legítima.

Será preciso pues, que en la medida judicial se respete: a) la proporcionalidad; b) especialidad de la materia delictiva a investigar; c) haya indicios delictivos, que no puedan ser confundidos con meras conjeturas o sospechas; d) que la necesidad de empleo de esta medida no pueda ser posible por un procedimiento menos restrictivo; y e) que se dé la motivación suficiente de la autorización judicial.

A pesar de eso, como indica la sentencia de la Audiencia Provincial de Madrid núm. 227/1999, de 26 de mayo (caso CESID), no hay causa de justificación que transforme en lícita *“la más cruda forma de razón de Estado”*.



No se puede amparar la violación que supone la grabación y archivo masivo de conversaciones telefónicas entre ciudadanos, sin autorización judicial aunque se aleguen “*superiores razones de seguridad de Estado*”.<sup>246</sup>

Tampoco cabe alegar el ejercicio legítimo de un derecho para obtener un medio de prueba, ni la información que así se consiga, salvo que haya autorización judicial expresa o en los casos previstos de suspensión de derechos del art. 55.2 de la CE.<sup>247</sup>

Un buen ejemplo a ello es el caso Garzón, en la STS núm. 79/2012, de 9 de febrero. Aquí se acusa de un delito de prevaricación a un juez, que, en la fase de Instrucción, autoriza la grabación de una conversación entre un abogado y su cliente, en la investigación de un delito económico.<sup>248</sup>

Esta grabación ilegítima hizo que no fuera usada como prueba al ser nula.

---

<sup>246</sup> Véase a tal efecto, GARRIDO FALLA, *Ética y razón de Estado: los documentos del CESID y el caso GAL*, Anales de la Real Academia de Ciencias Morales y Políticas, núm. 73, 1996, pág. 175- 192.

<sup>247</sup> El art. 55.2 CE establece: “*Una ley orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, pueden ser suspendidos para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas. La utilización injustificada o abusiva de las facultades reconocidas en dicha ley orgánica producirá responsabilidad penal, como violación de los derechos y libertades reconocidos por las leyes*”.

<sup>248</sup> Sobre ello véase, ANDRÉS IBÁÑEZ, *Caso Garzón: necesario distinguir*, Nuevo foro penal, núm. 77, 2011, pág. 17- 42; AGUILAR CABRERA, *Discusión sobre la ilegalidad de la prueba y la búsqueda de la impunidad. A propósito del caso Baltasar Garzón*, Revista Derecho y cambio social, núm. 35, año 11, 2014, pág. 2- 28.

## V. CONCLUSIONES

Tras realizar este trabajo e investigar sobre un tema tan sumamente relevante, como es la regulación de los delitos de descubrimiento y revelación de secretos en España, y teniendo en cuenta los objetivos mencionados al comienzo del presente trabajo, cabe destacar las siguientes conclusiones:

### *1. La libertad informática y la intimidad han de garantizarnos la misma protección.*

El bien jurídico protegido en los delitos de descubrimiento y revelación de secretos es la intimidad. Se acepta de manera unánime por la doctrina y la jurisprudencia, que uno de los bienes jurídicos protegidos es la intimidad, tanto personal como familiar.

No obstante, en lo referente a los delitos informáticos o al *habeas data* (art. 197.2, 197.3, 197 bis y 197 ter CP), opino que no es la intimidad el bien jurídico principal, como considera cierta parte de la doctrina penalista, sino que en estos casos es la libertad informática. Mediante la libertad informática, se garantiza el secreto de las comunicaciones, el cual no depende de la intimidad. En mi opinión, se trata de un derecho autónomo que se une con la intimidad, dándose una relación medial entre ambos.

No podemos seguir pensando que la libertad informática es un bien jurídico secundario, pues nos hallamos ante otro derecho fundamental, recogido en el art. 18.4 CE, que posee el mismo alcance que la intimidad. Otra muestra más de la ampliación del bien jurídico en los delitos informáticos, la encontramos en una de las sentencias pioneras sobre la libertad de las comunicaciones, como es la STC núm. 114/1984, de 29 de noviembre, que ya afirmaba en los años ochenta que la libertad informática era un derecho independiente de la intimidad. No hay pues, un orden jerárquico entre la intimidad y la libertad informática en la CE. Ambos derechos se encuentran al mismo nivel y se coadyuvan para un mismo fin, primando en los delitos informáticos la libertad informática.

### *2. Los delitos de descubrimiento y revelación de secretos están recogidos en el CP de forma asistemática.*

Gran cantidad de delitos relativos al descubrimiento y revelación de secretos se hallan dispersos a lo largo del CP, cuando en realidad deberían tener la misma ubicación que los delitos que sí se recogen en el correspondiente Cap. I (del descubrimiento y

revelación de secretos), del Tít. X (delitos contra la intimidad), puesto que este tipo de delitos atentan contra los mismos bienes jurídicos, la intimidad y la seguridad informática. Así por ejemplo, en el caso de los delitos de descubrimiento y revelación de secretos realizados por autoridad o funcionario público, mientras que en el art. 198 CP, del Tít. X del Cap. I, se castiga al funcionario público que revela o descubre secretos prevaliéndose de su cargo, otras conductas delictivas consistentes en hechos similares, como son la violación de la correspondencia privada o la interceptación de las comunicaciones personales, se hallan en los arts. 535 y 536 CP del Cap. V.

Ello no tiene sentido, pues es en el Cap. I (descubrimiento y revelación de secretos) del Tít. X (delitos contra la intimidad) del CP, donde se deben castigar todas las modalidades delictivas relativas a la interceptación de las comunicaciones y la difusión, revelación o descubrimiento de secretos.

Si todos los delitos relativos a estas conductas delictivas se regulasen en un mismo capítulo, sería más fácil poder comparar los elementos objetivos y subjetivos de los delitos y aplicar una pena más adecuada y precisa a cualquier supuesto de hecho penal.

*3. El legislador no ha logrado solucionar todo lo que se había propuesto a través de las modificaciones producidas por la LO 1/2015, de 30 de marzo y la LO 13/2015, de 5 de octubre.*

Por lo que se refiere a los cambios que introduce la reforma de la LO 1/2015, de 30 de marzo, cabe decir en mi opinión que, por una parte, aporta cierta homogeneidad al CP al intentar agrupar figuras delictivas que en el anterior CP estaban dispersas. Actualmente, el Cap. I, del Tít. X del CP, nos ofrece una protección más coherente y sistemática. Sin embargo, como dije en el punto 2, aún quedan muchas figuras delictivas que deben agruparse y unirse al Cap. I.

Por otra parte, creo que a pesar de haber creado el legislador nuevas conductas delictivas contra la libertad informática, no son suficientes. En mi opinión, debido a la gran magnitud, gravedad y a la frecuencia con la que se dan los delitos informáticos, debería barajarse la posibilidad de crearse un capítulo exclusivo para esta clase de delitos. No obstante, pienso que finalmente se creará dicho capítulo exclusivo en un futuro pues, como bien sabemos, el derecho siempre va un paso por detrás a lo que sucede en la sociedad.

También cabe destacar los cambios que ha producido la reforma proporcionada por la LO 13/2015, de 5 de octubre, la cual desde mi punto de vista, ha mejorado significativamente las garantías procesales en los delitos de descubrimiento y revelación de secretos al regular, de forma más específica, una materia parcialmente obsoleta que no ha garantizado la protección de la intimidad y de la privacidad de la población cuando se han llevado a cabo medidas de investigación tecnológica. Considero por ello, que esta modificación garantiza más la tutela judicial de las personas y fomenta la imposibilidad de que se cometan ciertos abusos por parte de los cuerpos y fuerzas de seguridad del Estado contra la intimidad, como sucedió en el explicado caso CESID.

Otro acierto del legislador con la reforma de la LO 1/2015, de 30 de marzo, es a mi modo de ver, la modificación que ha realizado en el tipo penal del art. 197 quáter CP (hechos cometidos por organización o grupo criminal). Antes de la reforma, este tipo penal agravado sólo se aplicaba a algunos apartados del art. 197 CP. Ahora en cambio, se aplica a todo el articulado del Cap. I, extendiéndose también a las conductas delictivas relativas al secreto laboral o profesional (art. 199 CP).

Por otro lado, en cuanto a la introducción del segundo apartado del art. 197. 4 CP (acceso ilícito a datos personales de la víctima sin su autorización), me parece irrelevante e innecesaria, puesto que la utilización no autorizada de datos personales ya se regula en el ámbito civil por el art. 10 de la LO 15/1999, de protección de datos de carácter personal (LODPD) y el RD 1720/2007, de desarrollo de la Ley Orgánica de Protección de Datos. No entiendo por ello que se dé cabida a castigar penalmente estos hechos cuando dichas leyes ya contemplan esta clase de actuaciones con repercusión penal.

*4. La regulación de la responsabilidad penal de las personas jurídicas y su protección en el CP era necesaria.*

Sobre la tipificación de la responsabilidad penal de las personas jurídicas (art. 197 quinquies CP) en los delitos contra la intimidad en el CP, creo que ha representado una gran mejora legislativa.

Una persona jurídica es un conjunto de personas físicas, en un ámbito societario o empresarial, que realizan actividades de vital trascendencia para el sector laboral y para el sector servicios. Igual que cualquier persona física, una persona jurídica también

puede atentar contra la intimidad de otra empresa u otra persona, cometiendo un delito de descubrimiento o revelación de secretos. Además, las consecuencias del delito que comete una empresa, tiene mayor repercusión que si lo hace una persona física.

Pensemos por ejemplo, en el supuesto basado en hechos reales, sobre el afán de Donald Trump por aprovecharse de su acomodada posición en el sector hotelero, para obtener secretos de Estado de gobiernos de otros países, como China o Turquía. ¿No se debería castigar también a su empresa, que es la que le ha permitido obtener dicha información secreta?

Sería totalmente injusto e incoherente que no se castigase en este supuesto a la empresa, pues fue mediante ella como Donald Trump obtuvo los secretos de Estado.

Gracias a la reforma de la LO 1/2015, de 30 de marzo, se amplía la responsabilidad penal de las personas jurídicas a todos los delitos del Tít. X, Cap. I CP, pudiendo ahora ser responsables de un delito de espionaje o sabotaje informático (art. 197 bis y 197 ter CP) por ejemplo, y no sólo de un delito de descubrimiento y revelación de secretos del art. 197 CP.

Por otra parte, cabe también mostrar mi disconformidad con la mayoría de la doctrina penalista sobre que no se deba proteger a las personas jurídicas en el art. 200 CP. Si las personas jurídicas son susceptibles de ser responsables penalmente de los delitos contra la intimidad, ¿no debe entonces existir la posibilidad de que también sean protegidas contra un delito de descubrimiento y revelación de secretos? Pongámonos en el caso, basado también en hechos reales, de que un grupo de hackers intenta acceder a todos los archivos informáticos de la empresa Movistar, ¿no se debe garantizar a Movistar una protección penal en ese supuesto?

En mi opinión, no tiene sentido que no se proteja a las personas jurídicas ante esta clase de atentados contra la intimidad, pues éstas también son un blanco fácil para los delitos de descubrimiento y revelación de secretos y además, también pueden ver dañadas su intimidad, su imagen de cara al consumidor o su derecho al secreto de las comunicaciones.

*5. Desacierto en la introducción de la conducta denominada sexting entre los adultos.*

En cuanto a la introducción en el art. 197.7 CP de la conducta delictiva consistente en la difusión, revelación, o cesión de imágenes o vídeos sin autorización de la víctima (sexting), cabe decir que desde un punto de vista teleológico, me parece que se cae en cierta forma en el populismo punitivo. El hecho que propició que se regulasen estas conductas en el CP, se debió al gran revuelo mediático que produjo el caso de la edil Hormigos. Considero que no se puede empezar a regular penalmente una materia por el hecho de que sea un cargo gubernativo el que se vio afectado por un atentado contra la intimidad. Aparte de esto, la LO 1/1982, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, ya regula la intromisión ilegítima y la captación, reproducción o publicación de imágenes que vulneran la intimidad, cuando no hay consentimiento, por lo que no comprendo que también se decida regular penalmente una conducta que ya tiene consecuencia jurídica cuando se produce realmente un atentado contra la intimidad, al no haber consentimiento de la persona que sufre el daño.

En mi opinión, no se debería castigar a una persona por difundir una foto o un vídeo de un sujeto mayor de edad, si éste le da su consentimiento para realizar dicha foto o vídeo. Cosa distinta es que la víctima de esa difusión, revelación o cesión fuese un menor de edad o un discapacitado necesitado de especial protección. En ese caso me parece un acierto, a la par que lógico, que se castiguen estas conductas, ya que se trata de sujetos en los que el consentimiento que se da para realizar el ilícito penal se encuentra viciado o es nulo, debido a la falta de madurez o de consciencia para comprender lo que están haciendo y lo que ello supone. Además de esto, también hay que tener en cuenta que la población más joven o los discapacitados necesitados de especial protección, pueden verse desorientados y confusos por el amplio abanico de redes sociales y las actuaciones de otros jóvenes adolescentes en ellas para realizar estas conductas, las cuales muchos de ellos ven como algo normal.

No obstante, en el caso de que la víctima sea un adulto, creo que éste posee las suficientes habilidades psíquicas y la necesaria madurez como para saber los riesgos que pueden conllevar sus actos, aparte de que, como ya he dicho, ya se castigan esta clase de sucesos en la LO 1/1982, de protección civil al honor, a la intimidad personal y familiar y a la propia imagen.

6. *La gran importancia de estar preparados ante los delitos de espionaje y sabotaje informático sigue latente.*

Por último, respecto a la introducción de los arts. 197 bis y 197 ter CP (intrusismo informático), cabe concluir que estoy totalmente de acuerdo con que finalmente se hubiese decidido recoger estas conductas delictivas en el CP.

Los medios tecnológicos nos permiten obtener y ver cualquier tipo de datos, algunos de ellos confidenciales, como nuestras cuentas bancarias, una nómina de trabajo o una conversación íntima con un tercero, y es por ello por lo que creo que debe existir una regulación penal que nos garantice una protección más segura y más fiable. Aun así, considero que nos queda mucho por hacer. Hemos de empezar a regular, de forma más precisa, todos los posibles atentados contra la libertad informática y el secreto de las comunicaciones en todos los diferentes ámbitos jurídicos, desarrollando de una manera más amplia y específica la seguridad de los sistemas informáticos.

La mayoría de los delitos que se darán en el futuro, y que ya se dan en el presente, son cibernéticos, y no poseemos una adecuada legislación que nos proteja lo suficiente ante ello.

En un siglo de grandes cambios en el que un dron puede espiar cualquier movimiento animal o humano sin ningún tipo de injerencias, o una libélula puede ser manejada por control remoto al manipularse sus neuronas para convertirla en un *cyborg*, ¿de verdad creemos que el derecho actual nos proporciona la suficiente protección ante los graves daños que puede sufrir nuestra intimidad, dignidad, honor o cualquier otro derecho fundamental o no? Al respecto, concluyo con una frase del gran teórico canadiense, Northrop Frye, que dice: *“La máquina tecnológicamente más eficiente que el hombre ha inventado es el libro”*.

## VI. BIBLIOGRAFÍA

- ALEGRE MARTÍNEZ, Miguel Ángel, La dignidad de la persona como fundamento del ordenamiento constitucional español, Universidad de León, León, 1996.
- ALEGRE MARTÍNEZ, Miguel Ángel, El derecho a la propia imagen, Tecnos, Madrid, 1997.
- AGUILAR CABRERA, Denis Adán, Discusión sobre la ilegalidad de la prueba y la búsqueda de la impunidad, A propósito del caso Baltasar Garzón, Revista Derecho y cambio social, núm. 35, año 11, Perú, 2014.
- AGUSTINA SANLLEHÍ, José Ramón, Sexting en adolescentes: nuevos retos médico- legales, en Revista española de medicina legal: órgano de la asociación nacional de médicos forenses, Vol. 43, núm. 1, 2017.
- ÁLVAREZ CARO, María, Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la Era digital, Reus, Barcelona, 2015.
- ANARTE BORRALLO, Enrique, Delitos de descubrimiento y revelación de secretos, en: BOIX REIG, Francisco Javier (Coord.), en Derecho Penal, Parte especial, Vol. I, (La protección penal de los intereses jurídicos personales), Iustel, Valencia, 2016.
- ANDRÉS IBÁÑEZ, Perfecto, Caso Garzón: necesario distinguir, en Nuevo foro penal, núm. 77, 2011.
- BAJO FERNÁNDEZ, Miguel, El secreto profesional en el Proyecto de Código Penal, Anuario de Derecho Penal y Ciencias Penales, XXXIV, fascículo III, BOE, 1980.
- BENLLOCH PETIT, Guillermo, Obstrucción a la justicia y deslealtad profesional, en: SILVA SÁNCHEZ, Jesús María (Dir.) / RAGUÉS I VALLÉS, Ramón (Coord.), Lecciones de Derecho Penal, Parte especial, 4ª edición, Atelier, Barcelona, 2015.
- CASTIÑEIRA PALOU, María Teresa, Delitos contra la intimidad, en: SILVA SÁNCHEZ, Jesús María (Dir.) / RAGUÉS I VALLÉS, Ramón (Coord.), Lecciones de Derecho Penal, Parte especial, 4ª edición, Atelier, Barcelona, 2015.
- CASTELLÓ NICÁS, Nuria, Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor, en: MORILLAS CUEVA, Lorenzo (Dir.), Estudios sobre el Código Penal reformado, Dykinson, Madrid, 2015.



- CASTILLO JIMENEZ, Cinta, Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información, Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento, núm. 1, Huelva, 2001.
- CLAVERÍA GOSALBEZ, Luis Humberto, Notas para la construcción jurídica de los llamados derechos de la personalidad, Estudios de Derecho Civil en Homenaje al profesor J. Beltrán de Heredia, Universidad de Salamanca, Salamanca, 1984.
- COLÁS TURÉGANO, Asunción, Nuevas conductas delictivas contra la intimidad, en: GONZÁLEZ CUSSAC, José Luis (Dir.) / GÓRRIZ ROYO, Elena / MATALLÍN EVANGELIO, Ángela (Coords.), Comentarios a la reforma penal de 2015, 2ª edición, Tirant lo Blanch, Valencia, 2015.
- COMES RAGA, Ignacio, La protección penal de la intimidad a través de la difusión in consentida de sexting ajeno, La ley penal: Revista de derecho procesal, penal y penitenciario, núm. 105, 2013.
- CONTRERAS NAVIDAD, Salvador, La protección del honor, la intimidad y la propia imagen en Internet, Thomson Reuters Aranzadi, Navarra, 2012.
- DE CARRERAS SERRA, Lluís, Las normas jurídicas de los periodistas: Derecho español de la información, UOC, Barcelona, 2008.
- DE PIERO, Jose Luis, Prácticas juveniles éxtimas: sexting y vlogging, Aposta: Revista de ciencias sociales, núm. 69, 2016.
- DÍAZ GÓMEZ, Andrés, El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest, Revista Hologramática, Vol. 5, núm. 14, 2011.
- DOVAL PAIS, Antonio, Límites de la protección penal de la intimidad frente a la grabación de conversaciones e imágenes, en: BOIX REIG, Francisco Javier (Dir.) / JAREÑO LEAL, Angeles (Coord.), La protección jurídica de la intimidad, Iustel, Madrid, 2010.
- DOVAL PAIS, Antonio, Delitos de descubrimiento y revelación de secretos, en: BOIX REIG, Francisco Javier (Coord.), Derecho Penal, Parte especial, Vol. I (la protección penal de los intereses jurídicos personales), Iustel, Valencia, 2016.
- EVANGELINA NARVAJA, María, Prácticas juveniles éxtimas: sexting y vlogging, Aposta: Revista de ciencias sociales, núm. 69, 2016.
- ESPÍN, Eduardo, Derecho Constitucional, Vol. I. 6ª ed. El ordenamiento constitucional, Derechos y deberes de los ciudadanos, Tirant lo Blanch, Valencia, 2003.

- ESTRADA i CUADRAS, Albert, Delitos contra la intimidad, en: SILVA SÁNCHEZ, Jesús María (Dir.) / RAGUÉS I VALLÉS, Ramón (Coord.), Lecciones de Derecho Penal, Parte especial, 4ª edición, Atelier, Barcelona, 2015.
- GACITÚA ESPÓSITO, Alejandro Luis, El derecho fundamental a la protección de datos personales en el ámbito de la prevención y represión penal europea, (En busca del equilibrio entre la libertad y la seguridad), Tesis doctoral, Universitat Autònoma de Barcelona, Barcelona, 2014.
- GALLARDO ORTIZ, Miguel Ángel, Problemas morales de las intrusiones, grabaciones y escuchas: Hacia una ética del descubrimiento y la revelación de secretos, Tesis doctoral, Universidad Complutense de Madrid, Madrid, 2015.
- GARRIDO FALLA, Fernando, Ética y razón de Estado: los documentos del CESID y el caso GAL, Anales de la Real Academia de Ciencias Morales y Políticas, núm. 73, 1996.
- GONZÁLEZ MONTES, José Luis, La prueba ilícita (STC 114/1984, de 29 de noviembre), Persona y derecho: Revista de fundamentación de las Instituciones Jurídicas y de Derechos Humanos, núm. 56, Navarra, 2006.
- GONZÁLEZ PORRAS, Andrés José, Los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica, La vigilancia masiva, Tesis doctoral, Universidad de Castilla la Mancha, Toledo, 2016.
- JAÉN VALLEJO, Manuel, Delitos informáticos, en: JAÉN VALLEJO, Manuel / PERRINO PÉREZ, Angel Luis (Dirs.), La reforma penal de 2015, Dykinson, Madrid, 2015.
- JUANATEY DORADO, Carmen, Límites de la protección penal de la intimidad frente a la grabación de conversaciones e imágenes, en: BOIX REIG, Francisco Javier (Dir.) / JAREÑO LEAL, Angeles (Coord.), La protección jurídica de la intimidad, Iustel, Madrid, 2010.
- JORGE BARREIRO, Agustín, El delito de revelación de secretos (profesionales y laborales), La Ley: Revista jurídica española de doctrina, jurisprudencia, y bibliografía, núm. 3, 1996.
- JORGE BARREIRO, Agustín, en: COBO DEL ROSAL, Manuel (Dir.), Comentarios al Código Penal, Tomo VII, 1999, Edersa, Madrid, 1999.
- LIBANO BERISTAIN, Arantza, Los delitos de descubrimiento y revelación de secretos, Revista electrónica V/Lex España, Información jurídica inteligente, España, 2017.

- LIBANO BERISTAIN, Arantza, La perseguibilidad a instancia de parte como proyección de las facultades de la víctima, en: DE HOYOS SANCHO, Montserrat (Coord.), La víctima del delito y las últimas reformas procesales penales, Aranzadi, Valladolid, 2017.
- LONDOÑO TORO, Beatriz, El derecho a la intimidad, el honor y la propia imagen enfrentado a las nuevas tecnologías informáticas, Revista Facultad de Derecho y Ciencias Políticas, núm. 77, Colombia, 1987.
- LÓPEZ BARJA DE QUIROGA, Jacobo López, Los secretos de empresa, en: MORALES PRATS, Fermín / SANZ MORÁN, Ángel José (Dir.), Revista Aranzadi de Derecho y Proceso Penal, núm. 44, Thomson Reuters Aranzadi, Pamplona, Octubre - Diciembre 2016.
- LÓPEZ VALLEJO, Marco Roberto, Hacking ético, Vulnerabilidad de sistemas operativos en el acceso por contraseñas, Revista Publicando, Vol. 4, núm. 10, Ecuador, 2017.
- MARTÍNEZ OTERO, Juan María, La difusión de sexting sin consentimiento del protagonista: un análisis jurídico, Revista online especializada en Derecho de la Comunicación (Derecom), núm. 18, 2014.
- MENDO ESTRELLA, Álvaro, Delitos de descubrimiento y revelación de secretos: acerca de su aplicación al sexting entre adultos, Revista electrónica de ciencia penal y criminología, núm. 18, 2016.
- MONTIEL, Irene, Sexting en adolescentes: nuevos retos médico- legales, Revista española de medicina legal: órgano de la asociación nacional de médicos forenses, Vol. 43, núm. 1, España, 2017.
- MORALES PRATS, Fermín, La proyectada reforma de los delitos contra la intimidad a propósito del “Caso Hormigos”, Revista de derecho y proceso penal, núm. 31, España, 2013.
- MORALES PRATS, Fermín, en: QUINTERO OLIVARES, Gonzalo (Dir), Comentarios a la reforma penal de 2015, Thomson Reuters Aranzadi, Navarra, 2015.
- MUÑOZ CONDE, Francisco, Derecho Penal, Parte Especial, 20ª edición, Tirant lo Blanch, Valencia, 2015.
- NAVAS SÁNCHEZ, María del Mar, El uso informativo de la imagen, Indret: Revista para el análisis del derecho, núm. 1, enero, 2017.

- OLMO FERNÁNDEZ – DELGADO, Leopoldo, El descubrimiento y la revelación de secretos documentales y de las telecomunicaciones, Estudio del art. 197.1º del Código Penal, Dykinson, Madrid, 2009.
- ORTIZ DE URBINA GIMENO, Íñigo, Delitos contra la Administración Pública, en: SILVA SÁNCHEZ, Jesús María (Dir.) / RAGUÉS I VALLÉS, Ramón (Coord.), Lecciones de Derecho Penal, Parte especial, 4ª edición, Atelier, Barcelona, 2015.
- PÉREZ DE LA OSSA, Ana Vidal, Descubrimiento y revelación de secretos, Cuaderno jurídico, Práctica penal, núm. 86, Sepín, Madrid, 2017.
- PERRINO PÉREZ, Ángel Luis, Delitos informáticos, en: JAÉN VALLEJO, Manuel / PERRINO PÉREZ, Angel Luis (Dirs.), La reforma penal de 2015, Dykinson, Madrid, 2015.
- POLAINO NAVARRETE, Miguel, Descubrimiento y revelación de secretos, en: COBO DEL ROSAL, Manuel (Dir.), Curso de Derecho Penal español, Parte especial, I, Marcial Pons, Madrid, 1996.
- PUENTE ABA, Luz María, Difusión de imágenes ajenas en Internet: ¿ante qué delitos nos encontramos?, en: GONZÁLEZ CUSSAC, José Luis/ ORTS BERENGUER, Enrique /CARBONELL MATEU, Juan Carlos / CUERDA ARNAU, María Luisa (Coords.), Constitución, derechos fundamentales y sistema penal, (Semblanzas y estudios con motivo del setenta aniversario del profesor Tomás Salvador Vives Antón), Vol. II, Tirant lo Blanch, Valencia, 2009.
- RAGUÉS I VALLÉS, Ramón, Delitos contra la libertad, en: SILVA SÁNCHEZ, Jesús María (Dir.) / RAGUÉS I VALLÉS, Ramón (Coord.), Lecciones de Derecho Penal, Parte especial, 4ª edición, Atelier, Barcelona, 2015.
- RAMOS VÁZQUEZ, José Antonio, *Grooming y sexting*, en: GONZÁLEZ CUSSAC, José Luis (Dir.) / GÓRRIZ ROYO, Elena / MATALLÍN EVANGELIO, Ángela (Coords.), Comentarios a la reforma penal de 2015, 2ª edición, Tirant lo Blanch, Valencia, 2015.
- REY HUIDOBRO, Luis Fernando, La estafa informática, Relevancia penal del phishing y el pharming, La ley penal: Revista de derecho penal, procesal y penitenciario, núm. 101, 2013.
- RODRÍGUEZ LAINZ, José Luis, SITEL, Nuevas tendencias, nuevos retos, Diario la Ley, núm. 8082, 2013.

- RODRÍGUEZ LAINZ, José Luis, El secreto de las telecomunicaciones y su interceptación legal, Sepin, Madrid, 2016.
- RODRÍGUEZ MARIN, Fernando, Los delitos de escuchas ilegales y el derecho a la intimidad, Anuario de derecho penal y ciencias penales, tomo 43, fasc. 1, Madrid, 1990.
- ROMEO CASABONA, Carlos María, Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías, Revista Poder Judicial, núm. 31, 1993.
- RUEDA MARTÍN, M<sup>a</sup> Angeles, Protección penal de la intimidad personal e informática, Atelier, Barcelona, 2004.
- RUÍZ DORADO, María / VIDAL MARÍN, Tomás, Análisis de la constitucionalidad del SITEL, Breves consideraciones a partir de la LO 13/2015, de reforma de la Ley de Enjuiciamiento Criminal, Revista Aranzadi Doctrinal, núm. 9, España, 2016.
- RUIZ MARCO, Francisco, en: COBO DEL ROSAL, Manuel (Dir.), Comentarios al Código Penal, Tomo VII, 1999, Edersa, Madrid, 1999.
- SÁNCHEZ GARCÍA DE PAZ, Isabel, De las causas que eximen de la responsabilidad criminal, Art. 20.7 CP, en: GÓMEZ TOMILLO, Manuel (Dir.), Comentarios al Código Penal, 2<sup>a</sup> edición, Lex Nova, Valladolid, 2011.
- SÁNCHEZ RUBIO, Alfonso María, Ciberseguridad y hacking ético, Revista Auditoría interna: publicación periódica del Instituto de auditores internos de España, año 32, núm. 111, 2016.
- SERRANO BUTRAGUEÑO, Ignacio, Causas que extinguen la responsabilidad penal, en: SERRANO BUTRAGUEÑO, Ignacio (Coord.), Código Penal de 1995, (Comentarios y jurisprudencia), Comares, Granada, 1999.
- Servicios de Estudios y Publicaciones sobre la Constitución española. Trabajos parlamentarios, I, Cortes Generales, BOE, 1980.
- TOMÁS-VALIENTE LANUZA, Carmen, Del descubrimiento y revelación de secretos, en: GÓMEZ TOMILLO, Manuel (Dir.), Comentarios al Código Penal, 2<sup>a</sup> edición, Lex Nova, Valladolid, 2011.
- VILLANUEVA TURNES, Alejandro, El derecho al honor, a la intimidad y a la propia imagen, y su choque con el derecho a la libertad de expresión y de información en el ordenamiento jurídico español, Revista Díkaion, Vol. 25, núm. 2, 2016.

- VILLAVERDE MENÉNDEZ, Ignacio, Protección de datos personales, Derecho a ser informado y autodeterminación informativa del individuo, A propósito de la STC 254/1993, Revista Española de Derecho Constitucional, núm. 41, Mayo-Agosto, año 14, 1994.
- VILLAVERDE MENÉNDEZ, Ignacio, La intimidad, ese “terrible derecho” en la era de la confusa publicidad virtual, Revista Espaço jurídico, núm. 3, Vol. 14, 2013.
- WARREN, D. Samuel / BRANDEIS, D. Louis, El derecho a la intimidad, Traducido por Benigno Pendás y Pilar Baselga, Civitas, Madrid, 1995.

## **VII. JURISPRUDENCIA CITADA**

### **1. SENTENCIAS DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS**

Sentencia del Tribunal Europeo de Derechos Humanos núm. 5029/1971, de 6 de septiembre de 1978 (caso Klass versus Alemania)

Sentencia del Tribunal Europeo de Derechos Humanos núm. 8691/1979, de 4 de agosto de 1984 (caso Malone versus Reino Unido)

### **2. SENTENCIAS DEL TRIBUNAL CONSTITUCIONAL**

Sentencia del Tribunal Constitucional núm. 114/1984, de 26 de noviembre

Sentencia del Tribunal Constitucional núm. 172/1990, de 12 de noviembre

Sentencia del Tribunal Constitucional núm. 254/1993, de 20 de julio

Sentencia del Tribunal Constitucional núm. 104/1998, de 18 de mayo

Sentencia del Tribunal Constitucional núm. 134/1999, de 15 de julio

Sentencia del Tribunal Constitucional núm. 290/2000, de 30 de noviembre

Sentencia del Tribunal Constitucional núm. 292/2000, de 30 de noviembre

Sentencia del Tribunal Constitucional núm. 12/2012, de 30 de enero

Sentencia del Tribunal Constitucional núm. 115/2013, de 9 de mayo

Sentencia del Tribunal Constitucional núm. 7/2014, de 27 de enero

Sentencia del Tribunal Constitucional núm. 145/2014, de 22 de septiembre

Sentencia del Tribunal Constitucional núm. 2/2015, de 19 de enero

### **3. SENTENCIAS DEL TRIBUNAL SUPREMO**

Sentencia del Tribunal Supremo núm. 4191/1989, de 13 de mayo

Sentencia del Tribunal Supremo núm. 234/1999, de 18 de febrero

Sentencia del Tribunal Supremo núm. 1641/2000, de 23 de octubre

Sentencia del Tribunal Supremo núm. 49/2001, de 26 de enero

Sentencia del Tribunal Supremo núm. 574/2001, de 4 de abril

Sentencia del Tribunal Supremo núm. 224/2004, de 31 de marzo

Sentencia del Tribunal Supremo núm. 864/2008, de 16 de diciembre  
Sentencia del Tribunal Supremo núm. 906/2008, de 19 de diciembre  
Sentencia del Tribunal Supremo núm. 419/2009, de 5 de noviembre  
Sentencia del Tribunal Supremo núm. 1328/2009, de 30 de diciembre  
Sentencia del Tribunal Supremo núm. 1045/2011, de 14 de octubre  
Sentencia del Tribunal Supremo núm. 79/2012, de 9 de febrero  
Sentencia del Tribunal Supremo núm. 478/2012, de 29 de mayo  
Sentencia del Tribunal Supremo núm. 794/2012, de 11 de octubre  
Sentencia del Tribunal Supremo núm. 990/2012, de 18 de octubre  
Sentencia del Tribunal Supremo núm. 209/2013, de 6 de marzo  
Sentencia del Tribunal Supremo núm. 298/2013, de 13 de marzo  
Sentencia del Tribunal Supremo núm. 569/2013, de 26 de junio  
Sentencia del Tribunal Supremo núm. 424/2014, de 28 de mayo  
Sentencia del Tribunal Supremo núm. 525/2014, de 17 de junio  
Sentencia del Tribunal Supremo núm. 1945/2014, de 27 de noviembre  
Sentencia del Tribunal Supremo núm. 786/2015, de 4 de diciembre  
Sentencia del Tribunal Supremo núm. 40/2016, de 3 de febrero  
Sentencia del Tribunal Supremo núm. 407/2016, de 12 de mayo  
Sentencia del Tribunal Supremo núm. 509/2016, de 10 de junio  
Sentencia del Tribunal Supremo núm. 586/2016, de 4 de julio  
Sentencia del Tribunal Supremo núm. 201/2017, de 27 de marzo

#### **4. SENTENCIAS DE LAS AUDIENCIAS PROVINCIALES**

Sentencia de la Audiencia Provincial de Madrid, núm. 227/1999, de 26 de mayo  
Sentencia de la Audiencia Provincial de Pontevedra, núm. 314/2011, de 10 de noviembre  
Sentencia de la Audiencia Provincial de Álava, núm. 74/2013, de 7 de marzo  
Sentencia de la Audiencia Provincial de Granada, núm. 351/2014, de 5 de junio



Sentencia de la Audiencia Provincial de Vizcaya, núm. 90307/2014, de 23 de julio

Sentencia de la Audiencia Provincial de Cuenca, núm. 8/2015, de 13 de enero

Sentencia de la Audiencia Provincial de Vizcaya, núm. 43/2016, de 28 de julio

Sentencia de la Audiencia Provincial de Asturias, núm. 39/2017, de 15 de febrero

## **5. OTRAS RESOLUCIONES JUDICIALES**

Auto del Tribunal Constitucional núm. 257/1985, de 17 de abril