# Delitos contra la intimidad y otros derechos afines

PID_00267792

Alfonso Galán Muñoz

Tiempo mínimo de dedicación recomendado: 6 horas

Universitat Oberta de Catalunya

**Alfonso Galán Muñoz**

Profesor titular de Derecho penal de la Universidad Pablo de Olavide, doctor en Derecho y becario Formación de Profesorado Universitario (FPU) del Ministerio de Educación, de la Fundación Alexander von Humboldt y del Servicio Alemán de Intercambio Académico (DAAD). Ha realizado numerosas estancias de investigación en las universidades alemanas de Friburgo, Múnich, Tubinga y Berlín. Es experto en criminalidad informática y económica, temas a los que ha dedicado numerosas publicaciones, tanto nacionales como internacionales. Es investigador principal y miembro de varios proyectos de investigación nacionales y autonómicos, y responsable del Grupo PAIDI SEJ-571: Grupo de Investigación sobre el Sistema Penal y Criminología (SISPECRIM). También es el director del máster de Criminología y ciencias forenses de la Universidad Pablo de Olavide.

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Josep Maria Tamarit Sumalla (2019)

Primera edición: septiembre 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

# Índice

# Introducción

Si hay un valor ante el que la implantación y la expansión de las nuevas tecnologías se ha mostrado desde el primer momento como vulnerable, este es el referido a la intimidad.

No es solo que las nuevas tecnologías de la información y la comunicación hayan hecho posible que terceros puedan acceder a los miles de datos referidos a nuestras vidas privadas que almacenamos, en muchos casos de forma ciertamente descuidada, tanto en nuestros ordenadores como en nuestros cada vez más pequeños, pero también, según se nos dice, más inteligentes teléfonos móviles, o que hayan abierto la posibilidad de acceder y de seguir el normal discurrir de la vida de las personas de una forma tan amplia y precisa (videovigilancia, geolocalización, etc.), que a todos nos hace temer la posible implantación de un verdadero «gran hermano» cibernético que conozca hasta nuestros más oscuros secretos. Además, los ordenadores se mostraron, ya desde su nacimiento, como instrumentos tremendamente eficientes para poder acceder a muchos de tales secretos sin necesidad siquiera de tener que realizar las severas intromisiones en la esfera privada de las personas que supondrían, por ejemplo, la captación subrepticia de imágenes de su vida privada, la interceptación de alguna de sus telecomunicaciones o su seguimiento continuado. Bastaría con utilizar dichos sistemas para que el cruce automatizado de algunos datos personales, aparentemente inocuos (por ejemplo, los gastos realizados con su tarjeta de crédito, los referidos a los periódicos que consulta o las comidas que solicita en sus vuelos, etc.), facilitase perfiles de dichos sujetos que nos informarían sin problemas tanto sobre sus preferencias comerciales (algunas tal vez inconfesables) como sobre otros aspectos de su personalidad tan fundamentales para su intimidad como los referidos a su ideología política o sus creencias religiosas.

Los riesgos que el uso de estas nuevas tecnologías representan para la salvaguarda de la vida privada de las personas no son, por tanto, algo nuevo ni reciente, aunque, sin duda, el peligro que ha generado la implantación e imparable expansión de dichas tecnologías en nuestras vidas cotidianas no ha hecho sino aumentar a medida que convertíamos dichos sistemas en instrumentos y «confidentes» necesarios de nuestro día a día.

Precisamente para luchar contra estos riesgos, nuestro legislador ha venido creando nuevos tipos delictivos que tratan directamente de afrontar y neutralizar algunos de los peligros que el uso y el abuso de las nuevas tecnologías generan con respecto a la salvaguarda de la vida privada y la intimidad de los ciudadanos. Unos delitos cuyo número y amplitud típica no ha dejado de crecer durante los últimos años, a través de las sucesivas reformas realizadas de

nuestro Código penal, como consecuencia, entre otras cosas, de la aprobación de numerosas normas y convenios tanto a nivel internacional como supranacional.

Así, por ejemplo, cabe destacar la normativa contemplada respecto a esta cuestión en el celebre Convenio de Budapest del Consejo de Europa sobre ciberdelincuencia, de 8 de noviembre de 2001 y, sobre todo, la prolija normativa emitida por la Unión Europea, entre la que destacan, por su directa incidencia en varias de las reformas penales españolas de la materia que nos vamos a ocupar, la que contemplaba la Decisión Marco 2005/222/JAI, del consejo de Europa, y la que establece su sucesora, la vigente Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de ataques a sistemas informáticos (DAI), texto que, como veremos, ha tenido una directa y muy notable influencia en la redacción de muchos de los delitos contra la intimidad contenidos en los artículos 197 y siguientes de nuestro Código penal tras su todavía cercana reforma realizada por la LO 1/2015.

Fruto de este proceso de reformas, no siempre coordinadas entre sí, ni suficientemente meditadas, nos encontramos ante un texto normativo abigarrado y complejo, que contempla una serie de delitos y de tipos cualificados ciertamente difíciles de interpretar y de delimitar, lo que ha planteado infinidad de problemas tanto a la doctrina como a la jurisprudencia que ha tratado de definirlos y aplicarlos.

De hecho, su complejidad es tal que ha llevado a la doctrina a cuestionar y discutir hasta el contenido de los valores o intereses que muchos de estos delitos vendrían a proteger, ya que, si bien nadie cuestiona que algunos de estos delitos tutelan la **intimidad**, sí que se pone en tela de juicio que eso mismo se pueda predicar con respecto a todos. Así, mientras algunos autores se decantan por considerar que entre estas figuras se contienen algunas que protegen valores distintos de la intimidad, aunque conectados o afines con esta (por ejemplo, la denominada ***privacy***, el **derecho a la protección de datos de carácter personal**), otros llegan incluso a entender que también los hay que tutelan intereses completamente desconectados de dicho derecho fundamental, como sucede con la denominada **seguridad de los sistemas informáticos**, lo que, a su modo de ver, debería llevar a que estos delitos fueran extraídos del título en que actualmente están ubicados, para pasar a integrar uno específicamente referido a este nuevo interés tutelado.

En el presente módulo veremos cada uno de estos delitos y analizaremos cuál de estas posturas parece la más acorde con su actual configuración.

# Objetivos

Después de trabajar los materiales que componen este módulo didáctico, el estudiante podrá alcanzar los siguientes objetivos:

**1.** Conocer la polémica doctrinal y jurisprudencial relativa a la delimitación de los diferentes bienes jurídicos protegidos por los contra la intimidad y otros derechos afines.

**2.** Adquirir un conocimiento general de los ataques realizados a la intimidad mediante el uso de las nuevas tecnologías de la información y la comunicación que pueden llegar a tener relevancia penal.

**3.** Conocer la influencia que ha tenido la normativa procedente de la Unión Europea en la vigente regulación penal española relativa a los ataques contra la intimidad.

**4.** Comprender y ser capaz de diferenciar y aplicar los diferentes tipos delictivos protectores de la intimidad y otros derechos fines.

**5.** Tener un conocimiento general de la protección que otorga el derecho penal a los datos de carácter personal frente a determinados abusos.

**6.** Conocer y diferenciar las diferentes modalidades de interceptación de comunicaciones penalmente relevantes.

**7.** Tener un conocimiento general de los problemas específicos que plantea la protección penal de la intimidad y los derechos de los menores frente a las nuevas tecnologías.

**8.** Dar solución a los problemas concursales que plantean los delitos contra la intimidad analizados en este capítulo entre sí y también entre dichas figuras y otras contempladas en nuestro Código penal.

# 1. El delito de descubrimiento y revelación de secretos

El primero de los delitos referidos a la intimidad y a otros derechos afines o conexos es el de **descubrimiento y revelación de secretos**[1] del artículo 197.1 CP. En este precepto se establece que: «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».

(1)Art. 197.1 CP.

## 1.1. Bien jurídico protegido

Este precepto, cuya polémica y controvertida estructura básica se ha mantenido prácticamente inalterada desde la aprobación del Código penal de 1995, protege, a nuestro modo de ver, el derecho fundamental a la intimidad, contemplado en el artículo 18.1 CE en su versión más tradicional. Esto es, en la faceta que otorga el derecho a las personas a dejar lo que se estime conveniente de su vida al margen del posible conocimiento de terceros. El famoso derecho a ser dejado solo (*right to let be alone*).

Mucho se ha discutido sobre si este delito protegería también el derecho a la propia imagen, tal y como parece indicar tanto el título en el que se encuentra incardinado («Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio»), como el hecho de que su tipo de injusto sancione, entre otras, la conducta referida a la utilización de artificios técnicos de grabación o reproducción de la imagen. Sin embargo, en nuestra opinión, al requerir su injusto, como veremos, que también las conductas captadoras de la imagen de las que habla deban realizarse con el fin de «descubrir los secretos o vulnerar la intimidad de otro» para poder ser típicas del mismo, se hace evidente que la captación de imágenes solo será tenida como tal si se realiza para afectar a la intimidad de otro, convirtiéndose así el derecho a la intimidad en el valor cuya puesta en cuestión castiga el injusto del delito y, por tanto, también en el verdadero bien jurídico protegido por dicha modalidad comisiva.

Lo mismo sucede con el **derecho fundamental a la inviolabilidad o el secreto de las comunicaciones**[2] reconocido en el artículo 18.3 CE, derecho relacionado, aunque independiente de la intimidad que garantiza a los ciudadanos que ciertos medios comunicativos quedaran exentos de intromisiones ajenas no deseadas, con total independencia de que los contenidos que se trasmitan a través de ellos sean íntimos o no, para que estos puedan desem-

(2)Art. 18.3 CE.

peñar su vida privada y relaciones con total confianza en dichos medios. Pese a ser cierto que entre las modalidades comisivas de este delito se contempla la interceptación no autorizada de las telecomunicaciones o la utilización de artificios destinados a grabar su contenido, ambas actuaciones tan solo serán delictivas si se realizan para descubrir secretos o aspectos de la intimidad de otro, lo que nuevamente determinará que queden al margen de este delito los ataques exclusivamente referidos a dicha inviolabilidad que no estén, además, subjetivamente orientados a atacar a la intimidad de otro, lo que de nuevo convierte la **intimidad** en el verdadero bien jurídico tutelado también por dichas modalidades comisivas.

Sea como fuere, el delito ahora analizado contempla varias conductas que pueden ser realizadas mediante el uso de nuevas tecnologías y de la informática. Veámoslas.

### 1.2. Conductas típicas

El artículo 197.1 CP contiene toda una serie de posibles modalidades comisivas alternativas[3], cuya realización individual determina la automática consumación formal de su injusto, aunque, en realidad, la gran disparidad de muchas de las actuaciones contempladas más parece indicar que nos encontramos ante un precepto que contiene varios delitos diferentes, agrupados en un mismo artículo en razón del bien jurídico que protegen, que ante un único y verdadero delito.

(3) Art. 197.1 CP.

Dentro de estas posibles conductas típicas diferenciadas hay que destacar algunas por su clara naturaleza o referencia informática.

#### 1.2.1. El apoderamiento de correos electrónicos

La primera de las conductas contempladas en el artículo 197.1 CP con clara naturaleza informática es aquella que hace referencia al **apoderamiento de correos electrónicos**. En concreto, se castiga apoderarse sin consentimiento de «papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales». Mucho se ha discutido sobre la delimitación de la conducta de apoderamiento de correos electrónicos.

Para algunos (por ejemplo, Muñoz Conde, 2017), dado que el apoderamiento debe consistir, siempre y en todo caso, en un acto físico de toma o aprensión de algo material, solo se podrá apreciar la comisión de esta modalidad comisiva para los correos electrónicos en la medida en que la actuación recaiga sobre correos ya impresos, dado que la mera captación intelectual, o incluso la informática o digital de los mismos, dará lugar a la apreciación de la modalidad referida a la interceptación de las comunicaciones que, como veremos, con-

templa este mismo precepto, y no a un acto de apoderamiento propiamente dicho. Otros, sin embargo, mantienen que el concepto de apoderamiento referido a los e-mails debe ser interpretado atendiendo precisamente a la naturaleza claramente inmaterial e informática que tienen, lo que les lleva a entender que tendrían perfecta cabida en esta modalidad comisiva, por ejemplo, los actos de mera captación intelectual no consentida del mensaje trasmitido en un correo electrónico (Morales Prats, 2016).

A nuestro modo de ver, lo más correcto es mantener una interpretación amplia del concepto de apoderamiento referido a los correos electrónicos. En primer lugar, porque entendemos que la expresa alusión legal al correo electrónico como posible objeto material de esta modalidad comisiva solo tiene sentido en la medida en que se considera en su faceta no física, sino digital, ya que si el legislador hubiera querido limitar los apoderamientos típicos de dichos mensajes a los primeros, habría bastado con que hubiese dejado la referencia al apoderamiento de «papeles» o de «cualquier otro tipo de documento o efectos personales» para conseguir tal fin, sin necesidad, por tanto, de aludir expresamente a los mensajes de correo electrónico. Pero es que además, en segundo lugar, también consideramos que dicha interpretación es la más adecuada, porque, en realidad, a diferencia de lo que sostienen los defensores de la propuesta restrictiva, no creemos que se pueda mantener que todo acto de captación intelectual o digital de un correo electrónico dé automáticamente lugar a la apreciación de una interceptación de comunicaciones típica del artículo 197.1 CP, lo que podría determinar que, atendiendo a lo que comentaremos en el siguiente apartado, se generase una inadmisible laguna de punibilidad, dado que podría llevar a que todos aquellos actos de apoderamiento digital o intelectual del contenido trasmitido en un e-mail que se realizasen una vez acabado su proceso de transmisión, ni se pudiesen castigar como interceptaciones de comunicaciones, ni como conductas de verdadero apoderamiento, con lo que quedarían en la más absoluta atipicidad, pese a su manifiesta lesividad.

Ahora bien, una vez que se afirma que la captación electrónica y también la meramente intelectual de un correo electrónico tienen cabida en la modalidad de apoderamiento contemplada en esta figura, habrá que concretar entonces cuándo dichas captaciones podrían constituir, sin embargo, interceptaciones de comunicaciones también contempladas en el artículo 197.1 CP.

### 1.2.2. La interceptación de comunicaciones

Como ya hemos adelantado, el artículo 197.1 CP castiga con la misma pena a quien se apodera de documentos o correos ajenos y a quien intercepta las telecomunicaciones de otro. Es decir, a quien consiga hacerse con lo que otra persona trasmite mediante el uso de cualquiera de los sistemas de comunicación al uso, tanto digitales como analógicos.

Pese a lo controvertido que ha resultado concretar el ámbito de protección de este delito en lo que se refiere a los correos electrónicos, a nuestro modo de ver, lo más correcto es entender que, dado que la interceptación de las comunicaciones afecta y tiene que afectar a estas, es decir, a las comunicaciones, solo se podrá dar cuando se capte el contenido trasmitido mediante el uso de correos electrónicos durante el proceso comunicativo que va desde el envío de dichos mensajes hasta su recepción por su destinatario. Esto es, mientras se produce la comunicación, lo que, por otra parte, nos lleva a entender que si el mensaje ya ha sido recibido en el terminal del receptor y ha quedado allí almacenado, y un tercero consigue apoderarse de él bien porque consigue hacerse con una copia impresa o digital de su contenido, bien porque lo capta intelectualmente mediante su no deseada visualización, no habrá interceptado una comunicación, sino que simplemente se habrá apoderado del mensaje y, por tanto, solo podrá ser castigado mediante la modalidad comisiva de apoderamiento de la que hablamos en el epígrafe anterior.

**Lectura complementaria**

Véase lo establecido por los artículos 588 ter a y siguientes y artículo 588 sexies a y siguientes de la LEcrim, respecto a la posible habilitación legal para interceptar un correo electrónico o para acceder al sistema que contiene el mensaje una vez terminada la comunicación.

Similares consideraciones podrán hacerse en relación con otros sistemas de comunicación o mensajería, como podrían ser los mensajes de texto que nos enviamos a través de los teléfonos móviles o los que trasmitimos y recibimos a diario a través de algunas redes sociales de comunicación como WhatsApp o Telegram, dado que, a pesar de que dichos mensajes digitales no aparecen expresamente citados en el artículo 197.1 CP, su trasmisión sí que tendrá perfecta cabida en el concepto de telecomunicación, pudiendo considerarse que cuando esta acaba, sus mensajes quedarán protegidos frente a posibles apoderamientos digitales o intelectuales atendiendo a que dicha modalidad comisiva también permite castigar la realización de tal conducta con respecto a «cualesquiera otros documentos», algo que, sin duda, todos estos mensajes son, especialmente si se tiene en cuenta la amplia definición de documento que establece, a efectos penales, el artículo 26 de nuestro Código penal.

Habrá que entender, por tanto, que la interceptación de comunicaciones castigada en este delito se podrá apreciar tanto cuando se interceptan de forma no autorizada las llamadas realizadas a través de teléfono fijo o móvil, como cuando se hace lo propio con las que se efectúan mediante otros sistemas de telecomunicación personales y privados (Skype, WhatsApp, etc.) o con los mensajes que se trasmiten y comunican en todo tipo de chats privados, no abiertos al conocimiento público, mientras que todos estos mensajes quedarán protegidos frente a posibles accesos intrusivos no autorizados, una vez estén almacenados en los ordenados de sus destinatarios, mediante la posible apreciación de la modalidad de apoderamiento de documentos anteriormente comentada.

Un sector doctrinal (por ejemplo, Muñoz Conde, 2017; Colás Turégano, 2015), apoyándose en algunas resoluciones judiciales (como la ST AP Huesca de 21 de septiembre de 2001), se ha decantado por trasladar la exigencia de la utilización de los artificios técnicos de escucha, trasmisión, grabación o reproducción de la que habla la siguiente modalidad comisiva del artículo 197.2 CP también a la relativa a la efectiva consecución de la interceptación, lo que, si bien tiene una encomiable finalidad limitadora del amplio ámbito típico de este delito, no podemos compartir. Y no podemos hacerlo porque dicha interpretación no se ajusta al tenor literal del precepto analizado, contrasta con que en otros delitos del código se aluda a la necesidad de utilizar tales instrumentos para realizar las interceptaciones que sancionan (por ejemplo, art. 197 bis.1 CP) y, además, tampoco parece compaginarse demasiado bien con el hecho de que el artículo ahora analizado castigue con la misma pena al que intercepta una telecomunicación que al que simplemente emplea dichos aparatos para hacerlo.

De hecho, mucho más lógico resulta, a nuestro modo de ver, pensar que es precisamente el mayor desvalor de acción que representa el uso de dicho tipo de instrumentos o artificios de escucha o interceptación frente a la posible interceptación conseguida mediante, por ejemplo, la mera escucha subrepticia realizada usando un teléfono supletorio mientras otro habla (conducta dotada, sin duda, de mayor desvalor del resultado que la de la mera instalación de aparatos o instrumentos de escucha, pero también de menor desvalor de acción), lo que justificará que ambas actuaciones se castiguen con la misma pena por este delito, aun cuando el empleo de los referidos aparatos no consigan su propósito interceptador.

### 1.2.3. La utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación

Como hemos visto, interceptar supone apoderarse de algo antes de que llegue a su destino, con lo que la modalidad comisiva analizada en el apartado anterior solo se completará en el momento en que quien la realice llegue realmente a hacerse con el contenido de lo trasmitido, algo que no siempre es fácil de demostrar. Tal vez por ello, el legislador decidió en su día castigar con la misma pena a quien intercepta una comunicación y a quien simplemente «utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación».

**Aplicación de penas**

Se permitiría así castigar con la misma pena al que, por ejemplo, utilizando un programa espía (*sniffer*), consigue hacerse con el contenido trasmitido desde un ordenador a un tercero y a quien simplemente instalase dicho programa en el ordenador para conseguirlo, pero no alcanzase su objetivo.

Debe señalarse, en cualquier caso, que el uso de las nuevas tecnologías ha ampliado exponencialmente el ámbito de aplicación de esta última modalidad comisiva, la referida a la utilización de artificios técnicos no solo de escucha, grabación o reproducción del sonido, sino también, no lo olvidemos, de la

imagen o de cualquier otra señal de comunicación, ya que, además de que cada vez es más frecuente que incluso personas sin especiales conocimientos informáticos se hagan e instalen programas en los terminales de terceras personas que les permiten interceptar las comunicaciones que éstas realizan mediante el uso de dichas tecnologías, también lo es que se empleen otros programas (troyanos, virus, etc.) que permiten controlar las cámaras y/o micrófonos de los propios terminales de dichos sujetos (móviles, ordenadores o incluso los televisores inteligentes), convirtiéndolos así en verdaderos aparatos de escucha y trasmisión de sus conversaciones y/o de su imagen, con la grave puesta en peligro que ello supone para su intimidad. Evidentemente, en todos estos casos, la mera instalación de dichos programas o artificios dará lugar, por sí sola, a la consumación del delito que venimos analizando, sin ser necesario, por tanto, tener que acreditar para hacerlo que se emplearon de forma exitosa y permitieron realmente que se llegase a escuchar, grabar o trasmitir, de forma clandestina y no consentida, alguna imagen o sonido referido a sus posibles víctimas, algo que, como ya vimos, es castigado por la modalidad precedente.

### 1.3. Elementos comunes a todas las conductas contempladas en el artículo 197.1 CP

Para que cualquiera de las conductas anteriormente descritas llegue a ser típica del delito contemplado en el artículo que venimos comentando, deberá realizarse concurriendo una serie de circunstancias.

En primer lugar, tendrán que haberse efectuado **sin el consentimiento del titular del secreto** que se pretende descubrir.

Esta exigencia es muestra evidente del carácter netamente disponible de la intimidad como bien jurídico protegido. Es dicho carácter el que determina que si su titular consiente expresa o tácitamente la intromisión realizada por un tercero, esta pase a ser completamente irrelevante a efectos penales y atípica. En cualquier caso, para que el consentimiento sea efectivo, debe ser emitido por una persona dotada de capacidad y legitimación para darlo, lo que, entre otras cosas, debe ser muy tenido en cuenta a efectos de analizar las posibles actuaciones realizadas en relación con la intimidad de los menores.

**Derecho a la intimidad de los menores**

Los menores tienen reconocido expresamente el derecho a la intimidad en el artículo 4 de la Ley orgánica 1/1996, de 15 de enero, de protección jurídica del menor, de modificación del Código civil y de la Ley de enjuiciamiento civil, precepto que les otorga una protección cualificada, que, entre otras cosas, habilita al Ministerio Fiscal para intervenir en salvaguarda de su intimidad, incluso en algunos casos en que conste el consentimiento del menor a la intromisión producida o, también, el de sus representantes legales.

Precisamente, es el artículo 3 de la referida Ley orgánica el que autoriza a los menores a que gocen del grado de madurez suficiente para poder disponer de su intimidad sin necesidad de consentimiento de sus tutores, mientras que el apartado 5 del artículo 4 de la LO 1/1996 establece que sus padres o tutores estarán obligados no solo a proteger, sino también a respetar el derecho a la intimidad de los menores, lo que ha planteado serias dudas a hora de determinar si estarán habilitados legalmente o no para, por ejemplo, poder acceder sin su consentimiento a los correos electrónicos que dichos menores se envíen o a lo que publican en sus redes sociales, incluso si lo hacen con el muy loable

**Lectura complementaria**

Sobre la viabilidad y eficacia del consentimiento exclusivo del menor, dotado de madurez suficiente para ello, véase el artículo 3 de la LO 1/1982, de 5 de mayo.

fin de protegerlos de los posibles ataques que les podrían dirigir terceros mediante el uso de las nuevas tecnologías.

A nuestro modo de ver, el hecho de que los padres y tutores sean los destinatarios del deber de proteger a los menores bajo su patria potestad o tutela frente a los múltiples ataques que pueden sufrir, también hace que se les otorgue el legítimo derecho a limitar la intimidad del menor cuando ello sea necesario para cumplir con dicha obligación protectora, con lo que, siempre que haya cualquier indicio de posible afectación de los derechos de los menores, las intervenciones que realicen sus padres o tutores sobre su intimidad o la inviolabilidad de sus comunicaciones se efectuarán de forma justificada por haber sido ejecutadas en cumplimiento del deber tuitivo que le dirige el ordenamiento jurídico.

Sin embargo, ante la falta de indicios racionales sobre la existencia de dichos ataques y gozando el menor de la madurez que le habilitaría legalmente para poder disponer, sin autorización de sus padres o tutores, de su derecho a la intimidad, estos últimos no podrán realizar controles de sus comunicaciones, limitando así su intimidad sin violar dicho derecho fundamental del menor. Esto, evidentemente, impide que los padres puedan establecer controles generalizados y sistemáticos de las comunicaciones realizadas por los menores dotados de dicha madurez, por más que los quisiesen implantar con la muy loable finalidad de proteger y salvaguardar al menor y creyendo que tienen derecho a hacerlo, lo que, sin embargo, podrá y deberá ser tenido en cuenta a la hora de apreciar el correspondiente error de prohibición, generalmente vencible, que también se tendrá que apreciar si hubiesen actuado pensando erróneamente que el menor no gozaba de la madurez que le permitiría disponer de su intimidad sin su supervisión y autorización.

Por otra parte, por lo que respecta a la **tipicidad subjetiva** de estos delitos, nos encontramos ante figuras eminentemente dolosas, lo que determinará que queden en la más absoluta atipicidad todas aquellas intromisiones que se realicen en la intimidad de otra persona por error.

**Ejemplos de atipicidad**

Por ejemplo, la interceptación no deseada de una llamada telefónica realizada al descolgar el teléfono supletorio de una línea mientras un tercero habla o el acto de lectura de un e-mail ajeno recibido por error como consecuencia de la equivocación en la dirección de envío por parte de su emisor.

No obstante, la configuración subjetiva de este delito queda ciertamente limitada por la expresa exigencia de que todas sus posibles conductas típicas (las de apoderamiento, las de interceptación de comunicaciones y las de uso de artificios técnicos) tengan que ser realizadas «para descubrir los secretos o vulnerar la intimidad de otro». Esta exigencia típica introduce un especial elemento subjetivo en el injusto de este delito que lo convierte en un delito de tendencia interna trascendente y mutilado en dos actos, lo que tiene importantes efectos.

En primer lugar, resulta evidente que si el autor de este delito ha de actuar necesariamente para descubrir los secretos o afectar a la intimidad de otro, esto es, con la intención de conseguir cualquiera de dichos fines, se excluye de forma completa la posible comisión de este delito con un mero dolo eventual respecto a la posible producción de alguno de tales resultados. No bastará, por tanto, con que el sujeto realice, por ejemplo, un acto de apoderamiento de un documento simplemente sabiendo que tal vez en el mismo pueda recogerse algún secreto, sino que se necesitará que lo haga con el propósito y el fin precisamente de descubrir el secreto que pensaba que contenía el documento en cuestión.

Por otra parte, dado que todas sus conductas típicas tienen que haber sido llevadas a cabo con dicha finalidad, se excluirá la posibilidad de que este delito pueda llegar a castigar los actos de apoderamiento o interceptación realizados

con un propósito distinto, como, por ejemplo, los actos de apoderamiento de cartas que se efectúen por pensar que en su interior había dinero o los que recaigan sobre efectos que se sabía que no podrían contener ningún contenido que pudiese afectar a la intimidad (por ejemplo, de un simple folleto publicitario de descuento dejado en el buzón del venido mediante «buzoneo» generalizado). Del mismo modo, también quedarán al margen de esta figura los actos de apoderamiento o de interceptación que no se realicen movidos por ninguna de dichas finalidades, por más que una vez realizados alguna de ellas pudiese aparecer, con lo que, por ejemplo, no será típico de este delito el acto que realiza aquel sujeto que, tras haberse apoderado de un correo electrónico ajeno por creer que contenía un contrato públicamente conocido, pero que se quería destruir, una vez descubierto que el documento no era tal, sino una carta privada de un tercero, se decidiese leer su contenido para afectar así a su intimidad, ya que en esos casos, el acto de apoderamiento inicialmente realizado, aunque doloso, no se habría efectuado con la finalidad exigida por este tipo delictivo.

Por último, solo resta por señalar que la exigencia de este especial elemento subjetivo del injusto determina que nos encontremos ante un delito que no necesitará que el sujeto que lo efectúe tenga que conseguir su objetivo y, en consecuencia, llegue a descubrir aspectos secretos o informaciones de la intimidad de su sujeto pasivo para considerar que había realizado y consumado su injusto.

Bastará con que el sujeto se apodere, por ejemplo, físicamente de un e-mail ajeno sin llegar a leer su contenido, instale aparatos de grabación de las comunicaciones realizadas por Internet por un tercero pero no los llegue a captar o intercepte de forma efectiva el contenido trasmitido sin llegar a conocerlo para que se pueda apreciar este delito en su modalidad consumada. Lo mismo que sucederá si quien realiza cualquiera de las actuaciones anteriores con los referidos fines, consigue acceder al contenido del correo electrónico sustraído o de la videoconferencia interceptada, resultando finalmente que estos no están referidos a ningún secreto de su emisor (por ejemplo, se intercepta una videconferencia realizada por Internet para descubrir secretos de los interlocutores, pero resulta que en la misma estos solo se comunicaban cosas públicamente conocidas o completamente irrelevantes en términos de su intimidad, como el tiempo que hacía en la ciudad en que cada uno de ellos estaba).

## 2. El delito de abuso de datos de carácter personal

Como ya señalamos, el hecho de que los sistemas informáticos representen un riesgo para la protección de la intimidad de las personas no es algo recientemente descubierto. De hecho, ya en el año 1978 nuestro constituyente fue consciente de que dichos sistemas pueden ser utilizados para cruzar datos referidos a las personas, aparentemente inocuos o irrelevantes, pero que, si se procesan de la forma adecuada, permitirían obtener perfiles respecto a dichos sujetos que aporten informaciones tremendamente precisas referidas a sus vidas privadas, lo que sin duda representa un gran peligro para su intimidad. Precisamente por ello, nuestro constituyente decidió establecer, en el artículo 18.4 de nuestra carta magna, que «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

Pese a lo claro del mandato constitucional, lo cierto es que no fue sino hasta catorce años más tarde cuando nuestro legislador trató de darle un primer cumplimiento mediante la aprobación de la Ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal (LOTADP). Esta norma fue profundamente reformada para cumplir con lo exigido por la Directiva 1995/46/CE, de 24 de octubre, cuyo articulado fue determinante en la reforma efectuada con la aprobación de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPDP), que se ha mantenido vigente hasta tiempos bien recientes.

Precisamente, ha sido de nuevo un mandato europeo (el contenido en el vigente Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, por el que se deroga la Directiva 95/46/CE [RGPD]) el que ha llevado a la todavía reciente aprobación de la nueva Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), que constituye, desde su entrada en vigor el día 7 de diciembre de 2018, junto con el reglamento comunitario antes señalado (no olvidemos que con eficacia directa en nuestro ordenamiento), uno de los dos principales, aunque no únicos, referentes normativos de la protección de los datos de carácter personal en nuestro país.

No obstante, mucho antes de esta última reforma, nuestro Código penal ya estableció un delito tendente, precisamente, a proteger a los ciudadanos frente a algunos de los ataques más graves que se les pueden dirigir mediante el **uso de sus datos de carácter personal**[4]. Se trata del contemplado en el artículo 197.2 CP, en el que se establece que: «Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, da-

(4)Art. 197.2 CP.

tos 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».

Como se puede comprobar, la redacción del comentado precepto resulta compleja, farragosa y en ocasiones repetitiva, pese a lo cual, y aunque no han sido pocas las posibilidades que ha tenido el legislador desde su aprobación inicial para mejorarla y aclararla, se ha mantenido inalterada. De hecho, como vamos a comprobar, todo o casi todo en lo que se refiere a este delito es objeto de controversia, comenzando, como no podía ser de otra forma, por la propia delimitación de su bien jurídico protegido.

### 2.1. El bien jurídico protegido

Como ya hemos señalado, la delimitación del bien jurídico protegido por este delito resulta extremadamente controvertida.

Algunos autores señalaron inicialmente, atendiendo a su ubicación sistemática dentro de los delitos contra la intimidad, que lo que esta figura protegía era precisamente dicho valor, es decir, la intimidad. Sin embargo, esta postura fue pronto rechazada por la mayor parte de la doctrina, que entendió que el referido derecho fundamental –cuando menos en su concepción tradicional, que aludía a un derecho negativo o de exclusión a terceros respecto a la vida privada de cada uno (el anteriormente citado derecho a ser dejado solo)– no terminaría de casar con las facultades y los derechos positivos de información y control que la normativa administrativa otorga al ciudadano con respecto a sus datos personales, y que este delito parecía proteger, lo que determinaba que sancionase conductas tales como, por ejemplo, las de mera utilización no autorizada de los datos personales ajenos, algo que evidentemente puede y suele hacerse sobre datos ajenos que el autor de esta conducta ya tendría en su poder, con lo que no afectaría en nada al derecho de su titular a conservarlos en secreto.

Por ello, teniendo en cuenta precisamente esos derechos positivos de control informativo, algunos autores optaron por entender que el bien jurídico de esta figura era el denominado **derecho a la privacidad informática**, que otorgaría al ciudadano un nuevo *habeas* (*el habeas data*) que garantizaría su derecho a la autodeterminación informativa con respecto a sus datos personales que hubiesen sido informatizados. Sin embargo, esta postura también fue rechazada por otros que señalaron, con acierto, a nuestro juicio, que tras la reforma realizada por la LO 15/1999 (LOPD) a resultas de lo exigido por la Directiva 95/46/CE, los datos personales se protegían y han de seguir protegiéndose, tanto penal como administrativamente, con independencia del formato en que estu-

viesen contenidos o archivados, ya fuese este digital o no, o de cómo se procesasen (informática o físicamente), lo que impedía que se pudiese considerar la privacidad informática como el valor tutelado por el delito ahora analizado.

Este hecho, llevó a que otro sector doctrinal se decantase por considerar que lo protegido por este delito sería, en realidad, el derecho a la autodeterminación informativa, que otorgaba potestades positivas a los ciudadanos para controlar, e incluso denegar, que terceros pudiesen tener o recibir sus datos sin su conocimiento y consentimiento, y que, por otra parte, algunos entendiesen que, en realidad, dicho supuesto nuevo derecho solo se presentaría como la faceta o el reverso positivo del nuevo concepto de intimidad definido por nuestro TC, que otorgaba, junto a su faceta tradicional negativa o individual, también una positiva y social que permitía que toda persona tuviese poderes sobre la información relativa a su persona (como respaldo de esta visión de la intimidad, véase, por ejemplo, la STC 134/1999, de 15 de junio).

Pese a lo sugerente de esta propuesta y al hecho de que haya sido acogida por un importante y nutrido grupo de penalistas, consideramos que la misma no permite delimitar en su concreta medida el valor que el delito del artículo 197.2 CP viene a proteger. No lo hace, en primer lugar, porque como ya señaló en su día Romeo Casabona (2004), por más que se integren en la intimidad derechos positivos de control sobre la información relativa a una persona, dicho derecho fundamental seguirá girando en torno al concepto de vida privada, lo que no se corresponde, o no se tendría que corresponder, como veremos, con la naturaleza de los datos que quedan protegidos por el delito ahora analizado, ya que tales datos no siempre tienen que estar referidos a esa esfera de la vida de una persona, ni tampoco han de ser desconocidos o secretos para la generalidad de la sociedad.

Por otra parte, tampoco parece que la referida propuesta case con el hecho de que el delito ahora analizado castigue conductas tales como la de alterar o manipular los datos de una persona, algo que sin duda lesiona el derecho a la fiscalización de la calidad y la corrección que todo sujeto tiene sobre los datos que se refieren a él mismo, pero que, por una parte, no afecta directamente a su derecho a controlar la difusión de sus datos (su supuesto derecho a la autodeterminación informativa) y, por otra, incluso puede ser precisamente lo que impida que los datos alterados puedan servir para llegar a conocer aspectos reales de la vida privada que el derecho a la intimidad, incluso con su nueva faceta positiva, vendría a proteger (Galán Muñoz, 2013).

Por eso consideramos que la única manera de delimitar de forma correcta el bien jurídico tutelado por la figura que estamos analizando es precisamente considerar que viene a proteger el derecho fundamental que toda persona tiene a controlar no solo la distribución, sino también cuándo y con qué límites se pueden procesar y utilizar sus datos de carácter personal. **El derecho a la protección de datos de carácter personal** que el artículo 18.4 de nuestra constitución obliga al legislador nacional a tutelar, y que tanto nuestro Tribunal Constitucional, en su STC 292/2000, como el propio texto de la nueva LOPDGDD, en su preámbulo, consideran un derecho conectado, pero diferente, autónomo y más amplio que el referido a la intimidad.

## 2.2. El objeto material: la compleja delimitación de los datos personales

Llama poderosamente la atención el hecho de que el delito del artículo 197.2 CP no venga a proteger todos los datos de carácter personal frente a las conductas que contempla su tipo de injusto, sino solo algunos. En concreto, el referido precepto solo protege los «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»[5].

(5)Art. 197.2 CP.

Para definir esta compleja delimitación típica, se ha de acudir a la normativa extrapenal referida a la misma. Una normativa que, como ya hemos señalado, ha sufrido numerosas y profundas modificaciones a lo largo del tiempo, cambios que, sin embargo, no han encontrado adecuado reflejo en la regulación penal de este delito, lo que, como tendremos ocasión de comprobar, ha dado lugar a numerosos problemas.

Lo primero es definir qué ha de entenderse por datos reservados de carácter personal o familiar.

Por **dato de carácter personal o familiar** habrá que entender, conforme a lo establecido en el artículo 4.1 del RDPD, «toda información sobre una persona física identificada o identificable ("el interesado")», señalando a continuación que: «se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona».

Estamos hablando, por tanto, de datos como el nombre, los apellidos, números de identificación fiscal, etc. Pero también de otros como las imágenes, los biológicos o biomédicos que permitan identificar a una persona y el sin fin de datos de nuevo cuño que nos identifican en muy diferentes esferas. Nuestro número de teléfono móvil, nuestra dirección de correo electrónico, el perfil de la red social que utilizamos o el avatar del juego en línea con el que nos entretenemos son, sin duda, informaciones que nos identifican directamente o que, cuando menos, permiten identificarnos de forma indirecta, con lo que tienen que ser considerados como datos personales susceptibles de ser tutelados por el delito que venimos analizando. Se pueden proteger así todos esos datos de nuevo cuño que permiten el desarrollo de ese verdadero «ecosistema de identidades» (sobre todo digitales) en el que hemos empezado a vivir.

De hecho, la protección de los datos de carácter personal, como hemos señalado, se extiende a los datos referidos no solo a personas identificadas, sino identificables, lo que, como establece el Reglamento comunitario anteriormente citado (RGPD), en su considerando 26, determina que se consideren penalmente protegidos los datos relativos a un persona incluso si han sido seudonimizados. Esto es, si han sido tratados «de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable» (art. 4.5 Reglamento 2016/679).

Ahora bien, para que cualquiera de estos datos pueda recibir la protección penal que otorga a su titular el artículo 197.2 CP, tendrán que ser datos «**de otro**», «**reservados**» y «**que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado**».

Lo primero determina que quede al margen de este tipo delictivo cualquier conducta que el titular de los datos personales en cuestión (la persona a la que identifican o pueden identificar) pueda efectuar sobre sus propios datos, aun cuando dicha conducta resulte ilegal y se realice sobre los datos que tenga almacenados un tercero en algún fichero, conducta que, sin embargo y evidentemente, en algunos casos podrá determinar la apreciación de otros delitos diferentes al aquí analizado, como podría ser el de daños informáticos.

Lo segundo, por su parte, exigir que los datos tengan que ser «reservados», ha sido objeto de una gran controversia doctrinal, porque en ningún lugar de la anterior LOPDP o de la actualmente vigente LOPDGDD se define expresamente qué habría de entenderse por tal clase de datos.

Para algunos serán datos reservados los que no sean de público conocimiento. Otros, por el contrario, proponían considerar por tales los datos especialmente protegidos por su carácter especialmente sensible (los relativos a la ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico de los que hablaba el art. 7 de la LOPDP, ya derogada). No faltaron quienes, considerando que lo que esta figura venía a proteger era la privacidad informática frente a los peligros que se derivaban del posible cruce de datos mediante la utilización de sistemas de dicha naturaleza, optaron por entender que en realidad se protegían todos los datos de carácter personal que pudiesen ser tratados informáticamente, con independencia de a qué aspecto de la vida de la persona estuviesen referidos o de si eran conocidos o no.

A nuestro modo de ver, ninguna de estas posibles interpretaciones resulta acertada.

La primera porque convertiría esta figura en una suerte de modalidad específica del delito de revelación de secreto del artículo 197.1 CP, protector de la intimidad en su sentido más tradicional o negativo, algo que, como ya hemos visto, no se corresponde con la naturaleza de esta figura ni con la de las conductas que viene a castigar. La segunda, porque tanto antes como ahora, cuando las conductas analizadas recaigan sobre los datos sensibles a los que alude, darían lugar a la apreciación de un tipo cualificado de este delito (el ahora contemplado en el art. 197.5 primer inciso CP), lo que evidencia que no serán solo dichos datos los que se protegen y tutelan en la modalidad básica de esta figura. Mientras que la última, además de que, como ya vimos, no se corresponde con la verdadera finalidad protectora de este delito que tutela tanto datos informatizados como los que no lo son, por otra parte, al haber considerado que este delito solo podría proteger datos informatizados por ser los únicos que podrían afectar a la *privacy*, convertiría la exigencia de que los datos tuviesen que ser informáticos para ser reservados en algo redundante, intrascendente y carente de cualquier clase de utilidad.

En realidad, la delimitación de este elemento se tiene que efectuar teniendo en cuenta, precisamente, los cambios legislativos producidos en relación con esta materia en el ámbito extrapenal. En concreto, consideramos que se debe definir atendiendo a lo que en su día establecía el artículo 1 del RD 1332/1994, que desarrollada la LOTADP, precepto que definía los datos «accesibles al público» señalando que serían los que se encontraban «a disposición del público en general, no impedida por cualquier norma limitativa», lo que permitía considerar como reservados precisamente todos aquellos que no procediesen de dichas fuentes. Esta fácil interpretación se oscureció notablemente como consecuencia de la aprobación del también ya derogado artículo 3 LOPDP, que pasó a aludir a las «fuentes accesibles al público» y no a los datos, fuentes que, sin embargo, se definían en el todavía vigente artículo 7.2 del RD 1701/2007, de 21 de diciembre, como «aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, sin más exigencia que, en su caso, el abono de una contraprestación». El cambio de denomi-

nación legislativa producido no tuvo reflejo alguno en la delimitación del delito que venimos analizando, lo que determinó que se produjese una descoordinación entre dicha figura y la normativa administrativa que delimitará los datos que son públicamente accesibles y los que son reservados, descoordinación que lamentablemente se ha mantenido y se mantiene a día de hoy, por lo que tanto la vigente LOPDGDD (véase, por ejemplo, su DA tercera, dos) como el Reglamento general de protección de datos (por ejemplo, en su art. 14.2.f) hablan de «fuentes de acceso público» y no de los datos accesibles como tales.

En cualquier caso, pese a que la falta de adaptación penal a los cambios normativos administrativos producidos haya dificultado la interpretación de este elemento típico, parece lógico pensar que cuando el Código habla de datos reservados, está aludiendo a datos que no se pueden obtener libremente. Es decir, a aquellos que no se hayan obtenido de alguna de las fuentes accesibles o de acceso público de las que habla la normativa administrativa vigente, con lo que habrá que entenderse que todos los datos personales que se obtengan de un lugar diferente de dichas fuentes (aunque fuesen conocidos) deberán ser considerados como reservados, por lo que pueden ser por ello objeto material de este delito, que los tutelará frente a sus usos y abusos contemplados en el artículo 197.2 CP.

Sin embargo, para ello los datos «reservados» y «de otro» en cuestión tendrán que estar «registrados en ficheros», informáticos o no, ya sean públicos o privados. Por registro hay que entender una de las fases del posible procesamiento de datos, que consiste en su inclusión en un fichero, entendiéndose por tal, conforme establece el artículo 4.6 del RGPD, «todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica».

Esto determina que no se consideren incluidos en ficheros y, por tanto, no gocen de la protección del artículo 197.2 CP los datos personales que no se encuentran recogidos junto con otros y los que, estándolo, lo hagan de tal forma que no permitan su ordenación u localización dentro del conjunto. Solo cuando tengamos unos datos personales que estén registrados (incluidos, almacenados) con otros en un fichero que permita su indexación y organización, y dicho fichero no constituya una fuente de acceso público, tendremos datos susceptibles de ser objeto del delito del que nos venimos ocupando, consideración que será independiente, además, por expresa decisión legislativa, de si dicho fichero tiene naturaleza informática o no (cabe que los datos estén en ficheros físicos, como archivadores, etc.) y de si el fichero tiene naturaleza pública o privada (desde el fichero de datos que tenga una Administración pública para el cumplimiento de sus fines hasta el que tenga, por ejemplo, un empresario o un particular para los suyos).

No obstante, antes de su registro, esto es, antes de que los datos estén incluidos y registrados en uno de los referidos ficheros, el artículo 197.2 CP resultará completamente inoperante a efectos de sancionar las conductas lesivas que se

puedan realizar sobre los datos de terceros, lo que determinará, por ejemplo, que aunque se consigan recoger o captar datos personales de terceros de forma ilícita, por ejemplo, mediante engaño o cualquier otra técnica de ingeniería social (por ejemplo, mediante su captación por *phishing* o *pharming*), dicha actividad se mantenga al margen del ámbito típico de este delito mientras los datos personales recopilados no pasen a estar incluidos junto con otros en un fichero que permita su organización y clasificación. Esto es, mientras no estén en un verdadero fichero, y no se realice sobre los mismos alguna de las conductas prohibidas por este delito.

Algunos autores (Puente Aba, 2007) han considerado que los datos recogidos ilegalmente, incluso si se incluyen en ficheros y se usan o modifican en perjuicio de su titular, siguen sin estar amparados por el delito aquí comentado, ya que, a su modo de ver, no puede considerarse que estén realmente registrados, al haberse creado el fichero en el que se incluyeron ilegalmente y no haberse comunicado su existencia a la Agencia Nacional de Protección de Datos. No podemos compartir esta postura, entre otras razones porque, además de ser contraproducente desde un punto de vista político-criminal (deja sin sanción al que crea el fichero y usa los datos registrados en el mismo ilegalmente y sanciona, sin embargo, al que solo efectúe la segunda de dichas conductas), parece confundir la protección que otorga la LOPDGDD a las personas con respecto a sus datos con la que les otorga el Código penal, y conviene no olvidar que, si bien nuestro Código brinda una protección más limitada en algunos aspectos que la norma administrativa, también la da más amplia en otros, ya que no solo protege los datos o ficheros de los que habla la referida Ley orgánica, sino todos los que contengan datos personales, sean estos públicos o privados y estén sometidos o no a las prescripciones de la LOPDGDD (por ejemplo, ficheros familiares o destinados a la prevención o investigación de delitos excluidos de su ámbito de aplicación conforme a los artículos 2.2 RGPP y 2.2 LOPDGDD), con lo que, a efectos penales, resultará del todo irrelevante si los ficheros que contienen los datos en cuestión se crearon legal o ilegalmente atendiendo a las prescripciones de dicha Ley orgánica.

Un tema que también se ha cuestionado y que, a nuestro modo de ver, se va a volver a cuestionar como consecuencia de la entrada en vigor de la LOPDGDD es el relativo a si los datos personales publicados en Internet pueden ser objeto material del delito aquí analizado. Para algunos, la red de redes, que sin duda contiene infinidad de datos personales registrados que pueden ser fácilmente indexados, era en líneas generales un ejemplo de fuente accesible al público, con lo que los datos que se obtuviesen de ella, por estar accesibles sin restricciones a todos los cibernautas, nunca podrían ser considerados como datos reservados. Otros, de forma más acertada, a nuestro modo de ver, señalaban que, en realidad, el catálogo de fuentes de acceso público no es abierto, sino que aparece expresamente tasado en el primer apartado del artículo 7 del RD 1701/2007, postura que fue incluso compartida por la Agencia Nacional de Protección de Datos.

**Lectura recomendada**

Véase en relación a la no consideración de las webs como fuentes de acceso público, por ejemplo, el informe jurídico 0342/2008 de la Agencia Nacional de Protección de datos.

Sin embargo, la entrada en vigor del RGPD y de la propia LOPDGDD han venido a cuestionar esta última postura, por cuanto no solo no han establecido un catálogo cerrado y general de fuentes de acceso público, sino que, además, en el caso de la última norma citada, incluso parece aludir a Internet como una de las posibles fuentes de acceso público de las que habla. En concreto, lo hace en su disposición final tercera, dos, que reforma la Ley electoral general y establece que los partidos políticos podrán, «para la realización de actividades políticas durante el período electoral», utilizar los datos personales que captasen en «páginas webs y en otras fuentes de acceso público».

La polémica generada por la aprobación de este precepto estaba plenamente justificada. Considerar que la red, y en concreto las páginas webs que contienen, son «fuentes de acceso público» es tremendamente peligroso, dada la enorme cantidad de información personal que almacenan. Lo es incluso si ello se hace de forma limitada (solo a partidos políticos y durante el periodo electoral) y por eso entendemos que debe afirmarse que la red sigue siendo un fichero de datos personales que no constituye una fuente de acceso público, con lo que los datos que se obtengan de ella serán reservados y estarán protegidos por el delito del artículo 197.2 CP, postura que se ve claramente reafirmada una vez que la reciente STC de 22 de mayo de 2019 ha declarado inconstitucional el apartado 1 del citado y controvertido artículo de la Ley electoral general.

### 2.3. Conductas típicas

La descripción de las conductas que constituirán delito[6] según el artículo 197.2 CP en caso de ser realizadas sobre los datos personales de los que hablamos en el apartado anterior resulta abigarrada y, en ocasiones redundante. En concreto, se castiga en primer lugar al que «sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero» de dichos datos, para a reglón seguido sancionar con la misma pena a quien «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».

(6)Art. 197.2 CP.

El solapamiento típico de algunas de las referidas actuaciones resulta evidente, sin que se entienda muy bien, por ejemplo, por qué razón el legislador castiga en dos apartados diferentes la utilización de datos en perjuicio de su titular o por qué tipifica en el primero la modificación de datos y en el segundo su alteración, actuaciones ambas que resultan a todas luces idénticas. La razón de esta situación, como acertadamente puso de manifiesto en su día Mata y Martín (2001), se encuentra en el defectuoso proceso legislativo que llevó, durante la fase de enmiendas a la inclusión y modificación del segundo párrafo contenido en el referido artículo, inicialmente referido tan solo a la conducta

de acceso, proceso que dio lugar a esta errónea redacción que, pese a todo y a las múltiples ocasiones que el legislador ha tenido para subsanarla, continúa vigente en nuestro texto penal.

Por *apoderarse* habrá que entender el hecho de hacerse con los datos e incorporarlos al dominio de quien así actúe, mientras que por *acceder* habrá que entender aquella conducta, de la que hablan los artículos 15 RGPD y 13 de la LOPDGDD, que realiza quien llega a tener contacto y a conocer el dato ajeno en cuestión, sin necesidad de que se llegue a hacer o a apoderarse del mismo. *Utilizar* será emplear los datos de cualquier forma o manera (no solo mediante su procesamiento a través del uso de sistemas informáticos), mientras que *alterar* o *modificar* será cambiar o incluso destruir el contenido del dato registrado.

Todas estas conductas suponen «**violaciones de la seguridad de los datos personales**»[7], conforme a lo establecido en el artículo 4.13 del RGPD, que dan lugar a diversas infracciones administrativas, contempladas tanto en dicho reglamento como en la LOPDPD, si se realizan de forma no autorizada, esto es, sin consentimiento del titular de los datos cuando ello sea necesario o bien sin el respaldo de una habilitación normativa que permita realizar tales conductas sin necesidad de tal consentimiento.

(7)Art. 4.13 del RGPD.

Habrá que atender, por tanto, aunque no solo, a lo establecido en los artículos 6 del RGPD y del 6 a 10 de la LOPDGDD en relación con los requisitos y exigencias que han de cumplirse para que se puedan realizar estas conductas de forma autorizada.

Precisamente, es en el artículo 7 de esta última Ley orgánica donde se establece que los mayores de catorce años podrán consentir directamente el tratamiento de sus datos personales, mientras que los menores de dicha edad necesitarán de la autorización de los padres o tutores para poder hacerlo, y, por otra parte, se reserva el ejercicio de los derechos de acceso, rectificación, cancelación, oposición (los célebres derechos ARCO) y del resto de los otorgados por la referida Ley a los titulares de la patria potestad tan solo en lo que se refiere a los datos de los menores de catorce años que estuviesen bajo su tutela (art. 12.6 LOPDGDD), lo que, en principio, les impediría ejercerlos en relación con los datos de los mayores de catorce años sin contar con su consentimiento.

Pese a ello, a nuestro modo de ver habrá que entender que los padres también podrán ejercitar dichos derechos para proteger a los menores de los ataques que se realicen con respecto a los datos de los hijos mayores de catorce años (por ejemplo, pidiendo la cancelación de imágenes y datos personales lesivos de dichos menores difundidos en Internet) actuando al amparo, de nuevo, de la causa de justificación de ejercicio legítimo de un deber (el de protección de los menores), aunque habrá que esperar a que el legislador cumpla con el mandato que se ha autoimpuesto en la disposición adicional 19 de la LOPDGDD y que le obliga a remitir al Congreso, en el plazo de un año, «un proyecto de ley dirigido específicamente a garantizar los derechos de los menores ante el impacto de Internet, con el fin de garantizar su seguridad y luchar contra la discriminación y la violencia que sobre los mismos es ejercida mediante las nuevas tecnologías», para dotar de una mayor certeza y seguridad jurídica a los progenitores a tales efectos.

**Observación**

Resulta llamativo que el legislador español haya reducido la edad que el artículo 8 RDPD establece con carácter general para estos efectos, haciendo uso de la habilitación que le otorgaba el segundo párrafo de dicho artículo.

No obstante, como hemos señalado, las conductas de las que venimos hablando, a diferencia de muchas de las que dan lugar a alguna infracción administrativa (véase, por ejemplo, los art. 71 y sigs. de la LOPDGDD), solo serán delictivas si se realizan «en perjuicio del titular de los datos o de un tercero».

Mucho ha discutido la doctrina sobre la concreta naturaleza y efectos de esta exigencia típica, propugnándose desde interpretarla como un elemento delimitador del resultado consumativo de este delito que obligará a constatar la efectiva lesión de la intimidad de otro para poder apreciar su completo injusto, hasta considerarla como un elemento subjetivo del injusto que exigiría que este delito deba ser realizado con dolo directo de lesionar la intimidad de otra persona o bien que se efectúe con la intención de dañar cualquier otro valor diferente de aquel, como podría ser, por ejemplo, el patrimonio.

A nuestro modo de ver, una vez que hemos considerado que lo protegido por este delito no es la intimidad, ni siquiera en su concepción más amplia o moderna, sino el derecho fundamental autónomo referido a la protección de datos personales, la mejor forma de interpretar este elemento no puede ser ni extendiendo su protección a las conductas realizadas con la finalidad de atacar bienes jurídicos completamente diferentes de dicho valor (como el patrimonio), ni tampoco limitándolo a los que afecten o traten de afectar exclusivamente a la intimidad.

Mucho más adecuado, a nuestro juicio, es entender, atendiendo a lo establecido en el propio artículo 18.4 CE, que lo que aquí se tutela es el derecho a la protección de datos personales en tanto derecho autónomo, pero instrumental y garantizador de aquellos otros valores a que dicho precepto constitucional alude expresamente. Esto es, entender que, dado que el referido precepto constitucional establece este derecho «para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos», solo podrá considerarse que se da el delito aquí analizado cuando el apoderamiento, el acceso, el uso, la modificación o la alteración de los datos personales de los que habla resulten realmente perjudiciales (es decir, representen una lesión o, cuando menos, una puesta en peligro relevante) de tales derechos fundamentales: de la intimidad, del honor o de la libertad.

Esta interpretación llevará, entre otras cosas, a que solo puedan castigarse por esta figura los actos de apoderamiento o de acceso ilícitos a datos ajenos que puedan realmente llegar a afectar a alguno de dichos derechos (por ejemplo, los apoderamientos que se realizan sobre tal cantidad de datos personales, que pueden permitir conocer mediante su procesamiento partes de la vida privada de sus titulares o la utilización no autorizada de datos ajenos en alguna «lista de morosos», de forma que pueda afectar al honor de su titular), pero no aquellos otros que no lo hagan (por ejemplo, los apoderamientos referidos a un dato individual o a una cantidad de datos que no permitan afectar a la intimidad o a los usos no autorizados que en modo alguno afecten a su intimidad, honor o libertad), lo que, sin duda, limitará el ámbito de aplicación de esta figura delictiva a las violaciones realmente graves del derecho a la protección de datos personales, quedando el resto de actuaciones amparadas mediante la apreciación de la correspondiente infracción administrativa.

Finalmente, señalar que este delito solo puede cometerse de forma dolosa, con lo que cualquier error, incluso el vencible, referido, por ejemplo, al carácter no autorizado de los datos o a la idoneidad lesiva o perjudicial de la conducta realizada sobre los mismos determinará la automática atipicidad de la actuación realizada.

## 3. La cuestionable relevancia penal de las conductas de revelación, difusión o cesión no autorizada de secretos o datos personales

El apartado 3 del artículo 197 CP castiga con una pena de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos o las imágenes a los que se refieren los apartados precedentes de dicho artículo. Esto es, los datos o informaciones que se hubiesen obtenido o descubierto mediante la comisión de alguno de los delitos contemplados en los apartados 1 y 2 del artículo 197 CP.

El hecho de que este precepto establezca una mayor pena para quien realiza tales actuaciones que para el que ejecuta las de los apartados que lo preceden, unido a que el mismo artículo 197.3 CP venga a contemplar una pena reducida para los que realicen alguna de tales conductas, es decir revelen, difundan o cedan dichas informaciones sin haber tomado parte en su descubrimiento o relevación delictiva, pero conociendo su origen delictivo, ha determinado que se considere de forma unánime que el precepto ahora analizado define lo que sería un subtipo cualificado de los delitos que le preceden y a los que alude. Es decir, un tipo cualificado de los delitos contemplados en los apartados 1 y 2 del artículo 197 CP.

Nos encontramos entonces, ante una cualificación que incrementa la pena que se deberá aplicar a quien, habiendo tomado parte en alguno de dichos delitos, proceda a difundir ceder o divulgar las informaciones o datos que obtuvo gracias a su realización, lo que atiende, sin duda, a la mayor afectación de los derechos a la intimidad y a la protección de datos personales que supone la comunicación de lo obtenido a terceros.

Será necesario, por tanto, que un sujeto haya realizado de forma acumulada y sucesiva estas dos conductas prohibidas (la de descubrir el secreto o los datos y la de revelarlos) para que se le puedan sancionar atendiendo a lo establecido en este precepto, lo que abre toda una serie de interrogantes con respecto a qué hacer cuando ello no suceda. Es decir, qué hacer tanto con respecto a aquellos sujetos que, no habiendo participado en la obtención ilícita de los datos personales o en el descubrimiento ilícito de informaciones secretas ajenas, pero teniéndolos como consecuencia de su realización, procediesen a difundirlos de forma no autorizada, como con aquellos otros que, habiéndolos tenido incluso lícitamente o de forma consentida por parte de su titular, decidiesen difundirlos o cederlos, pese a no estar autorizados para ello, dado que, en cualquiera de estos supuestos, sus actuaciones difusoras quedarían siempre, y en todo caso, al margen del tipo cualificado ahora comentado.

La primera de las posibilidades planteadas es respondida, como ya adelantamos, directamente por nuestro legislador al establecer en el siguiente párrafo del mismo precepto que será castigado con una pena 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». Esto es, difunde, revela o cede la información que ha recibido.

Se permite así que se pueda castigar, aunque con una pena incluso inferior a la de los tipos básicos de los delitos del artículo 197.1 y 2 CP, a quien, por ejemplo, revele o ceda el contenido obtenido mediante una interceptación de telecomunicaciones realizada por un tercero o los datos personales ajenos de los que otro se hubiese apoderado con anterioridad, algo que resulta relativamente frecuente en determinados ámbitos donde algunos sujetos comercializan o incluso subastan por Internet datos personales ajenos (especialmente los referidos a tarjetas de crédito) que sabían que habían sido previamente obtenidos por terceras personas, sin su participación, mediante la comisión de alguno de los referidos delitos (por ejemplo, mediante su delictiva sustracción de las bases de datos de las entidades emisoras).

Para ello, eso sí, será necesario que quien realice dicha conducta tuviese conocimiento del origen delictivo de los datos o informaciones que revelaba o cedía, lo que determinará que solo se le pueda castigar por esta figura cuando actúe abarcando en su dolo tal origen.

La segunda de las posibilidades comentadas, la referida a la **difusión o cesión de datos que no se obtuvieron mediante la comisión de ningún delito o incluso se tenían lícitamente**, fue objeto de cierta polémica doctrinal antes de la reforma realizada por la LO 1/2015, ya que, a juicio de algunos autores, aunque quien dispone legítimamente de datos personales ajenos (por ejemplo, una foto o un vídeo) y los difunde sin contar con autorización para hacerlo no podía ser castigado mediante la apreciación ni del tipo cualificado anteriormente comentado, ni del más leve delito de relevación contemplado en segundo párrafo del artículo 197.3 CP, sí que podría serlo, sin embargo, apreciando el tipo básico contenido en el segundo apartado de dicho artículo, ya que la difusión sería una de las muchas posibles modalidades de utilización no autorizada de datos castigada en dicho tipo básico.

Esta interpretación fue rechazada, ya entonces, por quienes señalamos (Galán Muñoz, 2013) que su mantenimiento resultaba difícilmente compatible con el hecho de que el artículo 197.3 CP castigase, como sigue haciendo ahora, con una pena menor que la prevista en el tipo básico del artículo 197.2 CP, al que difunda los datos personales de otro que sabía que habían sido obtenidos mediante la comisión de un delito, ya que de mantenerse que la difusión sería una modalidad de utilización de datos de las que habla el tipo básico,

se llevaría a que se castigase a quien revelase datos que tenía inicialmente de forma legítima con una pena mayor que a quien hiciera lo mismo con unos que hubiese obtenido de forma ilegítima por haberlos alcanzado a resultas de la previa realización de un delito por parte de un tercero, lo que resulta a todas luces incoherente y absurdo, dado que supondría castigar con mayor pena al sujeto que realiza una conducta menos grave (al que solo difunde ilegítimamente) que a aquel que efectúa la más grave (al que no solo distribuía, sino que también obtenía los datos de forma ilegítima). Si a esto se le añade que, como veremos, en la reforma realizada en el año 2015, nuestro legislador penal ha decidido castigar tan solo algunas de las revelaciones de ciertos datos personales lícitamente obtenidos (por ejemplo, imágenes) mediante la inclusión del nuevo y controvertido delito del artículo 197.7 CP y optó además por hacerlo con una pena aún menor que la del tipo privilegiado contemplado en el segundo párrafo del artículo 197.3 CP, no quedará más remedio que entender que resulta absolutamente imposible que las difusiones de datos no autorizadas que se tengan legítimamente o las que se reciban como consecuencia de una infracción que no sea constitutiva de delito puedan ser consideradas como uno de los usos de datos personales que prohíbe y castiga el tipo básico del artículo 197.2 CP.

Por otra parte, resulta interesante comentar, continuando con el estudio de las conductas que nos ocupan, que algunos autores (Morales Prats, 2016) han considerado que, en caso de que los responsables, los encargados o los técnicos informáticos que traten datos personales ajenos obtenidos lícitamente fuesen los que los difundiesen de forma no autorizada, se les podrá castigar mediante la apreciación del delito de revelación de secreto profesional del artículo 199.2 CP, dado que consideraban que la realización de dicha conducta por su parte determinaría el quebranto del deber de sigilo profesional que les impone la LOPDGDD.

Varias son las razones que nos llevan a no compartir dicha postura.

En primer lugar, no lo hacemos porque, a nuestro juicio, olvida que no todos los responsables o encargados de tratamientos de los que habla la LOPDGDD son realmente profesionales. En segundo lugar, porque de hecho resulta harto cuestionable que se pueda mantener que el deber de confidencialidad que establecen y atribuyen tanto la LOPDGDD como el RGPD a tales sujetos pueda ser considerado como un verdadero deber profesional, máxime si se tiene en cuenta que dichas normas reconocen en varias ocasiones la posible superposición del deber de sigilo que establecen con verdaderos deberes de dicha naturaleza, como sucede, por ejemplo, con el artículo 5.2 de la LOPDGDD.

**Secreto profesional**

De hecho, llama la atención que el artículo 28.2.a LOPDGDD aluda a la especial protección que han de recibir los datos amparados por secreto profesional, lo que de mantenerse la interpretación aquí rechazada, carecería de todo sentido, ya que obligaría a tener por tales y proteger especialmente todos los datos que se procesan y no solo algunos, dado que todos deberían considerarse amparados por el deber de secreto profesional predicable respecto a los responsables o encargados de su procesamiento.

Pero es que, además, finalmente tampoco podemos compartir la comentada postura porque la misma, a nuestro modo de ver, viene a obviar el hecho de que no todos los datos personales que procesan dichos sujetos podrán ser con-

siderados como «secretos», como exige el artículo 199.2 CP, ya que muchos de ellos son, como hemos tenido ocasión de comprobar, incluso públicamente conocidos.

Todo ello nos lleva a entender que no resulta sostenible que se pueda mantener que todas las revelaciones no autorizadas que efectúen los referidos sujetos se puedan castigar mediante la apreciación del delito de revelación de secreto profesional, lo que, sin embargo, no supone evidentemente que no pueda haber supuestos de revelaciones de informaciones y datos, personales o no, y que siendo realizada por algunos sujetos que los tienen lícitamente, sí que podrán dar lugar al delito del artículo 199.2 CP.

A nuestro juicio, así sucederá, por ejemplo, con aquellos proveedores de servicios de comunicaciones que difundan de forma no autorizada los datos de tráfico que están obligados a conservar conforme a lo establecido en la Ley 25/2007, de conservación de datos de telecomunicaciones, sujetos estos que, por una parte, sí que son profesionales y confidentes necesarios de dichos datos (tienen que captarlos y almacenarlos por mandato legal [art. 4]), por lo que están obligados a conservar el sigilo sobre los mismos sin poder cederlos sin orden judicial (art. 6.1) mientras que, por otra, actúan sobre unos datos (los de tráfico) que, además, a nuestro modo de ver, atendiendo a lo dictaminado por el TEDH (por ejemplo, STEDH casos *Malone vs Reino Unido o Reino Unido vs Copland*), están amparados por el secreto de las comunicaciones, luego son secretos.

Así, pues, habrá que entender que, con la salvedad de supuestos como estos referidos a la violación de verdaderos secretos profesionales, solo resultará posible castigar la mera difusión no autorizada de informaciones o datos personales ajenos obtenidos de forma no delictiva si se cumplen los requisitos que, como veremos posteriormente, abren las puertas a la apreciación del nuevo delito de difusión no autorizada de imágenes o grabaciones audiovisuales en lugares reservados contemplado en el artículo 197. 7 CP (véase, *infra* epígrafe 5).

# 4. Tipos cualificados

El artículo 197 CP contempla toda una serie de circunstancias[8] que, como la ya comentada contenida en su apartado 3, determinarán un incremento de la pena aplicable al autor de los delitos anteriormente realizados, dando lugar a la aparición de toda una serie de posibles subtipos cualificados que analizamos a continuación.

(8)Art. 197 CP.

## 4.1. Los tipos cualificados del artículo 197.4 CP

El apartado 4 del artículo 197 CP contempla dos subtipos cualificados alternativos y uno supracualificado predicable con respecto a los dos anteriores.

En primer lugar, el referido precepto establece en su letra *a* que se aplicará una pena de tres a cinco años a los autores de los delitos de los dos primeros apartados de dicho artículo (luego no a los del simple delito de revelación, difusión o cesión del segundo párrafo de dicho artículo del apartado 3 de dicho precepto), cuando quienes los realicen sean «**las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros**».

El problema estará, entonces, en determinar qué deberá entenderse por cada uno de dichos sujetos. Un interesante referente normativo a tal efecto lo encontramos en lo establecido en el artículo 4.7 RGPD, donde se define al **responsable** del tratamiento de datos personales como «la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento», mientras que se considera **encargado** del mismo, conforme a lo que establece el apartado 8 del mismo artículo, a «la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento».

Estos referentes normativos nos permitirán considerar como «responsable» a la persona que decide el fin para el que se efectúa el tratamiento de datos incluidos en el fichero del que habla el artículo 197.2 CP, mientras que podremos tener por «encargado» a aquel que efectivamente realiza su tratamiento, lo que abrirá las puertas a que se les pueda castigar cualificadamente si cometen tal delito.

**Responsable frente a encargado**

Es responsable, por ejemplo, el empresario que ordena recoger y procesar de determinada forma los datos de sus clientes para agilizar el pago de sus facturas.

Es encargado, por ejemplo, el informático contratado para realizarlo.

Sin embargo, existe una evidente discrepancia normativa entre la expresión utilizada por el legislador penal a la hora de definir los sujetos de los que habla este tipo cualificado («personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros») y la

que emplea la referida normativa administrativa protectora de los datos personales al definir los suyos («responsables o encargados del tratamiento»), de manera que, sin duda, la primera es mucho más amplia que la segunda. Ello, como señala Morales Prats, parece responder al intento legislativo de extender la aplicabilidad de este tipo cualificado a algunas de las conductas que castiga el delito de revelación de secreto del artículo 197.1 CP (por ejemplo, a la interceptación de comunicaciones que realice el responsable del soporte informático que se utiliza para efectuarlas), evitando así que esta cualificación solo resulte aplicable a aquellas actuaciones que recaigan sobre datos personales de las que habla el segundo apartado del referido artículo (Morales Prats, 2016).

Resulta entonces que lo que justificará el incremento punitivo contemplado en este precepto no podrá ser ya, o por lo menos no lo será de forma exclusiva, la mera violación del deber de confidencialidad o sigilo que la normativa administrativa establece con respecto a los encargados o responsables del tratamiento[9], deberes que, por una parte, han adquirido tras la última reforma una faceta mucho más proactiva –tendente a garantizar la confidencialidad de los datos frente a posibles intromisiones de terceros– que meramente pasiva y limitada a no realizar revelaciones, como establecía la normativa anterior, pero que, por otra, solo son predicables, en cualquier caso, con respecto a tales sujetos y no en relación al resto de los que pueden ser castigados en este tipo cualificado (por ejemplo, con respecto al encargado del servidor de mensajería informática del que hablamos anteriormente).

[9] Arts. 5.1 LOPDGDD y 5.2 RDPD.

Mucho más adecuado resulta entonces entender que lo que fundamenta el aumento de penas que este precepto determina será el hecho de que, al tener dichos sujetos acceso y gestionar los soportes en los que se contienen o por los que trasmiten la información sensible que estos delitos quieren proteger, tienen mucho más fácil poder cometerlos, con lo que será el prevalimiento de su especial posición lo que determine que sus actuaciones presenten un mayor desvalor de acción que justificará su mayor pena.

Más cuestionable resulta la otra circunstancia cualificadora contemplada en la letra *b* del apartado que venimos comentando. Aquella que permite aplicar la referida pena cualificada a quienes realicen los delitos de los apartados 1 y 2 del artículo 197 CP «**mediante la utilización no autorizada de datos personales de la víctima**». El origen de esta posible cualificación alternativa hay que buscarlo en el artículo 9.5 de la ya citada Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto, relativa a los ataques contra los sistemas de información, y por la que se sustituye la Decisión Marco 2005/222/JAI del Consejo (DAI). Fue en dicho precepto donde se estableció que: «cuando las infracciones a que se refieren los artículos 4 y 5 sean cometidas utilizando ilícitamente datos de carácter personal de otra persona con la finalidad de ganar la confianza de un tercero, causando así daños al propietario legítimo de la identidad, ello pueda ser considerado, de conformidad con

el derecho nacional, como circunstancia agravante, a menos que tal circunstancia ya esté contemplada en otra infracción que sea sancionable con arreglo al derecho nacional».

Lo primero que llama la atención en relación con este precepto comunitario es que, si bien el mismo obliga a incrementar las penas de algunos delitos cuando son cometidos mediante esta concreta forma de lo que se ha dado en llamar «**robo de identidad**», lo hace, como bien señala Colás Turégano (2015), obligando a incrementar las penas tan solo de los delitos contemplados en los artículos 4 y 5 de la Directiva (el de interferencia ilegal de sistemas de información [art. 4] y el de interferencia ilegal de datos [art. 5]) y no de ninguno de los delitos contra la intimidad y la protección de datos personales de los que nos venimos ocupando.

Habrá que atribuir, entonces, la cuestionable decisión de prever la posible aplicación de esta modalidad cualificada a los delitos ahora analizados exclusivamente al legislador patrio, decisión que parece que no fue demasiado meditada y que le ha llevado, en cualquier caso, a no realizar una directa traslación de lo establecido en el precepto comunitario al artículo ahora analizado, ya que mientras aquel exige que los datos personales en cuestión se utilicen para «ganar la confianza de un tercero» y causando un «daño al propietario de la identidad», ninguna de estas dos exigencias aparecen contempladas en el texto normativo español. Ello permite, en primer lugar, que este tipo cualificado pueda ser aplicado a los casos en que los datos personales se utilizan en sistemas informatizados y no frente a terceras personas (por ejemplo, cuando se usa el *login* de una persona para acceder a sus comunicaciones telemáticas o apoderarse de sus correos) y también que se pueda aplicar aun cuando la conducta realizada no culmine ocasionando el daño pretendido (por ejemplo, cuando se utilice dicho *login* para introducirse en el terminal de un tercero con el fin de apoderarse de sus documentos y descubrir sus secretos, pero no se llegue a conseguir esto último).

Sin embargo, resulta evidente que cuando la conducta que hubiese fundamentado la apreciación del tipo básico sobre la que este subtipo podría aplicarse fuese precisamente la referida a la utilización no autorizada de datos personales que sanciona el artículo 197.2 CP, resultará imposible valorar nuevamente dicha conducta para aplicar a dicho delito esta cualificación, ya que ello infringiría el principio de *ne bis in idem*, quedando, sin embargo, abierta la posibilidad de apreciarla en todos aquellos supuestos en los que el uso ilícito de datos personales inicialmente realizado no constituyese dicho delito, pero sí hubiese sido el medio empleado para realizarlo (por ejemplo, cuando se usasen los datos personales de un sujeto obtenidos mediante *phising* para suplantarlo y conseguir así acceder y apoderarse de los datos personales que estaban almacenados en el fichero, incluso físico, que otro gestionaba).

Cabe señalar que la suplantación de identidad que contempla este tipo puede ser puramente temporal u ocasional, con lo que la apreciación de esta cualificación no siempre supondrá la comisión de un delito de usurpación de estado civil del artículo 401 CP, delito cuya apreciación, evidentemente absorbería la suplantación puntual de identidad que define el tipo cualificado ahora comentado, por lo que entrará, en su caso, en el correspondiente concurso de leyes con este tipo cualificado (no con el tipo básico del mismo, que siempre se tendrá que apreciar), concurso que se deberá solventar, a nuestro modo de ver, a favor de la calificación que determine la aplicación de la mayor pena. Esto es, aplicando el principio de alternatividad (de otra opinión, por ejemplo, Morales Prats, 2016, quien opta por resolverlo por especialidad).

Finalmente, el apartado 4 del artículo 197 CP, en su último párrafo, eleva las penas de estos tipos cualificados a su mitad superior «si los datos reservados se hubieran difundido, cedido o revelado a terceros».

Se establece así un **tipo supracualificado** para los supuestos en los que, tras haberse realizado uno de los delitos de los dos primeros apartados del artículo 197 CP y concurriendo en su realización alguna de las dos posibles circunstancias de su apartado 4 (lo cometió el responsable o encargado o se realizó mediante el uso no autorizado de datos personales), se procede además a difundir, revelar o ceder los datos obtenidos mediante dicha actuación. Ello se fundamenta nuevamente en la mayor afectación de los derechos a la intimidad y a la protección de datos personales que supone su difusión a terceros de lo ilícitamente obtenido, debiendo entenderse que cuando el referido precepto alude a los «datos reservados», engloba en dicha expresión tanto los datos personales que tengan el carácter del que habla el apartado 2 del artículo 197 CP, como los datos e informaciones de la vida privada que se hubiesen podido obtener mediante la realización del delito de su apartado 1, no solo, por tanto, los primeros.

### 4.2. La cualificación por la naturaleza de los datos afectados o del sujeto pasivo

El apartado 5 del artículo 197 CP establece que cuando cualquiera de las conductas contempladas en los preceptos 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»[10].

[(10)]Art. 197. 5 CP.

Lo primero que hay que señalar en relación a esta cualificación es que la misma resulta, por expreso mandato legislativo, aplicable a cualquiera de los tipos que le preceden. Esto es, tanto a los tipos básicos de los dos primeros apar-

tados del artículo 197 CP como a sus tipos cualificados (lo que determinaría que este precepto pueda actuar como tipo supracualificado si se aplica sobre alguno de los tipos cualificados anteriormente comentados y no sobre sus tipos básicos), y también al delito más leve de revelación de secreto descubierto delictivamente por un tercero del párrafo final del artículo 197.3 CP.

Dos son las circunstancias que pueden dar lugar al incremento punitivo contemplado en este precepto.

La primera es la referida a **la naturaleza especialmente sensible de ciertos datos personales** que se consideran especialmente peligrosos (los referidos a ideología, religión, creencias, salud, origen racial o vida sexual), datos que, como ha demostrado desgraciadamente la historia, han sido utilizados para realizar todo tipo de atropellos y persecuciones (desde discriminaciones hasta genocidios), lo que ha determinado que tanto el derecho administrativo como el penal les otorguen especial atención (a este respecto, véase lo establecido en los arts. 9 RGPD y 9 LOPDGDD).

No obstante, lamentablemente es en relación con estos datos donde se vuelve a poner de manifiesto la descoordinación normativa existente entre la protección penal y administrativa vigentes tras la última reforma realizada tanto por el RGPD como por la LOPDGDD. No es solo que estas normas consideren especialmente sensibles y protejan con mayor cuidado (por ejemplo, exigiendo para su tratamiento el consentimiento expreso y no el meramente tácito del afectado) un grupo de datos mucho mayor que los contemplados en este precepto (por ejemplo, los biométricos), sino que además, mientras que la normativa administrativa protege todos los datos personales que revelen información respecto a dichas cuestiones y los que se utilicen para hacerlo[11], la penal solo protege los primeros, esto es, los datos que «revelen» directamente información referida a dichas cuestiones.

[11] Art. 9.1 LOPDGDD.

Habrá que entender, por tanto, que aunque la normativa administrativa proteja especialmente datos que, pese a su aparente inocuidad, podrían servir, por ejemplo, para deducir la ideología de una persona (por ejemplo, los que permitieran identificar los periódicos que lee o los grupos de una determinada tendencia ideológica a los que está suscrito en alguna red social), el tipo delictivo aquí comentado **solo podrá apreciarse en la medida en que su realización recaiga sobre datos que directamente y sin necesidad de tratamiento o de inferencia revelen dicha información** (por ejemplo, los referidos a su afiliación a un partido o que muestren sus preferencias sexuales), algo que tal vez debería ser revisado por nuestro legislador en futuras reformas.

La segunda alternativa cualificadora determina la cualificación de todos los delitos anteriores cuando su **víctima sea menor de edad**, esto es, menor de dieciocho años, o una persona con discapacidad necesitada de especial protección, lo que, sin duda, incrementa la pena aplicable al autor de estos delitos atendiendo a la mayor vulnerabilidad de ambas clases de sujetos.

En cualquier caso, no debe olvidarse que para que cualquiera de las circunstancias cualificadoras que hemos comentado determine que se incremente la pena aplicable al autor de estos delitos, dicho sujeto deberá haber obrado con dolo con respecto a las mismas, lo que impedirá, por ejemplo, que se pueda incrementar la pena de aquel que interceptase dolosamente las comunicaciones de otro sin saber que este era menor o la de aquel otro que se apoderase de datos personales ajenos de forma no autorizada y con intención de descubrir algún secreto, pero sin tener consciencia de que dichos datos revelaban información relativa a su vida sexual o a sus creencias religiosas.

### 4.3. La actuación con fines lucrativos

Finalmente, el apartado 6 del artículo 197 CP determina que se incrementen las penas de todos los delitos contemplados en los apartados 1 a 4 de dicho precepto si son **cometidos con fines lucrativos**[12].

(12)Art. 197. 6 CP.

Este precepto obliga a incrementar las penas tanto del que realiza cualquiera de los referidos delitos porque le pagan por efectuarlos (por ejemplo, el detective que se contrata para vigilar la vida privada de otro accediendo ilícitamente a su cámara web), como de quien los lleva a cabo porque pretende obtener un enriquecimiento patrimonial gracias a dicha actuación (por ejemplo, tanto del que se apodera de los datos de otro para venderlos como de aquel que, no habiendo participado en su apoderamiento, los recibe de quien sí lo hizo y, conociendo dicho hecho, los vende o subasta en alguno de los nada infrecuentes mercados creados a tales efectos, cometiendo así el delito del art. 197.3 segundo párrafo CP con una finalidad lucrativa).

No será necesario, en cualquier caso, para apreciar esta cualificación que llegue a alcanzar el enriquecimiento perseguido, sino que bastará con que se acredite que se perseguía, lo que permitirá, por ejemplo, incrementar la pena tanto del sujeto que hubiera cometido el delito en cuestión a cambio de un pago, por más que no llegase a recibirlo, como de aquel otro que subastase en Internet secretos o datos ajenos delictivamente obtenidos, aunque no llegase a venderlos o, habiéndolo hecho, no consiguiese cobrar el importe al que los había adjudicado.

Si el autor de las conductas realizadas con finalidad lucrativa las efectuase, además, **actuando sobre alguno de los datos especialmente sensibles** de los que habla el apartado anterior (no lo olvidemos, los que revelan ideología,

religión, creencias, salud origen racial o vida sexual) se apreciará el tipo supracualificado contemplado en el artículo 197.6 *in fine* CP que determina que se incremente la pena que se le deberá imponer hasta la de prisión de cuatro a siete años.

# 5. El delito de revelación de imágenes o grabaciones audiovisuales reservadas captadas de forma autorizada

## 5.1. Tipo básico

Como ya tuvimos ocasión de comentar, antes de la reforma realizada por la LO 1/2015, la mera difusión no autorizada de informaciones íntimas o de datos personales de un sujeto solo podía tener relevancia penal si dichos contenidos habían sido previamente obtenidos mediante la realización de uno de los delitos contemplados en los apartados 1 o 2 del artículo 197 CP o si estaban protegidos por un deber de sigilo profesional que prohibía a quien los tenía que los pudiese difundir de forma legal.

**Ved también**

Para más información véase el apartado «La cuestionable relevancia penal de las conductas de revelación, difusión o cesión no autorizada de secretos o datos personales».

Esto determinaba que cualquier difusión, revelación o cesión de datos obtenidos de cualquier otra forma, incluso los logrados ilícitamente, pero no de forma delictiva –por ejemplo, por haberse obtenido mediante engaño (*phishing*)–, quedasen en la más absoluta atipicidad.

Sin embargo, la proliferación de casos cada vez más frecuente de difusiones de contenidos de naturaleza íntima y sexual de personas efectuados por sujetos que inicialmente los habían conseguido de forma lícita e incluso con el consentimiento expreso del concreto afectado por los mismos (recuérdese, por ejemplo, el mediático caso de la concejala Olvido Hornillos), hicieron que el legislador se replantease dicha postura inicial e introdujese una nueva figura delictiva, acompañada de un tipo cualificado, que vendría, precisamente, a acabar con esa situación.

Se trata del delito contemplado en el nuevo apartado 7 del artículo 197 CP, que establece que será castigado con pena de prisión de tres meses a un año «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».

Como se puede comprobar, el punto de partida y la novedad de esta figura con respecto a las anteriormente analizadas es que en esta se castiga la **revelación, difusión o cesión de contenidos que necesariamente tendrán que haber sido obtenidos con la anuencia del afectado**[13]. Esto es, con el consentimiento del sujeto pasivo del delito, bien porque este sujeto se los hubiese entregado o cedido al tercero que posteriormente los difundió o bien porque hubiese sido este último quien los hubiese grabado o documentado contando con la anuencia o consentimiento de aquel (Morales Prats, 2016).

(13) Art. 197.7 CP.

Este hecho, el que este delito solo pueda ser cometido por quien tiene alguno de los contenidos a los que su tipo alude con el consentimiento de la persona a cuya intimidad afectan, convierte esta figura en un delito especial propio que solo puede ser cometido por quien goza de dicha cualidad. Esto es, la de autorizado poseedor del contenido en cuestión, sujeto que, por el mero hecho de tenerlo de forma autorizada, pasará a estar vinculado por una suerte de mandato u obligación penal de confidencialidad o discreción que lo vincula con el sujeto pasivo que le autorizó a tener el contenido en cuestión, pero no le capacitó para que pudiese difundirlo. Esta violación de la obligación es esencial para dotar de contenido material al injusto propio de esta figura, con lo que se esta convierte en un ejemplo de verdadero delito de infracción de un deber.

De hecho, todas aquellas difusiones no autorizadas que se realicen por sujetos no vinculados por el deber de confidencialidad que le vinculaba con el afectado por el contenido que poseían legítimamente quedarán completamente al margen de este tipo delictivo, lo que llevará, entre otras cosas, como bien señala Colás Turégano (2015), a que queden al margen de este delito, por ejemplo, todas los reenvíos no autorizados del contenido en cuestión que efectúen quienes los hubiesen recibido previamente del tercero, que los poseía con la autorización del afectado, pero que los había distribuido sin su consentimiento, lo que provoca que quede en la más absoluta atipicidad toda la posible cadena de remisiones que podrían seguir a dicho primer acto de difusión ilícita, por más que tales actuaciones intensifiquen sin duda la afectación del derecho a la intimidad que su inicial divulgación había producido.

Sin embargo, la conducta típica de este delito puede consistir, alternativamente, en **difundir** (comunicar a otros), **revelar** (mostrar a un tercero) o **ceder** (entregarle a un tercero) de forma no autorizada (esto es, sin contar con autorización o excediéndose de la que se tenía, como sucederá, por ejemplo, si se trasmitiese a un tercero diferente de aquel al que el titular había autorizado a que se le cediese el contenido en cuestión) alguno de los posibles objetos materiales de este delito.

Precisamente, este elemento, el del objeto material, se convierte en el elemento central de este delito. No cualquier dato o información ajena obtenida con el consentimiento del afectado, pero trasmitida o difundida sin su autorización, permite apreciar este delito. Solo será constitutiva de esta figura la revelación que recaiga sobre «imágenes o grabaciones audiovisuales» del afectado, obtenidas con su anuencia «en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros».

Lo primero determina que **permanezcan al margen de este delito todas aquellas conductas difusoras referidas a contenidos que no sean imágenes o grabaciones audiovisuales**. Así, podrá ser delictiva la difusión de fotos de la persona o de grabaciones que contengan imagen y sonido, pero no las que solo tengan lo segundo, con lo que, por ejemplo, la grabación meramente sonora de una conversación mantenida y grabada con el consentimiento del grabado no constituirá delito aun cuando se realice contra su voluntad y pueda afectar a su intimidad tanto o más que muchos contenidos con su imagen (Colás Turégano, 2015).

Por otra parte, las imágenes, como ya hemos señalado, deben ser de la persona afectada, esto es, de la persona que sufre la merma en su intimidad a resultas de su difusión, lo que determina que nos encontremos ante un delito que solo protege la intimidad de dicho sujeto. Del sujeto o de los sujetos cuya imagen aparezca recogida en la grabación y no la de otros cuyos secretos la persona grabada pueda estar revelando, con lo que permanecerán al margen de este delito, por ejemplo, la divulgación no autorizada de una grabación consentida, pero que no se ha autorizado a difundir, en la que una persona revele un secreto referido a otro (por ejemplo, su orientación sexual o su ideología).

Por otra parte, **las imágenes deberán haber sido captadas en un domicilio o en cualquier otro lugar fuera del alcance de la vista de terceros**, exigencia que restringe, sin duda, el ámbito típico de esta figura, al limitar su posible objeto material, pero que permite incluir en su seno prácticamente cualquier imagen o contenido audiovisual que no haya sido obtenido en un lugar público y a la vista de terceros. Desde los obtenidos en una casa, hasta los realizados en un coche o en un lugar apartado y oculto de un parque (Muñoz Conde, 2017).

Podría pensarse entonces que las difusiones, nada infrecuentes, de imágenes o grabaciones efectuadas con la anuencia de quien aparece en ellas, e incluso en su domicilio, pero que se publican en redes sociales (Facebook, Instagram, etc.) sin su consentimiento, o incluso con su oposición, podrían llegar a tener cabida en este delito. Sin embargo, afortunadamente el legislador, siendo consciente de lo frecuente que es dicha práctica y de lo poco lesiva que resulta en la mayoría de los casos para la intimidad de los afectados, ha exigido, pa-

ra que dichas actividades puedan ser típicas de este delito, que su realización «menoscabe gravemente la intimidad de esa persona». Esto es, la de la persona captada en las imágenes y afectada por su difusión.

El problema radica en determinar cuándo se producirá dicho menoscabo y, sobre todo, cuándo será grave. Se ha propuesto realizar una interpretación restrictiva de dicha exigencia que limitaría la apreciación de este delito tan solo a las actuaciones que recaigan en imágenes o grabaciones que estén referidas a los aspectos más sensibles de su intimidad, en concreto, a los que determinan la apreciación del tipo cualificado del apartado 5 del artículo 197 CP (ideología, religión, creencias, salud, origen racial o vid sexual), sugerente propuesta interpretativa que habrá que ver si es acogida finalmente por los tribunales, ya que no se ajusta exactamente al tenor literal del precepto analizado, lo que, en principio, puede permitir incardinar en este tipo otras actuaciones gravemente lesivas de su intimidad, pero no relativas a tales materias (por ejemplo, una que revele las malas, pero no públicamente conocidas, relaciones existentes entre dos miembros de una familia).

Finalmente, por lo que respecta a la delimitación de su tipo básico, señalar que este delito, como sucede con todos los aquí analizados, es eminentemente **doloso**, con lo que cualquier error, incluido el vencible, referido a cualquiera de sus elementos típicos excluirá su tipicidad (por ejemplo, la difusión realizada por error al confundir el archivo que se remite a terceros, la efectuada creyendo que se cuenta con la anuencia del interesado o la que se hace creyendo que lo que se difunde no afecta gravemente a su intimidad).

### 5.2. Tipos cualificados

Entrando ya en el estudio de los tipos cualificados[14] de este delito contemplados en el segundo párrafo del artículo 197 CP, hemos de señalar que dicho precepto contempla tres posibles tipos cualificados alternativos.

(14)Art. 197 CP.

El primero de ellos permite incrementar la pena hasta su mitad superior «cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia».

Se trata así de dar respuesta a uno de los casos más frecuentes de comisión de este tipo de relevaciones o indiscreciones: aquellos que se dan cuando dos personas que mantienen una relación sentimental, sacan fotos o se graban

individual o mutuamente vídeos íntimos, generalmente de naturaleza sexual, que incluso se remiten entre sí (*sexting*), y uno de ellos los revela o los difunde a terceros sin el consentimiento del otro y en muchos casos por venganza.

Parece que el fundamento de esta cualificación, evidentemente incompatible con la simultánea apreciación de la circunstancia del parentesco del artículo 23 CP como agravante, ha de encontrarse en el mayor quebranto del deber de confidencialidad, propio de este delito, que se da cuando se efectúa por parte de personas con las que se mantiene o se ha mantenido este tipo de relaciones. Solo así se entiende, por ejemplo, que el tipo cualificado ahora comentado no resulte aplicable a los casos en los que quien difunda el vídeo lo haya obtenido de forma consentida, pero a resultas de una relación sexual esporádica, no asimilable o análoga al matrimonio, sujeto cuya conducta, pese a afectar a la intimidad de la otra persona en la misma medida que lo haría la efectuada por aquel que hubiese sido su pareja estable, solo podrá ser castigado mediante la apreciación del tipo básico de este delito.

El segundo posible subtipo cualificado, por su parte, incrementa la pena aplicable al autor de este delito cuando «la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección». El fundamento de esta cualificación se encuentra, sin lugar a dudas, en la especial vulnerabilidad de los sujetos pasivos de los que habla.

Resulta evidente, por otra parte, que cuando las imágenes del menor o discapacitado en cuestión sean de naturaleza sexual, tendrá que apreciarse el correspondiente concurso con el delito contra la indemnidad sexual del menor, generalmente con el del artículo 189 CP en su modalidad de distribución o exhibición de pornografía infantil, modalidad típica cuyo injusto, a nuestro modo de ver, ya valora el ataque a la intimidad aquí castigado, dado que, al considerarse que el consentimiento del menor referido a la distribución del contenido pornográfico en que aparecía del artículo 189 CP no tiene validez alguna –ni a efectos de poder disponer de su indemnidad sexual, ni tampoco en relación con su intimidad–, deberá considerarse que la distribución de los contenidos que castiga el delito de pornografía infantil del artículo 189 CP siempre conllevará y castigará también el ataque que produce a la intimidad del menor su no autorizada difusión, con lo que de la apreciación de este delito absorbería el injusto propio de la figura aquí analizada, entrando, por tanto, con ella en concurso de leyes y no de delitos, tal y como algunos autores mantienen (a favor del concurso de delitos se manifiesta, por ejemplo, Colás Turégano, 2015).

Finalmente, el referido precepto termina estableciendo que también se incrementará la pena «cuando los hechos se hubieran cometido con una finalidad lucrativa», lo que determinará que se incremente la pena aplicable al autor cuando difunda o revele las imágenes o grabaciones que tenía lícitamente con la intención de obtener una remuneración o incluso pretendiendo lucrarse gracias a los ingresos publicitarios que le produjese tal conducta (por ejemplo, por su publicación en páginas web), sin que sea necesario para apreciar esta cualificación que llegue objetiva y efectivamente a obtener el lucro perseguido, sino tan solo que actúe con la intención o finalidad de alcanzarlo.

## 6. El delito de acceso, facilitación del acceso o mantenimiento no autorizado a sistema de información

Si hay una conducta abusiva realizada mediante el uso de sistemas informáticos cuya posible tipificación ha sido tradicional objeto de controversia, tanto doctrinal como legislativa, esta ha sido, sin lugar a dudas, la referida a lo que se dio en denominar como ***hacking* blanco**. Es decir, la conducta que realiza quien accede a un sistema informático ajeno, sin consentimiento de su titular, pero también sin intención alguna de realizar ningún mal posterior a dicho sujeto ni a terceros (ni dañar, ni descubrir secretos, etc.).

Pese a lo controvertido del tema, la discusión político-criminal referida a la posible incriminación y castigo penal de este tipo de actuaciones parece que terminó cuando la reforma realizada por la LO 5/2010, tratando de dar respuesta a la obligación de tipificación de estas conductas establecida en la Decisión Marco 2005/222/JAI del Consejo, de ataques a sistemas informáticos (DMAI), introdujo en nuestro código penal el delito de acceso no autorizado a sistemas de información contemplado en el aquel momento vigente artículo 197.3 CP.

La influencia comunitaria de este delito, por más que tenga algunos otros precedentes internacionales como el ya citado Convenio de Budapest contra la cibercriminalidad, resulta indudable. No es solo que esta figura fuese creada atendiendo al mandato y a los parámetros contenidos en la DMAI, es que, además, también ha sido la normativa comunitaria la que ha venido a determinar que dicho delito haya sido reformado en tiempos bien recientes. En concreto, como consecuencia de la reforma efectuada por la LO 1/2015, una reforma que, como expresamente reconoce su preámbulo, ha venido a modificar este delito con el fin responder a lo exigido por el artículo 3 de la Directiva 2013/40/UE, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, que sustituyó a la anteriormente citada Decisión Marco, en la que este delito encuentra su origen (DAI), lo que determina que esta norma comunitaria se convierta en referente fundamental a la hora de realizar una interpretación adecuada de su injusto.

El nuevo delito de acceso o mantenimiento no autorizado a sistema de información[15] ha pasado, tras la reforma efectuada en 2015, a estar ubicado en el nuevo delito del artículo 197 bis.1 CP, que establece que: «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».

(15)Art. 197 bis.1 CP.

Muchas son las cuestiones y problemas que plantea esta figura en su nueva redacción, comenzando por la referida a la cuestionable y cuestionada delimitación de su bien jurídico protegido.

## 7. Bien jurídico

Pese a su ubicación sistemática dentro del título referido a los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, la verdad es que si en algo parece estar de acuerdo la mayor parte de la doctrina, es en que esta figura no viene a tutelar ninguno de dichos valores o, por lo menos, no los tutela de forma exclusiva.

Mientras algunos autores consideraban, ya antes de su última reforma, que lo que aquí se protege era la seguridad de los sistemas informáticos de forma exclusiva, otros entendían que, si bien era ese el valor que se tutelaba, solo se hacía en la medida en que servía para amparar a su vez, siquiera de forma abstracta, la intimidad propiamente dicha o la privacidad, entendiendo esta última como el valor que tutela los datos personales frente a posibles tratamientos no deseados.

Así, en esta misma línea de pensamiento, se ha afirmado que el hecho de que el comentado delito haya pasado, tras la reforma, a castigar el mero acceso o el mantenimiento al conjunto o a una parte del sistema de información y no, como hacía antes de su aprobación, a los datos o programas en ellos contenidos, deja de una vez por todas definitivamente claro que este delito no protege los datos personales ni íntimos que dichos sistemas pueden almacenar, sino los sistemas en sí mismos, con lo que el bien jurídico tutelado por esta figura se desvincularía completamente de la intimidad y quedaría referido de forma exclusiva a la seguridad propiamente dicha de los sistemas informáticos (por ejemplo, Colás Turégano, 2015).

Sin embargo, a nuestro modo de ver, esta interpretación se enfrenta a varios problemas. No es solo que su mantenimiento sea abiertamente contradictorio con la ubicación sistemática del delito ahora analizado, lo que obliga a sus defensores a pedir una reubicación de *lege ferenda* del mismo mediante su inclusión en un nuevo y actualmente inexistente capítulo propio referido a este bien jurídico. Es que, además, hablar de la «seguridad de los sistemas informáticos» en general y convertir dicho valor en el bien jurídico protegido por este delito supone fijar como tal un interés, a nuestro juicio, difuso, dotado de un muy escaso, por no decir nulo, contenido material, lo que difícilmente permitiría dotar de verdadera lesividad y antijuridicidad material al injusto propio de esta figura, más allá del que vendría dado por la violación formal de la norma no invasiva que viene a establecer.

Aparte de plantear serios problemas a la hora de legitimar la propia existencia de esta figura, esto también llevaría a que la misma se enfrente a graves dificultades interpretativas.

Por ejemplo, si lo que se protege en este delito es la seguridad informática referida a los sistemas en sí mismo considerados, ¿cuándo se lesionaría o se pondría en peligro dicho valor? ¿Bastaría para apreciar la afectación de dicho bien jurídico que castiga este delito con que alguien, por ejemplo, accediese físicamente y de forma no autorizada al teclado de un ordenador forzando el candado que impedía entrar en el lugar donde este se encontraba, incluso aunque dicho sistema no tuviese ningún dato almacenado o tratado?

Para responder a esta cuestión es necesario determinar, en primer lugar, qué se debe entender por uno de los sistemas de información protegidos por este delito, para lo que se hace necesario acudir a la normativa comunitaria en la que esta figura tiene su origen. Es precisamente allí, en concreto en el artículo 2.a DAI, donde se establece que se entenderá por **sistema de información**: «todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento».

Como se puede comprobar, el precepto analizado distingue claramente dos componentes dentro de lo que puede entenderse por uno de los sistemas de información cuyo acceso ilícito castiga nuestro artículo 197 bis.1 CP. Por otra parte, están los **aparatos individuales o conectados entre sí** (hardware). Por otra, los **datos informáticos**, esto es, por expreso mandato del artículo 2.b DAI, tanto las informaciones almacenadas, tratadas, recuperadas o trasmitidas por tal aparato o grupo de aparatos, como los programas que sirven para que los mismos realicen una función.

La expresa alusión normativa a este último componente deja claro que el acceso a los datos o programas informáticos sigue constituyendo un acceso a un sistema de información de los que habla el delito ahora analizado, con independencia del tipo de datos de que se trate (no tienen que ser, por tanto, datos íntimos, ni personales), mientras que la referida a los componentes físicos, por su parte, como señalan los defensores de establecer la seguridad informática como bien jurídico protegido por este delito, determina que pueda haber accesos que no tengan por qué recaer sobre datos o programas informáticos, sino que pueden hacerlo sobre el hardware que conforma el sistema.

No obstante, conforme a la referida norma comunitaria, un hardware solo se considerará parte del sistema de información y, por tanto, será susceptible de sufrir los accesos ilícitos de los que venimos hablando si es el que trata de forma automatizada datos informáticos (por ejemplo, el concreto ordenador que ejecuta el procesamiento) o si por lo menos está conectado con otros componentes que realicen dicho tratamiento (por ejemplo, es un sistema de almace-

namiento que todavía no se ha utilizado para guardar datos, pero que está conectado al ordenador que los trata o al enrutador, los *switches* o conmutadores conectados a dicho ordenador que podría emplearse para trasmitir los datos que el mismo procesaba, pero que todavía no lo está haciendo).

Esta exigencia excluye, sin duda, de entre los accesos típicos a los que se efectúen sobre aquel hardware que no tenga dicha cualidad, como, por ejemplo, aquel que se haga sobre un ordenador que no contenga dato alguno y no esté conectado a otros que los tengan y procesen. Por otra parte, también nos indica que, pese a que la reforma producida haya venido a ampliar el número de objetos protegidos frente a posibles accesos no deseados, extendiendo su punición no solo a los que no se realizan sobre datos o programas, sino también a los que recaen sobre los componentes en sí mismos, solo lo hace si tales aparatos contienen y procesan datos informáticos o están conectados con otros aparatos que lo hacen. Esto, a nuestro modo de ver, pone de manifiesto que lo que aquí se trata de proteger no son los aparatos informáticos en sí mismos, sino estos en la medida en que delimitan y definen el entorno virtual que, al estar interconectado entre sí, podría permitir acceder a los datos informáticos ajenos contenidos y procesados en algún lugar del completo sistema protegido.

Por eso consideramos, como considerábamos antes de la reforma, que lo que este delito viene a proteger no son los sistemas informáticos en sí mismos, ni su seguridad, sino el derecho que tiene toda persona a conservar al margen de intromisiones no deseadas determinados espacios digitales en los que almacenan y procesan sus datos informáticos. Un derecho de nuevo cuño, pero que lejos de aludir a la mera seguridad de los sistemas informáticos, tiene por finalidad, a nuestro modo de ver, garantizar a su titular que podrá tratar en dicho espacio los datos que estime pertinente con la garantía de estar penalmente protegido frente a posibles intromisiones y que, precisamente por ello, recuerda claramente a otros derechos que se han reconocido al ciudadano a lo largo de la historia precisamente con el fin de garantizarle el seguro ejercicio de su vida privada y la intimidad en determinados espacios, aun cuando no los hubiese empleado aún de forma efectiva para ejercitarlos.

Recuerda, en concreto, a los derechos fundamentales a la inviolabilidad de las comunicaciones y, especialmente, a la inviolabilidad domiciliaria que nuestra constitución reconoce y que, de hecho, nuestro Código penal protege mediante el castigo del delito de allanamiento de morada del artículo 202 CP, figura con la que el delito aquí analizado encuentra un claro paralelismo típico, dado que, del mismo modo que aquella protege el espacio definido como domicilio tanto frente a acceso como frente a mantenimientos de terceros no deseados, el delito aquí analizado hace lo propio con el entorno digital del que habla, castigando tanto acceder de forma no autorizada al mismo como en mantenerse «contra la voluntad de quien tenga el legítimo derecho a excluirlo».

Precisamente, este hecho fue el que nos llevó, hace ya tiempo, a afirmar que lo más correcto sería considerar que lo que aquí se protege es ese derecho de exclusión que se otorga a los ciudadanos. Un derecho que pasaría a actuar como una nueva inviolabilidad. La denominada **inviolabilidad informática** (Galán Muñoz, 2006) que, como la de las comunicaciones o la domiciliaria, también constituye un derecho diferente y autónomo de la intimidad, pero es instrumental y tendente a garantizar el libre ejercicio de esta dentro de los sistemas informáticos, postura que dotará de un contenido cierto al injusto del delito ahora analizado y, además, como veremos, tendrá importantes efectos concursales en relación con los delitos que vendrían a proteger este último bien jurídico.

### 7.1. Conductas típicas

El delito ahora analizado castiga tanto **acceder**, por cualquier medio o procedimiento, vulnerando medidas de seguridad y sin estar debidamente autorizado, al conjunto o a una parte de un sistema de información, como **facilitar** dicho acceso o también mantenerse en el sistema contra la voluntad de quien tenga legítimo derecho a excluirlo.

**Acceder supone introducirse o alcanzar**, conducta que, a nuestro modo de ver, una vez que se ha definido esta figura como un delito protector de los entornos digitales que quedan protegidos por la inviolabilidad informática por contener o procesar datos informáticos o estar conectados con componentes que lo hacen (y no la mera seguridad de los sistemas), deberá considerarse que solo se dará si se efectúa en un sentido digital y no meramente físico, con lo que se podrá apreciar su realización si el sujeto en cuestión logra introducirse y tener contacto con la parte lógica del sistema protegido y no, simplemente, con el mero hecho de que logre tocar alguno de los componentes del sistema protegido (el teclado, el disco duro, etc.). No hará falta, sin embargo, que llegue a tener el dominio efectivo sobre el sistema o de una parte del mismo para entender consumado este delito. Bastará con que alcance a tener contacto con los datos o el software que contienen y protegen para considerar completa dicha actuación y, por tanto, también la modalidad comisiva que venimos analizando.

El problema que se plantea entonces es cómo definir los accesos a aquellas partes del sistema que no tienen ni contienen los datos o programas que se emplean para efectuar el procesamiento de datos que, sin embargo, puede y debe estar realizándose en el sistema como conjunto, para que este pueda ser considerador como un sistema de información.

A nuestro modo de ver, la única forma de entender que se accede digitalmente a los componentes del sistema que no contengan los datos o programas que se procesan en otro lugar del sistema será entender que se llegue a tener contacto con sus correspondientes BIOS. Esto es, se acceda al *firmware* que todos estos aparatos digitales tienen preinstalados y que es el que inicia y determina cómo deberá funcionar ese concreto elemento del sistema ilícitamente accedido, por más que el mismo no contenga los datos o programas que estén siendo procesados en otra parte del sistema (por ejemplo, el que determina cómo funcionará el sistema de almacenamiento vacío pero conectado a un ordenador que procesa datos, o el que hace lo mismo con el del enrutador o el del *switch* al que dicho ordenador está conectado).

Sin embargo, para que dicho acceso a la totalidad o a parte del sistema sea delictivo, tendrá que haber sido realizado, como ya hemos señalado, de forma no autorizada y vulnerando las medidas de seguridad establecidas para impedirlo.

Lo primero determina, atendiendo a lo establecido en el artículo 2.d DAI, que queden al margen de este tipo tanto los accesos que se efectúen gozando de una **autorización legal o judicial** a tal efecto (por ejemplo, los registros remotos sobre equipos informáticos ajenos efectuados lícitamente conforme a lo establecido en el artículo 588 septies LECrim), como los que se realicen con el **consentimiento de la persona que está legitimada para acceder al sistema**, algo que habrá que determinar en cada caso concreto atendiendo a múltiples factores, ya que no siempre el titular del sistema de información será el legitimado para autorizar el acceso a los datos que almacena (por ejemplo, el titular de un servidor de almacenamiento en la nube en muchas ocasiones no tiene legitimación ni puede autorizar el acceso a los datos que terceros almacenan en el mismo).

Lo segundo, la exigencia de la **vulneración de medidas de seguridad** (exigencia de potestativa inclusión, conforme a la DMAI de 2005, pero que se ha convertido en obligatoria tras su modificación por la DAI de 2010), juega, a nuestro modo de ver, un papel fundamental en la delimitación de este delito. Por una parte, porque incrementa sin duda la gravedad que ha de tener el acceso realizado al sistema de información para que pueda ser típico de este delito, ya que determina que solo se puedan tener por tales a aquellos que conlleven la mayor energía criminal que se deriva del quebranto de la medida protectora vulnerada, sin puedan serlo, por ejemplo, los accesos no consentidos que se realicen simplemente aprovechando un mero descuido del titular del sistema o a sistemas que no tengan ninguna protección que se haya de vulnerar.

Además, como ya propusimos en su momento (Galán Muñoz, 2006), dicho elemento es el que permite delimitar con seguridad las partes del sistema informático que quedan excluidas de accesos de terceros cuando el uso de los sistemas en cuestión es compartido por varias personas.

Piénsese, por ejemplo, en aquel caso en que un mismo sistema u ordenador de la empresa es empleado por varios sujetos que están autorizados a usarlo, pero uno de ellos tiene una carpeta donde almacena datos a los que solo él está autorizado a acceder, para lo que los protege encriptándolos o los almacena en un servidor del sistema que está protegido por una clave. En estos supuestos, el establecimiento de la medida de seguridad resulta fundamental para concretar con seguridad qué partes del sistema son accesibles para cada uno de sus posibles usuarios y cuales, por el contrario, no lo son y, por ello, están amparadas por el derecho a la inviolabilidad informática de alguno de dichos sujetos. Por otro lado y a mayor abundamiento, al tener que ser vulneradas dichas medidas para dar lugar a este delito, se facilitará enormemente la prueba de la ejecución dolosa del acceso producido, ya que resultará muy difícil que aquel sujeto que las hubiese esquivado para acceder a una parte del sistema pueda después decir que lo hizo por error o pensando que estaba autorizado para actuar como lo hizo.

La exigencia, por tanto, del establecimiento y la vulneración de las comentadas medidas es fundamental para la configuración del injusto propio de este delito, no solo por incrementar la gravedad del ataque realizado, sino también porque es un claro indicador de la voluntad excluyente de intromisiones del que los utiliza y de la voluntad infractora del que lesiona el derecho que tiene a excluirle, con lo que su exigencia resulta, pese a las críticas de algunos, del todo acertada y necesaria.

Otra cuestión que ha generado cierta controversia con respecto a esta exigencia típica es la relativa a la magnitud o idoneidad protectora que ha de tener la medida implantada para que su vulneración permita apreciar la realización de este delito, cuestión a la que algunos han respondido exigiendo que la medida se adecue al estado de la técnica (Morales García, 2010), pero que, a nuestro modo de ver y atendiendo a la inexistencia de prescripción normativa en tal sentido, ha de ser resuelta atendiendo a la verdadera finalidad de dicha exigencia típica, que no es otra que la de delimitar el espacio incluido en el nuevo derecho a la inviolabilidad informática, lo que nos ha llevado a entender que la medida en cuestión podrá ser de cualquier naturaleza y magnitud, desde un complejo y avanzado sistema de encriptación hasta el simple establecimiento de una clave en la BIOS del ordenador o la utilización de cortafuegos comerciales o gratuitos que traten de dificultar el acceso al sistema finalmente vulnerado (Galán Muñoz, 2006).

Una vez que la medida se haya vulnerado y el sujeto haya accedido de forma dolosa al sistema, se habrá completado el injusto típico de este delito, lo que determinará su consumación, y podrá ser castigado. Sin embargo, **el mero intento de vulneración de la medida o la consecución de su elusión no seguida del efectivo acceso al sistema en cuestión solo se podrá sancionar mediante la apreciación de la tentativa de este delito**, dado que al ser la conducta de acceso resultativa, como lo son las de matar o sustraer de las que

hablan otros delitos, nos encontraremos ante un delito doloso, de resultado y de lesión que permite sancionar su imperfecta realización sin mayores problemas.

Por otra parte, entrando ya en lo que se refiere a la segunda de las posibles modalidades comisivas, sorprende un poco que nuestro legislador haya optado por ir más allá de lo exigido por la DAI y haya decidido configurar como modalidad autónoma de este delito el mero hecho de «**facilitar a otro el acceso» a los sistemas de información**. El castigo específico de este tipo de conductas no aparece exigido en el artículo 3 de la DAI. De hecho, lo único que dicha Directiva establece respecto al posible castigo de conductas que faciliten o favorezcan la realización de accesos no autorizados a terceros es que los Estados miembros deberán garantizar el castigo de la complicidad en los actos de accesos no autorizados a sistemas de información de los que habla su artículo 3 (art. 8 DAI), algo que nuestro ordenamiento evidentemente ya garantizaba mediante la posible apreciación de las diferentes formas de participación contempladas en los artículos 28 y siguientes de nuestro Código penal con respecto a los accesos castigados por el artículo 197 bis.1 CP.

La finalidad de la inclusión de esta posible modalidad comisiva no era, por tanto, la de impedir la impunidad de este tipo de actuaciones. En realidad, a nuestro modo de ver, lo que aquí se hace es convertir en delito autónomo la conducta del facilitador del acceso, para garantizar así que este sujeto sea castigado como autor y mediante la apreciación de este delito en su forma consumada, con independencia de que el acceso que facilite al tercero se llegue o no a producir. Es decir, con independencia de si el tercero a quien pretendía ayudar a acceder al sistema ajeno de forma no autorizada consiguiese hacerlo o no.

Algunos autores (Colás Turégano, 2015) han considerado, sin embargo, que para que se pueda castigar esta conducta será necesario que el receptor de la ayuda del facilitador logre acceder al sistema en cuestión, ya que entienden que solo de esta forma se comprendería la concreta pena que se le prevé a quien realiza esta actuación (la misma que la prevista para el autor del acceso ilícito efectivamente consumado) y se podrían delimitar sus conductas facilitadoras de las que, como veremos, castiga el nuevo artículo 197 ter CP.

Sin embargo, dicha propuesta, a nuestro modo de ver, no consigue solventar el primero de los problemas que plantea, por cuanto, si bien permite que solo se castigue al autor de dicha conducta con la pena completa de este delito cuando el mismo se consume, lo hace incluso aunque su contribución al acceso realizado por otro hubiese sido tan escasa que solo permitiese considerarle, en su caso, como mero cómplice de dicho hecho, lo que, sin duda, también supondría una desproporcionada reacción frente a la contribución delictiva que habría realizado tal sujeto.

Más correcto nos parece, entonces, entender que cuando el legislador habla de facilitar el acceso, no está queriendo aludir al mero hecho de ayudar o auxiliar de cualquier modo y mediante cualquier contribución a que el tercero receptor de la ayuda consiga acceder al sistema, sino al hecho efectivo de darle la posibilidad a dicho sujeto de que acceda directamente y sin más al sistema (en similares términos, Morales Prats, 2016), dado que solo entonces, a nuestro juicio, se habría facilitado, y no meramente favorecido, dicho posible acceso.

Para ello, atendiendo a la configuración típica de este precepto, se necesitará, en primer lugar, que se vulnere, esto es, se inhabiliten las medidas de seguridad establecidas para impedir accesos no deseados, lo que nos lleva a entender que solo cuando el facilitador sea el que inhabilite tales medidas, para que sea otro el que pueda realizar y dominar el acceso ilícito pretendido sin mayores problemas, se podrá entender que le ha facilitado, es decir, le ha entregado el acceso y, por ello, se le podrá castigar mediante la apreciación de esta modalidad comisiva, aun cuando el acceso pretendido no se llegue finalmente a realizar.

Se determinaría así que solo se pudiese castigar por esta modalidad comisiva a quienes realicen unas contribuciones delictivas que, en caso de llegar a consumarse el acceso, obligarían a considerar a quienes las realizaron como coautores o, como mínimo, como cooperadores necesarios de tal conducta, algo que reduce los problemas de proporcionalidad que planteaba la propuesta anterior y deja, por otra parte, el castigo del resto de posibles contribuciones menores, meramente intentadas, a los accesos ajenos en manos de la eventual apreciación del controvertido delito del artículo 197 ter CP que analizaremos posteriormente.

Por último, este delito también castiga como modalidad consumada el mero hecho de **mantenerse en el sistema contra la voluntad de quien tiene el legítimo derecho a excluirlo**, conducta cuya sanción tampoco es exigida por el artículo 3 DAI, como tampoco lo estaba en la Decisión Marco 2005/222/JAI que precedió a tal Directiva, pero que, de hecho, ya aparecía expresamente contemplada en la versión anterior del delito que venimos analizando, establecida por nuestro legislador en el año 2010.

Pese a que algunos autores han planteado la posibilidad de que esta conducta solo sea sancionable por este delito cuando su realización también haya supuesto la vulneración de alguna medida de seguridad establecida para impedir el acceso, parece evidente que, atendiendo al tenor literal del precepto y si se quiere dotar de sentido propio a esta modalidad comisiva frente a la de acceso propiamente dicha, tal vulneración no resulta necesaria para apreciar su realización. Bastará, por tanto, con que quien hubiera accedido al sistema informá-

tico o a una parte de él de forma lícita o incluso expresamente consentida, se mantenga dentro, obviando la petición de quien tenía legitimación tanto para autorizarle a acceder como para pedirle que lo abandonase (esto es, del titular del derecho a excluir intromisiones ajenas en el sitio en cuestión). Cuando esto suceda, se deberá considerar que quien así actuó se había mantenido ilícitamente en el mismo y, por tanto, habría realizado esta modalidad comisiva, lo que vuelve a poner de manifiesto el hecho de que lo tutelado aquí no es la seguridad de los sistemas informáticos como se ha pretendido mantener, sino precisamente el derecho que se otorga a dichas personas a excluir todo o parte de sus sistemas de información de posibles intromisiones no deseadas realizadas por parte de terceros. Su derecho a mantener la inviolabilidad informática.

Finalmente, solo resta recordar que también las conductas de facilitación de acceso o de mantenimiento no autorizado en los sistemas deberán realizarse de forma dolosa para poder ser típicas de este delito, con lo que cualquier error, incluso el vencible, referido, por ejemplo, al hecho de estar facilitando el acceso no autorizado al tercero o al carácter no autorizado del mantenimiento en el sistema que se estaba realizando, determinará la atipicidad de las actuaciones efectuadas. No será necesaria, sin embargo, la concurrencia de ninguna intención adicional. Esto es, no se necesitará que se acceda para dañar el sistema, ni tampoco que se haga con la finalidad de descubrir secretos o la intimidad de la persona, lo que vuelve a poner de manifiesto el carácter exclusivamente protector de la inviolabilidad informática y no de la intimidad que presenta el delito aquí analizado.

No obstante, este hecho, a nuestro modo de ver, no impedirá que si la comisión de este delito se viese seguida por la de uno de los ataques a este último derecho fundamental de los que habla, por ejemplo, el artículo 197.1 CP (por ejemplo, se accede ilícitamente al sistema y se apodera delictivamente de los secretos), se tenga que apreciar el correspondiente concurso de leyes, y no de delitos, entre ambas figuras delictivas, dado que el carácter netamente instrumental que dicha inviolabilidad presenta con respecto a la intimidad finalmente atacada, determinará que el desvalor propio del injusto típico del delito del artículo 197 bis.1 CP quede absorbido por el que valora y castiga el delito contra la intimidad posteriormente cometido.

## 8. El delito de interceptación de trasmisiones no públicas de datos informáticos

En cumplimiento de lo exigido por el artículo 6 DAI, el legislador español decidió crear un nuevo tipo delictivo, contenido en el nuevo apartado 2 del artículo 197 bis CP, que castiga al «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».

Varios son los problemas interpretativos a que se enfrenta este nuevo delito, aunque tal vez el principal de ellos es el que concierne a la diferenciación de su injusto típico del referido a la interceptación de telecomunicaciones que castiga el apartado 1 del ya comentado artículo 197 CP.

Atendiendo a lo que nos indica el propio preámbulo de la LO 1/2015 que introdujo este delito, mientras el delito del artículo 197.1 CP estaría destinado a castigar las interceptaciones de comunicaciones personales, esto es, de las que realiza un individuo (una videollamada, un chat, un e-mail, etc.), en el ahora analizado se tratará de sancionar las interceptaciones de las **transmisiones que realizan los sistemas de información de forma automatizada**[16].

(16)Art. 197 bis.2 CP.

Parece evidente, entonces, que mientras el delito del artículo 197.1 CP castigará cualquier interceptación realizada sobre lo comunicado por una persona, el ahora estudiado hará lo propio tan solo con las que los sistemas de información de que se trate efectúen sin necesidad de intervención humana directa, sino de forma automática, como sucede, por ejemplo, con las transmisiones de datos que realizan de forma periódica y autónoma nuestros teléfonos móviles para mantenerse conectados a los repetidores que les permiten mantenerse en red.

Se entiende así que el precepto ahora analizado hable de las trasmisiones que se produzcan (no se efectúen) desde, hacia o dentro de un sistema de información y también que se aluda expresamente a las electromagnéticas, ya que todas estas opciones pueden darse de forma automatizada. Esto se refiere tanto a que un sistema envíe la señal, inalámbrica o no, hacia otro con el que todavía no está conectado (por ejemplo, el móvil recién encendido enviará datos hacia el repetidor del sistema con el que todavía no estaba conectado o el ordenador al servidor a través del que pretende conectarse a la red), que el sistema envíe datos hacia otros sistemas no predeterminados (por ejemplo, el enrutador de una vivienda mandará su señal y sus datos de identificación en general sin estar dirigido a otro sistema en concreto) o que los diferentes com-

ponentes de un sistema conectado a otros componentes integrados en el mismo se envíen datos entre sí para identificarse y mantenerse conectados (por ejemplo, los datos que se envían en una misma red sus diferentes terminales para identificarse –IP, MAC, protocolos de transmisión, etc.–).

Algunos autores han considerado que la expresa exigencia legislativa referida a que dichas transmisiones tengan que ser **no públicas** para que su interceptación pueda dar lugar a la apreciación de este delito, pese a venir expresamente contemplada en la DAI, resulta desafortunada y contraproducente (Morales Prats, 2016), crítica que no podemos compartir, ya que consideramos que lo que dicha exigencia trata es de excluir la posible tipicidad penal de las interceptaciones de transmisiones automatizadas de datos que se realicen en abierto, esto es, de forma pública (por ejemplo, la que efectúa quien conecta su móvil a una red de telefonía interceptando los datos que emite el repetidor que le permite el acceso a la misma o la que efectúa quien conecta su ordenador a un enrutador que da acceso a Internet en abierto a cualquiera que quiera conectarse al mismo).

Solo si los datos trasmitidos no son de acceso público y alguien las intercepta podrá apreciarse este delito.

No obstante, para hacerlo será necesario que la interceptación, ahora sí y a diferencia de lo que sucede en el artículo 197.2 CP, se efectúe **utilizando artificios o instrumentos técnicos**, esto es, mecanismos o programas tendentes a conseguir dicha captación (por ejemplo, barredores de frecuencias, programas rastreadores de IPS, etc.) y se haga además **actuando «sin estar debidamente autorizado»**, algo que, atendiendo de nuevo a lo establecido en el artículo 2.d DAI, determinará que queden al margen de este precepto tanto aquellas interceptaciones de transmisiones automáticas no públicas que se realicen con consentimiento del afectado, como las que se efectúen de forma legal.

**Interceptaciones legales**

Por ejemplo, las que efectúan los proveedores de servicios para atender a lo exigido por el artículo 4 de la Ley de conservación de datos o las realizadas por la policía judicial al amparo del cuestionable artículo 588 ter.1 LEcrim.

Nada más, aparte del dolo, exige este tipo delictivo para permitir su apreciación. Ni que la actuación se realice con la intención de conocer secretos, ni con la de afectar a la intimidad del afectado, como sucede con el delito del artículo 197.1 CP, lo que nos lleva a entender, por una parte, que el nuevo delito del artículo 197 bis.2 CP, a diferencia de aquel, sí que vendría a proteger directamente la **inviolabilidad de las comunicaciones** como derecho diferente pero instrumental de la intimidad y, por otra, que su creación lo que trata es de extraer este tipo de interceptaciones menores, referidas, por ejemplo, a la IP, IMEI, MAC, etc. que identifican a un sistema para comunicarlo con otros, del ámbito típico del artículo 197.1 CP para aplicarles una pena que atienda a la menor gravedad que presentan tales captaciones frente a las que se castigan en este último delito.

## 9. La facilitación de delitos contra la intimidad y los derechos afines mediante el suministro de instrumentos creados para cometerlos

El nuevo artículo 197 ter de nuestro Código penal trata de responder a lo exigido por el artículo 7 de la DAI al establecer 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; o

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

Se castigan así toda una serie de conductas cuya realización individual dará lugar a la consumación de este delito, sin que su ejecución acumulada sobre un mismo objeto determine la apreciación de varios, lo que lleva a que nos encontremos ante un claro ejemplo de tipo mixto alternativo.

En concreto, esta figura castiga producir, adquirir para el uso, importar o, de cualquier otro modo, facilitar a terceros determinados objetos, cuando tales actuaciones se realizaran de forma no autorizada, es decir, ni consentida ni realizada con autorización legal (piénsese, por ejemplo, en los programas que pueda crear la Policía para realizar los registros remotos de ordenadores ajenos autorizados por los arts. 588 sexties y sigs. LECrim), y con una determinada finalidad, la de facilitar la comisión de los delitos de los artículos 197.1, 197.2 o 197 bis de nuestro Código penal.

Los objetos sobre los que dichas conductas pueden recaer son dos alternativos:

- programas informáticos principalmente concebidos o adaptados para cometer delitos, o
- contraseñas de ordenador, códigos de acceso a datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Dentro de los primeros entrarán tanto los **programas** que se creen y tengan por única finalidad facilitar alguno de los delitos anteriormente citados (por ejemplo, programas keygen, keyloggers, troyanos, etc. que permiten realizar accesos no autorizados a sistemas ajenos), como los que, pudiendo ser utilizados para realizar otro tipo de actividades, solo tengan dicha posible utilidad al-

ternativa como algo meramente marginal, estando, por ello, primordialmente, aunque no exclusivamente, destinados a facilitar la comisión de tales actos delictivos (por ejemplo, un programa desencriptador que permita cometer uno de los comentados delitos y también realizar complejos cálculos matemáticos, aunque esta segunda utilidad queda como algo completamente residual y de difícil empleo frente a la primera).

Por su parte, entre los segundos estarían incluidos desde las simples **claves** de un ordenador, de un correo electrónico, de un archivo o carpeta, hasta los datos biométricos que, cada vez de forma más frecuente, identifican a una persona a la hora de acceder a un sistema de información.

No obstante, para que la realización de cualquiera de las comentadas conductas, de forma no autorizada y sobre alguno de estos dos posibles objetos, dé lugar a la apreciación de este delito[17], tendrá que haberse ejecutado, además de dolosamente, «con la intención de facilitar la comisión de los delitos de los apartados 1 y 2 del artículo 197 o la del artículo 197 bis» de nuestro Código penal.

(17)Art. 197 ter CP.

Esta exigencia introduce un especial elemento subjetivo del injusto en este delito, que determina que solo pueda apreciarse cuando quien efectúe alguna de las señaladas conductas, lo haga teniendo la intención y finalidad de favorecer la comisión, bien por su parte, bien por parte de un tercero, de algún delito concreto de entre los citados en el comentado precepto.

Esta figura se convierte, así, en un delito de tendencia interna trascendente y mutilado en dos actos que exige que su conducta típica se efectúe con intención de cometer otra posterior (uno de los referidos delitos) para poder ser apreciado, pero que no requiere para hacerlo que esta segunda conducta se llegue ni siquiera a comenzar a ejecutar. Lo que hará falta es que se efectúe con la intención de cometer o ayudar a cometer uno de los referidos delitos. Uno concreto y determinado, exigencia típica que evidentemente excluye del ámbito típico de esta figura todas aquellas actuaciones que recaigan sobre los referidos objetos y que se realicen de forma no autorizada, pero que se hagan, por ejemplo, con la intención de favorecer la comisión general de dicha clase de delitos y no la de uno en concreto, quedando así claro que estamos ante una figura que castigará como delito autónomo y consumado lo que no serían sino una serie de actos preparatorios de la autoría o de la participación en el concreto delito que se pretendía cometer o favorecer con su realización.

Precisamente, el mantenimiento de esta configuración típica dará lugar a evidentes y graves problemas prácticos. Por ejemplo, si partimos, como hemos hecho, de que la figura ahora analizada vendría a castigar algunas modalidades meramente preparatorias de otros delitos, ello debería llevarnos a pensar que, en principio, si a su realización le siguiese la del delito que su ejecución

prendía favorecer, su injusto debería quedar absorbido por el de este con total independencia de si este último delito había quedado en grado de tentativa o se había llegado a consumar.

Sin embargo, dicha aparentemente evidente solución puede plantear serios problemas de proporcionalidad, ya que, al castigar al autor del delito del artículo 197 ter CP con la misma pena que la que impone, por ejemplo, el delito del artículo 197 bis.1 CP a quien comete su injusto en su forma consumada, se podría llegar a la absurda situación de que si un sujeto se hiciese, por ejemplo, con la clave de un ordenador ajeno para acceder a él de forma delictiva, pero no llegase a utilizarla para lograrlo, podría en principio ser castigado con la pena del delito consumado del artículo 197 ter CP, mientras que si la utilizase y, pese a ello, no consiguiese acceder al ordenador en cuestión, solo habría de responder con la pena rebajada que le correspondería por la tentativa del delito del artículo 197 bis.1 CP, algo que evidentemente carece de sentido, dado que este último ataque es más grave por representar un mayor desvalor de resultado que el efectuado por el sujeto anterior.

La única opción, entonces, para evitar este verdadero dislate punitivo será resolver el concurso de leyes que se dará en estos casos entre la figura ahora analizada y las que sancionen los posteriores ataques contra la intimidad a los que su realización hubiese llegado efectivamente favoreciendo la aplicación de la calificación que suponga una mayor pena al autor de dicha conducta. Esto es, solventar este concurso aplicando el siempre cuestionable **principio de alternatividad** y no el de consunción, un principio que en algunas ocasiones determinará que se aplique preferentemente el delito aquí analizado y no el posteriormente cometido, por más que el primero castigue lo que a todas luces serían meros actos preparatorios de la actuación que castigaría esa última figura.

No es este, sin embargo, el único problema que ha planteado la no demasiado meditada configuración y pena que se ha otorgado al delito que venimos analizando.

En este mismo sentido, también se ha criticado que esta figura castigue con la misma pena actos preparatorios considerados como independientes si se dirigen a realizar los delitos de los apartados 1 y 2 del artículo 197 CP o a los de los del 197 bis CP, olvidando que estos últimos delitos tienen penas significativamente inferiores a las previstas para los primeros. Sin embargo, este problema tal vez se pueda subsanar, o al menos paliar, imponiendo penas mayores al autor que realice dichos actos preparatorios con la finalidad de cometer alguno de los dos primeros delitos y menores al que lo haga con la intención de cometer uno de los últimos.

Sin embargo, si hay un problema referido a esta figura que ha planteado verdaderos quebraderos de cabeza es el que se deriva de la necesidad de diferenciar y delimitar las conductas facilitadoras que tendrán cabida en su tipo de

aquellas otras que la tendrán en el del delito contemplado en el apartado 1 del artículo 197 bis CP cuando castiga al que facilite a otro el acceso al sistema de información.

A nuestro modo de ver, como ya dijimos anteriormente, la única forma de dotar de una solución razonable y proporcionada a la cuestionada diferenciación de las conductas castigadas por cada uno de estos delitos, que atienda además al tenor literal de los preceptos que los establecen, es entender que mientras el artículo 197 ter CP sanciona la facilitación a terceros de determinados instrumentos favorecedores del acceso para que sea su receptor quien los emplee (por ejemplo, la clave para acceder la usará el que la recibe), el artículo 197 bis.1 CP sancionaría a quien no solo suministra alguno de tales instrumentos, sino que además los utiliza (por ejemplo, usa la clave y desbloquea el sistema) dejando así vía libre a otro para que ejecute materialmente el acceso ilícito, ya que solo así se podría entender que le habría facilitado el acceso tal y como exige el tenor literal del referido precepto de nuestro Código penal.

## 10. Tipos cualificados

Los artículos 197 quater y 198 CP contemplan dos posibles cualificaciones referidas a cualquiera de los delitos anteriormente comentados. Esto es, tanto a los delitos del artículo 197 como a los del 197 bis o el del 197 ter del CP.

> El primero 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».

El incremento de penas aplicables a estos delitos cuando se realizasen en el seno de estas organizaciones ya aparecía contemplado en la legislación penal previa a la reforma de 2015, atendiendo, entre otras cosas, al mandato comunitario existente en tal sentido desde la DAI de 2010. Sin embargo, tras la reforma efectuada por la LO 1/2015, esta cualificación, además de resultar predicable con respecto a los delitos del artículo 197 CP y al de intrusismo informático del artículo 197 bis.1 CP, como sucedía antes de dicha LO, también podrá apreciarse no solo en relación con el nuevo delito de interceptación de comunicaciones informáticas no públicas del artículo 197 bis.2 CP, sino incluso con respecto al delito de revelación de secreto profesional o laboral del artículo 199 CP, extensión que no parece tener demasiado sentido ni encuentra fundamento con lo exigido por el vigente DAI, dado que el artículo 7.2 de dicha Directiva tan solo obliga a incrementar las penas de los delitos que contemplan sus artículos 4 y 5 (esto es, de nuevo, los referidos a los daños constitutivos de interferencia ilegal en datos o en sistemas informáticos) y, por ello, ha sido severa y fundadamente criticada por la doctrina (véase Morales Prats, 2016).

Finalmente, cabe señalar que este tipo cualificado será aplicable sin necesidad de que la organización criminal en cuestión esté destinada a cometer este tipo de delitos (puede estar dirigida a cometer otros, siendo la ejecución de uno de los aquí comentados meramente ocasional o puntual) y que su apreciación es evidentemente incompatible con la del delito de pertenencia a este tipo de organizaciones del artículo 570 bis.1 CP.

Sin embrago, aunque la extensión del ámbito de aplicación de este tipo cualificado plantea serías dudas y no parece haber sido suficientemente meditada, mayores problemas genera aún el contemplado en el artículo 198 CP, precepto donde se 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».

Ya desde un primer momento la redacción este artículo genera problemas y se muestra como técnicamente incorrecta, ya que, si nos fijamos, el comentado tipo cualificado limita expresamente su aplicación a «las conductas descritas en el artículo anterior», esto es, a las conductas de las que habla el artículo 197 quater CP, precepto que no describe conducta delictiva alguna, sino que se limita a establecer la posible sanción de la persona jurídica atendiendo a lo exigido por el artículo 31 bis CP.

Cierto es que en dicho precepto se alude a los delitos de los artículos 197, 197 bis y 197 ter CP, pero no parece que dicha alusión general sea suficiente para permitir aplicar este tipo cualificado a las conductas contempladas en los mismos sin poner en entredicho el principio de legalidad penal (obsérvese que se habla de las conductas descritas en el artículo anterior, no de las meramente mencionadas), ni tampoco que el legislador tuviese en la cabeza dicha mención cuando mantuvo este precepto. Más bien parece que las prisas del legislador y su incompetencia le llevaron a mantener la redacción del anterior artículo 198 ACP, que lógicamente aludía a las conductas del entonces vigente 197 CP, olvidando que en la actualidad, tras la reforma de 2015, hay varios artículos más que preceden al actual 198 CP, entre los cuales se encuentra, precisamente, el artículo 197 quater CP que le precede.

En cualquier caso, el fundamento para el incremento de penas contemplado por este precepto resultaba obvio. Se sustentaba en el abuso del cargo público que efectúa quien emplea dicha posición para realizar un delito contra la intimidad.

No obstante, para que se pudiese apreciar este cuestionado tipo cualificado, haría falta además que el funcionario o autoridad en cuestión los hubiese cometido **sin que mediase causa por delito**. Esto es, sin estar actuando dentro y al amparo de una investigación por delito, lo que podría permitirle realizar algunas intromisiones legítimas, aunque limitadas, en la intimidad de terceros, y llevaría a que si las realizasen en tales supuestos, pero de forma que superase los límites establecidos, se tuviese que castigar al funcionario conforme a lo establecido en los delitos de los artículos 535 y 536 CP y no atendiendo a lo que define el tipo cualificado aquí comentado. Así sucedería, por ejemplo, cuando el funcionario en cuestión hubiese prolongado una interceptación de comunicaciones realizada al amparo de una investigación por delito más allá de lo que se le había autorizado judicialmente o la hubiese extendido a terminales no incluidos en su autorización.

Lo importante, en cualquier caso, no es si el funcionario realizó la violación de la intimidad ajena con intención o no de investigar un delito, sino si lo hizo al amparo de una investigación reconocida como tal en la que se hubiera extra-

limitado de lo que estaba autorizado a hacer. Esto llevaría a que, si un funcionario atentase contra la intimidad de un tercero actuando completamente al margen de un procedimiento de investigación por delito como tal, responderá por este tipo cualificado y no por los delitos de los artículos 535 y 536 CP, por más que lo hubiese hecho con la intención de investigar o perseguir un hecho delictivo que creyese cometido.

Por otra parte y en relación con las conductas realizadas por funcionarios, cabe señalar que si ya el legislador se ha mostrado descuidado, como hemos visto, al regular el tipo cualificado del artículo 198 CP que les resulta aplicable cuando cometan algún delito contra la intimidad de los que venimos comentando, lo ha sido aún más en lo que se refiere a la regulación de los artículos 535 y 536 CP, dado que al continuar manteniendo dichos preceptos su redacción previa a 2015, mantienen muchas de las nuevas conductas delictivas contra la intimidad y otros derechos afines introducidos por la reforma efectuada ese mismo año al margen de sus respectivos tipos delictivos, lo que, lejos de determinar la impunidad de tales actuaciones, obliga, a nuestro modo de ver, a que se tenga que castigar a los funcionarios o autoridades que las realicen (cuando lo hagan mediando causa por delito) por los delitos comunes que hemos analizado, apreciando la agravante de abuso de prevalimiento del cargo del artículo 22.7ª CP, algo que debería corregirse lo antes posible, como también tendría que serlo el tenor literal del artículo 198 CP para subsanar el evidente problema de legalidad que plantea su actual y descuidada redacción.

Finalmente, no queremos terminar esta breve exposición referida a los tipos cualificados aplicables a los delitos anteriormente estudiados sin destacar el hecho de que el artículo 573 CP establece que tendrán la consideración de **delitos terroristas** los contemplados en los artículos 197 bis y 197 ter CP cuando concurran en su realización alguna de las finalidades de las que habla el primer apartado de dicho artículo, mientras que el 573 bis.3 CP determina que en tales casos se tenga que aplicar a sus responsables la pena superior en grado a la generalmente prevista para su comisión, algo cuando menos cuestionable, ya que pasa a convertir en delito terrorista (con todo lo que ello implica, tanto material como procesalmente) actuaciones que no parece que presenten siempre la suficiente gravedad para recibir tan severo tratamiento y, además, deja sin que se pueda tener por tales otras actuaciones delictivas contra la intimidad (por ejemplo, las de los dos primeros apartados de los arts. 197 CP), mucho más graves y lesivas que aquellas.

Tal vez en tan cuestionable decisión legislativa haya pesado el hecho de que los dos delitos aludidos (los de los arts. 197 bis y 197 ter CP) contengan nuevas figuras directamente conectadas con la, como ya vimos, siempre considerada especialmente peligrosa criminalidad informática, lo que, además de olvidar que puede haber ataques no informáticos a la intimidad igual o más graves que los que lo son, también obvia el hecho de que muchas de las actuaciones

del artículo 197 CP pueden estar, como también hemos visto, referidas a dicha forma de criminalidad (por ejemplo, la interceptación de comunicaciones o el apoderamiento de datos personales).

## 11. Algunas consideraciones generales

No se puede terminar este análisis general de los delitos informáticos protectores de la intimidad y de los derechos afines (protección de datos, inviolabilidad informática o de las comunicaciones) sin señalar que todas las figuras anteriormente comentadas, con excepción de las contempladas en el artículo 198 CP, de las de los artículos 535 y 536 CP y de las modalidades calificadas como terroristas, son delitos privados que solo pueden ser perseguidos a instancia de parte y que permiten que quienes los cometen puedan quedar exentos de pena en caso de que los perdone el ofendido (art. 201 CP).

También conviene indicar que el artículo 197 quinquies CP contempla expresamente la posible responsabilidad penal de la persona jurídica cuando concurran los requisitos del artículo 31 bis CP respecto a la comisión de los delitos que hemos analizado, con excepción hecha del tipo cualificado contenido en el artículo 198 CP, figura posiblemente excluida de entre las que pueden determinar la responsabilidad penal de tales entidades como consecuencia de que, al contemplar dicho tipo una figura especial que solo puede ser cometida por funcionario o autoridad pública que actúe mediando causa por delito, se partió de que tales sujetos solo podrían cometerlo en el seno de alguna de las personas jurídicas que el artículo 31 quinquies CP expresamente excluye de tal posible sistema de responsabilidad penal (Estado, Administraciones públicas, etc.).

Para finalizar, solo nos resta señalar que el artículo 200 CP declara 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», lo que extiende de forma discutible la protección prevista en delitos como los de los artículos 197.1, 2 y 3 CP a las entidades dotadas de personalidad jurídica, pese a que se ha cuestionado y se cuestiona que puedan ser realmente titulares de un verdadero derecho a la intimidad. En cualquier caso, es necesario recalcar que si los datos reservados de tales entes tuviesen trascendencia económico-competitiva, su descubrimiento o revelación serían preferentemente castigados mediante la apreciación de los delitos de revelación de secreto empresarial contemplados en los artículos 278 y siguientes de nuestro Código penal y no por los delitos que hemos analizado a lo largo de este módulo.

# Ejercicios de autoevaluación

**1.** La interceptación no autorizada de una telecomunicación ajena...

**a)** siempre será delito, ya que afecta al derecho fundamental al secreto de las comunicaciones.
**b)** solo será delito si se efectúa utilizando algún artificio técnico que sirva para realizarla.
**c)** tendrá que realizarse con el fin de descubrir secretos de su víctima para que pueda ser delito.
**d)** no se aplicará en ningún caso a los supuestos referidos a mensajes de correo electrónico.

**2.** Habrá que entender que un dato personal tendrá el carácter de reservado del que habla el delito del artículo 197.2 CP...

**a)** solo si está recogido en formato digital.
**b)** si no es públicamente conocido.
**c)** si está referido a cuestiones especialmente sensibles para la intimidad, como pueden ser las relativas a la tendencia política o las creencias religiosas del sujeto al que está referido.
**d)** si no se ha obtenido de una fuente de acceso público.

**3.** Los correos electrónicos...

**a)** solo pueden ser objeto del delito de apoderamiento de documentos.
**b)** solo pueden dar lugar al delito de interceptación de las comunicaciones.
**c)** pueden dar lugar al delito de apoderamiento o al de interceptación, dependiendo de cuál sea la conducta no autorizada que se realice sobre los mismos.
**d)** solo quedan amparados por los delitos contra la intimidad en la medida en que contengan información reservada.

**4.** El intento de obtener datos personales ajenos mediante engaño, por ejemplo mediante el envío indiscriminado y masivo de correos electrónicos engañosos a diferentes sujetos (*phishing*)...

**a)** constituye siempre un delito contra el derecho a la protección de datos personales del artículo 197.2 CP.
**b)** no constituye por sí mismo delito contra la protección de datos personales.
**c)** solo constituirá delito contra los datos personales si se realiza sobre datos especialmente sensibles, como los referidos a la orientación sexual o la ideología del afectado.
**d)** solo dará lugar a delito si se realiza ante menores de catorce años que no puedan consentir por sí solos el tratamiento de los datos obtenidos.

**5.** Si un sujeto recibe en su móvil unas fotos íntimas pertenecientes a otra persona que le reenvía un tercero que las tenía de forma autorizada, pero que las había distribuido sin la autorización del afectado, y decide, pese a conocer dicho hecho, proceder a su vez a reenviar dichas imágenes a su lista de contactos...

**a)** no comete delito alguno.
**b)** comete un delito de revelación de secreto profesional al ser el encargado del tratamiento de dichas fotos.
**c)** comete un delito de revelación de imágenes reservadas captadas de forma autorizada (art. 197.7 CP).
**d)** comete un delito de revelación de secreto obtenido mediante la previa comisión de un delito por parte del tercero que sanciona el artículo 197.3 *in fine* CP.

**6.** Si un sujeto, mediante un barredor de frecuencia, obtiene los números de identificación de los móviles (IMEI) conectados al repetidor de la zona donde vive con el fin de averiguar si su novia estaba por dicha zona...

**a)** cometerá un delito de interceptación de telecomunicaciones del artículo 197.1 CP.
**b)** cometerá un delito de interceptación de trasmisiones no públicas de datos informáticos del artículo 197 bis.2 CP.
**c)** realiza una conducta completamente atípica, pues no ha efectuado la interceptación para descubrir ningún secreto.
**d)** cometerá un delito contra el derecho a la protección de datos personales del artículo 197.2 CP.

# Solucionario

## Ejercicios de autoevaluación

**1. c**

**2. d**

**3. c**

**4. b**

**5. a**

**6. b**

# Bibliografía

**Colás Turégano, M. A.** (2015). «Nuevas conductas delictivas contra la intimidad (art. 197, 197 bis y 197 ter». En: *Comentarios a la reforma del Código penal de 2015*. Valencia: Tirant lo Blanch.

**Galán Muñoz, A.** (2006). «Ataques contra sistemas informáticos». *Boletín de Información del Ministerio de Justicia* (ejemplar dedicado a la armonización del derecho penal español: una evaluación legislativa; año 60, n.º 2015 [extraordinario], págs. 225-239).

**Galán Muñoz, A.** (2009). «La internacionalización de la represión y la persecución de la criminalidad informática: Un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales». *Revista Penal* (n.º 24, págs. 90-107).

**Galán Muñoz, A.** (2010). «El robo de identidad: aproximación a una nueva y difusa conducta delictiva». En: A. Rallo Lombarte; L. Arroyo Zapatero; I. Alamillo Domingo, y otros. *Robo de identidad y protección de datos* (págs. 169-198). Cizur Menor: Aranzadi.

**Galán Muñoz, A.** (2013). «¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación». *Revista General de Derecho Penal* (n.º 19).

**Mata y Martín, R.** (2001). *Delincuencia informática y Derecho penal*. Madrid: Edisofer.

**Morales García, O.** (2010). «Delincuencia informática, intrusismo, sabotaje informático y uso ilícito de tarjetas (artículos 197.3 y 8, 264 y 268)». En: G. Quintero Olivares (dir.). *La reforma penal de 2010, análisis y comentarios*. Cizur Menor: Aranzadi.

**Morales Prats, F.** (2016). «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio». En: *Comentarios al Código penal* (tomo I). Cizur Menor: Aranzadi.

**Muñoz Conde, F.** (2017). *Derecho penal. Parte especial*. Valencia: Tirant lo Blanch.

**Puente Aba, L. M.** (2007). «Delitos contra la intimidad y nuevas tecnologías». *Eguzkilore* (n.º 21).

**Romeo Casabona, C. M.** (2004). *Comentarios al Código penal. Parte especial II*. Valencia: Tirant lo Blanch.