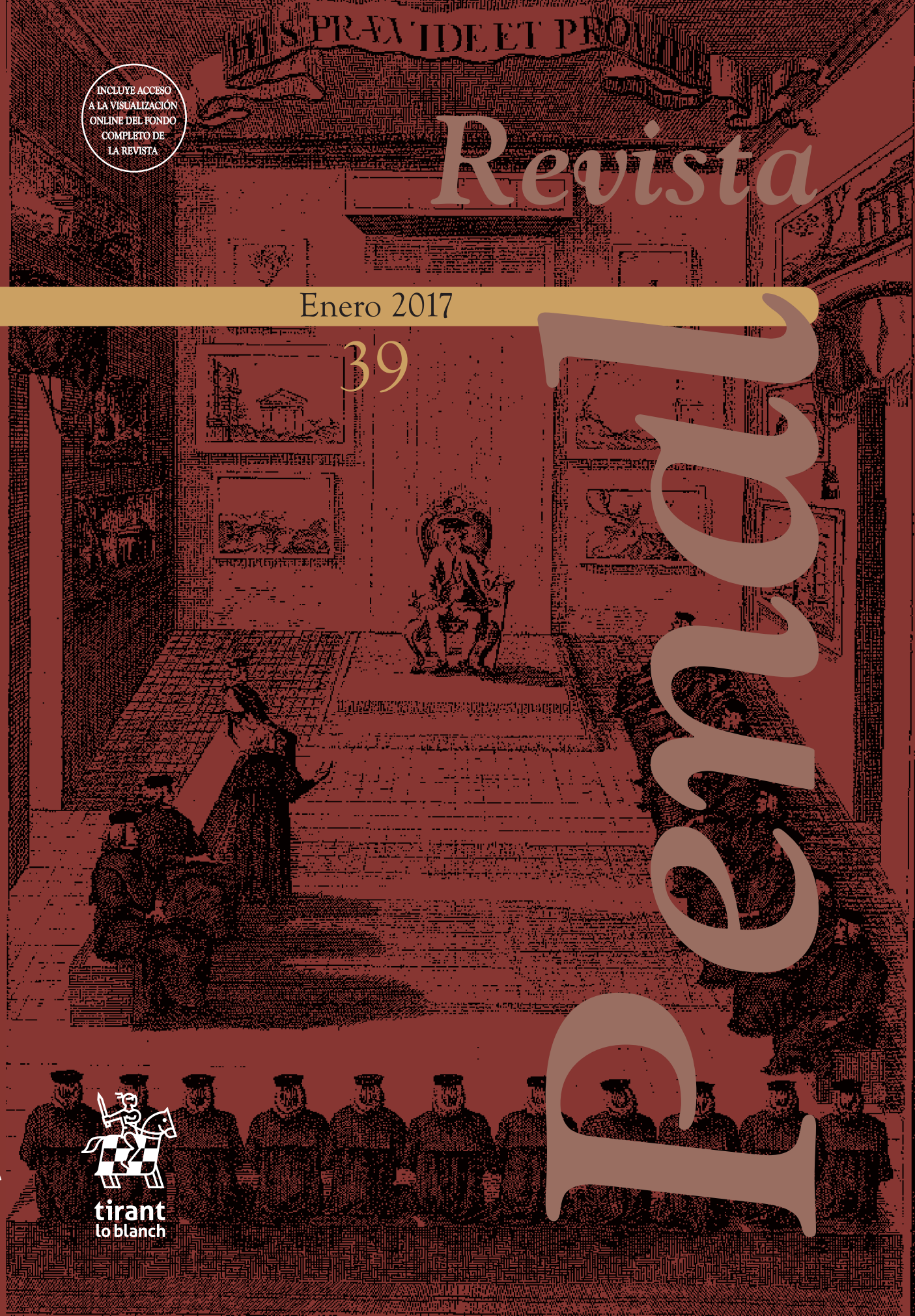
39

INCLUYE ACCESO A LA VISUALIZACIÓN ONLINE DEL FONDO COMPLETO DE LA REVISTA

Revista Penal

Enero 2017

39



Revista Penal

Enero 2017

tirant lo blanch

tirant lo blanch

Revista Penal

Número 39

Sumario

Doctrina:

– Caso *Rwabukombe:* interpretación del Tribunal Supremo Federal alemán de la (co)autoría y la intención de destruir en el genocidio, por *Kai Ambos* 5
– Política criminal y terrorismo en el Reino de España: ¿tiempos nuevos o *déjà vu*?, por *David Castro Liñares* 16
– Sobre la delimitación entre el delito de blanqueo de capitales del art. 301.1 CP y la participación por título lucrativo del art. 122 CP: una primera aproximación, por *Juana del Carpio Delgado* 31
– Revisión crítica de los presupuestos, carácter y alcance de la pena de inhabilitación profesional en el CP español: referencia especial a la inhabilitación profesional médica, por *Javier de Vicente Remesal* 50
– A vueltas con el bien jurídico protegido en el art. 290 CP, por *Paz Francés Lecumberri* 66
– Artículo 76.2 CP: una evolución jurisprudencial aún inacabada, por *Manuel Gallego Díaz* 78
– Responsabilidad penal y responsabilidad política: elementos para la diferenciación y la confluencia, por *Mercedes García Arán* 95
– ¿Es posible la comisión imprudente del delito de falsificación de documentos públicos cometido por funcionario? Hacia una clarificación del tipo subjetivo del artículo 250 CP cubano, por *Dayan G. López Rojas* 113
– La cuestionable regulación penal de los delitos de financiación ilegal de partidos políticos, por *Elena Núñez Castaño* 125
– El derecho de la víctima a ser informada en el sistema penal español, por *Natalia Pérez Rivas* 154
– Los delitos de descubrimiento y revelación de secretos en el Código Penal de 2015: artículos 197, 197 bis, 197 ter, 197 quáter, 197 quinquies y 198, por *María del Valle Sierra López* 174
– Los círculos restaurativos como complemento de la justicia, por *Rocío Zafra Espinosa de los Monteros* 200

Sistemas penales comparados: La administración desleal de patrimonio ajeno (Embezzlement) 216

Jurisprudencia: Un nuevo despropósito jurídico en el caso *Prestige:* ahora el Tribunal Supremo (comentario a la STS nº 865/2015, Sala Segunda, de lo penal, de 14 de enero de 2016), por *Carlos Martínez-Buján Pérez* 256

Noticias: VIII Foro Internacional sobre Delincuencia y Derecho Penal en la Era Global (Beijin- octubre 2016), por *Miguel Abel Souto* 284

Universidad de Huelva · VNiVERSiDAD D SALAMANCA · UCLM Universidad de Castilla-La Mancha · Universidad Pablo de Olavide Sevilla Año 1997 · Cátedra de Derechos Humanos Manuel de Lardizábal · Santander

tirant lo blanch

Publicación semestral editada en colaboración con las Universidades de Huelva, Salamanca, Castilla-La Mancha, Pablo Olavide de Sevilla y la Cátedra de Derechos Humanos Manuel de Lardizábal.

www.revistapenal.com

EDITA: TIRANT LO BLANCH
C/ Artes Gráficas, 14 - 46010 - Valencia
TELFS.: 96/361 00 48 - 50
FAX: 96/369 41 51
Email:tlb@tirant.com
http://www.tirant.com
Librería virtual: http://www.tirant.es
DEPÓSITO LEGAL: B-28940-1997
ISSN.: 1138-9168
IMPRIME: Guada Impresores, S.L.
MAQUETA: Tink Factoría de Color

Los delitos de descubrimiento y revelación de secretos en el Código Penal de 2015: artículos 197, 197 bis, 197 ter, 197 quáter, 197 quinquies y 198

María del Valle Sierra López

Revista Penal, n.º 39 - Enero 2017

Ficha Técnica

Autor: M.ª del Valle Sierra López. Profesora Titular de derecho Penal
Title: Offences of discovery and disclosure of private information after the reform of 2015 (Sections 197, 197 bis, 197 ter, 197 quarter, 197 quinquies and 198 of the Penal Code).
Adscripción profesional: Profesora titular de Derecho penal (Universidad Pablo de Olavide).

Sumario: 1. Introducción. 2. Evolución legislativa. 3. Descubrimiento y revelación de secretos antes de la reforma del Código Penal de 2015. 3.1. Descubrimiento de secretos documentales. 3.2. Interceptación de comunicaciones y control audiovisual clandestino. 3.3. Descubrimiento de secretos recogidos en archivos o registros. 3.4. Acceso a datos y sistemas informáticos. 4. Los delitos de descubrimiento y revelación de secretos tras la reforma de 2015. 4.1. Los tipos cualificados. 4.1.1. «Si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores». 4.1.2. «Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros o se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima». 4.1.3. Por el carácter «sensible» de los datos. 4.1.4. Por el fin lucrativo. 4.1.5. La difusión no autorizada de imágenes o grabaciones audiovisuales obtenidas con el consentimiento de la víctima. 4.2. Las conductas delictivas recogidas en el artículo 197 bis. 4.3. El delito de facilitación de programas informáticos, contraseñas de ordenador o códigos de acceso o similares para facilitar la comisión de otros delitos, recogido en el artículo 197 ter. 4.4. El artículo 197 quáter: Cualificación en caso de organización o grupo criminales. 4.5. La responsabilidad de las personas jurídicas: artículo 197 quinquies. 4.6. Por el carácter de autoridad o funcionario público del sujeto activo (artículo 198 del Código Penal). 5. Conclusiones.

Resumen: La reforma operada en 2015 ha afectado también a los delitos de descubrimiento y revelación de secretos. Concretamente ha supuesto el mantenimiento de algunas figuras delictivas, el cambio de ubicación de algunos tipos penales, la modificación de algunas figuras delictivas, así como la creación de algunas nuevas. En este último caso debido a la transposición de la Directiva Europea 2013/40/UE. Todos estos cambios exigen una revisión de los tipos penales más significativos del Capítulo I del Título X del Código penal, su valoración y repercusión a partir de ahora.
Palabras clave: Descubrimiento y revelación de secretos; interceptación de comunicaciones; Descubrimiento de secretos recogidos en archivos y registros; acceso a datos y sistemas informáticos; tipos cualificados

Abstract: The reform of the Penal Code enacted in 2015 has also had its effect on the discovery and disclosure of private information offences. In particular, while maintaining some types of crimes, this reform moved other offences to other locations, changed some types of crimes and created new offences. These new criminal offences have been created in order to adopt the transposition of European Directive 2013/40/UE. All changes will require a review of the most significant criminal offences of Chapter I, Title X of Penal Code, an assessment and its effect from this point on.
Key words: Discovery and disclosure of private information; Interception of communications; Discovery of recorded or archived confidential information; Access to electronic data and systems; Aggravated offences.

Observaciones: Trabajo de investigación realizado dentro del Grupo de investigación Ciencias Penales y Criminología SEJ 047.

Rec: 13-09-2016 **Fav:** 03-11-2016

1. Introducción

La ley de reforma 1/2015, de 30 de marzo ha sido y está siendo enormemente criticada no sólo por su evidente carácter conservador y en ocasiones autoritario, sino por el galimatías en el que ha terminado convirtiendo nuestro Código Penal. Pocos son los tipos penales que mantiene inalterables y las modificaciones, en la mayoría de los casos son tan profundas y drásticas que conllevan una nueva concepción de las figuras delictivas. En definitiva, el nuevo texto legal revela las verdaderas intenciones del legislador: otorgar una nueva trayectoria político-criminal y estructural a la legislación punitiva.

La reforma operada por la ley 1/2015, de 30 de marzo afecta también a los delitos contra la intimidad, justificándose por parte del preámbulo de la ley por la necesidad de «solucionar los problemas de falta de tipicidad de algunas conductas». En principio las reformas parecen meramente formales exceptuando la inclusión de los nuevos tipos penales o la cualificación del nuevo apartado 7 del artículo 197, con este trabajo pretendo analizar cómo quedan situados los delitos contra la intimidad objeto de este estudio.

Desde el Código Penal de 1995 se ha considerado que el artículo 197 recoge un conglomerado de figuras delictivas entre tipos básicos y cualificados, que lejos de aclararse se complicó aún más con la reforma de la LO 5/2010 que introdujo el nuevo tipo de acceso a datos y sistemas informáticos, pasando los hasta entonces apartados 3, 4, 5 y 6 a los hasta hace poco 4, 5, 6 y 7 y añadiéndose un nuevo apartado 8. Con la nueva ley del 2015 el artículo 197 pasa a tener siete apartados reubicándose en él los ya existentes o bien otros pasan a reubicarse en un nuevo precepto (arts. 197 quáter y 197 quinquies), por lo que, entre otras cosas, se introduce el artículo 197 bis, y se añade una nueva figura delictiva en el artículo 197 ter.

2. Evolución legislativa

La regulación anterior al Código Penal de 1995 era obviamente muy rudimentaria y simplista. En el antiguo artículo 497[1] se protegía la intimidad[2] a través del delito de descubrimiento de secretos personales, de una manera que hoy calificaríamos de bastante arcaica. En el artículo 497 se recogía un tipo básico y un tipo privilegiado en virtud de si el secreto se divulgaba o no y una excusa absolutoria para los padres o tutores en relación al apoderamiento de papeles o cartas de sus hijos o tutelados. Básicamente el delito se centraba en el apoderamiento del soporte documental en el que se sustentaba el secreto (papeles o cartas)[3] y en estos dos elementos se recogía dicho secreto. No obstante, nuestra jurisprudencia entendía que aún siendo el apoderamiento el elemento central de esta figura delictiva no solamente comprendía el desplazamiento material, sino también la captación mental o intelectual sin desplazamiento físico [STS de 3 de abril de 1957] sin olvidar que también debía estar presente el elemento finalista integrado por la intención de descubrir los secretos. Por tanto, ya desde el nacimiento de esta figura delictiva se planteaba la discusión acerca del alcance del término «apoderamiento», dado que en la doctrina no había consenso[4]. Así para un sector

1 Redacción prácticamente inalterable desde su redacción originaria en el Código Penal de 1848 hasta las modificaciones efectuadas en los años ochenta.

2 El Derecho a la intimidad no en todas sus facetas, sino la «*privacy*» como la facultad de exclusión de terceros con relación a hechos y circunstancias relativas a la intimidad con relevancia jurídica.

3 El antiguo delito de descubrimiento y revelación de secretos documentales se recogía en el artículo 497 que establecía: «*El que para descubrir los secretos de otro se apoderase de sus papeles o cartas y divulgare aquéllos será castigado con las penas de arresto mayor y multa de 100.000 a 2.000.000 de pesetas.*

Si no los divulgare, las penas serán de arresto mayor y multa de 100.000 a 500.000 pesetas

Esta disposición no es aplicable a los padres, tutores o quienes hagan sus veces en cuanto a los papeles o cartas de sus hijos o menores que se hallen bajo su dependencia».

4 Así por ejemplo había quien consideraba que se estaba ante un delito compuesto integrado por la conjugación de las siguientes acciones: a) apoderarse de papeles o cartas de otro con la finalidad de descubrir sus secretos b) descubrir los secretos en cuestión y c)

doctrinal el término debía entenderse normativamente «en el sentido de traslación posesoria cognitiva, que posibilitara el acceso intelectivo al contenido de los documentos[5]. Otros[6] precisaban que sería necesario el acto de aprehensión del soporte material o no restitución del mismo; el apoderamiento jugaría un papel tan fundamental que si se pudieran conocer los secretos documentales sin necesidad de apoderarse de sus papeles no existiría el delito. La jurisprudencia de antaño, a partir de las Sentencia de 3 de abril de 1957 y 22 de marzo de 1962 entendía que la expresión «*se apoderare*» debía entenderse como alusiva a la situación en la que quedaría el sujeto pasivo: «desposesión», es decir, dicho sujeto quedaría desposeído de los papeles o cartas. Ahora bien, el apoderamiento no debía entenderse en un sentido exclusivamente físico o material sino también intelectual[7]. No obstante, sin olvidar que para llegar a ese apoderamiento intelectual previamente tendría que haber habido una desposesión o actuación de señorío, de posesión de los papeles o cartas por parte del sujeto activo. Por tanto, el sujeto activo debería vencer algún tipo de obstáculo interpuesto por el sujeto pasivo para acceder al secreto[8]. En definitiva, tanto el término «apoderarse» debía entenderse en un sentido amplio, no sólo comprensivo de supuestos de sustracción con desplazamiento posesorio sino también supuestos en donde no se llevase a cabo la desposesión del documento.

Como veremos más adelante la acción típica ha seguido precisándose a lo largo de los años. En todo caso la estructura típica del delito, en aquel entonces, exigía un apoderamiento claramente instrumental («*para descubrir*»), lo cual suponía varias cosas: que el único medio para llegar al descubrimiento debía ser el apoderamiento (cualquier otro medio diferente para descubrir debía quedar fuera del tipo), que el apoderamiento se llevara a cabo con la intención de descubrir los secretos de otra persona (un apoderamiento sin dicha finalidad que conllevara el descubrimiento —por ejemplo casual—, quedaría fuera del tipo) y finalmente los secretos debían recogerse documentalmente (papeles o cartas), cualquier otro objeto en donde se custodiaran, recogiesen o incluso consistiesen dichos secretos no estaba recogido en el tipo penal por lo que su apoderamiento no daría lugar al delito.

Objeto de análisis fue también el concepto de «secreto», decantándose tanto doctrina como jurisprudencia[9] por un concepto amplio, no ceñido al sentido literal del término como «oculto y reservado» sino referido a lo que no es conocido o ignorado por el sujeto activo.

---

divulgar aquellos. Y ello en relación a la modalidad que exige divulgación. En sentido crítico, Manzanares Samaniego, J.L.: «El artículo 497 del Código Penal» en *Anuario de Derecho Penal y Ciencias Penales*, T. 31, 1978, pp. 300 y ss.

5 Vid. Cobo del Rosal, M. (Dir.): *Manual de Derecho Penal (Parte Especial)*, ed. Revistas de Derecho Privado, 1993, pp. 582 y ss.

6 Muñoz Conde, F.: *Derecho Penal. Parte Especial*, 9ª edición, ed. Tirant lo Blanch, 1993, p. 157.

7 «…hay que excluir el concepto material, por bastar el apoderamiento momentáneo para las operaciones mentales de conocer y entender, con la finalidad de descubrir y utilizar en cualquier forma los secretos de otro». STS de 3 de abril de 1957. Los hechos probados se refieren a un sujeto que, al encontrarse casualmente sobre la mesa de una agencia, a la que tiene acceso normal como viejo cliente, la documentación presentada por otro para obtener una patente de invención, la examina, sin necesidad de abrir sobre o sello alguno, y aprovecha los conocimientos así adquiridos para adelantarse en la inscripción registral. Vid. La referencia a esta sentencia en Manzanares Samaniego, JL.: «El artículo 497…» p. 306. En este caso únicamente se produjo una captación intelectual de los secretos sin sustracción por lo que entiendo, al igual que manzanares Samaniego, que la conducta debería haber sido considerada como atípica por no integrarse dentro de la modalidad de apoderamiento.

8 Por ejemplo, Manzanares Samaniego a la hora de determinar el concepto de «apoderamiento» pone el ejemplo del sujeto que se apodera de una carta que ha sido recibida por error en la variante de la carta que es entregada por un cliente al hotelero para que la guarde en la caja fuerte. Si el hotelero traslada la carta para leerla en su habitación no habría dificultades para admitir la tipicidad de la conducta, pero sigue diciendo el autor que, distinto sería cuando la carta se lee en el propio lugar en que se encuentra, sin necesidad de abrirla o de acceder a ella por medio no autorizado, aquí ya no habría apoderamiento. Manzanares Samaniego, J.L.: «El artículo 497…», p. 306.

9 Interesante resulta la sentencia del Tribunal Supremo nº 534/2011, de 10 de junio de 2011, que en relación al concepto de secreto afirmó lo siguiente: «La intimidad es, por eso, contenido de un derecho fundamental, que goza de la protección del art. 18 de la Constitución. En esta figura asimismo el secreto como derecho igualmente fundamental, que también comparte con aquella el tipo penal a examen. Ahora bien, esta contigüidad en el orden de la garantía normativa no puede hacer perder de vista la diversidad conceptual, que se proyecta también en este mismo plano. En efecto, pues el de intimidad es un concepto, ético-psíquico y, por eso, cabe decir, material o sustantivo; mientras el de secreto es un artificio jurídico-formal, puesto constitucionalmente al servicio de una diversidad de bienes jurídicos, y aquí, concretamente, de la primera, para tratar de preservarla o asegurarla cuando, por salir de su espacio original y entrar en el de la comunicación, resulta más vulnerable y debe ser más intensamente protegida. En este sentido y, en rigor, el término «secretos» yuxtapuesto al de «intimidad» en el art. 197, 1º del Código Penal, podría decirse que no añade nada a la segunda, o nada realmente significativo en el plano de los contenidos».

Con anterioridad a la entrada en vigor de la L.O. 7/84 de 15 de octubre[10] quedaban al margen de la conducta punible, el descubrimiento del secreto por medios distintos a los apoderamientos documentales tales como grabaciones, interceptaciones del sonido o de la imagen etc. Es a través de dicha ley cuando se introduce el delito de interceptación de las comunicaciones en lo que entonces era el artículo 497 bis. Recogiendo un tipo básico y un tipo cualificado en función de si se producía o no la divulgación de los secretos obtenidos[11]. La nueva modalidad delictiva fue deficitaria desde su nacimiento ya que únicamente recogía la interceptación o utilización de artificios técnicos de grabación, transmisión o reproducción del sonido. Y, de hecho, fue conocido como colocación ilegal de escuchas telefónicas, denominación ofrecida por la propia ley. Ley Orgánica que reflejó la enorme preocupación social que por aquel entonces suscitaban las escuchas ilegales[12]. No obstante, la redacción del precepto no sólo recogía las literalmente denominadas escuchas telefónicas, sino también la utilización de artefactos técnicos de grabación, transmisión o reproducción del sonido y, por tanto, actuación típica que comprendería otro tipo de «escuchas» para descubrir los secretos de otra persona. El tipo básico recogía dos modalidades de conducta: la interceptación de comunicaciones telefónicas y, la utilización de instrumentos o artificios técnicos de interceptación del sonido. La primera modalidad de conducta, la interceptación de comunicaciones implicó la interferencia de una comunicación telefónica ajena sin el consentimiento de los interlocutores, interferencia que debía llevarse a cabo con la finalidad de descubrir los secretos de otra persona. La utilización de instrumentos o artificios técnicos de escucha, transmisión, grabación o reproducción del sonido suponía la aplicación de estos medios fuera del ámbito de la comunicación telefónica, pero dentro de una comunicación interpersonal privada.

La Ley 7/84 posteriormente fue modificada por la L.O. 18/1994, de 23 de diciembre que justifica su presencia en dos razones: la primera en la necesidad de aumentar las penas ya que «las penas establecidas para estos supuestos concretos no tuvieron el efecto disuasorio perseguido, al no conseguir asegurar totalmente la defensa del secreto de las comunicaciones, habida cuenta de la gama de conductas que quedaron fuera de los tipos que se regularon, y de las modalidades de telecomunicaciones susceptibles de ser interceptadas, así como de la levedad de las penas previstas». Y la segunda razón implicó introducir una nueva modalidad delictiva para sancionar la conducta de quienes, no habiendo intervenido en la captación de la información, pero conociendo su ilícito origen, procedían a su divulgación[13].

El Código penal de 1995 supuso una modernización importante en esta materia, aunque éste mantiene buena parte de la estructura de la antigua figura delictiva por lo que se siguen manteniendo parte de las críticas, fundamentalmente aquellas referidas a lo prolijo y casuístico del precepto[14]. Los artículos 197 y 198 del Código son los que recogen los modernos delitos de descubrimiento y revelación de secretos (a excepción del artículo 199 en donde se regula el quebrantamiento del secreto profesional):

Artículo 197.

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o 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. 2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro

10 Dicha ley introducía en el Código Penal dos nuevas figuras delictivas. La contemplada en el que sería el nuevo artículo 192 bis y en el también novedoso artículo 497 bis. En el primero se recogía las denominadas escuchas ilegales por autoridad, funcionario público o agente de éstos y en el artículo 497 bis las escuchas ilegales cometidas por particulares. Vid. Higuera Guimerá, J.F.; «Los delitos de colocación ilegal de escuchas telefónicas en el Código Penal español» en *Boletín Informativo. Ministerio de Justicia e Interior*, nº 1414, 1986, pp. 4 y ss.

11 El artículo 497 bis de acuerdo con la redacción establecida por la LO 7/1984 expresaba. «El que para descubrir los secretos o la intimidad de otros sin su consentimiento interceptare sus comunicaciones telefónicas o utilizare instrumentos o artificios técnicos de escucha, transmisión, grabación o reproducción del sonido será castigado con las penas de arresto mayor y multa de 30.000 a 150.000 pesetas. Si divulgare o revelare lo descubierto incurrirá en las penas de arresto mayor en su grado máximo y multa de 30.000 a 500.000 pesetas».

12 Sobre la historia legislativa de la L.O. 7/84, de 15 de octubre, Rodríguez Marín, F.: «Los delitos de escuchas ilegales y el derecho a la intimidad» en *Anuario de derecho Penal y Ciencias Penales*, 1990, pp. 198 y ss.

13 Obviamente aquí la intimidad iba referida a las comunicaciones personales y a la propia imagen.

14 Muñoz Conde, F.: *Derecho Penal. Parte Especial*. 12ª edición, ed. Tirant lo Blanch, 1999, p. 243.

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.

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

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

4. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

Artículo 198.

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

El legislador aglutina en un único precepto una gran variedad de conductas delictivas a las que añade una serie de tipos cualificados. En el número 1 del artículo 197 se recogen conjuntamente el delito de secretos documentales, la interceptación de comunicaciones y el control audiovisual clandestino. El legislador del 95 decidió recoger en un único apartado conductas muy diferentes y valorativamente muy desiguales[15]. La modalidad consistente en el apoderamiento de secretos documentales, mantuvo una redacción sin grandes cambios con lo que prolongaba los problemas interpretativos que en su momento fueron señalados por doctrina y jurisprudencia. Uno de ellos es el de la interpretación del posesivo «*sus*» que innecesariamente sigue limitando el ámbito de actuación del precepto, pues excluiría la posibilidad de perseguirse el supuesto en el que no se corresponda la titularidad de la intimidad con la del objeto material[16]. Igualmente, el término apoderamiento que se interpreta en sentido similar al utilizado en el ámbito de los delitos patrimoniales, aunque en el ámbito de los delitos aquí comentados se vincula la acción de apoderarse con la finalidad de descubrir los secretos de otro o vulnerar su intimidad. La novedad en el Código del 95 es la ampliación del objeto material que ahora pasan a poder ser no sólo papeles y cartas sino también mensajes de correo electrónicos o cualesquiera otros documentos o efectos personales.

Respecto de la modalidad de interceptación de comunicaciones, ésta mantiene prácticamente su redacción ofrecida por la LO 18/1994, introduciéndose como novedad la inclusión de una cláusula abierta con la expresión «cualquier otra señal de comunicación» cláusula cuya finalidad consistía en permitir la entrada a futuras novedades tecnológicas que sean utilizadas con la finalidad de violar las comunicaciones. Todos estos actos (interceptación, grabación, etc.) deben llevarse a cabo con la finalidad de descubrir la intimidad de otra persona por lo que la estructura típica es similar al del primer apartado del artículo 197.

Aparece por primera vez la modalidad de conducta de descubrimiento del secreto recogido en archivos o registros en el apartado 2 del artículo 197, también denominados delitos contra la libertad informática o «*habeas data*»[17]. En este momento histórico queda claro que la «*privacy*» no podía seguir siendo entendida como la esfera de la intimidad en la que se excluye a terceros, sino que debía dar entrada al fenómeno de la intromisión informática en este ámbito. De este modo, la protección otorgada desde el apartado 2 del artículo 197 significaba una limitación al poder informático desde el propio individuo titular de los datos[18].

15 En parecidos términos Jorge Barreiro, A.: «El delito de descubrimiento y revelación de secretos en el Código Penal de 1995. Un análisis del artículo 197 del CP» en *Revista Jurídica Universidad Autónoma de Madrid*, nº 6, 2002, p. 100.

16 Críticamente Jorge Barreiro, A.: «El delito de descubrimiento…», p. 101.

17 Vid. Jorge Barreiro, A.: *op. cit.*, p. 113; Morales Prats, F.: en (Dir. Quintero Olivares) *Comentarios a la Parte Especial del Derecho Penal,* 2ª edición, 1999, ed. Aranzadi, p. 337.

18 Modernamente nuestros tribunales entienden el bien jurídico desde la consideración positiva de este derecho. Así, en la Sentencia de la Audiencia Provincial de Valencia de 30 de mayo de 2012 [ARP 2012/704] se afirma: «Los derechos a la intimidad personal y a la

Dada la redacción del precepto, lo primero que había que determinar era la expresión «datos reservados». En este sentido, resulta ilustrativa la sentencia de 18 de febrero de 1999, en donde se matizaba que «Parece razonable que no todos los datos reservados de carácter personal o familiar puedan ser objeto del delito contra la libertad informática. Precisamente porque el delito se consuma tan pronto el sujeto activo «accede» a los datos, esto es, tan pronto los conoce y tiene a su disposición, pues sólo con eso se ha quebrantado la reserva que los cubre, es por lo que debe entenderse que la norma requiere la existencia de un perjuicio añadido para que la violación de la reserva integre el tipo, un perjuicio que puede afectar, como hemos visto, al titular de los datos o a un tercero. No es fácil precisar, «a priori» y en abstracto, cuándo el desvelamiento de un dato personal o familiar produce ese perjuicio. Baste ahora con decir que lo produce siempre que se trata de un dato que el hombre medio de nuestra cultura considera «sensible» por ser inherente al ámbito de su intimidad más estricta, dicho de otro modo, un dato perteneciente al reducto de los que, normalmente, se pretende no trasciendan fuera de la esfera en que se desenvuelve la privacidad de la persona y de su núcleo familiar».

Uno de los mayores problemas planteados por esta modalidad delictiva se encuentra en la descripción llevada a cabo por el legislador que, al utilizar acciones sinónimas o incluso coincidentes, termina por generar confusión sobre el alcance de este delito. El legislador utiliza en el primer inciso del artículo 197.2 los vocablos «*apoderarse, utilizar, o modificar*», y en el inciso segundo emplea los términos «*acceder, alterar o utilizar*». Como puede apreciarse, algunos de los términos se repiten («utilizar»), otros son sinónimos («alterar» y «modificar») y únicamente presentan diferencias «apoderarse» y «acceder». En relación a estos dos últimos, según el diccionario de la Real Academia de la Lengua Española «apoderarse» se define como «hacerse dueño de algo, ocuparlo, ponerlo bajo su poder». «Acceder» se conceptúa como «entrar en un lugar o pasar a él». En el contexto en el que ambos términos son empleados, el apoderamiento, al exigir posesión, parecería aludir a una posesión del soporte o apoderamiento a través de un soporte físico, es decir, se trataría de adueñarse no sólo de los datos, elemento inmaterial e incorporal y consiguientemente de difícil apoderamiento, sino también, por ejemplo, del objeto en su caso donde estuviera plasmado (pendrive, cd, DVD…). Por otra parte, hay que tener en cuenta que el fichero o archivo donde se encuentren los datos reservados pueden ser del tipo convencional y quizás el término «apoderarse» sea el más adecuado para ponerse en relación con estos instrumentos de custodia y clasificación de datos, ya que aquí el soporte de los datos es material (documentos o muestras corporales, por ejemplo) y, por tanto, susceptible de apoderamiento[19].

Otra cuestión controvertida y vinculada a la anterior es la necesidad de establecer algún tipo de diferencias entre el inciso primero y el segundo. Como acabamos de ver, la acción en ambos es prácticamente la misma. También lo es el objeto de la acción: «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». Alguna diferencia se aprecia en relación al sujeto pasivo al que se refiere el inciso primero («en perjuicio de tercero») y el del segundo («en perjuicio del titular de los datos»), diferencia a la que nuestra jurisprudencia ha preferido restar importancia argumentando que el que con mayor frecuencia resulta perjudicado por la infracción es el titular de los datos, aunque inexplicablemente se le haya silenciado en la definición legal del primer inciso. Especialmente significativa resulta la determinación de qué se entiende por «reservados» en rela-

propia imagen garantizados por el art. 18.1 de la Constitución Española, forman parte de los bienes de la personalidad que pertenecen al ámbito de la vida privada. Salvaguardan estos derechos un espacio de intimidad personal y familiar que queda substraído a intromisiones extrañas, destacando la necesaria protección frente al creciente desarrollo de los medios y procedimiento de captación, divulgación y difusión de la misma y de datos y circunstancias que pertenecen a la intimidad. El Tribunal Constitucional si bien, en un primer momento, consideró que la intimidad se configura como el derecho del titular a exigir la no injerencia de terceros en la esfera privada, concibiéndola pues, como un derecho de corte garantista o de defensa; en un segundo momento, a partir de la STC 134/99 [RTC 1999, 134] de 15.7, consideró que la intimidad era un bien jurídico que se relaciona con la libertad de acción del sujeto, con las facultades positivas de actuación para controlar la información relativa a su persona y su familia en el ámbito público: el derecho a la intimidad garantiza al individuo un poder jurídico sobre la información relativa a una persona o a su familia, pudiendo imponer a terceros (sean estos simples particulares o poderes públicos), su voluntad de no dar a conocer dicha información, prohibiendo su difusión no consentida» SSTC. 134/99 [RTC 1999, 134] de 15/07, y 144/99 [RTC 1999, 144] de 22.7.

19 La Jurisprudencia próxima a la entrada en vigor de esta modalidad delictiva apreciaba «una diferencia de matiz en la intensidad de la acción entre apoderarse y acceder por cualquier medio». STS de 18 de febrero de 1999.

ción a los datos. Personalmente coincido con el sector doctrinal que entiende que tal alusión iba referida a que los datos deben afectar a la intimidad personal, por tanto, similar al concepto de «secretos» en alusión a datos no conocidos por quien ilegítimamente accede a los mismos y el sujeto pasivo no desea que se conozcan[20].

Por lo demás, tanto el elemento del tipo («sin estar autorizado») como el resultado de la acción («en perjuicio de») aparecen expresados de la misma manera en los dos tipos. Pese a esta sustancial identidad, la diferencia de matiz que existe, según hemos señalado, entre apoderarse y acceder por cualquier medio (la primera expresión evoca la acción de sustraer, en tanto la segunda conviene a toda forma ilícita, puesto que no se está autorizado para llegar a conocer los datos reservados) autoriza a hablar de dos tipos delictivos, muy cercanos morfológicamente.

Finalmente, en su momento suscitó cierta controversia la expresión «*en perjuicio de*». Nuestra jurisprudencia en un primer momento histórico, cuando era de reciente introducción el precepto, entendía que dicha expresión, aunque pudiera suponer «la exigencia de un ánimo o especial intención de perjudicar al titular de los datos o a un tercero», no tenía que ser el único móvil ni siquiera el prioritario[21], posición que también se ha mantenido en la doctrina mayoritariamente.

3. Descubrimiento y revelación de secretos antes de la reforma del Código Penal de 2015

El artículo 197 contenía diversas modalidades de conductas lesivas del derecho a la intimidad, redactadas de una manera ciertamente compleja, en algunos casos, consecuencia de los escasos cambios en la redacción de dichas modalidades delictivas (por ejemplo, en relación al secreto documental), y en otros, producto de una cierta precipitación en la configuración de estos delitos por parte de nuestros legisladores. En relación al bien jurídico protegido, no solamente lo constituye la intimidad, sino también el derecho a la propia imagen. Muchas son las sentencias que han abordado el análisis de esta cuestión coincidiendo en entender la intimidad como «un concepto psicológico que remite a ese «mundo propio» en el que cada quien desarrolla su «vida interior». Por tanto, un reducto que está más allá de la privacidad y que conecta con los estratos más profundos de la personalidad, de la que es primera manifestación»[22].

En relación a las conductas delictivas se distingue las modalidades que estudiamos en los siguientes subapartados:

3.1. Descubrimiento de secretos documentales

Empezamos el análisis por la modalidad recogida en el apartado primero del artículo 197: descubrimiento de

20 Jorge Barreiro, A.: «El delito de descubrimiento y revelación…», p. 118.

21 STS 18 de febrero de 1999 en la que se establece: «El Tribunal de instancia ha considerado que la expresión «en perjuicio de» supone la exigencia de un ánimo o especial intención de perjudicar al titular de los datos o a un tercero y en tal exégesis descansa fundamentalmente su pronunciamiento absolutorio. Esta Sala no puede compartir esta lectura del precepto, aunque no deja de reconocer que la preposición «en» ha sido interpretada frecuentemente en dicho sentido. En el tipo que analizamos, sin embargo, situado inmediatamente después de otro —el del art. 197.1— en que el ánimo específico aparece indicado con la inequívoca preposición «para», el perjuicio producido por la acción tiene que estar naturalmente abarcado por el dolo, pero no tiene que ser el único ni el prioritario móvil de la acción. A esta conclusión debe conducir no sólo el argumento sistemático a que acabamos de aludir, sino la propia relevancia constitucional del bien jurídico lesionado por el delito, cuya protección penal no puede estar condicionada, so pena de verse convertida prácticamente en ilusoria, por la improbable hipótesis de que se acredite, en quien atente contra él, el deliberado y especial propósito de lesionarlo. Estamos, pues, ante un delito doloso, pero no ante un delito de tendencia».

22 En la STS 666/2006, de 19 de junio, se dice que «la idea de secreto en el artículo 197, 1º Código penal resulta conceptualmente indisociable de la de intimidad» que es, a su vez, «ese ámbito propio y reservado frente a la acción y el conocimiento de los demás» (SSTC 73/1982 y 57/1994, entre muchas). En este sentido, se ha dicho y es universalmente aceptado, que el de intimidad es un concepto psicológico que remite a ese «mundo propio» en el que cada quien desarrolla su «vida interior». Por tanto, un reducto que está más allá de la privacidad y que conecta con los estratos más profundos de la personalidad, de la que es primera manifestación.

Así las cosas, no hay duda: todo lo situado dentro de esa esfera tiene especial relevancia para el sujeto, en tanto que lo constituye como tal, y contribuye de manera decisiva a distinguirle. Esto no excluye que puedan darse grados de intensidad en la pertenencia o inherencia a ese espacio, de los concretos asuntos o actitudes que son propios del mismo. Y ello, por razón de su calidad específica y de la valoración que merezcan en el plano ético o de la autoestima al sujeto mismo; o incluso de la que este entienda que, de ser conocidos, pudieran obtener en el entorno, a tenor de los estándares de moral social imperantes. Pero en cualquier caso no hay duda: en rigor, lo íntimo estará siempre integrado por o tendrá que ver con el conjunto de vivencias, experiencias o rasgos caracteriales exclusivos que el individuo, como regla, aspira a mantener bajo reserva y para sí, al tratarse de datos que le comprometen de manera intensa, porque son de los que le hacen ser, precisamente, el que es como persona. Tanto es así que, en el lenguaje coloquial, cuando alguien invade de alguna forma y conoce lo que de otro se oculta en esa dimensión particularísima, se dice, bien expresivamente, que «lo tiene en sus manos».

secretos documentales. Hasta ahora se han reproducido los problemas interpretativos que hemos analizado en páginas anteriores (concepto de apoderamiento, el objeto material, interpretación del adjetivo «sus» o el elemento finalista de apoderarse para descubrir). De todos ellos, quiero destacar fundamentalmente tres: en relación al concepto de apoderamiento, se ha desarrollado una jurisprudencia más precisa de cara a su determinación; respecto del segundo (objeto material) porque la polémica ha continuado hasta nuestros días; e iguales razones hay que aducir respecto del tercero (el posesivo «sus» y su interpretación).

En relación a la determinación de la expresión «apoderarse», nuestra jurisprudencia más reciente entiende que con este vocablo se aludiría a conductas «consistentes en coger o hacerse con algo mediante el empleo de fuerza», lo que, trasladado analógicamente al terreno de los delitos de descubrimiento de secretos, implicaría vencer algún tipo de resistencia, como la consistente en la predisposición de alguna medida o cautela adoptada, precisamente, para evitar el conocimiento por otras personas de datos o informaciones que el directamente interesado buscara preservar [STS nº 487/2011, de 30 de mayo]. En la sentencia en la que se ofrece esta interpretación, se rechazó la calificación de descubrimiento de secretos al utilizar el acusado la astucia, sin necesidad de poner en práctica una conducta calificable de apoderamiento.

Doctrinalmente, ha seguido la discusión respecto del alcance del verbo apoderarse: junto con la tesis de que la simple captación mental puede dar lugar al tipo penal[23], la posición mayoritaria niega tal posibilidad al equiparar el apoderamiento con el apoderamiento patrimonial, al exigirse aprehensión física del soporte en donde se encuentren los datos[24]; o, en la actualidad, como se establece en la sentencia del Juzgado de lo Penal de Mérida de 29 de diciembre de 2009, «el apoderamiento exigido en el artículo 197 del CP no puede considerarse estrictamente como el apoderamiento físico de los mismos, basta su aprehensión virtual, de manera que el sujeto activo del delito se haga con su contenido de cualquier forma técnica que permita su reproducción posterior». También resulta de interés el concepto de apoderamiento que se utiliza en la sentencia de la Audiencia Provincial de Almería [SAP de Almería de 2 de noviembre de 2005]. Los hechos eran los siguientes: la víctima le entrega al acusado (compañero de trabajo) un carrete que contenía las fotos de su boda para que exclusivamente procediese al revelado de las mismas. De todas ellas, el acusado escaneó una en la que aparecía la mujer en ropa interior, y junto con otras tres fotografías en las que aparecía una chica de aspecto semejante a la víctima, desnuda de espaldas con un consolador, las envió sin su consentimiento a través de correo electrónico a unas 20 personas con la intención de hacerles creer que todas las fotografías se referían a la víctima, siendo publicadas en una página web. El tribunal entendió que los hechos eran constitutivos del delito recogido en los números 1 y 3 del artículo 197 sobre la base de entender el apoderamiento como «uso o utilización indebida», puesto que tiene el consentimiento para su posesión inicial pero no para el uso o destino que posteriormente le otorga el sujeto. Con esta sentencia se amplía el concepto de apoderamiento, incluyendo también la apropiación o uso indebido del documento, cosa o efecto personal.

De interés ha resultado también la interpretación del posesivo «sus» que desde siempre ha aparecido en la redacción de esta modalidad delictiva. El artículo 197.1 también alude a *«se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales*». Desde antiguo, la doctrina y la jurisprudencia, de acuerdo con una interpretación literal del precepto, vienen entendiendo que sean secretos de la persona a quien pertenezca la titularidad de los papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales[25], quizás por mantener una interpretación estricta del bien jurídico aquí protegido a la vez que vinculando intimidad con propiedad, pues se entiende que los secretos de otra persona no son parte de nuestra intimidad. En cualquier caso, como veremos, el legislador de 2015 ha perdido nuevamente la oportunidad de suprimir este adjetivo y ofrecer, desde mi punto de vista, una interpretación más coherente de la intimidad.

El concepto de secreto es otro de los elementos objeto de atención. En este sentido, nuestros tribunales vienen estableciendo los requisitos que debe poseer el

23 Polaino Navarrete, M.: en Cobo del Rosal (Dir.) *Curso de Derecho Penal Español. Parte Especial, I,* ed. Marcial Pons.

24 En igual sentido, Anarte Borrallo, E.: «Consideraciones sobre los delitos de descubrimiento de secretos (I). En especial, el artículo 197.1 del Código penal», en Jueces *para la Democracia*, n.º 43, 2002, p. 54.

25 Jorge Barreiro, A.: «El delito de descubrimiento…», p. 101. Morales Prats, F., en *Comentarios a la Parte Especial del Derecho Penal* (Dir. Quintero Olivares), 9.ª edición, p. 457, crítica la redacción del precepto calificándola de imprecisión técnica al exigir la correspondencia entre titularidad de la intimidad y titularidad del objeto material. Jurisprudencialmente, vid. SAP de Madrid de 4 de mayo de 2012.

objeto material a los efectos de alcanzar este atributo. Por ejemplo, la sentencia de la Audiencia Provincial de Huelva, al hilo de esta cuestión y refiriéndose a la intimidad como el bien jurídico protegido en estos delitos, establecía: «[…] Mas ello engarza con otra cuestión cual es el concepto legal de secreto, que no es sino cualidad que se predica de un dato, un hecho, una información, que tiene un soporte físico, cualidad que por otra parte es mutable en función de las decisiones del titular, de tal suerte que la condición de secreto (salvo presunciones, como las establecidas por el Tribunal Supremo, cfr. STS de 10.12.1957 a favor de la correspondencia particular), no se debe predicar a priori, sino que habrá que analizar el contexto y los datos concurrentes tales como la forma de guardar o vehicular la información, las manifestaciones de su titular, las cautelas empleadas para proteger los datos, el propio contenido de la información». En definitiva, queda claro que el contexto y las circunstancias influyen en la consideración de algo como secreto.

3.2. Interceptación de comunicaciones y control audiovisual clandestino

Estructuralmente mantiene las características del tipo recogido en el apartado primero del artículo 197: delito mutilado de dos actos que no requiere para su consumación el efectivo descubrimiento de los secretos. Los atentados a la propia imagen aparecen recogidos en este inciso, incriminándose conductas de grabación, transmisión o reproducción de la imagen con la finalidad de descubrir la intimidad de su titular.

En la descripción de esta modalidad delictiva el legislador ha tendido a la reiteración terminológica que no ha contribuido a su interpretación[26]. Nuevamente nos encontramos con dificultades para determinar la conducta delictiva, es decir, qué vamos a entender por «*interceptar*» y «*utilizar*». Precisamente, y en relación con el concepto de interceptación, la doctrina no parece haber mantenido una interpretación unánime ya que hay quien considera incluido en el tipo la mera captación mental sin desplazamiento ilícito[27] frente a quienes lo niegan[28]. Según el diccionario de la Real Academia Española de la Lengua, «*interceptar*» significa apoderarse de algo antes de que llegue a su destino o interrumpir, obstruir una vía de comunicación. Ello implica la utilización de instrumentos o artificios técnicos para captar o interrumpir las telecomunicaciones[29]. La utilización, en cuanto significa aprovecharse de algo, exige no la mera colocación de los aparatos sino también su uso. Por consiguiente, el instrumento deberá captar el sonido o la imagen para la consumación[30]. Especialmente interesantes son la Sentencia del Tribunal Supremo de 8 de julio de 1992 y el Auto de la Audiencia Provincial de Huesca de 29 de julio de 1996, en las que se interpreta el delito de interceptación de comunicaciones como un tipo en donde se deben de utilizar artificios *ad hoc*[31]. Por lo demás, y en relación

26 En parecidos términos Anarte Borrallo, E.: «Consideraciones sobre los delitos de descubrimiento de secretos (I)…, p. 52.

27 Morales Prats, F.: *op. cit.*, p. 455.

28 Muñoz Conde, F.: *Derecho Penal. Parte Especial*, 19ª ed. Tirant lo Blanch, Valencia, 2013, p. 259. quien considera que la captación de cualquier comunicación oral sólo es típica si se utilizan instrumentos o artificios técnicos.

29 Anarte Borrallo, E.: «Consideraciones sobre los delitos de descubrimiento de secretos (I)…». p. 56.

30 En el mismo sentido, Muñoz Conde, F.: *Derecho Penal. Parte Especial*, 19ª edición, ed. Tirant lo Blanch, Valencia, 2013, p. 259. También la jurisprudencia: vid. Sentencia de la Audiencia Provincial de Álava de 4 de abril de 2003, donde se establece: «Aunque la consecuencia lógica de la interceptación y utilización de artificios técnicos es la escucha y el descubrimiento de los secretos, no es necesario este requisito para entender que se ha cumplido el elemento objetivo, se haya vulnerado o no la intimidad de las personas la actividad delictiva existe y queda consumada tan sólo con la utilización de los artificios y aparatos destinados a tal fin». Igualmente, la Sentencia de la Audiencia Provincial de Valencia de 18 de diciembre de 2000: «Esta modalidad delictiva, aunque es de pura actividad y se configura como un tipo de consumación anticipada, pues basta la utilización de artificios técnicos de escucha, si bien sea preciso concretar cuál es el momento consumativo a partir de la cual dicha utilización comienza a tener relevancia penal. Parece razonable atender al inicio de la actividad de escucha, transmisión o grabación, independientemente del éxito o resultado, esto es, se consumaría con la puesta en marcha de mecanismos o artificios que sirvan expresamente para los fines perseguidos».

31 Auto de la Audiencia Provincial de Huesca de 29 de julio de 1996: «La conducta típica, según la doctrina, requiere el empleo de artificios «ad hoc», […] «la interceptación de las comunicaciones telefónicas es un acto directamente encaminado a interferirse en las conversaciones ajenas», es eminentemente doloso y supone la puesta en marcha de mecanismos o artificios que sirvan expresamente a los fines perseguidos · Sentencia del Tribunal Supremo de 8 julio 1992 [RJ 1992/6553].· En este caso el querellado, que se encontraba en la cocina de su domicilio, escuchó la conversación que se producía en el domicilio del querellante y trató de grabar con un aparato comercial de uso corriente las voces y sonidos que llegaban a su domicilio. Por consiguiente, no concurren los elementos característicos para dar vida a estos delitos, puesto que no se produjo una intromisión en el ámbito privado del querellante ni interceptó sus comunicaciones telefónicas, por lo que, como en el supuesto de la resolución antes reseñada, la mera u ocasional escucha producida de la conversación ajena debido a las características de las viviendas o al tono de voz empleado, no constituye el tipo que estamos examinando. Además, el juzgador des-

a las modalidades de conductas aquí recogidas, como establece nuestra jurisprudencia «se trata de conductas distintas que no precisan que el autor llegue a alcanzar la finalidad perseguida. En los dos primeros casos requiere sin embargo un acto de apoderamiento o de interceptación efectivos, mientras que en el supuesto de utilización de artificios basta con la creación del peligro que supone su empleo con las finalidades expresadas para la consumación de la infracción penal»[32].

3.3. Descubrimiento de secretos recogidos en archivos o registros

El apartado 2 del repetido artículo 197 del CP del 95 castiga tanto al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado, como a quien, sin estar autorizado, acceda por cualquier medio a los mismos (datos reservados de carácter personal o familiar de otro), y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

Esta modalidad delictiva presenta grandes dificultades de cara a su interpretación, pues sigue resultando compleja y en ocasiones reiterativa[33]. En este apartado se recogían los denominados delitos contra la libertad informática[34], bien jurídico protegido que supone no sólo las facultades de exclusión de terceros sino también el poder de control sobre los datos personales informatizados. En relación con el bien jurídico protegido, como se establece en la STS 1142/2009, de 30 de diciembre, «lo que se protege a través de las conductas previstas en el apartado segundo del artículo 197 del Código Penal, es «la libertad informática entendida como derecho del ciudadano a controlar la información personal y familiar que se encuentra recogida en ficheros de datos, lo que constituye una dimensión positiva de la intimidad que constituye el bien jurídico protegido»[35].

Esta figura delictiva está vinculada con la normativa administrativa reguladora de esta materia. Concretamente con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y el Real Decreto 1720/2007, de 21 de diciembre. Por ello estamos ante una descripción delictiva con un número elevado de elementos normativos que deben ser definidos de acuerdo a la normativa. Sobre dicha infracción punible la jurisprudencia viene considerando que se trata de un delito doloso, pero no de tendencia, bastando que el sujeto se represente la posibilidad de que cualquier persona pudiera resultar afectada por la utilización de los datos, sin exigir un ánimo específico de perjudicar a tercero[36]. Por lo tanto, al acceder a estos archivos, se asume como mínimo con dolo eventual (recogido por el Tribunal Supremo en numerosas resoluciones —Sentencias de 2 de diciembre de 2004 [RJ 2005, 368], 28 de septiembre de 2005 [RJ 2005, 7407] y 18 de noviembre de 2005, entre otras—) que con su proceder podría vulnerar la legalidad penal. Se trata de

taca en sus resoluciones y en el acta de transcripción de la cinta, folio 129, que no se escucha ni se puede apreciar nada audible ni mucho menos que tenga relación con la causa, por lo que procede desestimar el recurso y mantener la decisión del juzgador de instancia».

32 STS nº 358/2007, de 30 de abril de 2007.

33 Por ejemplo, para algunos autores este apartado constituye un auténtico «galimatías jurídico»: Tomás-Valiente Lanuza, C., en Gómez Tomillo, M. (Dir.): *Comentarios al Código Penal*, ed. Lex Nova, 2010, p. 800.

34 Jorge Barreiro, A: «El delito de descubrimiento…», p. 113.

35 En la Sentencia de la Audiencia Provincial de Valencia de 12 de marzo de 2013 se precisa todavía más qué intereses se consideran protegidos en esta modalidad delictiva, haciéndose eco de la posición de un sector doctrinal establece: «Por el contrario, los delitos recogidos en el segundo apartado del art. 197 tienen un sentido claramente distinto a los recogidos en el apartado primero: ya que las conductas afectan a datos que no están en la esfera de custodia del titular, sino en bancos de datos, y pueden causar perjuicios a terceros distintos del propio sujeto al que se refiere la información concernida. Un sector doctrinal considera que en el art. 197.2 se protegen, en realidad, dos bienes jurídicos. Por una parte, la intimidad del sujeto pasivo, en relación con las conductas de apoderarse, acceder y utilizar los datos. Por otra parte, la integridad de los datos, en relación con los comportamientos de modificar o alterar. Distinción, no obstante, relativa por el hecho de ·que quien pretende modificar o alterar, primero debe acceder, con lo que se habría lesionado también la intimidad en estas modalidades de conducta. Consecuentemente lo que se protege en este apartado segundo, establece el Tribunal Supremo, es la libertad informática entendida como derecho del ciudadano a controlar la información personal y familiar que se encuentra recogida en ficheros de datos, lo que constituye una dimensión positiva de la intimidad que constituye el bien jurídico protegido. Según el art. 3 a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LPDP), dato de carácter personal es «cualquier información concerniente a personas físicas identificadas o identificables». No se define, sin embargo, qué datos son reservados, ni siquiera se utiliza la denominación de datos de carácter familiar. Advierte la doctrina que el calificativo de reservado carece en absoluto de sentido.

36 Sentencias de 18 de febrero de 1999 [RJ 1999, 510] y 9 de octubre de 2000.

un delito en cualquiera de sus versiones que no precisa para su consumación el efectivo descubrimiento del secreto o de la intimidad del sujeto pasivo, pues basta la concurrencia del elemento objetivo, junto con la finalidad señalada en el precepto de descubrir los secretos o vulnerar la intimidad (elemento subjetivo).

Al igual que en su redacción original, sujeto activo puede ser cualquier persona, salvo que ésta fuere la persona encargada o responsable de los ficheros, soportes informáticos, archivos o registros en cuyo caso se aplicaría el tipo cualificado del artículo 197.4, o autoridad o funcionario público de acuerdo a lo establecido en el artículo 198[37]. En relación al sujeto pasivo, resulta de interés el que la referencia a que los datos reservados sean de carácter personal o familiar parece excluir a las personas jurídicas como sujetos pasivos de esta concreta modalidad delictiva, a pesar de lo establecido en el artículo 200 del Código Penal.

La nueva redacción del apartado 2 del artículo 197 intenta solucionar el problema que generó la descripción del sujeto pasivo del inciso primero y del segundo, pues ahora se refiere en el inciso segundo al «titular de los datos o de un tercero». Personalmente creo que la solución implica que ahora, en relación al primer inciso, al no venir expresamente mencionado, se genera la dificultad de entender incluido al titular de los datos. Una interpretación teleológica del precepto permitiría entenderlo incluido: lo que no puede resultar extraño es que también terceros puedan verse perjudicados a través de alguna de las modalidades de conductas descritas[38].

Precisamente en relación a los comportamientos típicos, la proliferación y en ocasiones reiteración de comportamientos dificulta la determinación del ámbito típico. El precepto alude a que el sujeto activo «*se apodere, utilice o modifique en perjuicio de tercero…*»; «*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*». Por tanto, el núcleo de la conducta gira en torno a las siguientes modalidades de comisión: el apoderamiento, la utilización, la modificación, el acceso o la alteración. En relación al apoderamiento, este debe ser entendido en el mismo sentido que referíamos para el descubrimiento del secreto documental, es decir, en la línea de apoderamiento patrimonial, que evidentemente implica la traslación de los datos (impresión, transmisión, fotocopiado…) a otro soporte para su posesión. Utilizar, según el diccionario de la Real Academia de la Lengua, significa «aprovecharse de algo», lo que implica hacer uso de los datos, lo que supone que previamente ha existido apoderamiento o acceso a los mismos, para luego poder aprovecharse de ellos. Modificar se define como transformar o cambiar los datos; alterar se define como dañar o estropear los datos, y finalmente acceder implica entrar o tener acceso a los datos. Como podemos apreciar, con estas modalidades se pretende aludir a situaciones diferentes, y de menor a mayor relevancia o invasión respecto de los datos reservados: entrar o acceder a los datos y conocerlos.

Después de definir las conductas, resulta de especial interés preguntarse si con estos dos incisos el legislador quiere aludir a que se están regulando situaciones diferentes, ya que en el primer inciso se refiere a apoderarse, utilizar o modificar en perjuicio de terceros datos reservados, mientras que en el segundo alude a quienes acceda por cualquier medio y a quienes los alteren o utilicen en perjuicio del titular de los datos o de un tercero. La diferencia más evidente se encuentra en los verbos *apoderarse* y *acceder*: parecería que el segundo vocablo hace referencia a apoderamientos meramente intelectuales en contraposición a las conductas a las que se quiere hacer referencia con el verbo *apoderarse*. El acceso, aunque aparezca vinculado a los datos que

37 Jorge Barreiro, A.: «El delito de descubrimiento y relevación de secretos…», p. 116.

38 Sobre esta cuestión se ha pronunciado también nuestra jurisprudencia, concretamente la STS de 3 de febrero de 2009, en donde se establece: «*tres formas comisivas se recogen en el párrafo segundo del artículo 197.2 del Código Penal: a) el apoderamiento, utilización o modificación de los datos que hemos descritos; b) el mero acceso; y c) la alteración o utilización.*

Sólo con relación a la primera y a la tercera de ellas, menciona expresamente el legislador que la conducta se haga en perjuicio de tercero, mientras que no exigiría tal perjuicio en el caso de la conducta de acceso. Pero como decíamos en la resolución ya mencionada, es necesario realizar una interpretación integradora del precepto, en el sentido de que como en el inciso primero se castigan idénticos comportamientos objetivos que el inciso 2º (apodere, utilice, modifique) no tendría sentido que en el mero acceso no se exija perjuicio alguno, y en conductas que precisan ese previo acceso añadiendo otros comportamientos, se exija ese perjuicio, cuando tales conductas ya serían punibles —y con la misma pena— en el inciso segundo.

La solución sería —partiendo de que en el termino "tercero" debe incluirse el afectado, en su intimidad, sujeto pasivo, al que esencialmente se refiere el tipo— entender que los apoderamientos, accesos, utilizaciones o modificaciones de datos de carácter personal, realizadas en perjuicio de tercero se incluirían en el inciso inicial del artículo 197 del Código Penal y en cambio, en el inciso segundo deberían ser subsumidas las conductas de acceso en perjuicio del titular de los datos».

se encuentren registrados a través de sistemas informáticos y podría entenderse entonces que su función quedaría limitada a conducta referida a datos ordenados por estos mecanismos informáticos, abre la posibilidad de aplicarse también a los datos que se encuentren registrados a través de mecanismos convencionales. Sin embargo, esta última interpretación nos llevaría a afirmar que, mientras en el número 1 del artículo 197 se exige un apoderamiento material respecto de papeles, cartas, mensajes de correo electrónico u otra clase de documentos, ahora en el número 2 del mismo precepto y en relación a datos registrados, bastaría con la mera captación intelectual. De acuerdo con el sentido literal del segundo inciso «*iguales penas se impondrán a quien…*» el legislador se está refiriendo a otro tipo de conductas, distintas a las recogidas en el inciso primero. Estas conductas diferentes sólo pueden ser aquellas en las que la utilización del vocablo *apoderamiento* no es omnicomprensiva de las diferentes conductas que se quieren incriminar, es decir, conductas relacionadas con el registro o fichado de los datos a través de sistemas informáticos. Precisamente en relación con las modalidades de conductas, se suscitan otros problemas tales como la cesión, sin autorización del titular, a terceras personas de datos recogidos en archivos o ficheros, pues el tipo cualificado de cesión a terceros del número 4 del artículo 197 exige una previa conducta delictiva del número 1 o del número 2. Es decir, la cesión sin un previo apoderamiento ilícito no está expresamente prevista. Desde mi punto de vista, esta conducta podría castigarse por la vía de la utilización de los datos sin autorización.

El Tribunal Supremo ha desarrollado una extensa doctrina acerca del ámbito del comportamiento punible en relación al descubrimiento de secretos recogidos en archivos o registros. De especial interés resulta la STS n.º 990/2012, de 18 de octubre de 2012, que establecía: «*Para su comisión, según esta misma resolución, los datos objetos de las mismas han de estar «recogidos» (registrados) en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado»; siendo un fichero a estos efectos, «todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso» (art. 3 b. LPDP)».* Además, dado el carácter reservado de los datos, continúa dicha resolución*, «los ficheros o registros han de ser de acceso y utilización limitada a personas concretas y con finalidades especificas, siendo indiferente, su naturaleza: personal, académica o laboral, medica, económica, etc… Se trata, en realidad, de informaciones de carácter personal relacionadas más con la privacidad que con la intimidad. No tienen por qué ser informáticos porque se acoge también a cualquier otro tipo de archivo o registro público o privado».*

También nuestros tribunales se han pronunciado respecto a la exigencia de que dichos ficheros o archivos hayan sido creados o no lícitamente. Así, la Sentencia de la Audiencia Provincial de Madrid de 11 de junio de 2010 establecía: «*Las conductas van dirigidas a datos que se hallen registrados, es decir a bancos de datos preexistentes, entendiéndose por la doctrina que no es típica la creación clandestina de bancos de datos, que queda en el ámbito administrativo sancionador*». Por todo ello debe concluirse que la realización de las distintas conductas nucleares previstas en los indicados preceptos que recaigan sobre datos reservados personales o familiares pero que no estén previamente registrados en los términos y lugares descritos en el precepto comentado no serían subsumibles en la descripción típica del delito[39].

En relación a qué debemos entender por «datos reservados de carácter personal», Jorge Barreiro considera que la expresión no es muy afortunada, ya que los datos personales en cuanto son introducidos en un fichero automatizado son sensibles y estarían protegidos por el artículo 197.2[40]. Por tanto, con la expresión, «datos reservados», se aludiría a datos no públicos, es decir, no conocidos por quien ilegítimamente accede a ellos y que el sujeto pasivo no desea que se conozcan[41]. Esta interpretación vendría respaldada por la pre-

39 En el mismo sentido, Frías Martínez en *Código penal comentado* (Román Valdés, A. dir.), ed. Bosch, Barcelona, 2015, p. 367.

40 Jorge Barreiro, A.: «El delito de descubrimiento y revelación de secretos en el Código Penal de…», p. 118. En parecidos términos la Sentencia del Tribunal Supremo n.º 725/2004, de 11 de junio de 2004, establece que «[…] *es claro que el dato referente al lugar de trabajo de una persona contenido en los archivos de la Seguridad Social es —en contra de la afirmación apodíctica del recurrente— un dato de carácter personal en el sentido del artículo 197.2 del Código Penal, pues se refiere a uno de los ámbitos en los que una persona desarrolla y realiza su personalidad. Si no fuera así no sería necesaria una intervención judicial motivada para su obtención. No son datos que están a disposición de cualquier solicitante y, como es obvio, no es un elemento con el que los funcionarios de la Seguridad Social puedan comerciar libremente».*

41 La doctrina mayoritaria parece mantener esta interpretación, pues entiende por «*datos reservados*» los datos personales de conocimiento limitado para terceros ajenos a los ficheros o archivos en donde se encuentren. Vid. Caruso Fontán, V.: «La responsabilidad

sencia de la cualificación 6 del artículo 197, referida a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere menor de edad o un incapaz y que lógicamente queda reservada para proteger estos datos más sensibles; luego los datos personales no incluidos en la cualificación quedarían protegidos por la vía del tipo básico del número 2 del 197. En su sentencia n.º 725/2004, de 11 de junio de 2004, el Tribunal Supremo considera *datos reservados* lo que ya anteriormente había considerado en otra sentencia: «[…] *La STS 234/1999, que acaso se podría relacionar con este caso concreto, considera que el tipo se refiere a datos que, normalmente, se pretende que no trasciendan fuera de la esfera de privacidad. Pero ello no significa que sea un elemento de los datos protegidos la suposición de un propósito de ocultarlos, pues la privacidad no es sólo, como derecho fundamental, un derecho al ocultamiento de circunstancias personales, sino un derecho a la no divulgación ilegal de los datos, dado que configura una forma del derecho a la libre realización de la personalidad*». La ·Ley de Protección de datos de carácter personal define en su artículo 3 lo que son «datos de carácter personal», expresión a la que en parte se vincula el tipo delictivo. Según el texto de la ley de carácter administrativo, por tales se entiende «cualquier información concerniente a personas físicas, identificadas o identificables». La definición es amplia y, en virtud del artículo 1.4 del Real Decreto 1332/1994, de 20 de junio, se detalla que comprendería «toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable». Quedarían fuera del ámbito de esta ·Ley los ficheros de datos personales en los que no estén identificadas personas[42]. Desde esta consideración igualmente quedarán fuera del tipo penal dichos ficheros de datos personales en donde no estén identificadas personas. No obstante, la cuestión que se plantea es si con la expresión «datos reservados de carácter personal o familiar» el legislador penal está queriendo diferenciarlos de los «datos de carácter personal» mencionados en la Ley de Protección de Datos. La doctrina considera que una interpretación amplia de esta última expresión tiene su razón de ser en la necesidad de abarcar cualquier información de persona física que afecte a la intimidad; dicha amplitud persigue facilitar su adaptación a la constante evolución de la informática[43]. Y, es más, según Muñoz Conde, si no se trata de datos que afecten directamente a la intimidad personal, sino a la privacidad, el delito aplicable sería el recogido en el artículo 197 bis[44].

Para finalizar, la expresión «*en perjuicio*» ha sido interpretada de diversas maneras, aunque mayoritariamente se entiende como un elemento subjetivo del injusto[45], no siendo necesario que se produzca el perjuicio para consumar el delito. A este respecto resulta interesante la STS de 30 de diciembre de 2009, en donde el TS estableció:

> *Un sector doctrinal considera que «en perjuicio» es un elemento subjetivo del injusto, de manera que el propósito de perjudicar a otro debe presidir el apoderamiento, la utilización o modificación de los datos. El inconveniente que tiene esta postura es que, aunque anticipa el momento de la intervención penal —pues la consumación ya no tiene que esperar a la efectiva producción de resultado alguno—, a la vez limita el ámbito de lo punible, pues solo los comportamientos que vayan presididos de esa particular intención resultan típicos. Por ello otro sector de opinión estima que el «en perjuicio de tercero» no debe ser interpretado como un elemento subjetivo del injusto, sino como el resultado de la conducta, causalmente añadido a la simple utilización, modificación o al apoderamiento de los datos. Esta es la línea que siguió esta Sala en la STS 234/99 de 18/02 [RJ 1999, 510], al matizar que parece razonable que no todos los datos reservados de carácter personal o familiar puedan ser objeto del delito contra la libertad informática, puesto que, precisamente porque el delito se consuma tan pronto el sujeto activo «accede» a los datos, esto es, tan pronto los conoce y tiene a su disposición (...), es por lo que debe entenderse que la norma requiere la existencia de un perjuicio añadido para que la violación de la reserva integre el tipo, un perjuicio que puede afectar, como hemos visto, al titular de los datos o a un tercero, perjuicio que se produce siempre que se trata de un dato considerado «sensible» por ser inherente al ámbito de su intimidad más estricta.*
>
> *Es cierto que esta postura ha sido objeto de criticas al limitar los datos que causan un perjuicio apreciable a los datos «sensibles», los de mayor relevancia para la intimidad y ha sido matizada en otras posteriores, como la*

penal de los encargados de bases de datos de ADN frente a la cesión de información contenida en los registros» en *Revista de Derecho Penal*, n.º 40, 2013, p. 43.

42 Vizcaíno Calderón, M.: *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, ed. Civitas, Madrid, 2001, p. 71.

43 Vizcaíno Calderón, M.: *op. cit.*, p. 72.

44 Muñoz Conde, F.: *Derecho Penal. Parte Especial*…, p. 237.

45 Muñoz Conde, F.: *Derecho Penal. Parte Especial*…, p. 261; Jorge Barreiro, A.: «El delito de descubrimiento…», p. 122.

1461/2001 de 11/07 [RJ 2003, 1056], que, a la pregunta de si la expresión de tercero debe interpretarse como un plus en la lesión del bien jurídico protegido, entendió que existían argumentos para responder negativamente:

a) Si el ámbito de la intimidad protegida se restringe mucho, se produce el efecto de asimilar el perjuicio a la parte más básica de la intimidad («núcleo duro de la privacidad»): salud, ideología, vida sexual, creencias, etc., que ya se castiga como subtipo agravado en el art. 197.5, lo que conllevaría la inaplicación del art. 197.2.

b) De la sentencia 18/02/99 [RJ 1999, 510] parece colegirse que ese posible mayor perjuicio proviene y se traduce en el desvelamiento de un dato personal o familiar, exclusivamente.

c) La conducta se consuma, sin necesidad de que un ulterior perjuicio se produzca, como textualmente exprese la tantas veces referida sentencia de esta Sala.

d) Derivada de la anterior afirmación hemos de entender que, si el perjuicio se materializa, habría que acudir a un concurso medial de infracciones penales.

e) El precepto analizado tutela o protege exclusivamente la intimidad y no contempla con tal previsión penal la lesión de otros bienes jurídicos. En realidad, se trata de poner freno a los abusos informáticos contra la intimidad, es decir, contra aquellas manifestaciones de la personalidad individual o familiar cuyo conocimiento queda reservado a su titular.

f) En una interpretación sistemática, si quisiéramos establecer una simetría con las descripciones típicas contenidas en el art. 197.1 y referidas al aspecto subjetivo del tipo, advertiríamos que en esta figura delictiva la acción típica se dirige «a descubrir los secretos o vulnerar la intimidad de otro», que en cierto modo estaría sustituida por la frase «en perjuicio de otro», contenida en el tipo penal previsto en el art. 197.2, habida cuenta de que ambas infracciones penales, tratan de proteger idénticos bienes jurídicos.

g) Asimismo la STS. 123/2009 de 03/02 [RJ 2009, 2433] —citada por el Ministerio Fiscal en su escrito de impugnación al recurso—, al analizar el hecho del «acceso» que se ubica en la modalidad básica del art. 197.2, indica que esta modalidad básica incluye, a su vez, tres figuras diversas: 1.ª apoderamiento, utilización o modificación de datos; 2.ª el mero acceso: y 3. la alteración o utilización.

h) Pues bien, por difícil que resulta comprenderlo, las modalidades 1.ª y 2.ª exigen que el sujeto actué en perjuicio de tercero, la 3.ª, que se haga en perjuicio de tercero o del titular del dato, y lo que aquí es relevante, en la 2.ª no se exige perjuicio alguno […]

Baste advertir que el supuesto típico imputado —mero acceso—, es decir, la modalidad 2.ª, no exige tal perjuicio de tercero. El perjuicio de tercero es presupuesto de las otras modalidades típicas del apartado 2.º del art. 197 CP. constituido por la conducta de «apoderarse, utiliza o modificar» y la de «alterar o utilizar» los datos a los que nos venimos refiriendo. Es decir: reservados y de carácter personal o familiar existentes en los ficheros o archivos allí indicados.

Pero cuando la conducta típica es la descrita en la primera parte del inciso segundo del mismo apartado 2º del citado art. 197 CP, es decir, el acceso a los datos por cualquier medio, no exige el perjuicio del tercero.

Pues bien creemos que es necesario realizar una interpretación integradora en el sentido de que, como en el inciso primero se castigan idénticos comportamientos objetivos que el inciso 2.º (apodere, utilice, modifique), no tendría sentido que en el mero acceso no se exija perjuicio alguno y en conductas que precisan ese previo acceso añadiendo otros comportamientos, se exija ese perjuicio, cuando tales conductas ya serian punibles —y con la misma pena— en el inciso segundo.

La solución seria —partiendo de que en el termino «tercero» debe incluirse el afectado, en su intimidad, sujeto pasivo, al que esencialmente se refiere el tipo— entender que los apoderamientos, accesos, utilizaciones o modificaciones de datos de carácter personal, realizadas en perjuicio de tercero se incluirían en el inciso inicial del art. 197.2, y en cambio, en el inciso segundo deberían ser subsumidas las conductas de acceso en perjuicio del titular de los datos.

Y en cuanto a la distinción entre datos «sensibles» y los que no lo son, debe hacerse en el sentido de que los primeros son por sí mismos capaces para producir el perjuicio típico, por lo que el acceso a los mismos, su apoderamiento o divulgación, poniéndolos al descubierto comporta ya ese daño a su derecho a mantenerlos secretos u ocultos (intimidad) integrando el «perjuicio» exigido, mientras que en los datos «no sensibles», no es que no tengan virtualidad lesiva suficiente para provocar o producir el perjuicio, sino que debería acreditarse su efectiva concurrencia y en el caso presente, no se ha acreditado —ni se ha articulado prueba en este sentido— que el acceso por parte del recurrente al nombre del médico de cabecera —dato administrativo, y en principio, inocuo— del Dr. Bienvenido haya ocasionado perjuicio a éste como titular de al dato.

Finalmente, el hecho quedaría justificado si hubiera autorización para llevar a cabo estas conductas.

3.4. Acceso a datos y sistemas informáticos

La modalidad delictiva recogida en el antiguo número 3 del artículo 197—acceso a datos y sistemas informáticos— es de nueva creación el año 2010. Según la exposición de motivos de la Ley Orgánica 5/2010, esta nueva figura tiene su razón de ser en los compromisos internacionales contraídos por España y, más concretamente, de los derivados de la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005. En dicha Decisión Marco se definen tanto el «acceso ilegal en los sistemas de información» como la «intromisión ilegal en los sistemas de información». Dicho *acceso ilegal* viene definido como «el acceso intencionado sin autorización al conjunto o a una parte de un sistema de

información» (artículo 2); la *intromisión ilegal*, por el contrario, vendría a consistir en «el acto intencionado, cometido sin autorización, de obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos» (artículo 3). Ambas definiciones resultan necesarias para entender las conductas que recoge el nuevo artículo 197.3. El resultado de este compromiso adquirido por nuestro país ha sido la inclusión en nuestro Código penal de un nuevo delito, que viene a reconocerse como «intrusismo informático» dentro de los delitos de descubrimiento y revelación de secretos. Lo primero que llama la atención es precisamente su ubicación, pues se introduce entre los delitos que protegen la intimidad, y por la redacción del tipo penal, poco tiene que ver con ésta. El antiguo artículo 197.3 establecía:

> *El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo 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.*
>
> *Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b a g del apartado 7 del artículo 33.*

Como ya he referido, la primera cuestión a abordar debe ser el bien jurídico tutelado en dicho apartado, pues no coincide con el de la intimidad de las personas. De la redacción del precepto se deduce que estamos ante un tipo mixto alternativo con dos modalidades de conducta diferentes[46]: el acceso ilícito y la permanencia en el sistema. La configuración de ambas modalidades se asemeja al delito de allanamiento de morada, en donde se castiga tanto la entrada como el mantenimiento sin autorización, estableciéndose un paralelismo entre el domicilio de la persona y el aquí ahora protegido domicilio informático, es decir, «el espacio en el que se encuentran los datos informáticos pertenecientes a una persona y que se protegen frente a cualquier tipo de intromisión no autorizada»[47].

Respecto de la modalidad de acceso, se plantean una serie de cuestiones: en primer lugar, qué se va a entender por acceso a los datos; en segundo lugar, su deslinde de la figura delictiva recogida en el apartado segundo del artículo 197, en cuanto que aquí, entre otras conductas, se castiga a los que sin estar autorizados accedan a 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. Sin embargo, el Informe del Consejo General del Poder Judicial del año 2008 entiende que el tipo delictivo recogido en el antiguo apartado 3 del artículo 197 no es redundante porque «no hay tal solapamiento con el actual artículo 197.2. Este artículo protege datos personales registrados en ficheros, en tanto que la conducta del antiguo artículo 197.3 afecta a datos que no necesariamente son personales, ni necesariamente están registrados en ficheros»[48]. Parece, pues, que el nuevo delito de acceso a datos y sistemas informáticos ha pretendido tutelar los sistemas informáticos protegidos por barreras de seguridad sin exigir que mediante dicho ataque se produzca atentado alguno contra la intimidad. Por consiguiente, se tipifica el simple intrusismo informático, caracterizado por saltar las barreras del sistema. De este modo el tipo delictivo no va a exigir un elemento subjetivo específico de vulnerar la intimidad, aunque implícitamente conlleve el de descubrir secretos. Esta afirmación resulta en sí misma contradictoria, pues el acceso informático debería ser, según la voluntad que el legislador ha mostrado con su ubicación sistemática de la conducta del antiguo n.º 3 del art. 197, el acceso a un lugar ligado a la intimidad. ¿Cómo resolver los casos en los que el sujeto accede a los sistemas informáticos (sin la correspondiente autorización) con el ánimo de conocer secretos de empresa? ¿Debemos entender que el sujeto realiza una conducta totalmente desligada del concepto de intimidad (bien jurídico de referencia en el Título X del Código Penal), o, por el contrario, entendemos que se lesiona también la *intimidad informática* del titular del sistema?

La figura delictiva también recoge otra modalidad de conducta, concretamente la de mantenimiento dentro del sistema informático sin autorización. Esta modalidad es alternativa a la primera e implica que haya habido un acceso inicial lícito, pero que posteriormente,

46 Muñoz Conde, F.: *Derecho Penal. Parte Especial*, 18ª edición, ed. Tirant lo Blanch, 2010, p. 277.

47 Carrasco Andrino, M. M.: «El delito de acceso ilícito a los sistemas informáticos» en *Comentarios a la Reforma Penal de 2010*, ed. Tirant lo Blanch, 2010, p. 250.

48 Informe del Consejo General del poder Judicial al Anteproyecto de Ley Orgánica de 14 de noviembre de 2008.

por las razones que sean, el titular deniega el acceso a ese sistema. Esto convertirá la permanencia en ilegal. Interesante resulta el supuesto en el que no haya habido medidas de seguridad para impedir el acceso, éste se haya otorgado y posteriormente se cancele el acceso. Tal hecho dejaría de ser delito conforme al antiguo apartado 3 del artículo 197; la cuestión es si podría considerarse delictivo en base al apartado 2 del mismo artículo. La primera cuestión a resolver es si pudiera considerarse «acceso sin autorización» lo que en puridad es un mantenimiento ilegítimo que inicialmente contó con autorización para el acceso. El segundo problema a resolver sería que la conducta del número 2 del artículo 197 es más específica por cuanto que requiere que el objeto del delito lo constituyan datos reservados de carácter personal o familiar de otro.

Dadas las conductas recogidas en el apartado 3 del artículo 197, puede ocurrir que se produzcan daños en el sistema al que se accede. En estos casos la cuestión a resolver será el tipo de concurso que se establece con el delito de daños de material informático tipificado en el artículo 264. Igualmente puede suceder que el acceso a los sistemas informáticos se produzca con la intención de defraudar, en cuyo caso los problemas concursales se establecerán con los delitos de estafa o apropiación indebida.

Finalmente, el legislador de 2010 había previsto la posibilidad de que las conductas descritas en el antiguo apartado 3 del artículo 197 fueran llevadas a cabo por una persona jurídica. Por otra parte, la redacción del párrafo segundo del antiguo número 3 del artículo 197 parecía permitir que todos los delitos comprendidos en dicho artículo pudieran ser cometidos por personas jurídicas.

4. Los delitos de descubrimiento y revelación de secretos tras la reforma de 2015

El legislador justifica las modificaciones llevadas a cabo en los delitos contra la intimidad recogidos en el artículo 197 en la necesidad de solucionar los problemas de falta de tipicidad de algunas conductas, entendiendo que «[…] el artículo 197 contempla como delito, por un lado, el apoderamiento de cartas, papeles, mensajes de correo electrónico o cualesquiera otros documentos de naturaleza personal de la víctima y, por otro, la interceptación de cualquier tipo de comunicación de la víctima, sea cual fuere la naturaleza y la vía de dicha comunicación interceptada. Ambas conductas exigen la falta de consentimiento de la víctima.

Los supuestos a los que ahora se ofrece respuesta son aquellos otros en los que las imágenes o grabaciones de otra persona se obtienen con su consentimiento, pero son luego divulgados contra su voluntad, cuando la imagen o grabación se haya producido en un ámbito personal y su difusión, sin el consentimiento de la persona afectada, lesione gravemente su intimidad».

En definitiva, el legislador lleva a cabo una serie de modificaciones meramente formales junto con la introducción de nuevas figuras delictivas. En relación a la reforma sobre cuestiones de forma, el artículo 197 sufre una reestructuración de algunos de sus tipos penales. No obstante, el delito de secreto documental permanece tal cual, al igual que la interceptación de comunicaciones y el control audiovisual clandestino (apartado 1 del artículo 197). El mantenimiento de estas figuras delictivas sin experimentar cambios conlleva que se sigan suscitando los problemas y cuestiones que se planteaban o se arrastraban de legislaciones anteriores. Del mismo modo, el legislador reproduce tal cual el delito de descubrimiento de secretos recogidos en archivos o registros. Respecto de esta última figura delictiva, el legislador ha perdido una oportunidad de aclarar si los datos de personas jurídicas recogidos en archivos o registros son datos reservados de carácter personal o no, o de aclarar las diferencias entre las diversas conductas a las que alude.

El delito de acceso a datos y sistemas informáticos sale del artículo 197 para reubicarse en el que es el artículo 197 bis. Finalmente se introducen nuevas figuras delictivas, como la transposición de la Directiva 2013/40/UE relativa a los ataques contra los sistemas de información y la interceptación de datos electrónicos cuando no se trata de una comunicación personal. El legislador justifica estas nuevas figuras delictivas sobre la idea de que suponen una «superación» de las limitaciones de la regulación vigente para ofrecer respuesta a la delincuencia informática en el sentido de la normativa europea. De acuerdo con estas consideraciones se distingue entre revelación de datos que afectan directamente a la intimidad personal y el acceso a otros datos o informaciones que puedan afectar a la privacidad pero que no estén referidos directamente a la intimidad. Como expresamente establece la Exposición de Motivos de la ley, con el mismo planteamiento se tipifica la interceptación de transmisiones entre sistemas

4.1. Los tipos cualificados

Los tipos agravados han sufriendo pocas modificaciones. Fundamentalmente se han producido pequeños retoques y se ha añadido una nueva agravación.

A. «Si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores»

Esta cualificación no ha sufrido cambios en su contenido con la reforma de 2015; tan sólo un cambio numérico, pues pasa ahora al apartado 3 del artículo 197. Con los términos *difundir*, *revelar* y *ceder*, el legislador quiere hacer referencia a conductas diferentes[49]. Por ejemplo, y en relación a la proyección de los términos, especialmente interesantes son los hechos probados descritos en la Sentencia del Tribunal Supremo de 5 de diciembre de 1958, en donde el sujeto activo se apodera de una carta no para conocer la relación sexual que ya conocía sino con la finalidad de poder demostrar a uno de los protagonistas que se estaba en tal conocimiento. El Tribunal entendió que se estaba ante la modalidad de divulgación del párrafo primero del antiguo artículo 497 del CP. Por el contrario, algún sector doctrinal[50] discrepó del fallo al considerar que la revelación al titular del secreto no tenía relevancia penal, porque faltaba la proyección hacia terceros. Compartiendo la posición de este sector doctrinal, y por tanto negando la aplicación del tipo cualificado, dicha conducta sería subsumible en el tipo básico del art. 197.1, pues independientemente del móvil que guiase al sujeto activo, es decir, si el apoderamiento de la carta se llevaba a cabo para descubrir algo desconocido o para confirmar una sospecha, el sujeto seguiría actuando «para descubrir un secreto». A lo que habría que añadir que el concepto de secreto que maneja el legislador en estas figuras delictivas está conectado a su vez, como no podía ser de otro modo, con el bien jurídico protegido: la intimidad.

El número 3 del artículo 197 establece: «*Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.*

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

Entrando en el análisis del primer inciso de la cualificación contenida en el nº 3 del artículo 197, aquí se recoge la agravación de revelación que presupone la previa realización de las conductas descritas en los números 1 o 2 del 197, es decir, conductas de intromisión ilícita en la intimidad de terceras personas a través de su configuración como delito mutilado de dos actos, uno de apoderamiento, interceptación o utilización de artificios técnicos, unido a un elemento subjetivo adicional al dolo, consistente en el ánimo de realizar un acto posterior, descubrir el secreto, o vulnerar la intimidad de otro, sin necesidad de que éste llegue a producirse. Por tanto, el fundamento de esta agravación radica en la mayor vulneración de la intimidad del sujeto pasivo[51], pues como hemos visto anteriormente para la consumación del tipo básico no es necesario que el secreto llegue efectivamente a descubrirse; por todo ello, la conducta de difundir revelar o ceder implica un plus de antijuricidad al presuponer que los secretos efectivamente han sido descubiertos, y supone una mayor vulneración de la intimidad al ampliarse el número de personas que conozcan los secretos. Los verbos empleados parecen aludir a conductas de diverso contenido: así, *difundir* se refiere a un mayor alcance en la divulgación a terceros que lo que implica el verbo *revelar*, mientras que la expresión *ceder* podría interpretarse de acuerdo con las conductas recogidas en el número 2 del 197. Esta última definición debe vincularse con la recogida en la legislación administrativa que regula esta materia: el artículo 3 de la Ley de protección de Datos de Carácter Personal, *cesión o comunicación de datos* es toda conducta de revelación de datos a una persona distinta

49 Con la introducción de esta cualificación desaparecen los problemas planteados con la redacción original del delito en el antiguo artículo 497 del Código Penal. El Código Penal actual suprime la terminología empleada en la legislación anterior (: «*El que para descubrir los secretos de otro se apoderase de sus papeles o cartas y divulgare aquéllos será castigado con las penas de arresto mayor y multa de 100.000 a 2.000.000 de pesetas. Si no los divulgare, las penas serán de arresto mayor y multa de 100.000 a 500.000 pesetas*»). Es decir: la expresión *divulgare* pasa ahora con mayor precisión hacer referencia a difundir, revelar o ceder. Con este cambio afortunadamente se zanjó la polémica suscitada por la antigua redacción que en la rúbrica del Capítulo recogía el término «revelación» mientras que el artículo 497 párrafo segundo aludía a «divulgación». Esta diferencia terminológica provocó un debate en torno a si ambos términos podían entenderse como sinónimos o no. Polémica que desaparece con la nueva redacción y estructura otorgada por el Código Penal de 1995.

50 Manzanares Samaniego, J.L.: «El artículo 497…», p. 309.

51 Jorge Barreiro, A.: «Los delitos de descubrimiento…», p. 124: Sentencia del Tribunal Supremo de 10 de diciembre de 2004 que establece: *«En relación con el subtipo agravado del 1º inciso del apartado 3º (revelación, difusión o cesión a terceros), que es aplicable a todos los tipos básicos anteriores, debemos señalar que tiene su fundamento en que dichas acciones suponen incrementar la vulneración de la intimidad del sujeto pasivo*».

del interesado. De acuerdo con el diccionario de la Real Academia de la Lengua, por *ceder* hay que entender transferir o traspasar, en nuestro caso los datos reservados de carácter personal. En definitiva, el legislador utiliza términos que, salvando pequeños matices, pueden entenderse como sinónimos: todos ellos coinciden en que exigen la comunicación a terceros distintos del interesado.

El segundo inciso del apartado 3 del artículo 197, por el contrario, pretende abarcar otro tipo de conductas consistentes en la revelación con conocimiento del origen ilícito de los datos o hechos o imágenes captadas, pero sin haber tomado parte en las conductas de descubrimiento de los mismos. Quedan fuera del tipo tanto los supuestos en donde hay consentimiento del titular del bien jurídico como cuando el origen de la obtención de los datos o hechos haya sido lícito, pero la difusión o revelación se lleva a cabo sin el consentimiento del titular del secreto. No obstante, dada la polémica redacción de este apartado antes de la reforma de 2015 y la imposibilidad de castigar la divulgación no autorizada de imágenes o grabaciones consentidas, la jurisprudencia había admitido en ocasiones la calificación de delictiva de conductas subsumibles en el tipo[52].

B. «Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros o se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima»

La primera modalidad agravatoria se mantiene sin cambios; por el contrario, la segunda es de nueva creación. Entrando en el análisis de la primera modalidad, ésta agrava la responsabilidad penal basándose en las características del sujeto activo que concretamente tiene que ser persona encargada o responsable de los ficheros y demás soportes descritos, lo que implica una mayor vulnerabilidad para el bien jurídico si la conducta la realiza quien está encargado de su custodia. Estamos ante elementos normativos del tipo y la Ley de Protección de Datos Personales, L.O. 15/1999, de 13 de diciembre define a ambos sujetos de acuerdo con el artículo 3 letras d y g como: «d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento[53]». Y «g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento[54]».

El legislador cualifica por las características del sujeto únicamente la realización de las conductas contempladas en los números 1 y 2 del artículo 197, excluyendo la recogida en el número 3. Tal forma de proceder es lógica puesto que, en este último número, se recoge la conducta consistente en acceder o mantenerse sin autorización a datos o programas informáticos vulnerando las medidas de seguridad establecidas para impedirlo, por lo que evidentemente el responsable o encargado no tiene por qué vulnerar tales medidas para acceder o mantenerse.

La segunda modalidad agravatoria consiste en la realización de los delitos recogidos en los números 1 o 2

52 Así, por ejemplo, la Sentencia de la Audiencia Provincial de Asturias de 1 de septiembre de 2010, sentencia nº 184/2010.

53 «Sobre el responsable del fichero recaen las principales obligaciones establecidas por la LOPD y le corresponde velar por el cumplimiento de la Ley en su organización. El responsable debe: notificar los ficheros ante el Registro General de Protección de Datos para que se proceda a su inscripción; asegurarse de que los datos sean adecuados y veraces, obtenidos lícita y legítimamente y tratados de modo proporcional a la finalidad para la que fueron recabados; garantizar el cumplimiento de los deberes de secreto y seguridad; informar a los titulares de los datos personales en la recogida de éstos; obtener el consentimiento para el tratamiento de los datos personales; facilitar y garantizar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación; asegurar que en sus relaciones con terceros que le presten servicios, que comporten el acceso a datos personales, se cumpla lo dispuesto en la LOPD; finalmente, cumplir, cuando proceda, con lo dispuesto en la legislación sectorial que le sea de aplicación». Guía Responsables ficheros publicada por la Agencia de Protección de datos en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf

54 «Asociada a la figura del responsable, está la figura del encargado, que es la persona o entidad, autoridad pública, servicio o cualquier otro organismo que, sólo o con otros, trate datos por cuenta del responsable del fichero. La realización de un tratamiento por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado tratará los datos conforme a las instrucciones del responsable, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. No se considera encargado del tratamiento a la persona física que tenga acceso a los datos personales en su condición de empleado dentro de la relación laboral que mantiene con el responsable del fichero». Guía Responsables Ficheros publicada por la Agencia de Protección de datos en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf

del artículo 197 mediante la utilización no autorizada de datos personales de la víctima. La creación de esta agravación viene a ser el cumplimiento de una de las recomendaciones de la Directiva 2013/40/UE que en su exposición de motivos establece: «*Otro elemento importante de un enfoque integrado contra la ciberdelincuencia es el establecimiento de medidas eficaces contra la usurpación de identidad y otras infracciones relacionadas con la identidad. Las necesidades inherentes a la actuación de la Unión relativa a este tipo de conducta delictiva podrían también ser tomadas en consideración en el contexto de la evaluación de la necesidad de un instrumento horizontal global de la Unión*». Y en su artículo 9.5 establece que: «*Los Estados miembros tomarán las medidas necesarias para garantizar 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».* Las infracciones recogidas en los artículos 4 y 5 de la Directiva se refieren a interferencias ilegales en los sistemas de información (tales como borrar, dañas, deteriorar…) e interferencias ilegales en datos informáticos que justifican la agravación por utilización no autorizada de datos de la víctima en otros delitos informáticos como los de daños, pero que no se justifica en los delitos contra la intimidad[55]. En cualquier caso, dicha cualificación quedará referida a supuestos en los que se produce una suplantación de identidad de una persona (para lesionar su intimidad) aprovechándose de la confianza que dicha suplantación genera en un tercero y ello en relación a las conductas mencionadas en los apartados 1 y 2 del artículo 197.

Finalmente, en el último párrafo del apartado 4 se prevé la imposición de las penas en su mitad superior para los casos en los que los datos reservados se hubieran difundido, cedido o revelado. Hay que señalar aquí que el legislador utiliza la expresión «datos reservados» vinculando directamente esta agravación a las conductas a las que se refiere el apartado 2 del artículo 197 cuando sabemos que el apartado 1 abarca a otros objetos del delito como papeles, cartas o efectos personales que, en puridad, no tienen por qué ni ser ni contener datos. No obstante, y para ofrecer un sentido a esta agravante, habrá que mantener una interpretación amplia del término «datos personales» que permita incluir los otros elementos a los que se refiere el apartado 1 del artículo 197.

C. Por el carácter «sensible» de los datos

Esta cualificación tampoco ha sufrido cambios en relación a su contenido. Únicamente pasa a ubicarse en otro apartado, concretamente en el número 5 del artículo 197 y se modifica la referencia al incapaz en tanto en cuanto pasa a ser referenciado como persona con discapacidad necesitada de especial protección. Esta agravación está prevista, como ya sabemos, para cuando tales hechos afecten a datos de carácter personal que revelen la ideología, religión, creencia, salud, origen racial o vida sexual o la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección.

En relación a la vida sexual, nuestra jurisprudencia ha desarrollado una línea interpretativa restrictiva, aplicando la cualificación en los casos en los que la vida sexual revele tendencias que pudieran considerarse al margen de la norma general [STS de 27 de mayo de 2008; SAP de Ciudad Real de 16 de mayo de 2014][56]. En relación con esta cuestión, resulta muy interesante la sentencia de la Audiencia provincial de Álava que, en

55 Colás Turégano, A.: «Nuevas conductas delictivas contra la intimidad (Arts 197; 197 bis; 197 ter) en *Comentarios a la Reforma del Código Penal de 2015* (Dir. González Cussac, J.L.), ed. Tirant lo Blanch, Valencia, 2015, p. 644.

56 «No estimamos, sin embargo, que sea de apreciación al caso la agravación derivada de la afectación de los hechos a datos de la vida sexual de la denunciante, prevista en el número 6 del repetido art. 197, siguiendo en esto la tesis de la STS 302/08 de 27 de mayo [RJ 2008,3240], resolución que sostiene que "la referencia del artículo 197.5º (en la redacción anterior a la reforma operada por LO 5/2010 [RCL 2010, 1658]) a los datos que revelen la ideología, religión, creencias, salud, origen racial o vida sexual no abarca la investigación ilícita de infidelidades o relaciones sexuales de cualquier índole, sino solamente aquellas que se refieran a la orientación sexual de la víctima poniendo de relieve tendencias que en el momento de la redacción del Código Penal [RCL 1995, 3170] y [RCL 1996, 777] pudieran considerarse por algunos sectores al margen de la norma general, como las relaciones homosexuales, circunstancia que está superada por la legislación que homologa los vínculos entre sexos, sea cual sea el género de la persona. La redacción del precepto está en íntima conexión con el artículo 16 de la Constitución [RCL 1978, 2836], estableciéndose la agravante en función de la discriminación social, lo que es radicalmente distinto de la posible inquietud, ansiedad o desasosiego que pueda producir en una persona el hecho de que se conozcan sus relaciones extramatrimoniales". Y esto sin desconocer la existencia de otros enfoques jurisprudenciales al respecto (p. ej.

relación al significado del dato relativo a la ideología de las personas, establecía: «Este tipo agravado sólo puede aplicarse cuando el acceso ilícito a la intimidad tiene por objeto revelar datos, sean relativos a la salud, vida sexual, creencias, origen racial, ideología o religión de las personas. Según el diccionario, «revelar» significa descubrir, manifestar un secreto, hecho que en el ámbito enjuiciado implicaría dar a conocer la ideología de las personas que permanecían en la sede de la coalición política, y es evidente que ninguna trascendencia puede tener este hecho en el caso que nos ocupa. Desde el piso superior se escuchaban y grababan conversaciones de las personas que estaban en el local inferior, sede de la formación política Herri Batasuna, luego las escuchas realizadas no podían descubrir ningún secreto respecto a la ideología de éstas personas, si estaban allí era porque pertenecían a la formación, la mayoría de ellas tenían cargos públicos como representantes del partido, siendo lógico que mantuviesen conversaciones políticas y profesionales, conversaciones que sin duda les relacionaba con una ideología concreta, la de Herri Batasuna. En consecuencia, la acción ilícita no iba dirigida a descubrir una ideología determinada, sino que partiendo del hecho de que el local era la sede de éste partido y que era frecuentado por sus miembros, se intentaba conocer sus planes, estrategias, relaciones con otros partidos, con otras formaciones, y en general todo lo que pudiese servir a estos fines» [AP de Álava de 4 de abril de 2003 62/2003].

D. Por el fin lucrativo

Aquí las modificaciones se reducen a un cambio de apartado, que del antiguo apartado 7 pasa ahora a ubicarse en el apartado 6 del artículo 197: «*Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años*». La jurisprudencia entiende que «*para apreciar la concurrencia de esta modalidad agravada no es necesario que efectivamente se lleguen a cobrar emolumentos por el trabajo; basta con que el sujeto activo actúe movido por el designio de obtener un beneficio económico. El móvil del lucro estará implícito cuando tal antijurídico que hacer forma parte de la actividad empresarial del autor*». [Sentencia de la Audiencia Provincial de Pontevedra de 18 de mayo de 2001].

E. La difusión no autorizada de imágenes o grabaciones audiovisuales obtenidas con el consentimiento de la víctima.

La reforma de 2015 ha introducido esta nueva figura delictiva en el apartado número 7 del artículo 197. En dicho apartado se establece:

> *Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.*
>
> *La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.*

La introducción de esta nueva modalidad delictiva venía siendo exigida por un sector de la sociedad que no se veía protegido ante la posibilidad de difundir sin el consentimiento de la víctima imágenes o grabaciones audiovisuales que hubieran sido obtenidas, sin embargo, con el consentimiento de ésta. Como sabemos, para su persecución penal, era necesario que la obtención de las mismas hubiera sido también ilícita.

El nuevo tipo penal recogido en el apartado 7 del 197 pretende cubrir esta laguna de punibilidad. No obstante, y entrando en un análisis del precepto, resulta criticable principalmente por la vaguedad de alguno de los términos empleados: por ejemplo, y de forma especialmente significativa, la expresión «cualquier otro lugar fuera del alcance de la mirada de terceros». Entiendo que la expresión «cualquier otro lugar» no tiene por qué referirse a un espacio cerrado, pudiendo ser éste un lugar abierto siempre y cuando quede fuera del alcance de la mirada de terceros. Y siempre y cuando no entre en contradicción con lo establecido por la legislación que regula el uso de videocámaras por las Fuerzas y Cuerpos de Seguridad (LO 4/19997, de 4 de agosto, por la que se regula el uso de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos).

vid. STS 694/2003, de 20 de junio [RJ 2003, 4359])». Sentencia de la Audiencia Provincial de Ciudad Real de 16 de mayo de 2014 [JUR 2014/180776].

La expresión más perturbadora es la que refiere «fuera del alcance de la mirada de terceros», pues permitiría la consideración de delictiva la difusión de imágenes o grabaciones audiovisuales que, habiéndose realizado en un lugar público, sin embargo, estuviera fuera del alcance de la mirada de terceros.

En relación a la alusión al hecho de que la divulgación de las imágenes o grabaciones menoscabe gravemente la intimidad personal, el legislador pretende la constatación de que efectivamente dicha conducta haya lesionado el bien jurídico protegido y que dicha lesión haya tenido la suficiente entidad como para ser perseguida penalmente. No obstante, quedará a criterio judicial la determinación de la gravedad del menoscabo. La figura delictiva queda circunscrita a la divulgación de imágenes o grabaciones audiovisuales que se hayan obtenido con el consentimiento de la víctima directa o indirectamente; por ejemplo, que la víctima las haya enviado a una persona para que se las envíe a su vez al sujeto activo. La conducta típica queda limitada a difundir exclusivamente imágenes o grabaciones audiovisuales.

El legislador ha previsto la posibilidad de agravar la responsabilidad criminal para los supuestos en los que los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aún sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección o los hechos se hubieran cometido con una finalidad lucrativa.

4.2. Las conductas delictivas recogidas en el artículo 197 bis

En este precepto se recogen dos figuras delictivas: la anteriormente denominada de acceso a datos y sistemas informáticos, y la de nueva creación, de interceptación de transmisiones no públicas de datos informáticos.

En relación a la figura delictiva recogida en el apartado primero del artículo 197 bis, aunque fue introducida por la ley de reforma de 2010, el legislador de 2015 la ha sometido a ciertos cambios[57]. Puede decirse que algunos no suponen una alteración significativa del delito, aunque de otros hay que afirmar lo contrario. Así, por ejemplo, la denominación de acceso a datos y sistemas informáticos deberá cambiarse ya que a partir de ahora no será necesario acceder a los datos para castigarlo penalmente al haberse producido un adelantamiento de la barrera de protección. Actualmente en el apartado 1 del artículo 197 bis se establece: «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 a 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». Como puede apreciarse, además de que el sujeto activo realice por sí mismo el acceso al sistema de información o se mantenga en el sin autorización y vulnerando las medidas de seguridad establecidas para impedirlo, el legislador de 2015 añade la posibilidad de incriminar al sujeto que facilite a otro el acceso al sistema informático habiendo previamente vulnerado las medidas se seguridad establecidas para impedirlo. Esta elevación a la categoría de autoría de lo que sería un acto de participación quizás se deba a la exigencia establecida en la Directiva europea 2013/40/UE, que en su artículo 8 establece la necesidad de que se garantice por los estados miembros que la inducción y la complicidad sean sancionadas penalmente. Quizás el legislador español peque de exceso de celo al elevar en este punto la participación a la autoría.

También el cambio de redacción afecta al objeto del delito, en tanto en cuanto ahora se penaliza el acceso al conjunto o a una parte de un sistema de información o se mantenga en el mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo. Recordemos que el antiguo delito del apartado 3 del artículo 197 castigaba el acceso a datos o programas informáticos contenidos en un sistema informático. Esta modificación, además de implicar obviamente un adelantamiento de la barrera de protección penal[58], supone también dar respuesta a las exigencias de la ya mencionada Directiva europea; Directiva que, entre otras cosas, define tanto qué se entiende por sistema de información como datos informáticos. En relación al primero, la Directiva considera que es «todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un pro-

57 Para Frías Martínez el tipo penal recogido en el artículo 197 bis. 1 es un tipo especial en relación al recogido en el 197.1. Por el contrario, creo que la distancia entre uno y otro es mayor, porque el artículo 197 bis.1 se refiere a conductas que afectan a una parte o a todo un sistema informático y no a datos personales. Frías Martínez, E.: en *Código penal*…, p. 368.

58 Igualmente, González Cussac, J.L.: en *Derecho Penal. Parte Especial* (Gónzalez Cussac, (coord.)), 4ª edición, ed. Tiran lo Blanch, Valencia, 2015, p. 288.

grama, 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». Los datos informáticos vienen definidos como «toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función». Como se establece en la propia exposición de motivos de la ley de 2015, estas modificaciones pretenden superar las limitaciones de la legislación vigente para ofrecer respuesta a la delincuencia informática en el sentido de la normativa europea. Por eso se introduce una separación entre los supuestos de revelación de datos que afectan directamente a la intimidad personal y por ejemplo el acceso a los sistemas informáticos.

Precisamente, y entrando en el análisis del apartado 2 del artículo 197 bis, se ha creado la nueva figura delictiva de interceptación de transmisiones no públicas. Aquí no se trata de castigar la interceptación de transmisiones personales sino de interceptar transmisiones entre sistemas de información. Según establece el número 2 del 197 bis: «El que, mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses».

Se adapta aquí el art. 6 de la Directiva 2013/40/UE. La misma Directiva define algunos de los conceptos fundamentales manejados, como los de «datos informáticos» o «sin autorización», que se conservan literalmente en la transposición. En concreto, define los datos informáticos como «toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función», y aclara el matiz de «sin autorización» como «un comportamiento al que se refiere la presente Directiva, incluido el acceso, la interferencia o la interceptación, que no haya sido autorizado por el propietario u otro titular del derecho sobre el sistema o parte del mismo o no permitido por el Derecho nacional».

Junto a los conceptos ya definidos, aparecen en este artículo 197 bis 2 otros que, por su especificidad técnica, merecen una mención especial. En primer lugar, se habla del uso «artificios o instrumentos técnicos». La Directiva, en su consideración 16, habla de «instrumentos» (el entrecomillado es del original), y añade que «pueden ser programas informáticos maliciosos, incluidos los que permiten crear redes infectadas, que se utilizan para cometer ciberataques». El uso de comillas que destacamos parece que revela las dificultades del legislador europeo a la hora de encontrar una denominación genérica para un concepto tan cambiante. Entendemos también que la concreción de los mismos («programas informáticos maliciosos») es abierta, como indica el propio verbo potencial («pueden ser»), y no excluye otras modalidades.

Quizá sea para complementar este concepto de «instrumento» por lo que el art. 197 incluye la mención de «artificio», que podemos entender bien en el sentido propio de «máquina o aparato» (RAE), bien en el más específico en que es usado, por ejemplo, en interceptación de comunicaciones.

A continuación, en el artículo 197 bis.2 se establece una importante referencia a la legitimidad de la acción: «sin estar debidamente autorizado». Sin duda, el problema reside en saber cuándo existe el derecho a interceptar las transmisiones no públicas. Desde mi punto de vista, existiría el derecho en casos en los que, por ejemplo, se llevan a cabo conductas como las pruebas de seguridad de sistemas informáticos que se realizan habitualmente, siempre que exista «autorización por el propietario».

Aborda luego el art 197 el núcleo principal de su contenido, y transcribe casi literalmente la Directiva. Importante es el matiz de «transmisiones no públicas», pues excluye de facto aquellas que sí lo sean (redes abiertas, por ejemplo), y a la vez concreta el bien jurídico protegido diferenciándolo claramente del art. 197.1, donde se habla de «interceptar sus telecomunicaciones» para vulnerar la intimidad. Es decir, se introduce un nuevo ámbito de protección que afecta no ya a lo privado, sino también a lo no público. En la exposición de motivos de la Ley de Reforma del Código Penal se justifica esta diferenciación al afirmarse: «De acuerdo con el planteamiento recogido en la Directiva, se introduce una separación nítida entre los supuestos de revelación de datos que afectan directamente a la intimidad personal, y el acceso a otros datos o informaciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal». Existirían, pues, tres niveles de protección: privacidad (que incluiría intimidad); no publicidad (que abarcaría todo tipo de datos dimanantes de un sistema de información no englobables en el primero, fundamentalmente datos

técnicos generados por el propio sistema); y, finalmente, un nivel público, que quedaría fuera de la protección penal.

En otro orden de cosas, se tipifica tanto el acceso como la facilitación del acceso a otras personas, hecho este último que entra en colisión con la conducta recogida en el art. 197 ter, como veremos.

Finalmente, se intenta proteger todo el circuito de transmisión de datos «desde, hacia o dentro de un sistema de información», previsión hecha para incluir en su ámbito de protección incluso el flujo de información interna de redes, dada la amplitud con que se definen esos «sistemas». También se protegen las emisiones electromagnéticas de dichos sistemas, como las producidas por tecnologías *wireless* tales como wifi, bluetooth o telefonía móvil, caracterizadas por la ausencia de cableado de conexión.

4.3. El delito de facilitación de programas informáticos, contraseñas de ordenador o códigos de acceso o similares para facilitar la comisión de otros delitos, recogido en el artículo 197 ter

Según establece el referido artículo:

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.

Comparativamente, la redacción de este artículo es idéntica al art. 264 ter CP, que prevé idénticas penas y conductas en relación con los delitos de los artículos 264 y 264 bis, que versan sobre protección contra daños informáticos. Nótese que allí se exige una afección sobre los datos y transmisiones, que además ha de ser grave, mientras que en el ámbito de este art. 197 bis sólo se mencionan el acceso o mantenimiento en un sistema de información, o la mera intercepción de transmisiones, sin que sea necesario el daño a los datos.

Este artículo transcribe el 7.º de la Directiva de forma casi literal. Ahora sí se hace mención expresa de la intencionalidad[59] que recalca la Directiva («con la intención de facilitar la comisión de alguno de los delitos…»). La precisión no es superflua, pues es posible imaginar programas de control creados y distribuidos con fines muy distintos y, en principio, legales, como los programas de monitorización de actividades o control parental, que se prestan a ser utilizados para obtener subrepticiamente datos privados. De hecho, una buena parte de los programas avanzados que usan los especialistas informáticos para su trabajo pueden ser utilizados con otras intenciones, en principio ilícitas.

La principal variación en la redacción del art. 197 ter respecto de la Directiva Europea es la introducción de un matiz de facilitación a terceros que no figura en ésta, y la supresión de la figura de «distribución u otra forma de puesta a disposición (de los programas o contraseñas)». La omisión pudiera considerarse salvada con la inclusión del inciso «de cualquier modo, facilite a terceros», pero, desde el punto de vista técnico, este inciso incurre en la mala práctica de provocar cierta ambigüedad en la relación de las conductas mencionadas anteriormente en el mismo (producción, adquisición, importación) con la intencionalidad de facilitar la comisión, pues ésta debe entenderse requerida en todas aquellas, y no sólo en la de facilitación. En este sentido, la redacción original de la Directiva resulta más clara e inequívoca. Finalmente, como apuntábamos, esta inclusión en la redacción del art. 197 ter entra en franca solapamiento con la previsión muy similar ya recogida en el 197 bis, donde ya se prevé la facilitación a otro del acceso a un sistema de información

En resumen, resulta chocante y hasta cínico enmarcar estas conductas dentro del Título de «Delitos contra la intimidad», cuando tanto la Directiva como la Exposición de Motivos de la Ley revelan otros intereses que nada tienen que ver con la protección de la intimidad de los sujetos. En realidad, se está buscando aquí garantizar la seguridad de los sistemas informáticos, sin duda, muy antes que la preservación de la intimidad. Cierto es que, en la sociedad de la información actual, la protección de los datos informáticos es fundamental para la de la intimidad personal, pero no deja de producirse un desajuste, una grieta, entre el espíritu del Título y los delitos que ahora se le incorporan, como si de un mero cajón de sastre se tratara. Las nuevas conductas punibles descritas en el tipo no afectan sino muy mediatamente al ámbi-

59 Para Vázquez Iruzubieta, se exige un dolo específico (facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el 197 bis. Vázquez Iruzubieta, C.: *Código Penal Comentado*, ed. Atelier, Barcelona, 2015, p. 372.

to de privacidad de las personas. En realidad, como confiesa la propia Directiva, sus objetivos son otros: «garantizar que los ataques contra los sistemas de información sean castigados […] y mejorar y fomentar la cooperación judicial» (consideración 33). El mismo espíritu imbuye el resto de planteamientos iniciales de la norma europea cuando habla de ataques cibernéticos de índole terrorista a infraestructuras críticas. En definitiva, estamos ante protección de bienes jurídicos que nada tienen que ver con la «intimidad» de las personas, o que, como mucho, constituyen una antesala dudosa a su hipotética vulneración.

Así pues, se produce un adelanto de la barrera de protección desde la salvaguarda de la intimidad a la de los propios sistemas informáticos. Pudiera ser que el legislador nacional se haya dejado arrastrar por la estructura de la Directiva europea y se ha limitado a volcarla en un Título existente, al que se asemeja relativamente. Igualmente, difícil habría sido encajar esta figura entre el articulado relativo a los daños informáticos (art. 264 y ss. CP), pues allí se exige, precisamente, el daño, mientras que aquí sólo se persigue el acceso, mantenimiento o interceptación. Tal vez el rápido desarrollo de las tecnologías de la información y la comunicación debiera obligar a la creación de nuevo Título que ampare estas conductas.

Este desajuste del marco normativo no es baladí si lo ponemos en relación con las críticas que se han realizado sobre la vaguedad de las definiciones y conceptos utilizados. Recordemos que la norma penal debe interpretarse de acuerdo con su propio contexto, y la realización de acciones que pudieran incurrir dentro de los nuevos tipos del art. 197 bis y ter han de ponerse en relación con el bien protegido (la intimidad), lo que a veces puede no resultar tan evidente, como en el caso de interceptación de meros datos técnicos de transmisiones.

Pero los riesgos derivados de esta indefinición no paran aquí. Debemos reparar en que el art 573 CP eleva estos delitos a la categoría de terrorismo[60]. Si a la vaguedad técnico-jurídica atribuible a estos artículos añadimos ahora la invocación a conceptos indeterminados como el de «paz pública», nos encontramos con un salto al vacío que deja un amplio campo de interpretación: actuaciones de difusión masiva de información sensible (no personal, sino de interés público) al estilo de las promovidas por Snowden o Wikileaks, ¿no podrían, en definitiva, estar poniendo en peligro la «paz púbica», o «desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado»?

En una sociedad globalizada, se imponen medidas de control también globales, que, en muchos casos, tienen un carácter horizontal, emanan de instancias superiores y han de ser encajadas en cada ordenamiento jurídico. Hemos visto cómo el encaje, en este caso, es, como poco, forzado. El legislador deberá plantearse en un futuro inmediato un cambio de esta sistematización obsoleta que se limita a incluir los delitos informáticos junto a los que, aparentemente, son sus correlatos «analógicos» o tradicionales. La rapidísima evolución tecnológica parece que nos aboca a otros sistemas en los que seguramente nuevos delitos exigirán nuevos agrupamientos, sin necesidad de forzar los ya existentes.

4.4. El artículo 197 quáter: cualificación en caso de organización o grupo criminales

El artículo 197 quáter establece: «*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*».

Esta cualificación supone un mayor desvalor de la acción por la mayor facilidad que supone realizar estas conductas a través de una organización o grupo criminal. ¿Qué se entiende por organización criminal? En los artículos 570 bis y 570 ter se castiga la pertenen-

60 Artículo 573: *1. Se considerarán delito de terrorismo la comisión de cualquier delito grave contra la vida o la integridad física, la libertad, la integridad moral, la libertad e indemnidad sexuales, el patrimonio, los recursos naturales o el medio ambiente, la salud pública, de riesgo catastrófico, incendio, contra la Corona, de atentado y tenencia, tráfico y depósito de armas, municiones o explosivos, previstos en el presente Código, y el apoderamiento de aeronaves, buques u otros medios de transporte colectivo o de mercancías, cuando se llevaran a cabo con cualquiera de las siguientes finalidades:*

1.ª Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo.

2.ª Alterar gravemente la paz pública.

3.ª Desestabilizar gravemente el funcionamiento de una organización internacional.

4.ª Provocar un estado de terror en la población o en una parte de ella.

2. Se considerarán igualmente delitos de terrorismo los delitos informáticos tipificados en los artículos 197 bis y 197 ter y 264 a 264 quater cuando los hechos se cometan con alguna de las finalidades a las que se refiere el apartado anterior.

3. Asimismo, tendrán la consideración de delitos de terrorismo el resto de los delitos tipificados en este Capítulo.

cia o constitución de la organización o grupo criminal, protegiéndose así el orden público como bien jurídico a tutelar[61]. Este interés es también el que justifica el mayor desvalor del hecho, además de la mayor facilidad que va a suponer la pertenencia a una organización o grupo criminal por la cobertura que ello va a suponer para el sujeto.

Esta cualificación ha sufrido un cambio de ubicación con la reforma de 2015: del apartado 8 del artículo 197 ha pasado a integrar el artículo 197 quáter. Esta modificación implica que a partir de ahora no sólo se aplicaría a las conductas descritas en el artículo 197 sino también a las demás recogidas en el Capítulo primero del Título X.

4.5. La responsabilidad de las personas jurídicas: artículo 197 quinquies

El legislador de 2015 ha establecido la posibilidad de exigir responsabilidad penal a las personas jurídicas a través de este precepto de una manera más clara que en la anterior regulación. El artículo 197 quinquies establece: «Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33». En el anterior artículo 197 apartado 3, párrafo segundo se establecía la responsabilidad de las personas jurídicas, pero no de manera tan precisa. Ahora queda claro que ésta está referida a la comisión de los delitos recogidos en los artículos 197, 197 bis y 197 ter.

4.6. Por el carácter de autoridad o funcionario público del sujeto activo (artículo 198 del Código Penal)

El artículo 198 del CP establece: «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». En este precepto, que no ha sufrido modificaciones con la reforma de 2015, por lo que se mantiene sin alteraciones, se recoge la agravación de la responsabilidad criminal para los casos en los que el sujeto activo sea autoridad o funcionario público. Concretamente la autoridad o funcionario público tiene que actuar fuera de los casos permitidos por la ley, si mediar causa legal por delito y prevaliéndose de su cargo. A partir de aquí se imponen la necesidad de diferenciar las conductas subsumibles en el artículo 198 de las recogidas en el artículo 417 del Código Penal que castiga la revelación de secretos o informaciones que no deban ser divulgadas y de las que la autoridad o funcionario público haya tenido conocimiento por razón de su oficio o cargo. El artículo 417 establece:

> *1. La autoridad o funcionario público que revelare secretos o informaciones de los que tenga conocimiento por razón de su oficio o cargo y que no deban ser divulgados, incurrirá en la pena de multa de doce a dieciocho meses e inhabilitación especial para empleo o cargo público por tiempo de uno a tres años.*
>
> *Si de la revelación a que se refiere el párrafo anterior resultará grave daño para la causa pública o para terceros, la pena será de prisión de uno a tres años, e inhabilitación especial para empleo o cargo público por tiempo de tres a cinco años.*
>
> *Si se tratara de secretos de un particular, las penas serán las de prisión de dos a cuatro años, multa de doce a dieciocho meses, y suspensión de empleo o cargo público por tiempo de uno a tres años.*

En relación a las diferencias entre el 198 y el artículo 417 del Código Penal, resulta especialmente interesante la sentencia del Tribunal Supremo de 11 de junio de 2004 que establece que: «*La relación existente entre estos dos tipos penales surge del texto de ambos. El artículo 417.1 se refiere en principio a secretos e informaciones que no necesitan ser de carácter personal. Por lo tanto, la cuestión sólo se puede plantear entre el artículo 197.2 y el 417.2 del Código Penal, dado que este último hace referencia a «secretos de un particular». Sin embargo, mientras en el caso del artículo 197.2 del Código Penal se trata de un acceso indebido a la fuente de los datos, pues la ley dice «sin estar autorizado», en el caso del artículo 417.2 del Código Penal el autor tiene un conocimiento propio de su cargo y obtenido por una necesidad del procedimiento administrativo. En ambos casos se vulnera un deber funcionarial de secreto, pero en el supuesto del artículo 197.2/198 del Código Penal, el funcionario,*

61 Vid. Sobre estas figuras delictivas, entre otros, Gómez Tomillo, M. (Dir.): *Comentarios al Código Penal*…, pp. 1922 y 1923; Muñoz Conde, F.: *Derecho Penal. Parte Especial*…, p. 829; Silva Sánchez, J.M. (Dir.): *Lecciones de*…, p. 401.

además, infringe otro deber, dado que él se «apodera» ilegalmente, abusando de su posición funcionarial, de datos que no debería conocer por su cargo. Esta doble infracción de deberes explica y justifica la diferencia de las penas previstas para ambos delitos». Nada tendríamos que objetar a esta argumentación en relación al ámbito de aplicación de ambos preceptos si no fuera por la perturbación que produce la cualificación 5 del artículo 197 («si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros»): en principio, en virtud de la interpretación ofrecida por el Tribunal Supremo en relación al ámbito de aplicación de la cualificación recogida en el artículo 198, éste y la recogida en el apartado 5 del artículo 197 serían incompatibles. Ello porque el encargado o responsable de los ficheros o soportes informáticos o electrónicos no se «apodera ilegalmente» de los mismos ya que el acceso a los datos por su parte sería legal. El legislador de 2015 ha perdido una oportunidad de aclarar el ámbito de actuación del artículo 198. Ciertamente resulta contradictorio que, por un lado, el artículo 198 exija que la autoridad o funcionario público se prevalga, abuse de su condición aunque no dentro de la actividad que le es inherente (exigencia ésta mayoritariamente establecida por doctrina y jurisprudencia, para poder así diferenciarlo de las conductas recogidas en el artículo 417) y, por otro, que la cualificación por ser encargado o responsable de los ficheros o datos que por definición exige que sea precisamente una persona que actúe dentro del marco de sus competencias, pretenda todo lo contrario. Visto así la relación entre el artículo 198 y el 197.4 es absolutamente perturbadora, planteando claros problemas de incompatibilidad. Los conceptos de «personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros» hay que conectarlos directamente con los ofrecidos por la Ley Orgánica de Protección de Datos de Carácter Personal de 19999 (LO 15/1999, de 13 de diciembre). La Ley de protección de datos en su artículo 3 define a la persona encargada del tratamiento de datos, que no coincide exactamente con la referida en el Código Penal, en donde se alude a la persona encargada de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros. En el mencionado artículo 3 de la legislación administrativa se describe esta figura como la de la persona que trata los datos personales siguiendo las instrucciones del responsable, aunque no bajo la dependencia o autoridad del mismo desde el punto de vista laboral[62]. Entiendo que este debe ser también el concepto que se maneje en el ámbito penal para no extender desmesuradamente el ámbito de la cualificación. Por tanto, la figura del encargado se circunscribiría a la persona que presta sus servicios al amparo de un contrato de esta índole, no coincidiendo, pues, con la persona del empleado. El responsable es también definido a nivel administrativo como la persona que tiene capacidad decisoria en relación a la creación de ficheros, finalidad, contenido y uso del tratamiento. En concreto, y respecto al tratamiento de datos, el responsable sería la persona que toma las decisiones sobre las concretas actividades del tratamiento no teniendo por qué coincidir, por ejemplo, con la persona que decide sobre la creación de un fichero de datos. Resulta difícil en tal contexto conciliar esta cualificación con la de ser el sujeto activo autoridad o funcionario público.

5. Conclusiones

En conclusión, la reforma en los delitos contra la intimidad ha sido dirigida a aspectos parciales y muy concretos, centrándose fundamentalmente en modificaciones en materia de intromisión informática y de transposición de la normativa europea sobre esta materia.

En algunos aspectos, la ley de reforma de 2015 ha perdido la oportunidad de solucionar de una vez algunas cuestiones que han venido generando dudas desde hace mucho tiempo, mientras que en otros la creación de nuevos tipos penales aumenta los problemas de concreción de muchos de los delitos recogidos en este Título. Además, hay que tener en cuenta que los delitos recogidos en los artículos 197 bis y 197 ter suponen una clara perturbación del bien jurídico protegido en el capítulo I del Título X; hubiera sido deseable la creación de un nuevo título que recogiese las mencionadas figuras delictivas.

62 Vid. Vizcaíno Calderón, M.: *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, ed. Civitas, Madrid, 2001, p. 83.