LOS DELITOS CONTRA LA INTIMIDAD TRAS LA REFORMA DE 2015: LUCES Y SOMBRAS

Tàlia González Collantes

Universitat de València

Resumen: Son cuantiosos y profundos los cambios introducidos en el Código Penal por la reforma de 2015, entre los cuales encontramos los que afectan a los delitos contra la intimidad, cuyo análisis constituye el objeto principal del presente trabajo, en el cual también examinamos una serie de preceptos que permanecen incólumes a pesar de las críticas realizadas por la doctrina, habiéndose desaprovechado la ocasión para modificarlos.

Abstract: The changes in the penal code reform for 2015 are large and deep, among which are those involving offenses against privacy, whose analysis is the main object of this study, in which we also examined a series of precepts that remain intact despite the criticisms made by the doctrine, having missed an opportunity to modify them.

Palabras clave: Reforma penal, delitos contra la intimidad, análisis crítico.

Key words: Penal reform, crimes against privacy, critical analysis.

1. Introducción

Son muchas las novedades introducidas en el Código Penal por la última reforma de 2015, y aunque las más polémicas atañen a la parte general también las hay que alteran la parte especial. Son unos cuantos los delitos que han sido afectados por la misma, entre los cuales se encuentran los delitos contra la intimidad, de los que nos ocuparemos a continuación, y como podremos comprobar se han incorporado modificaciones no sólo formales sino también sustanciales.

En concreto, en cuanto a las modificaciones sustanciales, a pesar de que en el Anteproyecto presentado en septiembre de 2012 por el entonces Ministro de Justicia la única novedad en materia de tutela del bien jurídico intimidad venía representada por la introducción de una figura delictiva nueva consistente en la difusión no autorizada de imágenes o grabaciones audiovisuales obtenidas con consentimiento de la víctima, tras la entrada de aquél en el Congreso de Diputados y su conversión en Proyecto se añadieron otras figuras delictivas en el ámbito del llamado delito de intrusismo informático, consistente una en interceptar ilegalmente transmisiones no públicas entre sistemas y la otra en facilitar instrumentos para la comisión del intrusismo informático, y también se introdujo un tipo cualificado, cuando en la realización de la conducta se utilizan datos personales de otra persona como instrumento para ganarse la confianza de la víctima y poder atacar su intimidad.

Y por otra parte, en relación a las novedades formales, se ha reorganizado el contenido del artículo 197, de manera que encontramos cambios de ubicación sistemática de las figuras aquí contempladas, se han incorporado los nuevos artículos 197 bis, ter, quáter y quinquies, la agravación prevista en el artículo 197 quáter consistente en cometer los hechos en el seno de una organización o grupo criminal se extiende a todos los delitos incluidos en el capítulo, y en el 197 quinquies encontramos cambios que afectan a la cláusula específica de responsabilidad penal de las personas jurídicas.

Algunas de las reformas incorporadas en el Capítulo primero del Título X del Libro II han sido solicitadas por la doctrina, otras las ha propuesto el Consejo General del Poder Judicial en el informe emitido sobre el Anteproyecto y otras responden a razones de armonización y transposición de la normativa europea. En general las mismas han sido positivamente valoradas si bien, como también veremos a continuación, hay algunos puntos criticables, tanto por exceso como por defecto.

Empezaremos este trabajo analizando los preceptos que permanecen incólumes a pesar de las críticas realizadas por la doctrina penal: los apartados primero, segundo y sexto del artículo 197. Seguidamente nos ocuparemos de aquellos otros preceptos que sí se han visto afectados por la reforma: los apartados cuarto, quinto y séptimo del artículo 197, el artículo 197 bis, el 197 ter, el 197 quáter y el 197 quinquies. Y por último, a modo de conclusión, realizaremos una reflexión final sobre algunos aspectos de la reforma penal de 2015 en materia de tutela de la intimidad.

2. Preceptos que permanecen incólumes a pesar de las críticas

2.1 El apartado primero del artículo 197

El artículo 197.1 no se ha visto afectado por esta última reforma de 2015, aunque tal vez sí debería haber sido modificado. Dice así:

> «El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.»

Más allá de que quizá hubiese sido aconsejable realizar alguna modificación léxica —puede llegar a entenderse que se haya optado por no hacerla—, debería haberse aprovechado la ocasión para dar solución a un problema de falta de tipicidad que se plantea, sobre todo teniendo en cuenta que los demás cambios operados en el Capítulo primero del Título X del Libro II se han justificado, al menos en parte, en la necesidad de superar las lagunas de punición existentes; y tampoco se entiende que una vez más se haya renunciado a una estratificación de las penas atendiendo a la gravedad de las modalidades delictivas aquí previstas.

Así pues, yendo por partes, decir cabe, en primer lugar, que la primera modalidad delictiva recogida en este artículo consiste en el apoderamiento de una serie de documentos de otra persona, sin su consentimiento y con el fin de descubrir sus secretos o vulnerar su intimidad, y no es su tipificación lo que se discute sino la elección del verbo «apoderarse», cuyo uso resulta especialmente polémico en

relación con los mensajes de correo electrónico —que con buen criterio, fueron incorporados por el legislador de 1995 entre los documentos susceptibles de contener secretos. Entre los autores críticos con la utilización de este verbo encontramos a POLAINO NAVARRETE[1] y a ROMEO CASABONA[2]. El primero lo rechaza por entender que se trata de un término equívoco, que en una acepción literal estricta en lugar de concretar remite a un tipo de delito patrimonial o contra la fe pública; y el segundo lo hace porque, sobre todo cuando el objeto material del delito es un correo electrónico, dicho verbo requiere de una interpretación espiritualizada. Esto es así en tanto en cuanto resulta punible la mera captación intelectual del contenido de un soporte, pero resulta fundamental tener en cuenta que para que lo sea se requiere que el sujeto activo haya desplegado alguna actividad previa para hacerse con él, dirigida a obtener los datos secretos, es decir, que haya de vencer la oposición del titular. La espiritualización que se produce en la interpretación del verbo en cuestión no se puede llevar a extremos absolutos. La concurrencia de este requisito ha sido defendida, por ejemplo, por ROMEO CASABONA[3], por ORTS BERENGUER y ROIG TORRES[4], por GONZÁLEZ RUS[5] y por TOMÁS-VALIENTE LANUZA[6], aparte de que también viene siendo exigida por la jurisprudencia. Puede que sea por esto por lo que el legislador no ha visto problema en mantener el verbo «apoderarse», por esto y porque tal vez está de

[1] POLAINO NAVARRETE, M., «Descubrimiento, revelación de secretos e interceptaciones ilegales», en *Lecciones de Derecho Penal. Parte especial*, tomo I, Tecnos, Madrid, 2010, p. 232.

[2] ROMEO CASABONA, C. M., «La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de Internet», *Derecho y Conocimiento*, vol. 2, 2002, pp. 131-137; «La protección penal de la intimidad y de los datos personales: los mensajes de correo electrónico y otras formas de comunicaciones de carácter personal a través de internet y problemas sobre la ley penal aplicable», en *Estudios jurídicos del Ministerio Fiscal,* 2003, p. 79; *Los delitos de descubrimiento y revelación de secretos*, Tirant lo Blanch, Valencia, 2004, pp. 728-732.

[3] ROMEO CASABONA, C. M., «La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de Internet», cit., p. 133; «La protección penal de la intimidad y de los datos personales: los mensajes de correo electrónico y otras formas de comunicaciones de carácter personal a través de internet y problemas sobre la ley penal aplicable», cit., p. 82.

[4] ORTS BERENGUER, E.-ROIG TORRES, M., *Delitos informáticos y delitos comunes cometidos a través de la informática*, Tirant lo Blanch, Valencia, 2001, p. 26.

[5] GONZÁLEZ RUS, J. J., «Delitos contra la intimidad, el Derecho a la propia imagen y la inviolabilidad del domicilio», en MORILLAS CUEVA, L. (Coord.), *Sistema de Derecho Penal español. Parte especial*, Dykinson, Madrid, 2011, p. 300.

[6] TOMÁS-VALIENTE LANUZA, C., «Del descubrimiento y revelación de secretos», en GÓMEZ TOMILLO, M. (Dir.), *Comentarios al Código penal*, 2.ª edición, Lex Nova, Valladolid, 2011, p. 796.

acuerdo con ORTS BERENGUER y ROIG TORRES[7] cuando afirman que «el uso de ese verbo, en lugar de otros que, en relación con los datos informáticos, resultarían más precisos (acceder, etc.), resulta justificado teniendo en cuenta el carácter heterogéneo de los soportes a los que está referido (papeles, cartas, mensajes de correo electrónico o cualquiera documentos o efectos personales)».

Por otra parte, en relación al problema de falta de tipicidad que queda sin resolver, en la modalidad delictiva a la que acabamos de referirnos se exige que los soportes que contienen datos personales o familiares sean del titular del secreto, pues se castiga a quien para descubrir los secretos o vulnerar la intimidad de otro se apodera de sus papeles, cartas, mensajes de correo electrónico o cualquiera otros documentos o efectos personales. Esto quiere decir que si los soportes son de un tercero el comportamiento será atípico, y que continúe siéndolo no se debe a que nos encontremos ante una laguna que ha pasado desapercibida, pues son diversos los autores que así lo han denunciado, como es el caso de MORALES PRATS[8], de GONZÁLEZ RUS[9] y de TOMÁS-VALIENTE LANUZA[10]. Debería haberse optado por suprimir la referencia al posesivo «sus».

Y el legislador tampoco ha considerado necesario introducir cambios en relación con las demás conductas tipificadas en el mismo artículo 197.1, consistentes en interceptar telecomunicaciones o utilizar artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación. Se ha dejando pasar una buena oportunidad no sólo, o no tanto, para realizar algún retoque lingüístico, sino de tipo penológico. Cierto es que se ha renunciado a sustituir la expresión «cualquier otra señal de comunicación», pero ello puede deberse a que, a pesar de que, como con razón apunta ROMEO CASABONA[11], puede resultar «confusa por lo que atañe a su naturaleza

---

[7] ORTS BERENGUER, E.-ROIG TORRES, M., *Delitos informáticos y delitos comunes cometidos a través de la informática*, *ob. cit.*, p. 25.

[8] MORALES PRATS, F., «Delitos contra la intimidad, el Derecho a la propia imagen y la inviolabilidad del domicilio», en QUINTERO OLIVARES, G. (Dir.), *Comentarios a la parte especial del Derecho Penal*, 9.ª edición, Aranzadi Thomson Reutersn, Cizur Menor (Navarra), 2011, p. 457.

[9] GONZÁLEZ RUS, J. J., «Delitos contra la intimidad, el Derecho a la propia imagen y la inviolabilidad del domicilio», cit., p. 306.

[10] TOMÁS-VALIENTE LANUZA, C., «Del descubrimiento y revelación de secretos», cit., p. 796.

[11] ROMEO CASABONA, C. M., «La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de Internet», *Derecho y Conocimiento*, vol. 2, 2002, p. 127.

y contenido», no es menos cierto que, como también indica este autor, el recurso a la misma se justifica porque «pretende asumir de nuevo una función de recogida o de escoba respecto a las innovaciones tecnológicas que puedan surgir en el futuro»; o como se afirma en la STS 694/2003, de 20 junio, se trata de una cláusula destinada a subsanar las eventuales «lagunas de punibilidad que se pueden derivar de los avances de la tecnología moderna». Pero como hemos avanzado, lo que sí debería haberse hecho es revisar las penas a imponer. Efectivamente, debe tenerse presente que a las diferentes modalidades delictivas contenidas en los dos pasajes de este artículo les corresponden las mismas penas de prisión de uno a cuatro años y de multa de doce a veinticuatro meses, y ello a pesar de la mayor gravedad objetiva que supone la utilización de aparatos técnicos de control auditivo o visual clandestino o de interceptación de las telecomunicaciones, por tratarse de medios más insidiosos y peligrosos para la integridad de la intimidad de las personas, por implicar su uso un ataque a la intimidad ajena más contundente y persistente en el tiempo y por reducir las posibilidades de que la víctima se aperciba y reacciones frente al mismo. Precisamente por ello debería preverse una pena superior en estos casos, o al menos así lo creen MORALES PRATS[12] y FERNÁNDEZ TERUELO[13], y nosotros con ellos. Esto no quiere decir que creamos conveniente sustituir la penalidad ahora prevista por otra superior, sino que apostamos por mantener la existente para las conductas del segundo pasaje del artículo 197.1 y por rebajar la correspondiente a la conducta del primero.

2.2 El apartado segundo del artículo 197

El artículo 197.2, donde encontramos tipificado el delito de descubrimiento de secretos informáticos, también mantiene su redacción original, esto es, no ha sufrido ningún cambio desde la aprobación del Código Penal el año 1995, y ello no obstante tratarse de una redacción compleja y confusa. En concreto dice así:

> «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

[12] MORALES PRATS, F., «Delitos contra la intimidad, el Derecho a la propia imagen y la inviolabilidad del domicilio», cit., pp. 454 y 461.

[13] FERNÁNDEZ TERUELO, J. G., *Cibercrimen. Los delitos cometidos a través de internet*, Constitutio Criminalis Carolina, 2007, pp. 133-134.

> ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.»

Hace tiempo que viene criticándose, en primer lugar, la utilización del calificativo «reservado»; en segundo lugar, se alega que una interpretación pegada a la literalidad del precepto nos lleva a entender que el perjudicado o a quien se pretende perjudicar con el apoderamiento, utilización o modificación de datos reservados de carácter personal o familiar registrados en ficheros o soportes informáticos, electrónicos o telemáticos o en cualquier otro tipo de archivo o registro público o privado, debe ser un tercero distinto al titular de dichos datos, mientras que en el caso de que haya acceso no autorizado a los mismos o de que éstos se alteren o utilicen, el perjuicio puede ocasionarse o querer causarse al titular de los datos o a un tercero; y en tercer lugar resulta censurable la selección y determinación de las acciones tipificadas, que aunque son aparentemente distintas en algunos casos pueden superponerse.

En relación con la polémica surgida en torno al uso del calificativo «reservado» la doctrina está dividida. Por una parte están quienes entienden que el recurso al mismo no tiene razón de ser, por cuanto lo interpretan como equivalente a no público y creen, por tanto, que debería integrarse en el ámbito típico cualquier dato personal o de carácter familiar registrado, todos los datos personales o familiares de acceso limitado para terceros ajenos al fichero donde se contienen; y por otra parte encontramos a quienes consideran que recurriendo a dicho calificativo el legislador ha querido referirse a datos que son reflejo de la intimidad más estricta y excluir del ámbito de protección de esta norma todas las acciones de apoderamiento, utilización o modificación que no recaen sobre datos archivados que no tienen un carácter estrictamente reservado. Por la primera opción se decantan Morales Prats[14], Romeo Casabona[15], Rueda Martín[16], Fernández Teruelo[17], Gómez Navajas[18],

---

[14] Morales Prats, F., «Delitos contra la intimidad, el Derecho a la propia imagen y la inviolabilidad del domicilio», cit., pp. 467-468.

[15] Romeo Casabona, C. M., «La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de Internet», cit., pp. 110-111.

[16] Rueda Martín, M. A., *Protección penal de la intimidad personal e informática*, Atelier, Barcelona 2004, p. 71.

[17] Fernández Teruelo, J. G., *Cibercrimen. Los delitos cometidos a través de internet*, cit., pp. 136-138

[18] Gómez Navajas, J., *La protección de los datos personales*, Aranzadi, Cizur Menor (Navarra), 2005, pp. 194-197.

Puente Aba[19], González Rus[20], Carbonell Mateu y González Cussac[21], mientras que a favor de la segunda interpretación, más restrictiva, se han pronunciado Orts Berenguer y Roig Torres[22], Queralt Jiménez[23], Anarte Borrallo y Doval Pais[24], así como también, aunque tímidamente, Tomás-Valiente Lanuza[25]. El Tribunal Supremo finalmente se ha inclinado por la interpretación más amplia, como se pone de manifiesto en las SSTS 1461/2001, de 11 de julio; 666/2006, de 19 de junio; 358/2007, de 30 de abril; 1328/2009, de 30 de diciembre; y 525/2014, de 17 de junio, aunque también existen otras resoluciones donde se avala la segunda interpretación, como por ejemplo la STS 234/1999, de 18 de febrero, en la cual se precisa que «no todos los datos reservados de carácter personal o familiar pueden ser objeto de delito contra la libertad informática» y que sólo pueden serlo «aquellos datos que el hombre medio de nuestra cultura considera 'sensibles' por ser inherentes a su intimidad más estricta, o dicho de otro modo, los datos pertenecientes 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». Y junto a ésta también pueden consultarse otras resoluciones posteriores, como la STS 725/2004, de 11 de junio. Se podría haber aprovechado la ocasión para aclarar en qué está o estaba pensando el legislador al utilizar dicho término, lo cual sería tan fácil como sustituir la expresión «datos reservados de carácter personal o familiar de otro que se hallen registrados» por otra del estilo «datos registrados de carácter personal o familiar que son de acceso limitado para terceros», o directamente prescindiendo del calificativo «reservados», o por

[19] Puente Aba, L. M., «Delitos contra la intimidad y nuevas tecnologías», *Eguzkilore*, núm. 21, 2007, pp. 167-168.

[20] González Rus, J. J., «Delitos contra la intimidad, el Derecho a la propia imagen y la inviolabilidad del domicilio», cit., pp. 314-315.

[21] Carbonell Mateu, J. C.-González Cussac, J. L., «Lección XV: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en Vives Antón. T.-Orts Berenguer, E.-Carbonell Mateu, J. C.-González Cussac, J. L.-Martínez-Buján Pérez, C., *Derecho Penal. Parte especial*, 3.ª edición, Tirant lo Blanch, Valencia, 2010.

[22] Orts Berenguer, E.-Roig Torres, M., *Delitos informáticos y delitos comunes cometidos a través de la informática*, ob. cit., pp. 31-33.

[23] Queralt Jiménez, J. J., *Derecho Penal español. Parte especial*, 6.ª edición, Atelier, Barcelona, 2011, p. 299.

[24] Anarte Borrallo, E.-Doval Pais, A., «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Delitos contra la intimidad y los datos personales», en Boix Reig, J. (Dir.), *Derecho Penal. Parte especial*, vol. I, Iustel, Valencia, 2012, pp. 452-453.

[25] Tomás-Valiente Lanuza, C., «Del descubrimiento y revelación de secretos», cit., pp. 800-801.

remplazar aquella expresión y en su lugar hacer referencia a los «datos de carácter personal o familiar que afecten a su intimidad».

Por lo que se refiere a la persona a la que se debe perjudicar o querer perjudicar, se exige que quien se apodera, utiliza o modifica datos de carácter personal o familiar de otro lo haga en perjuicio de tercero, con lo cual parece que ese tercero ha de ser una persona distinta a la titular de los mismos, por la manera en que está redactada esta primera parte del artículo 197.2 y porque con relación a las demás modalidades delictivas se exige actuar en perjuicio del titular de los datos o de un tercero. Sin embargo, no sólo no tiene sentido que se excluya del concepto de tercero a la persona titular de los datos, sino que incluso hay quien cree que el legislador únicamente debería haberse referido a ésta. Así lo entiende, por ejemplo, MORALES PRATS[26], el cual, no obstante, considera que «en aras a ofrecer una interpretación sistemática del concepto de "tercero", tendente a fijar más taxativamente su contenido, podría entenderse por tal no sólo a la persona física titular de los datos sino también a las personas jurídicas que ostentan (custodian y garantizan) datos reservados de personas físicas». Este autor entiende que «este sería el límite, que se situaría en la aduana conceptual del concepto legal de "tercero" del artículo 197.2 interpretado a la vista del artículo 200 CP». No coincide con la de este autor la opinión de la doctrina mayoritaria, que no limita tanto el concepto de tercero. Parece que lo más correcto es interpretar que bajo la referencia genérica al perjuicio de tercero cabe cualquier persona distinta al sujeto activo, incluido el titular de los datos. En este sentido se han pronunciado, entre otros, ORTS BERENGUER y ROIG TORRES[27], CARBONELL MATEU y GONZÁLEZ CUSSAC[28]. También el Tribunal Supremo se ha mostrado partidario de esta otra interpretación integradora. En tal sentido pueden consultarse las SSTS 1084/2010, de 9 de diciembre; 990/2012, de 18 de octubre; y 525/2014, de 17 de junio. No obstante, no hubiese estado de más dar una nueva redacción al precepto para aclararlo.

Y por lo que respecta a las dificultades que se presentan para distinguir las modalidades de conducta recogidas en los dos incisos del artículo que estamos analizando, es obvio que es así, pues en el

---

[26] MORALES PRATS, F., «Delitos contra la intimidad, el Derecho a la propia imagen y la inviolabilidad del domicilio», cit., pp. 470-471.

[27] ORTS BERENGUER, E.-ROIG TORRES, M., *Delitos informáticos y delitos comunes cometidos a través de la informática*, cit., p. 41.

[28] CARBONELL MATEU, J. C.-GONZÁLEZ CUSSAC, J. L., «Lección XV: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», cit., epígrafe 3.

primero se sanciona el apoderamiento, la utilización o modificación de los datos registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado, mientras que en el segundo se castiga el acceso a los mismos y, de nuevo, su alteración o modificación. Parece ser que estamos ante un error legislativo que tiene origen en una superposición descoordinada de enmiendas sobre el Proyecto de Código Penal de 1994, pero aun así la doctrina se ha esforzado tratando de encontrar alguna diferencia. Se han propuesto distintas soluciones interpretativas pero ninguna ha resultado del todo convincente. La más extendida se centra en el objeto material sobre el que recaen tales conductas, de manera que el de las conductas del primer inciso lo serían los datos reservados de carácter personal o familiar que se encuentran registrados, mientras que cuando en el segundo inciso se habla de «los mismos» seria para referirse no a los datos reservados sino a los ficheros, soportes y archivos en los que éstos están registrados. Así lo entendieron Carbonell Mateu y González Cussac[29], y coincidieron con ellos Castiñeira Palou[30] y también Polaino Navarrete[31]. Éste último llegó a afirmar que de no ser así la alteración y la utilización se estarían tipificando dos veces y nos encontraríamos entonces ante una reiteración superflua de las conductas descritas en la enumeración recogida en el primer inciso. Pero debe tenerse en cuenta que posteriormente, al menos los Catedráticos de Derecho Penal de la Universitat de València y el de la Universidad de Sevilla, han cambiado de parecer. Carbonell Mateu y González Cussac[32] ahora afirman que en ambas partes del artículo el objeto sobre el que han de recaer las diversas modalidades de la conducta es idéntico: datos reservados de carácter personal o familiar ajenos. Y Polaino Navarrete[33], por su parte, también se acoge a esta interpretación, o al menos así se deduce cuando afirma que la descripción separada

[29] *Ibidem,* segunda edición, 2008.

[30] Castiñeira Palou, M. T., «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en Silva Sánchez, J. M., *Lecciones de Derecho Penal. Parte especial*, 3.ª edición, Atelier, Barcelona, 2011, p. 147.

[31] Polaino Navarrete, M., «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (I). Descubrimiento y revelación de secretos», en Cobo Del Rosal, M., *Curso de Derecho Penal español. Parte especial*, Marcial Pons, Madrid, 1996.

[32] Carbonell Mateu, J. C.-González Cussac, J. L., «Lección XV: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», cit., tercera edición, 2010, epígrafe 3.

[33] Polaino Navarrete, M., «Descubrimiento, revelación de secretos e interceptaciones ilegales», en *Lecciones de Derecho Penal. Parte especial*, tomo I, Tecnos, Madrid, 2010, p. 234.

de las conductas de utilizar o modificar y de las acciones utilizar o alterar los datos reservados, «es puramente retórica y denota falta de rigor técnico del legislador penal». Tampoco creen que aquélla sea una lectura asumible y se decantan por entender que el objeto material en los dos incisos son los datos reservados de carácter personal o familiar registrados, entre otros, ORTS BERENGUER y ROIG TORRES[34], QUERALT JIMÉNEZ[35], GONZÁLEZ RUS[36], MORALES PRATS[37], TOMÁS-VALIENTE LANUZA[38] y MATA MARTÍN[39]. Podríamos realizar nuevos intentos de racionalizar el Derecho existente, pero como indica FERNÁNDEZ TERUELO[40], mejor que esto resulta exigir racionalidad al legislador en la elaboración de las leyes penales. No hay excusas para no enmendar este error y ha habido muchas ocasiones para hacerlo.

2.3 El apartado sexto del artículo 197

La aprobación de la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, entre otras cosas exigía a España y a los demás Estados miembros de la Unión Europa que sancionaran como infracción penal el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información, y ello provocó que a través de la reforma operada en 2010 se introdujera esta figura delictiva nueva, cuya ubicación en el artículo 197.3 del Código Penal provocó el desplazamiento de los tipos agravados contenidos en los antiguos apartados tercero, cuarto, quinto y sexto del artículo 197, los cuales ahora han recuperado su ubicación original, fruto de la última reforma de 2015, que lleva a cabo la transposición de la Directiva 2013/40/UE, de 12 de agosto.

---

[34] ORTS BERENGUER, E.-ROIG TORRES, M., *Delitos informáticos y delitos comunes cometidos a través de la informática*, ob. cit., p. 34.

[35] QUERALT JIMÉNEZ, J. J., *Derecho Penal español. Parte especial*, ob. cit., pp. 299-301.

[36] GONZÁLEZ RUS, J. J., «Delitos contra la intimidad, el Derecho a la propia imagen y la inviolabilidad del domicilio», cit., p. 313.

[37] MORALES PRATS, F., «Delitos contra la intimidad, el Derecho a la propia imagen y la inviolabilidad del domicilio», cit., pp. 471-472.

[38] TOMÁS-VALIENTE LANUZA, C., «Del descubrimiento y revelación de secretos», cit., p. 801.

[39] MATA MARTÍN, R. M., *Delincuencia informática y Derecho Penal*, Edisofer, Madrid, 2001, pp. 139-140.

[40] FERNÁNDEZ TERUELO, J. G., *Cibercrimen. Los delitos cometidos a través de internet*, ob. cit., p. 135, nota 206.

Así las cosas, en el apartado tercero volvemos a encontrar un tipo cualificado por razón de la divulgación[41]; en el apartado cuarto se recoge un tipo agravado por razón de la condición del sujeto activo, aunque no únicamente, pues como veremos en este caso el cambio de ubicación no es la única novedad introducida sino que hay otra más significativa[42]; en el apartado quinto ahora se recogen otros tipos agravados que se justifican en la naturaleza de los datos y en la especial vulnerabilidad del sujeto pasivo, aparte de que se incluye otro cambio que después comentaremos[43]; y en el apartado sexto ha quedado ubicada la agravante específica que atiende al fin lucrativo perseguido.

En relación a las modificaciones introducidas en los números cuatro y cinco del artículo 197, ahora sólo avanzaremos que la única que puede considerarse realmente significativa es la que afecta a aquél, pues el retoque producido en el apartado quinto no tiene consecuencias jurídicas. Comentaremos los cambios aquí incorporados por la reforma de 2015 más adelante, ya que lo que ahora interesa es subrayar que se ha dejado pasar la oportunidad para reformar el apartado sexto, tal y como viene reclamando la doctrina especializada desde hace tiempo. En concreto en este precepto se establece lo siguiente:

> «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.»

---

[41] Para ser exactos aquí se indica lo siguiente: «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».

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

[43] Después de algún retoque sin consecuencias jurídicas ha quedado redactado como sigue:«Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior».

Y así como no se considera excesiva la penalidad prevista en los demás casos, dado el mayor contenido de injusto que entraña el poner en conocimiento de la información reservada a un mayor número de personas, el violar los aspectos más reservados de la persona y la situación de especial vulnerabilidad en que se encuentran los menores y las personas con discapacidad, una parte importante de la doctrina no cree fundamentada la agravación de pena en los supuestos en los que existe un fin lucrativo. A pesar de que, como apunta Queralt Jiménez[44], la intimidad en ocasiones es una mercancía y se convierte en objeto de transacciones y del consiguiente lucro, debe tenerse en cuenta que no se exige habitualidad o reiteración, esto es, que el sujeto activo se dedique a ello. Creemos que sólo entonces la ofensa a la intimidad se vería incrementada, pues siendo de esta manera también sería mayor el peligro para el objeto tutelado. Así lo critican Orts Berenguer y Roig Torres[45], así como también Morales Prats[46]. Éste último además de criticar que el legislador haya teñido de coloración patrimonialista la tutela de un bien jurídico estrictamente personal como es la intimidad y de subrayar que en todo caso se debería haber aludido a la existencia de una estructura organizativa profesional dedicada al «tráfico de intimidades», apunta la difícil practicabilidad de este tipo agravado, por los problemas probatorios que suscita la concurrencia de los elementos subjetivos del injusto.

3. Preceptos que se han visto afectados por la reforma

3.1 El apartado cuarto del artículo 197

Tras la reforma de 2015 el artículo 197.4 ha quedado redactado como sigue:

> «Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:
>
> a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o

[44] Queralt Jiménez, J. J., *Derecho Penal español. Parte especial*, ob. cit., p. 310.

[45] Orts Berenguer, E.-Roig Torres, M., *Delitos informáticos y delitos comunes cometidos a través de la informática*, ob. cit., p. 45.

[46] Morales Prats, F., «Delitos contra la intimidad, el Derecho a la propia imagen y la inviolabilidad del domicilio», cit., p. 478.

b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.

Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.»

Este precepto en 2010 se había desplazado al apartado quinto del artículo 197, pero con la reforma de 2015 vuelve a estar ubicado en el apartado cuarto, aunque mucho más importante que esto es el hecho de que ahora aparecen recogidos dos tipos cualificados.

Por una parte se mantiene el tipo agravado que atiende a la especial condición del sujeto activo de los hechos descritos en los apartados 1 y 2, que debe serlo el encargado de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, cuyo fundamento radica en que éste, además de tener mayores posibilidades de comisión del delito y de hacerlo de manera sofisticada e inadvertida para las víctimas, en caso de cometerlo estaría a su vez incumpliendo sus deberes de lealtad, rectitud y de sigilo en el desempeño del cargo, a lo cual podría añadirse que también subyace un incremento del desvalor de resultado. En estos casos todavía se prevé imponer en su mitad superior las penas de prisión de uno a cuatro años y de multa de doce a veinticuatro meses establecidas en los apartados primero y segundo del artículo 197, esto es, castigar al encargado de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros que realice las conductas típicas aquí previstas con unas penas de prisión de dos años y seis meses a cuatro años y de multa de dieciocho a veinticuatro meses. No ha habido, por tanto, aparte del referido a su ubicación, ningún cambio en relación con este tipo agravado, ni penológico ni de otra clase, y ello a pesar de que quizá sí hubiese sido conveniente aprovechar la ocasión para hacerlo. Téngase en cuenta que, tal y como han criticado Orts Berenguer y Roig Torres[47], conforme está redactado el precepto parece que se exige una acción positiva y que con ello se imposibilita su aplicación en caso de que dicho sujeto se haya limitado a tolerar la vulneración por parte de terceros de los datos que se encuentran bajo su guarda.

Y por otra parte, en relación con el nuevo tipo agravado que se recoge en este artículo 197.4, importa anotar que fue propuesto por la Comisión de Justicia del Congreso de los Diputados. Su inclusión no estaba prevista inicialmente en el Proyecto de Reforma del Código Penal ni tampoco había sido solicitada por la doctrina, pero a

[47] Orts Berenguer, E.-Roig Torres, M., *Delitos informáticos y delitos comunes cometidos a través de la informática,* ob. cit., pp. 42-43.

pesar de ello el legislador finalmente ha considerado que es merecedor de una pena mayor quien para cometer las conductas de los artículos 197.1 y 2 haga uso, sin estar autorizado, de datos personales de la víctima. Por poner un ejemplo, a partir de ahora no merece la misma pena el apoderamiento de un correo electrónico que contiene elementos vinculados con la intimidad de su destinatario y titular, realizado con la intención de descubrir sus secretos o vulnerar su intimidad, cuando éste lo ha descargado y guardado en una carpeta de su ordenador y el sujeto activo para apoderarse de él lo que hace es acceder sin permiso al ordenador personal de la víctima después de averiguar su clave y buscar entre los documentos allí guardados (siempre y cuando dicha clave no coincida con el nombre y/o apellido de su titular, o con su número de DNI u otros datos personales), que el apoderamiento de ese mismo correo electrónico en caso de que para ello tenga que accederse a la cuenta de correo electrónico del sujeto pasivo, porque ello implica no sólo tener que averiguar su contraseña sino también hacerse con su correo electrónico y usarlo sin autorización, pues aquí sí habría una utilización no autorizada de datos personales, en tanto que el correo electrónico de una persona tiene esta consideración. Efectivamente, éste constituye una información que le concierne, que le afecta, y que forma parte del ámbito de su privacidad protegido por la Ley de Protección de Datos, siéndole plenamente aplicable su régimen jurídico, sin importar que la denominación de la dirección se corresponda o no con el nombre y apellido de su titular, país o empresa en la que trabaja, porque con independencia de ello se puede, mediante una operación nada difícil, identificar perfectamente a una persona física. Así ha sido reconocido por la Sala de lo Contencioso Administrativo de la Audiencia Nacional. Pueden consultarse las SSAN de 23 de marzo de 2006, de 25 de mayo de 2006 y de 15 de enero de 2011. Ésta última resolución además ha sido confirmada por el Tribunal Supremo, en STS 634/2014, de 3 de octubre.

Puede ser que se haya decidido incorporar este tipo agravado porque en el artículo 9.5 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013, relativa a los ataques contra los sistemas informáticos, se les exige a los Estados miembros que tomen medidas para garantizar que se pueda considerar una circunstancia agravante, a menos que la misma esté contemplada en otra infracción que sea sancionable con arreglo al Derecho nacional, el cometer las infracciones a que se refieren los artículos 4 y 5 de la citada Directiva, esto es, las referentes a la interferencia ilegal en los sistemas de información y en los datos que causan un daño o deterioro en los mismos, utilizando ilícitamente datos de carácter per-

sonal de otra persona con la finalidad de ganarse la confianza de un tercero, causando así daños al propietario legítimo de la identidad. Pero lo cierto es que así como sí tiene sentido la introducción de esta agravante en el delito de daños informáticos, no lo tiene en relación a los delitos contra la intimidad, ya que no se corresponde con las exigencias de la Directiva. Creemos que más bien el distinto trato punitivo se explica en que se produce una suplantación de la personalidad y que el sujeto activo se vale de la confianza que con dicha suplantación genera en un tercero. En cualquier caso, no estamos de acuerdo con COLÁS TURÉGANO[48] cuando afirma que esta figura guarde relación con el delito de usurpación del estado civil, y además de ello nos parece excesivo que el castigo sea exactamente el mismo para este tipo que para el otro recogido en la letra a) del artículo 197.4.

Por último, decir cabe que estos tipos agravados son objeto a su vez de agravación penal. Continúa previsto incrementar la pena agravada si los datos reservados se difunden, ceden o revelan, sólo que ahora esto resulta extensible al supuesto en que se ha obrado utilizando los datos personales de la víctima sin su autorización. Si así sucede, si las personas que han hecho uso de dichos datos personales o los encargados de los ficheros, soportes, archivos o registros difunden, ceden o revelan los datos reservados descubiertos a terceros la pena a imponer, en ambos casos, será de prisión de tres a cinco años. Esta agravación se corresponde con la figura agravada que para los tipos básicos se establece en el artículo 197.3; en lo único en que difiere es en la pena a imponer.

3.2 El apartado quinto del artículo 197

En este apartado quinto del artículo 197 se establece lo siguiente:

> «Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.»

Encontramos aquí dos tipos agravados que atienden uno a la naturaleza de los datos y el otro a la condición del sujeto pasivo. Su

[48] COLÁS TURÉGANO, A., «Nuevas conductas delictivas contra la intimidad (arts. 197; 197 bis; 197 ter)», en GONZÁLEZ CUSSAC, J. L., en Comentarios a la Reforma del Código Penal de 2015, segunda edición, Tirant lo Blanch, Valencia, 2015, p. 673

ubicación es nueva, pues hasta ahora los dos figuraban en el apartado sexto, y también es nueva la referencia que se hace a la persona con discapacidad necesitada de especial protección.

Por lo que se refiere a este segundo retoque, si nos detenemos a leer este precepto comprobaremos que ya no se hace referencia al sujeto pasivo menor o incapaz, o mejor, que ya no se habla de incapaz sino de persona con discapacidad necesitada de especial protección. Ello se debe a la voluntad del legislador de evitar el recurso a una terminología ya superada en nuestro ordenamiento jurídico, en concreto desde la aprobación de la Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad. En cualquier caso, éste es un cambio que más allá de demostrar mayor respeto con aquel colectivo, no pasa de ser una simple modificación léxica que no acarrea consecuencias jurídicas[49].

3.3 El apartado séptimo del artículo 197

Del desarrollo creciente de las nuevas tecnologías y de Internet se derivan peligros para los derechos fundamentales, y en particular para el derecho a la intimidad. Piénsese que hoy en día es difícil encontrar a alguna persona que no tenga un teléfono móvil que lleve instalada una cámara digital y que cuente con acceso ilimitado a Internet, con lo cual resulta muy fácil no sólo captar y grabar imágenes sino también difundirlas y hacerlas públicas. Hasta ahora se castigaba la divulgación no consentida de fotografías y videos de otra persona que comprometían su intimidad en los supuestos en los que se obtenían sin su consentimiento, pero en principio quedaban sin respuesta los casos en los que sí existía consentimiento, o al menos no recibían la respuesta más adecuada. Lo que venía pasando es que los operadores jurídicos, en ocasiones, en un intento de encontrar vías de punibilidad para evitar que estas conductas quedasen impunes, condenaban por un delito de injurias con publicidad. Pero lo cierto es que, teniendo en cuenta que además del honor también se lesiona la intimidad, se considera afortunada la introducción en el Capítulo primero del Título X del Libro II del nuevo delito consistente en

[49] Para más información vid. Martínez Garay, L., «Un interesante comentario del concepto penal de discapacidad y de persona con discapacidad necesitada de especial protección», en González Cussac, , J. L. (Dir.) Comentarios a la Reforma del Código Penal de 2015, segunda edición, Tirant lo Blanch, Valencia, 2015, pp. 125 y ss.

difundir, revelar o ceder a terceros, sin autorización de la persona afectada, imágenes o grabaciones audiovisuales realizadas con su anuencia cuando la divulgación menoscabe gravemente su intimidad personal. Normalmente se actúa así por venganza y las imágenes o grabaciones audiovisuales difundidas suelen ser de contenido sexual, por ello que dicha conducta recibe el nombre de *revenge porn*.

En concreto, en el párrafo primero de este artículo 197.7 se establece lo siguiente:

> «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.»

Tal y como han apuntado JUANATEY DORADO y DOVAL PAÍS, es preciso:

> «establecer una distinción entre consentir la realización de una grabación para uso privado de dos personas y consentir su realización para difundirla, puesto que es manifiesto que hay un aspecto importante de la intimidad para el que no hay consentimiento[50].»

Importa apuntar, por otra parte, que a partir de la Sentencia del Tribunal Constitucional 134/1999, de 15 de julio, la intimidad pasó a ser concebida como un bien jurídico relacionado con la libertad de acción de la persona, con las facultades positivas de actuación de ésta para controlar la información relativa a su persona y su familia en el ámbito público, pudiendo imponer a terceros su voluntad de no dar a conocer dicha información, prohibiendo su difusión no consentida. En este mismo sentido puede consultarse el Auto del Tribunal Supremo de 7 de noviembre de 2014.

No estamos de acuerdo con MORALES PRATS[51] cuando afirma que este tipo penal «no describe una conducta con la suficiente lesividad desde el punto de vista jurídico-penal». Aunque es criticable que el tipo no limite las conductas a aquéllas que afecten al núcleo duro de la intimidad, una interpretación respetuosa con el principio de

---

[50] JUANATEY DORADO, C.-DOVAL PAÍS, A., «Límites de la protección penal de la intimidad frente a la grabación de conversaciones o imágenes», en BOIX REIG, J. (Dir.), *La protección jurídica de la intimidad*, Iustel, Madrid, 2010, p. 163.

[51] MORALES PRATS, F., «Delitos contra la intimidad: Arts. 197.4 bis y 203.2-3», en ÁLVAREZ GARCÍA, F. J. (Dir.), *Estudio crítico sobre el anteproyecto de reforma penal de 2012*, Tirant lo Blanch, Valencia, 2013, p. 714.

intervención mínima debería circunscribir las conductas punibles a aquellas que difunden imágenes sensibles, tal y como apunta Colás Turégano[52] y como se viene haciendo con el tipo básico de descubrimiento y revelación de secretos del artículo 197.1 en relación con la captación de imágenes, la cual tendrá trascendencia penal únicamente si dichas imágenes son sensibles y siempre y cuando se haya realizado en lugares cerrados y privados.

Téngase en cuenta, asimismo, que se exige para poder hablar de conducta delictiva que las imágenes o grabaciones audiovisuales hayan sido obtenidas en un domicilio o en un lugar excluido del alcance de la mirada de terceros, precisión que nos parece afortunada, sobre todo teniendo en cuenta que el principal problema que plantea la captación de imágenes no consentidas es el de la delimitación de los campos de acción civil y penal[53]. El propio Consejo General del Poder Judicial subrayó que dicha precisión resulta lógica y ajustada a la Ley Orgánica 1/1982. Sin embargo, hubiese resultado más adecuado hablar de lugares cerrados y privados, en contraposición con los lugares abiertos al público a los que se refiere la citada Ley Orgánica para justificar la captación y reproducción de la imagen de personas públicas, además de que se trata de una terminología que goza de una amplia interpretación jurisprudencial, lo cual facilitaría la seguridad jurídica en la aplicación del tipo penal. Así lo apunta, con razón, Martínez Otero[54].

Y tomando en consideración lo dicho hasta ahora, no sólo no estamos de acuerdo con Morales Prats sino que además lamentamos que se hayan rechazado las enmiendas del Grupo Parlamentario Entesa pel Progrés de Catalunya y del Grupo Parlamentario Socialista para incluir de manera expresa una referencia a las imágenes y grabaciones realizadas directamente por la persona afectada, pues sin la misma el precepto queda configurado como un delito especial de propia mano, esto es, que sólo puede ser cometido por aquél que ha obtenido las imágenes o grabaciones audiovisuales con el consentimiento de la víctima. No nos cabe la menor duda de que se inten-

---

[52] Colás Turégano, A., «Nuevas conductas delictivas contra la intimidad (arts. 197; 197 bis; 197 ter)», cit., p. 668.

[53] Resulta de aplicación la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen a los casos en que dicha captación se produce en lugares abiertos al público, mientras que quedará reservada la aplicación del precepto que nos ocupa a aquellos supuestos en los que las imágenes se obtienen en lugares cerrados y privados.

[54] Martínez Otero, J. M., «La difusión de sexting sin consentimiento del protagonista: un análisis jurídico», *Derecom*, 12:1, 2013, p. 10.

tará interpretar este precepto de manera tal que sea posible incluir aquellos otros casos, pero la definición que nos da la Real Academia de la Lengua Española del término «anuencia» no da pie a otra lectura distinta a la indicada. Anuencia equivale a consentimiento y es la acción y efecto de consentir, y consentir significa permitir algo o condescender en que se haga.

Se ha renunciado con ello a cubrir una necesidad político-criminal de primera magnitud y no tiene sentido afirmar que es la naturaleza voluntaria de la toma y envío de las fotografías y grabaciones lo que hace imposible la protección penal a través de la figura del descubrimiento y revelación de secretos en la medida en que la intimidad constituye un bien jurídico disponible, porque ello no ha impedido la tipificación como delito de la difusión, revelación o cesión a terceros de imágenes o grabaciones audiovisuales de otra persona realizadas con su consentimiento. Es la falta de autorización para actuar de esta manera, esto es, para difundir, revelar o ceder ese material, lo que se tiene en cuenta en este caso y lo que debería tenerse en cuenta en aquél otro, y si en uno puede entenderse que cuando se emite el consentimiento para ser fotografiado o grabado está presente una expectativa de intimidad, en el otro puede afirmarse que esta misma expectativa existe cuando las fotografías o los videos realizador por uno mismo son enviados a otra persona. Así lo entiende también LLORIA GARCÍA[55].

Volviendo a la modalidad típica sí introducida, parece acertada la pena de prisión de tres meses a un año o de multa de seis a doce meses que lleva aparejada este nuevo delito. Se trata de una pena menor a la que se impone en caso de que las imágenes y sonidos se obtienen sin el consentimiento de la personas afectada porque la conducta es menos reprochable. Puede decirse que se cumplen las exigencias de proporcionalidad. Además, la pena a imponer resulta superior a la que hasta ahora venían imponiendo los tribunales en caso de que se decantasen por condenar por la vía de los delitos de injurias, lo cual también resulta correcto, pues además de verse comprometido el honor —aunque sólo sea tangencialmente— también se produce una injerencia directa a la intimidad y a la propia imagen.

La pena será superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida al sujeto pasivo por análoga relación de afectividad, aun sin convivencia, tal y como pedía que se hiciese el Consejo General del Poder Judicial

[55] LLORIA GARCÍA, P., «La difusión inconsentida de imágenes íntimas (sexting) en el proyecto de Código Penal de 2013», *El Derecho*, 2013.

y tal y como está previsto en el párrafo segundo del artículo 197.7. Esta agravación responde, en términos de injusto, a las mayores posibilidades de comisión del delito por parte de aquellos sujetos, por lo fácil que les resulta o les puede resultar acceder a fotografías y videos íntimos de quien es o ha sido su pareja y que han sido realizados en común. No puede pasarse por alto, además, que la tipificada es una conducta que se desata cada vez con mayor frecuencia en el seno de rupturas sentimentales abruptas, las cuales crean un terreno propicio para traicionar la expectativa de intimidad de la otra parte, con lo cual razones de prevención general también pueden haberse tenido en cuenta a la hora de incluir este tipo agravado. Conviene subrayar, igualmente, que la llamada intimidad compartida no se considera por la jurisprudencia causa de justificación. Pueden consultarse, entre muchas otras, las SSTS 1219/2004, de 10 de diciembre, y 569/2013, de 26 de junio. Sin embargo, puede criticarse que, como indica Colás Turégano[56], en la práctica este supuesto agravado se aplicará con mayor frecuencia que el básico, pues difícilmente la captación de las imágenes sensibles se da entre personas que no han mantenido una relación afectiva, aunque sea de corta duración.

Junto al anterior encontramos otros supuestos agravados, también en el segundo párrafo del artículo que estamos analizando. Uno responde a la condición desvalida y vulnerable de la víctima y el otro atiende a la concurrencia de una finalidad lucrativa en el sujeto activo. En concreto el citado párrafo dispone lo siguiente:

> «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.»

Pero así como la agravación de pena en el primer caso viene avalada por la doctrina, que subraya la necesidad de redoblar la tutela de la intimidad de esos sujetos frente a los medios de control e instrumentalización existentes, no sucede lo mismo en el segundo. Este tipo agravado no tiene fundamento político-criminal a menos que exista habitualidad, que el sujeto activo en cierta medida se dedique al tráfico de material íntimo de otras personas, tal y como hemos indicado al comentar el artículo 197.6.

---

[56] Colás Turégano, A., «Nuevas conductas delictivas contra la intimidad (arts. 197; 197 bis; 197 ter)», cit., p. 670.

3.4 El artículo 197 bis

La reforma de 2015 ha añadido un nuevo artículo 197 bis, con la siguiente redacción:

> «1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.
>
> 2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.»

Como puede comprobarse, este artículo 197 bis está formado por dos apartados, y en el primero se recoge lo que desde la reforma operada en 2010 constaba en el artículo 197.3, pretendiéndose con ello que el artículo 197 quede reservado para los supuestos de revelación de datos que afectan directamente a la intimidad personal e introducir una separación entre éstos y aquellos otros casos en los que se accede a datos o informaciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal. El legislador ha tenido en cuenta, por tanto, lo muy criticada que fue la anterior ubicación de la intromisión informática o *hacking*, pero dichas críticas todavía tienen sentido y las tendrán a menos que finalmente se opte por desterrar esta figura delictiva del Capítulo primero del Título X del Libro II, aunque para que así se haga, si es que algún día se hace, deberemos esperar a que vuelva a reformarse el Código Penal.

Son diversos los autores, como Carrasco Andrino[57] o Tomás-Valiente Lanuza[58], los que, partiendo de que el bien jurídico de este delito debe buscarse en el ámbito de la seguridad de las redes y de los sistemas informáticos, de que lo que se trata de preservar es la seguridad en el tráfico informático y, en particular, la integridad y confidencialidad de los datos y programas informáticos como

[57] Carrasco Andrino, M. M., «El delito de acceso ilícito a los sistemas informáticos», en Álvarez García, F. J.-González Cussac, J. L., *Comentarios a la reforma penal de 2010*, Tirant lo Blanch, Valencia, 2010, p. 249.

[58] Tomás-Valiente Lanuza, C., «Del descubrimiento y revelación de secretos», cit., pp. 802-803.

elementos de los sistemas informáticos, han criticado, con razón, que la ubicación entre los delitos contra la intimidad de la intromisión informática resulta desafortunada, pues una interpretación en clave de intimidad personal plantea problemas respecto de la delimitación de alguno de sus elementos típicos, como los datos o programas referidos, cuya vinculación con aquélla es nula. Tampoco Morales Prats[59] ha dudado en calificar de grave error sistemático la introducción de este delito en el seno de los delitos contra la intimidad, y ello a pesar de estar de acuerdo con Muñoz Conde[60], en que dentro de la seguridad de los datos y sistemas informáticos, que sería la que se pretende proteger directamente, también se protegen la intimidad y los datos, secretos o no, que pueden encontrarse dentro del sistema.

La incorporación de este delito nuevo en el Código Penal se debe a la ratificación por España de la Decisión Marco 205/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, en la cual, sin embargo, únicamente se exigía sancionar como infracción penal el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información. No se pedía castigar penalmente a quien vulnerando las medidas de seguridad establecidas para impedirlo se mantuviera dentro del sistema informático en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, pero el legislador español quiso hacerlo, a pesar de ello y de que un mantenimiento en el sistema con vulneración de las medidas de seguridad constituye ya en sí mismo un acceso ilícito. Así lo hizo en 2010, y aunque hubiese podido eliminar la referencia al mantenimiento en esta última reforma de 2015, no ha sido así. Creemos que esta segunda modalidad delictiva sólo tiene razón de ser en caso de que no se exija vulnerar las medidas de seguridad, pero siendo así no se entiende que la pena a imponer en ambos casos sea la misma, consistente en una prisión de seis meses a dos años. Por razones de proporcionalidad las dos conductas merecerían un trato punitivo distinto, más grave para aquélla otra.

Como novedad, se tipifica la facilitación del acceso a datos o programas informáticos contenidos en un sistema informático o en parte del mismo vulnerando para ello las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado. Al respecto quisiéramos comentar un par de cosas: la primera, que ha

---

[59] Morales Prats, F., «Delitos contra la intimidad, el Derecho a la propia imagen y la inviolabilidad del domicilio», cit., pp. 481-483.

[60] Muñoz Conde, F., *Derecho Penal. Parte especial*, Tirant lo Blanch, 19.ª edición, Valencia, 2013, cit., p. 261.

sido la rectificación del convenio sobre Cibercriminalidad lo que ha obligado a la incriminación no sólo del delito de intrusismo informático, sino también de las conductas a las que ahora nos referiremos, tal y como ya se hacía en otras figuras delictivas, entre las cuales encontramos la estafa informática (artículo 248.2), los delitos contra la propiedad intelectual (artículo 270.3) o los delitos contra los servicios de radiodifusión e interactivos (artículo 286); en segundo lugar, que con ello no se viene a cubrir una laguna de impunidad existente, porque hasta ahora el facilitador debía responder bajo el paraguas de alguna de las formas de participación previstas legalmente en los artículos 28 y 29 del Código Penal, sino que se amplia el ámbito de lo punible elevándose su contribución a la categoría de autoría; y en tercer lugar, que puede facilitarse el acceso proporcionando un programa informático específicamente concebido para ello o 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, y si así sucede debemos plantearnos si aplicaremos el artículo 197 bis o el 197 ter. A nuestro entender, en caso de que se haya propiciado la comisión del delito por parte de otro, esto es, de que este otro haya conseguido acceder sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo, entonces aplicaríamos el artículo 197 bis, pues los previstos en aquel otro artículo son actos meramente preparatorios o todo lo más de tentativa, lo cual explicaría por qué en el apartado primero del artículo 197 bis se prevé imponer una pena de prisión de seis meses a dos años, mientras que si la condena lo es por el artículo 197 ter el juez o tribunal podrá optar entre imponer una pena de prisión de seis meses a dos años o una multa de tres a dieciocho meses.

Por otra parte, pasando ya a comentar el apartado segundo, nos encontramos con otra modalidad delictiva nueva, que lleva aparejada una pena de prisión de tres meses a dos años o una multa de tres a doce meses. Se amenaza con imponer una de estas penas a quien intercepte mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, 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. La incorporación de este tipo en el Código Penal es consecuencia de la ratificación por España del Convenio sobre Cibercriminalidad o Convenio de Budapest, de 23 de noviembre de 2001, donde sin embargo aparece clasificado entre los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, y no como delito contra la intimidad, con lo cual serían

extensibles a este caso las críticas que una parte de la doctrina ha realizado a la ubicación de la intromisión informática entre los delitos que tutelan la intimidad, además de que no en todos los supuestos subsumibles en este apartado segundo serviría la justificación dada por MUÑOZ CONDE.

También con relación a la conducta contemplada en este segundo apartado cabe decir que no puede ser confundida con la prevista en el artículo 197.1, pues entre ambas existen algunas diferencias, siendo la primera que en este caso no se exige actuar para descubrir secretos o vulnerar la intimidad de otro, con lo cual, y por poner un ejemplo, ya no quedaría impune la interceptación de una comunicación a través de Skype en los casos en los que la finalidad perseguida fuese otra diferente. Importa subrayar, asimismo, que en el artículo 197.1 lo que se castiga es interceptar las telecomunicaciones del titular de la intimidad vulnerada mientras que el objeto de intercepción aquí lo son las trasmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, siendo ésta otra diferencia entre ambas conductas típicas, aunque no un obstáculo a aplicar el artículo que estamos analizando en el caso puesto de ejemplo, pues las llamadas a través de Internet tienen tal consideración. La tercera diferencia es que no se habla de obrar sin el consentimiento del titular de los datos informáticos sino de hacerlo sin estar debidamente autorizado, expresión que nos parece más acertada porque, aunque no suceda en el caso del ejemplo, habrán otros en los que el acceso a esos datos requerirá someterse a un severo régimen de autorizaciones, no siendo posible acceder a ellos acudiendo directamente a su titular, ya sea persona física o jurídica, para que dé su consentimiento.

No es el expuesto el único supuesto en el que sería de aplicación este apartado segundo del Código Penal. Teniendo en cuenta que se indica de manera expresa que también se castiga la intercepción de emisiones electromagnéticas de los datos informáticos referidos, igualmente tendría cabida aquí el ataque conocido como interferencia de Van Eck, que consiste en espiar la imagen emitida en una pantalla LCG o CTR de ordenador detectando las emisiones electromagnéticas del monitor y su cableado con el fin de acceder a la información protegida de empresas y organismos nacionales. Otro ataque que caería dentro del paraguas de este precepto es el conocido como Air Hopper, al que se recurre con el mismo propósito y consiste en acercar un dispositivo a una red aislada del exterior y utilizarlo para captar las señales electromagnéticas de los equipos que la componen y enviar al exterior la información que se encuentra confinada en una red aislada de Internet. Y también le sería de

aplicación este precepto a quien, sin estar autorizado, accediera e hiciera uso del sistema de espionaje militar denominado «Programa Santiago», puesto en marcha para captar emisiones electromagnéticas y de imágenes en zonas que tienen un interés estratégico para la seguridad nacional, lo cual se consigue con la ayuda de una red de sensores capaces de proporcionar una cobertura óptima del espacio estratégico de interés nacional. En este caso, si el sujeto activo es un militar funcionario público deberíamos plantearnos si resultaría de aplicación el artículo 198 y procedería imponer la pena prevista en el artículo que estamos analizando en su mitad superior y, además, una de inhabilitación absoluta por tiempo de seis a doce años. Por otra parte, en caso de resultar afectada la seguridad nacional también debería tenerse en cuenta lo dispuesto en los artículos 583 y siguientes.

3.5 El artículo 197 ter

Encontramos aquí un adelanto de la intervención penal a conductas meramente preparatorias del ataque a la intimidad, o todo lo más estaríamos ante conductas de tentativa. Se advierte lo siguiente:

> «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.»

No es suficiente con la producción, adquisición, importación o facilitación a terceros del objeto material sino que se requiere hacerlo sin autorización, con lo cual ésta se configura como el eje sobre el que se vertebra el marco de licitud de la acción correspondiente, esto es, su ausencia convierte en ilícita la conducta. Siendo como es la autorización un elemento objetivo del tipo penal, el error sobre su concurrencia se tratará conforme a las reglas del error del tipo, y como no está previsto en el Código Penal sancionar la actuación

imprudente, el error siempre resultará impune, tanto si es invencible como si es vencible.

Además, y por otra parte, también debe dejarse claro que no importa que los programas aludidos puedan cumplir otras funciones distintas, pero se requiere que estén concebidos o adaptados principalmente para cometer alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis. Aparte de que dicha intención o elemento subjetivo del tipo debe probarse, de que no puede presumirse sin más —pues ello atentaría contra la presunción de inocencia—, no se cometerá ningún delito si se han producido, adquirido, importado o facilitado a otros con una finalidad distinta a la de facilitar la comisión de alguno de estos delitos.

Y a lo dicho hasta ahora todavía queda por añadir que a estos actos preparatorios elevados a la categoría de figura autónoma se les asigna una penalidad independiente, significativamente menor a la que corresponde imponer por la comisión de alguno de los delitos de los apartados 1 y 2 del artículo 197 y también, aunque no tanto, a la que se impondría en caso de que se condene por el artículo 197 bis. En concreto en el artículo 197 ter se permite al juez o tribunal elegir entre la imposición de una pena de prisión de seis meses a dos años o recurrir a una pena de multa de tres a dieciocho meses. Siendo así se cumplen las exigencias de proporcionalidad; no puede decirse que se pongan al mismo nivel la autoría directa y los actos preparatorios.

Téngase en cuenta, ya por último, que si partimos de entender que estamos ante delitos de peligro abstracto podríamos plantear la posibilidad de un concurso de delitos en caso de que, por ejemplo, un mismo sujeto primero produzca alguno de los medios comisivos citados y después decida no conformarse con programar la herramienta y cometa alguno de aquellos delitos.

3.6 El artículo 197 quáter

De acuerdo con lo exigido en la Decisión Marco 2005/222/JAI, en 2010 se incluyó en el Código Penal una nueva agravación de pena para el caso de que los hechos delictivos se cometieran en el seno de una organización o grupo criminal, lo cual debe entenderse en el sentido de que procede su aplicación cuando tales delitos se realicen

por quienes pertenecen a una organización o grupo criminal. Esta agravación figuraba en el artículo 197.8 y ahora en el artículo 197 quáter, en el cual se indica lo que sigue:

> «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.»

Pero no es el cambio de ubicación la única novedad introducida. A pesar de que este tipo agravado tiene fundamento, pues se detecta una mayor insidiosidad y ofensividad en la conducta típica, por ser cometida en un contexto criminal organizado, el legislador se excedió en 2010 al establecer su ámbito de aplicación y lo ha vuelto a hacer en 2015 con una ampliación del mismo. Si entonces se quiso que fuese aplicable a todos los hechos tipificados en los diferentes apartados del artículo 197, y no sólo a los que en aquel momento se encontraban recogidos en el apartado tercero, tal y como se pedía en la Decisión Marco, ahora se ha querido ir más allá y la aplicación de la agravación se extiende a todas las figuras delictivas del Capítulo primero del Título X del Libro II. Esto es, se prevé imponer una pena superior cuando los hechos previstos en los diferentes apartados de los artículos 197, 197 bis, 197 ter, 198, 199 y 200 se cometan en el seno de una organización o grupo criminal. Concretamente se prevé aplicar respectivamente las penas superiores en grado.

3.7 El artículo 197 quinquies

Fue también la necesidad de dar cumplimiento a las obligaciones contraídas por España en el ámbito de la armonización jurídica europea lo que explica que se pidiera responsabilidad a las personas jurídicas, en concreto así lo exigía la Decisión Marco 2005/222/JAI. Ello parece acertado si se tiene en cuenta el perfil criminológico que en ocasiones presentan los autores de intrusiones en los sistemas informáticos, pero no tenía por qué tratarse de una responsabilidad de naturaleza penal, pues en dicha Decisión Marco no se exige que así sea. A pesar de ello el legislador español en 2010 decidió introducir una cláusula específica de responsabilidad penal de las personas jurídicas en el mismo artículo en el que se tipificó el acceso —y el mantenimiento— sin autorización y vulnerando las medidas de seguridad al conjunto o a una parte de un sistema de información, donde se dispone que en caso de que de acuerdo con lo establecido en el artículo 31 bis —que constituye otra de las novedades incorporadas aquel año en el Código Penal— aquéllas

resultasen responsables, se tendrían que enfrentar a un conjunto de sanciones que, aparte de que pueden no ser adecuadas para los delitos a los que nos estamos refiriendo, resultan desproporcionadas. Téngase en cuenta que además de preverse imponer una pena de multa de seis meses a dos años, se facultó a los jueces y tribunales para que, atendidas las reglas establecidas en el artículo 66 bis —también nuevo—, pudiesen imponer las penas recogidas en las legras b) a g) del apartado 7 del artículo 33. Es más, no sólo se les exigió responsabilidad en caso de que de acuerdo con lo establecido en el artículo 31 bis resultasen responsables del delito entonces recogido en el artículo 197.3 —y ahora en el artículo 197 bis— sino para el caso de que lo fueran de cualquiera de los delitos comprendidos en los diferentes apartados del artículo 197. Esto causó perplejidad en muchos penalistas, los cuales también hemos recibido con asombro la actual extensión de la responsabilidad penal de las personas jurídicas a otros delitos.

Se ha aprovechado esta última reforma de 2015 para introducir cambios que afectan a esta cláusula específica de responsabilidad penal de las personas jurídicas, pero no los esperados. Además de que se ha cambiado su ubicación, pues ahora la encontramos en el artículo 197 quinquies, se prevé la imposición del mismo conjunto de penas que antes a las que resulten ser responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, incluidas las nuevas figuras delictivas recogidas en los mismos. Para ser exactos en el precepto analizado se dispone lo siguiente:

> «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.»

Importa tener en cuenta, además de todo lo dicho hasta ahora y de que la actual regulación de la responsabilidad penal de las personas jurídicas está contenida en cuatro preceptos sucesivos (los artículos 31 bis, 31 ter, 31 quáter y 31 quinquies), que en el actual artículo 31 bis encontramos nuevos criterios de transferencia, que se han introducido cambios en relación a los sujetos responsables, esto es, a las personas físicas idóneas para provocar la contaminación penal de una sociedad, y que también es nueva la noción del «debido control» de la que se parte.

4. Observaciones finales

No creemos necesario enumerar una a una las reformas introducidas en el Capítulo primero del Título X del Libro II del Código Penal, ni tampoco hacer un listado de los aspectos criticables de las mismas, pues a todo ello nos acabamos de referir en páginas anteriores. Sin embargo, sí queremos insistir en que el legislador ha desaprovechado la ocasión para realizar ciertos cambios que venía pidiendo la doctrina especializada, y ello no obstante haber pasado mucho tiempo desde la entrada del Anteproyecto de 2012 en el Congreso de los Diputados y su conversión en Proyecto hasta la aprobación del mismo, esto es, a pesar de haber tenido tiempo más que suficiente para recapacitar sobre los retoques que convenía realizar, sobre las mejoras a incorporar en el Código Penal. Así, por ejemplo, se ha dejado pasar la oportunidad de introducir determinadas modificaciones léxicas y de dar una redacción menos compleja y confusa a algunos preceptos, o para realizar una estratificación de las penas atendiendo a la gravedad de las modalidades delictivas recogidas en otros, o de dar una nueva ubicación a los delitos en los que el bien jurídico es otro diferente a la intimidad.

Además, a pesar del mucho tiempo que ha costado aprobar la reforma penal de 2015 y aunque el legislador presuma de que a través de ésta se ha dado solución a los problema de falta de tipicidad existentes, todavía quedan algunas lagunas de punición, y un ejemplo claro de ello lo encontramos en el denominado *revenge porn*, o mejor dicho, en cómo está tipificado. La introducción de una referencia expresa a esta especie de venganza pornográfica era la única novedad a incorporar en el Capítulo primero del Título X del Libro II del Código Penal que aparecía prevista en el Anteproyecto de 2012, presentado apenas un mes después, dicho sea de paso, de que se difundiera un video erótico protagonizado por una concejal hasta entonces desconocida, aunque tanto entonces como ahora dicha difusión quedaría impune. Efectivamente, no habría delito porque la persona afectada es quien grabó el video con su teléfono móvil y envió voluntaria y libremente la grabación audiovisual al acusado, quien a su vez lo reenvió a otras personas. En el momento en que se produjeron los hechos no estaba tipificado el *revenge porn* y sólo se podría hablar de un delito contra la intimidad en caso de que el acusado hubiera accedido al teléfono móvil de la denunciante sin autorización, y a día de hoy, a pesar de que sí está tipificado, es una conducta configurada como un delito de propia mano, esto es, quien difunde las imágenes tiene que ser a la vez quien las graba. Al no hacerse referencia a las imágenes y grabaciones realizadas directamente por la persona afec-

tada se ha perdido la oportunidad de cubrir una necesidad político-criminal de primera magnitud.

Por otra parte, también creemos conveniente anotar, en relación a la extensión de la responsabilidad penal de las personas jurídicas, que se ha realizado sin ser exigida en la Decisión Marco 2005/222/JAI, sin ser requerida por la doctrina especializada ni tampoco por el Consejo General del Poder Judicial y del Consejo Fiscal, y sin haberse podido evaluar la eficacia de la normativa original de 2010, pues no se ha planteado en ningún asunto judicial.

Y para acabar, en relación con los casos en los que se ha optado por un adelantamiento de la intervención penal a conductas meramente preparatorias del ataque a la intimidad, sería interesante realizar una profunda reflexión sobre la existencia, o no, de una razón sólida para ello y sobre la importancia de cumplir la exigencia de acciones u omisiones contenida en el artículo 25.1 de nuestra Constitución. No es éste el momento de hacerlo, entre otras cosas porque excede de los objetivos que nos hemos fijado, pero nos comprometemos a ocuparnos de esta cuestión en otro momento.

Bibliografía

ANARTE BORRALLO, E.-DOVAL PAIS, A., «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Delitos contra la intimidad y los datos personales», en BOIX REIG, J. (Dir.), *Derecho Penal. Parte especial*, vol. I, Iustel, Valencia, 2012.

CARBONELL MATEU, J. C.-GONZÁLEZ CUSSAC, J. L., «Lección XV: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en VIVES ANTÓN. T.-ORTS BERENGUER, E.-CARBONELL MATEU, J. C.-GONZÁLEZ CUSSAC, J. L.-MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho Penal. Parte especial*, 2.ª edición, Tirant lo Blanch, Valencia, 2008.

— «Lección XV: Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en VIVES ANTÓN. T.-ORTS BERENGUER, E.-CARBONELL MATEU, J. C.-GONZÁLEZ CUSSAC, J. L.-MARTÍNEZ-BUJÁN PÉREZ, C., *Derecho Penal. Parte especial*, 3.ª edición, Tirant lo Blanch, Valencia, 2010.

CARRASCO ANDRINO, M. M., «El delito de acceso ilícito a los sistemas informáticos», en ÁLVAREZ GARCÍA, F. J.-GONZÁLEZ CUSSAC, J. L., *Comentarios a la reforma penal de 2010*, Tirant lo Blanch, Valencia, 2010.

CASTIÑEIRA PALOU, M. T., «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en SILVA SÁNCHEZ, J. M., *Lecciones de Derecho Penal. Parte especial*, 3.ª edición, Atelier, Barcelona, 2011.

COLÁS TURÉGANO, A., «Nuevas conductas delictivas contra la intimidad (arts. 197; 197 bis; 197 ter), en GONZÁLEZ CUSSAC, J. L., en Comentarios a la Reforma del Código Penal de 2015, segunda edición, Tirant lo Blanch, Valencia, 2015, pp. 661 y ss.

FERNÁNDEZ TERUELO, J. G., *Cibercrimen. Los delitos cometidos a través de internet*, Constitutio Criminalis Carolina, 2007.

GONZÁLEZ RUS, J. J., «Delitos contra la intimidad, el Derecho a la propia imagen y la inviolabilidad del domicilio», en MORILLAS CUEVA, L. (Coord.), *Sistema de Derecho Penal español. Parte especial*, Dykinson, Madrid, 2011.

JUANATEY DORADO, C.-DOVAL PAÍS, A., «Límites de la protección penal de la intimidad frente a la grabación de conversaciones o imágenes», en BOIX REIG, J. (Dir.), *La protección jurídica de la intimidad*, Iustel, Madrid, 2010.

LLORIA GARCÍA, P., «La difusión inconsentida de imágenes íntimas (sexting) en el proyecto de Código Penal de 2013», *El Derecho*, 2013.

MARTÍNEZ OTERO, J. M., «La difusión de sexting sin consentimiento del protagonista: un análisis jurídico», *Derecom*, 12:1, 2013.

MATA MARTÍN, R. M., *Delincuencia informática y Derecho Penal*, Edisofer, Madrid, 2001.

MORALES PRATS, F., «Delitos contra la intimidad, el Derecho a la propia imagen y la inviolabilidad del domicilio», en QUINTERO OLIVARES, G. (Dir.), *Comentarios a la parte especial del Derecho Penal*, 9.ª edición, Aranzadi Thomson Reutersn, Cizur Menor (Navarra), 2011.

— «Delitos contra la intimidad: Arts. 197.4 bis y 203.2-3», en ÁLVAREZ GARCÍA, F. J. (Dir.), *Estudio crítico sobre el anteproyecto de reforma penal de 2012*, Tirant lo Blanch, Valencia, 2013.

MOYA FUENTES, M. M., «El nuevo delito de acceso ilícito a sistemas informáticos: art. 197.3 CP», *Revista General de Derecho Penal*, núm. 14, 2010.

MUÑOZ CONDE, F., *Derecho Penal. Parte especial*, Tirant lo Blanch, 19.ª edición, Valencia, 2013.

GÓMEZ NAVAJAS, J., *La protección de los datos personales*, Aranzadi, Cizur Menor (Navarra), 2005.

ORTS BERENGUER, E.-ROIG TORRES, M., *Delitos informáticos y delitos comunes cometidos a través de la informática*, Tirant lo Blanch, Valencia, 2001.

POLAINO NAVARRETE, M., «Descubrimiento, revelación de secretos e interceptaciones ilegales», en *Lecciones de Derecho Penal. Parte especial*, tomo I, Tecnos, Madrid, 2010.

— «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (I). Descubrimiento y revelación de secretos», en COBO DEL ROSAL, M., *Curso de Derecho Penal español. Parte especial*, Marcial Pons, Madrid, 1996.

PUENTE ABA, L. M., «Delitos contra la intimidad y nuevas tecnologías», *Eguzkilore*, núm. 21, 2007.

QUERALT JIMÉNEZ, J. J., *Derecho Penal español. Parte especial*, 6.ª edición, Atelier, Barcelona, 2011.

ROMEO CASABONA, C. M., «La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de Internet», *Derecho y Conocimiento*, vol. 2, 2002.

— *Los delitos de descubrimiento y revelación de secretos*, Tirant lo Blanch, Valencia, 2004.

— «La protección penal de la intimidad y de los datos personales: los mensajes de correo electrónico y otras formas de comunicaciones de carácter personal a través de internet y problemas sobre la ley penal aplicable», en *Estudios jurídicos del Ministerio Fiscal,* 2003.

RUEDA MARTÍN, M. A., *Protección penal de la intimidad personal e informática*, Atelier, Barcelona 2004.

TOMÁS-VALIENTE LANUZA, C., «Del descubrimiento y revelación de secretos», en GÓMEZ TOMILLO, M. (Dir.), *Comentarios al Código penal*, 2.ª edición, Lex Nova, Valladolid, 2011.