LA PROTECCIÓN DE LOS DATOS PERSONALES EN EL CÓDIGO PENAL ESPAÑOL

Justa Gómez Navajas
Profesora investigadora contratada del Programa «Ramón y Cajal»

En el presente trabajo, tras exponer la actual regulación penal de las conductas que atentan contra los datos reservados de carácter personal y cuáles son las cuestiones más discutidas doctrinal y jurisprudencialmente, se pretende poner de manifiesto cómo la protección de los datos personales en el vigente Código Penal, si bien tuvo buena acogida cuando se introdujo en 1995 y tiene aspectos positivos, presenta defectos de técnica legislativa y de contenido, y precisa de una reforma. Así, se hace necesaria una mejora de la redacción de las figuras delictivas castigadas en el artículo 197 del CP, ya que en ellas hay reiteraciones y expresiones de difícil interpretación que obstaculizan una correcta aplicación por los Tribunales de los distintos apartados de este precepto, que garantice la seguridad jurídica.

Por otro lado, y de cara a una reforma, se evidencia la necesidad o conveniencia de introducir una referencia expresa a algunos datos especialmente sensibles y dignos de ser específicamente protegidos, como pueden ser los datos genéticos o los relativos a los antecedentes penales.

Del mismo modo, convendría que la redacción legal despejara las dudas sobre la punición en nuestro ordenamiento jurídico de conductas tales como el hacking o intrusismo informático.

Todo ello redundaría en una protección más correcta y eficaz de los datos personales y, en consecuencia, en una tutela más adecuada del irrenunciable y esencial derecho fundamental a la autodeterminación informativa, libertad informática o habeas data.

SUMARIO

1. INTRODUCCIÓN.

2. EL ARTÍCULO 197.2 DEL CP.

2.1. El bien jurídico protegido.

2.2. Los sujetos de las conductas castigadas en el artículo 197.2 del CP.

2.3. Las conductas típicas del artículo 197.2 del CP.

2.3.1. Apoderamiento, utilización o modificación de datos registrados (artículo 197.2 del CP, inciso 1.º).

2.3.2. Acceso, utilización o alteración por cualquier medio de datos reservados de carácter personal (artículo 197.2 del CP, inciso 2.º).

2.4. Objeto del delito: los datos reservados de carácter personal o familiar.

3. LOS TIPOS AGRAVADOS DEL ARTÍCULO 197 DEL CP.

3.1. Difusión, revelación o cesión de secretos (artículo 197.3 del CP).

3.2. El tipo agravado en función del sujeto activo: artículo 197.4 del CP.

3.3. El tipo agravado en función del carácter sensible de los datos y del sujeto pasivo: artículo 197.5 del CP.

3.4. El tipo agravado en función de la finalidad lucrativa: artículo 197.6 del CP.

3.5. El tipo agravado en función de la cualidad de funcionario del sujeto activo: artículo 198 del CP.

4. LA PROTECCIÓN PENAL DE LOS DATOS DE LAS PERSONAS JURÍDICAS.

5. JUSTIFICACIÓN, CULPABILIDAD Y CIRCUNSTANCIAS.

6. ¿DELITO DE TENDENCIA O DE RESULTADO?

7. PENA CORRESPONDIENTE A LOS DELITOS QUE AFECTAN A DATOS PERSONALES.

8. CUESTIONES PROCESALES.

8.1. Perseguibilidad.
8.2. Eficacia del perdón del ofendido.
8.3. Competencia judicial.
8.4. Utilización procesal de pruebas obtenidas vulnerando la intimidad.

9. REFLEXIÓN FINAL: LOGROS Y DÉFICITS.

Listado de abreviaturas utilizadas:

AAP	Auto de la Audiencia Provincial.
Ar.	Repertorio Aranzadi de Jurisprudencia.
ATC	Auto del Tribunal Constitucional.
ATSJ	Auto de Tribunal Superior de Justicia.
CE	Constitución Española.
CP	Código Penal.
CPC	Cuadernos de Política Criminal.
INSS	Instituto Nacional de la Seguridad Social.
FJ	Fundamento Jurídico.
LECrim	Ley de Enjuiciamiento Criminal.
LL	La Ley.
LOPJ	Ley Orgánica del Poder Judicial.
LOTC	Ley Orgánica del Tribunal Constitucional.
AP	Sentencia de la Audiencia Provincial.
SJP	Sentencia del Juzgado de lo Penal.
StGB	Código Penal alemán.
STS	Sentencia del Tribunal Supremo.

1. INTRODUCCIÓN

El Título X del Código Penal, bajo la rúbrica «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», contiene los delitos de descubrimiento y revelación de secretos en su Capítulo primero (artículos 197 a 201 del CP). En él se agrupan distintas modalidades típicas básicas y varios tipos agravados. La introducción de un tipo delictivo como el artículo 197.2 del CP, que protege expresamente los datos reservados de carácter personal, representó una novedad en el Código Penal español [(1)]. Sin embargo, no puede afirmarse que la redacción de este precepto sea afortunada y, por tanto, si bien su incorporación al catálogo de figuras delictivas de nuestro texto punitivo fue un acierto, no lo es el modo en el que se han tipificado las conductas delictivas en él previstas. De ello me ocuparé en las páginas que siguen.

2. EL ARTÍCULO 197.2 DEL CP

2.1. EL BIEN JURÍDICO PROTEGIDO

El artículo 197.2 del CP se inserta dentro de los delitos contra la intimidad. Ésta, como reiteradamente ha declarado el Tribunal Constitucional, *«en cuanto derivación de la dignidad de la persona que reconoce el artículo 10 de la CE, implica la existencia de un ámbito propio y reservado frente a la acción*

1. HAMM, R., en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, ROMEO CASABONA, C.M.ª (coord.), pp. 191 y ss.; CAMPUZANO TOMÉ, H.: *Vida privada y datos personales*, Tecnos, Madrid, 2000.

y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calida mínima de la vida humana» [2]. A la intimidad se refiere nuestra Constitución en su artículo 18.1. Como establece la STC núm. 134/1999, de 15 de julio, lo que garantiza el artículo 18.1 de la CE *«es un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos»* [3]. Coincide esta idea con la definición clásica de intimidad como derecho a ser dejado solo *(to be let alone)* [4].

Aunque guarda estrecha relación con la intimidad, lo que protege el artículo 197.2 del CP es la libertad informática o *habeas data*, o sea: el derecho a la intimidad entendido en sentido positivo, como afirmación de la propia libertad y dignidad de la persona frente al poder informático, reconociéndole al individuo facultades de control sobre los datos personales informatizados (STC 254/1993) [5]. Ello tiene su fundamento en la Constitución, que en su artículo 18.4 establece que *«la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».* Así, la CE incorpora una garantía constitucional como respuesta ante una nueva amenaza a la dignidad y derechos de la persona. Como ha reiterado el Tribunal Constitucional, se trata de un instituto básicamente de garantía del derecho al honor y la intimidad pero también de un instituto que es un derecho o libertad fundamental: el derecho a la libertad frente a las potenciales agresiones a la dignidad y libertad de la persona provenientes del uso ilegítimo del tratamiento automatizado de datos informáticos. La garantía de la intimidad adopta un contenido positivo como derecho de control sobre los datos relativos a la propia persona. La llamada *libertad informática* es el derecho a controlar el uso de los datos que se encuentran en un programa informático o en otro tipo de archivo (SSTC 101/91, 254/1993 o 143/1994) [6].

---

2. SSTC 209/1988, de 27 de octubre, 231/1988, de 1 de diciembre, 197/1991, de 17 de octubre, 99/1994, de 11 de abril, 143/1994, de 9 de mayo, 207/1996, de 16 de diciembre y 98/2000, de 10 de abril.

3. SSTC 186/2000, de 10 de julio, 119/2001, de 29 de mayo, 156/2001, de 2 de julio y 121/2002, de 20 de mayo.

4. WARREN, S./BRANDEIS, L.: *El derecho a la intimidad*, Cuadernos Civitas, Madrid, 1995; CABEZUELO ARENAS, A.L.: *Derecho a la intimidad*, Tirant lo Blanch, Valencia, 1998.

5. ÁLVAREZ CIENFUEGOS SUÁREZ, J.M.ª: «La libertad informática, un nuevo derecho fundamental en nuestra Constitución», *La Ley*, 2001-1, pp. 1724-1731.

6. A ella se refiere el Tribunal Constitucional en otras muchas sentencias: ATC 642/1986, de 23 de julio, SSTC 11/1998, 33/1998, 35/1998, 45/1998, 60/1998, 77/1998,94/1998, 104/1998, 105/1998, 106/1998,

El artículo 18.4 de la CE consagra, pues, *el derecho a la autodeterminación informativa*, que, así formulado, fue reconocido por vez primera en la Sentencia del Tribunal Constitucional Federal Alemán de 15 de diciembre de 1983. Éste *«debe entenderse como aquél que ostenta toda persona física a la reserva y control de los datos que le conciernen en los distintos ámbitos de la vida, de tal suerte que pueda decidir en todo momento cuándo, cómo y en qué medida esa información sea recogida, almacenada, tratada y en su caso transferida a terceros, así como a ser informado de los datos personales que a estos efectos se encuentren almacenados en ficheros o bases de datos, pudiendo acudir a los mismos con la posibilidad de exigir su identificación, puesta al día o cancelación»* (STS de 14 de febrero de 2006, Ar. 717).

El derecho fundamental a la protección de datos abarca:

> «*cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18.1 de la CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo»* (STC 292/2000, de 30 de noviembre).

123/1998, 124/1998, 125/1998,126/1998, 158/1998, 198/1998, 223/1998, 45/1999, 44/1999, 30/1999, 202/1999, 292/2000, 290/2000, ATC 29/2008 y, entre otras muchas, STEDH, *caso Ernst y otros contra Bélgica*, de 15 de julio de 2003 (Ar. 162863). Resulta imposible soslayar la importancia que en este ámbito, como en otros, tiene la jurisprudencia del TEDH y la normativa europea. CONDE ORTIZ, C.: *La protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad,* Universidad de Cádiz/Dykinson, 2005; ROMEO CASABONA, C.M.ª: «Los datos de carácter personal como bienes jurídicos penalmente protegidos», en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, ROMEO CASABONA, C.M.ª (coord.), Comares, Granada, 2006, pp. 167 y ss.

Respecto al apoderamiento, utilización o modificación de datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, establecen las SSTS de 11 de junio de 2004 (Ar. 5625) y 18 de febrero de 1999 (Ar. 510) que *«el tipo se refiere a datos que, normalmente, se pretende que no trasciendan fuera de la esfera de la privacidad, pues ésta no es sólo, como derecho fundamental, un derecho al ocultamiento de circunstancias personales, sino un derecho a la no divulgación ilegal de los datos, ya que configura una forma del derecho a la libre realización de la personalidad»* (SAP de Madrid de 7 de diciembre de 2005 —Ar. 70—).

2.2. LOS SUJETOS DE LAS CONDUCTAS CASTIGADAS EN EL ARTÍCULO 197.2 DEL CP

El artículo 197.2 del CP no presenta particularidades por lo que respecta al sujeto activo. Se trata de un delito común. Las dudas se plantean por lo que se refiere al sujeto pasivo. Y es que si se analiza el artículo 197.2 del CP se observa cómo el legislador no ha derrochado claridad a la hora de determinar quién puede ser sujeto pasivo de este delito. De este modo, en relación con el primer inciso del artículo 197.2 del CP, el sujeto pasivo es el tercero, mientras que en el segundo inciso de este mismo precepto se refiere el Código Penal al *titular de los datos o a un tercero*. La perplejidad que provoca esta redacción, tan imprecisa e ilógica, es enorme, por varias razones:

1.ª No alcanzamos a saber por qué el sujeto pasivo es distinto en un inciso y en otro del artículo 197.2 del CP.

2.ª No hay razón para incluir en el primer inciso al *tercero* (omitiendo como sujeto pasivo —al menos, nominalmente— al titular de los datos, principal perjudicado por las conductas en él castigadas).

Han sido varios los intentos doctrinales por salvar la falta de precisión legislativa del artículo 197.2 del CP. Así, un sector considera que la expresión *«tercero»* se refiere al titular de los datos personales mientras que otro sector entiende que el término *«tercero»* no comprende al titular de los datos porque, si así fuera, no tendría sentido el segundo inciso del artículo 197.2 del CP

(que se refiere al titular de los datos o tercero) [7]. Ambas posturas se apoyan en argumentos razonables. En efecto, si bien, evidentemente, referirse al titular de los datos como *«tercero»* no parece lo más acertado, es cierto que a nadie perjudican más las conductas previstas en el tipo del artículo 197.2 del CP que al propio titular de los datos. Por tanto, y aunque, siguiendo los dictados de la lógica, *tercero* es, por definición, cualquiera que no sea el titular de los datos [8], y a pesar de que no entender incluido al titular de los datos sería congruente con el tenor literal de la ley (puesto que el titular no es un tercero), una interpretación pegada a la literalidad del CP nos llevaría a entender que el titular de los datos queda fuera del círculo de sujetos pasivos, lo que resulta absolutamente paradójico, contradictorio y absurdo [9]. No tienen por qué coincidir tercero y víctima [10].

2.3. LAS CONDUCTAS TÍPICAS DEL ARTÍCULO 197.2 DEL CP

2.3.1. Apoderamiento, utilización o modificación de datos registrados (artículo 197.2 del CP, inciso 1.º)

El artículo 197.2 del CP tipifica los abusos informáticos sobre datos personales, automatizados o no, obrantes en cualquier tipo de archivos públicos o pri-

---

7. MORALES PRATS, F.: *Comentarios a la Parte especial del Derecho Penal*, Thomson/Aranzadi, 6.ª ed., 2007, p. 425. Véase, del mismo autor, *La tutela penal de la intimidad: privacy e informática*, Destino, Barcelona, 1984; el mismo: «La protección penal de la intimidad frente al uso ilícito de la informática en el Código Penal de 1995», en *Delitos contra la libertad y seguridad, CDJ*, CGPJ, Madrid, 1996; el mismo: «Internet: riesgos para la intimidad», en *Internet y derecho penal*, *CDJ*, CGPJ, Madrid, 2002; GARCÍA GARNICA, M.ª C.: «El derecho a la protección de los datos personales como derecho fundamental», *Los derechos humanos. Libro Homenaje al Excmo Sr. D. Luis Portero García*, Universidad de Granada, 2001, pp. 211-221.

8. CASTIÑEIRA PALOU, M.ª T.: *Lecciones de Derecho Penal, Parte Especial*, Atelier, Barcelona, 2006, p. 133.

9. *«Tercero»* no es el titular de los datos. Por definición, tercero es toda persona distinta del sujeto activo y del sujeto pasivo (titular de los datos). Véase JORGE BARREIRO, A., en *Comentarios*, RODRÍGUEZ MOURULLO, G. (dir.), Civitas, Madrid, p. 575; LOZANO MIRALLES, J., en BAJO FERNÁNDEZ, M.: *Compendio de Derecho Penal, Parte Especial* (vol. II), Centro de Estudios Ramón Areces, Madrid, 1998, pp. 194-238; STS de 9 de octubre de 2000 (Ar. 8755).

10. CARBONELL MATEU, J.C./GONZÁLEZ CUSSAC, J.L.: *Comentarios al Código Penal de 1995*, vol. I., VIVES ANTÓN, T.S. (coord.), Tirant lo Blach, 1996, pp. 990-1.011, p. 1000. *Tercero* es *«cualquier persona que pudiera resultar afectado por el apoderamiento, utilización o modificación de los datos registrados, incluidas obviamente las personas físicas titulares de los datos objeto de apoderamiento»* (STS de 9 de octubre de 2000, Ar. 8755).

vados [11]. O, si se prefiere, castiga los delitos contra la libertad informática *(habeas data)* [12] o contra la autodeterminación informativa, y representó una novedad en el Código Penal [13].

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

Ha de tenerse en cuenta que aquellas conductas de manipulación y tratamiento informatizado, o no, de datos que queden fuera del ámbito de protección del Código Penal pueden ser castigadas como infracciones administrativas, previstas en la LO 15/1999, de Protección de Datos de Carácter Personal y sancionadas por ésta (Título VII, artículos 43 a 49).

La redacción del artículo 197.2 del CP dista de ser la mejor de las posibles, ya que incurre en reiteraciones que han dado lugar a diversas interpretaciones doctrinales y jurisprudenciales [14].

---

11. JAREÑO LEAL, Á./DOVAL PAÍS, A.: «Revelación de datos personales, intimidad e informática. Comentario a la STS 234/1999, de 18 de febrero», *La Ley*, 1999, pp. 1672-1680, p. 1675 [también en QUINTERO OLIVARES, G./MORALES PRATS, F. (coord.): *El Nuevo Derecho penal Español. Estudios penales en memoria del prof. José M. Valle Muñiz*, Aranzadi, 2001]. Puede verse la SAP de 8 de junio de 2002 (Ar. 210565). ROMEO CASABONA, C.M.ª: *Comentarios al Código Penal*, artículo 197, en DÍEZ RIPOLLÉS/ROMEO CASABONA (coord.); RUEDA MARTÍN, M.ª Á.: *Protección penal de la intimidad e informática*, Atelier, Barcelona, 2004, p. 68; SAP de Cantabria de 8 de junio de 2002 (Ar. 210565) y SAP de Baleares de 14 de marzo de 2001 (Ar. 118392).

12. JORGE BARREIRO, A.: *Comentarios al Código penal*, RODRÍGUEZ MOURULLO, G. (dir.), Civitas, Madrid, 1997, p. 571; MORALES PRATS, F. *Comentarios,* ob. cit., p. 417. Debe decirse que, referida a estos delitos, no es exacta la expresión *«delitos informáticos»* [utilizada por CARBONELL MATEU, J.C./GONZÁLEZ CUSSAC, J.L.: *Comentarios al Código Penal de 1995*, vol. I., VIVES ANTÓN, T.S. (coord.), Tirant lo Blanch, Valencia, 1996, p. 999].

13. STS de 18 de febrero de 1999, AAP de Lérida de 29 de julio de 1999 (Ar. 2715), SAP de Madrid de 3 de julio de 2000 (Ar. 3384), SSTS de 4 de diciembre de 2000 (Ar. 10178) y 11 de julio de 2001 (Ar. 1056), SAP de Zaragoza de 26 de diciembre de 2002 (Ar. 848) y STS de 11 de junio de 2004.

14. En general y ampliamente sobre el artículo 197.2 del CP, GÓMEZ NAVAJAS, J.: *La protección de los datos personales. Un análisis desde la perspectiva del Derecho Penal*, Thomson/Civitas, Madrid, 2005. Véase COBOS GÓMEZ DE LINARES, M.A., en *Derecho Penal. Parte Especial*, II, Servicio de Publicaciones de la

En su inciso primero, el artículo 197. 2 del CP tipifica las conductas de apoderamiento, utilización o modificación de datos reservados de carácter personal o familiar de otro, registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

- ❑ Apoderamiento de datos reservados de carácter personal o familiar en perjuicio de tercero.
- ❑ Utilización de datos reservados de carácter personal o familiar en perjuicio de tercero.
- ❑ Modificación de datos reservados de carácter personal o familiar en perjuicio de tercero.

Conviene analizar, siquiera brevemente, en qué consisten estas conductas típicas [(15)].

Por *apoderamiento de datos reservados de carácter personal* se entiende la acción consistente en hacerse con el control de los datos de otra persona. A diferencia de lo que sucede en el tipo básico del artículo 197.1 del CP, en el que el objeto del apoderamiento lo constituyen cualesquiera *«documentos o efectos personales»,* en el tipo del artículo 197.2 del CP el apoderamiento recae sobre *«datos reservados»* de carácter personal o familiar.

Facultad de Derecho, Universidad Complutense de Madrid, 1997, pp. 27 y ss. La SAP de Madrid de 15 de abril de 1999 (Ar. 1762), en su FJ 3.º, declara, refiriéndose al artículo 197.2 del CP: *«Se trata de un precepto en el que la reiteración de sus verbos nucleares dificulta notablemente su interpretación, ya que en un primer inciso nos habla de "apoderarse, utilizar o modificar" y en un segundo de "acceder, utilizar o modificar" los datos reservados de carácter personal y familiar».*

15. Véase sobre estas conductas y la relación entre intimidad y nuevas tecnologías, MATA MARTÍN, R.: *Delincuencia informática y Derecho Penal*, Edisofer, Madrid, 2001; «La protección penal de datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías», *Revista Penal* 18, julio de 2006, pp. 217-235; CÓRDOBA RODA, J./GARCÍA ARÁN, M.: *Comentarios al Código Penal, Parte Especial*, t. I, Marcial Pons, Madrid, 2004, pp. 451 y ss.; ALFONSO LASO, Daniel de: «Intimidad y protección de datos en el Derecho Penal», *Delincuencia informática. Problemas de responsabilidad*, Cuadernos de Derecho Judicial, CGPJ, Madrid, 2003, pp. 35-75; CARBONELL MATEU. J.C./GONZÁLEZ CUSSAC, J.L., en AA.VV.: *Derecho Penal. Parte Especial*, Tirant lo Blanch, Valencia, 2004, pp. 324 y ss.; SEGRELLES DE ARENAZA, I.: «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en COBO DEL ROSAL, M. (dir.), *Compendio de Derecho Penal Español, Parte Especial*, Marcial Pons, Madrid, 2000, pp. 269 y ss.; SUÁREZ-MIRA RODRÍGUEZ, C. (coord.)/JUDEL PRIETO, Á./PIÑOL RODRÍGUEZ, J.R.: *Manual de Derecho Penal*, t. II, Parte Especial, 3.ª ed., Thomson/Civitas, Aranzadi, 2005, pp. 192-201.

En el primer inciso del artículo 197. 2 del CP se castiga el apoderamiento (no meramente material sino también cognitivo). Llama la atención que en el inciso 2.º del artículo 197.2 del CP se castiga el acceso por cualquier medio a los datos reservados (16). ¿Qué diferencia hay entre apoderarse de unos datos o acceder a ellos? Hay autores que interpretan que el artículo 197.2 del CP, en su segundo inciso, castiga conductas que recaen sobre los ficheros o soportes y no directamente sobre los datos. De esta manera, intentan salvar la falta de lógica del precepto que, de no seguirse esta interpretación, abocaría a afirmar que está tipificando dos veces la conducta de apoderamiento, así como la de alteración y utilización de datos personales.

Sobre este extremo se ha pronunciado el Tribunal Supremo en sentencia de 18 de febrero de 1999 (Ar. 510) en la que sostiene:

> *«a primera vista, parecen recogidos en cada uno de los dos incisos de dicha norma dos tipos delictivos distintos, pero hay que reconocer que no resulta fácil precisar cuáles son sus elementos diferenciadores. La acción es, en ambos casos, prácticamente la misma: apoderarse, utilizar o modificar en el primer inciso, y acceder, utilizar o modificar en el segundo, aunque puede apreciarse una diferencia de matiz en la intensidad de la acción entre apoderarse y acceder "por cualquier medio". El objeto de la acción delictiva es exactamente el mismo».*

¿Qué sucede con el denominado espionaje o intrusismo informático *(hacking)* (17)? La conducta de mero intrusismo informático quedaría fuera del ám-

---

16. SAP de Barcelona de 4 de octubre de 2001 (Ar. 20856). Sobre el apoderamiento de numeración de tarjeta de crédito, véase la SAP de Barcelona de 6 de noviembre de 2001 (Ar. 891) y la SAP de Barcelona de 10 de marzo de 2006 (Ar. 510).

17. El Proyecto de Código Penal de 2007 (que decayó por disolución de las Cortes al término de la pasada legislatura, BOE de 15 de enero de 2008) tipificaba expresamente el *hacking*. En el artículo 197 del CP se introducía un nuevo apartado 3, pasando los actuales apartados 3, 4, 5 y 6 a ser los apartados 4, 5, 6 y 7, y se añadía un apartado 8, que quedaban redactados como siguen:

> *«3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo, será castigado con pena de prisión de seis meses a dos años».*
>
> *«8. Si los hechos descritos en los apartados anteriores se cometiesen en el seno de una organización criminal, se aplicarán respectivamente las penas superiores en grado».* *(sigue)*

bito de protección del artículo 197.2 del CP si no está presidida por la intención de actuar *«en perjuicio del titular de los datos o de un tercero»* (18). No obstante, hay quien considera que incluso la mera intrusión constituye un ilícito penal porque el intruso debe vulnerar las claves secretas, contraseñas o *passwords* para acceder a datos confidenciales (19).

El artículo 2 de la Convención del Consejo de Europa sobre delincuencia informática (Budapest, 23 de noviembre de 2001) considera que el acceso ilegal a un sistema informático debe ser una infracción criminal:

> *«Los Estados Parte deberán adoptar las medidas legislativas o de otro género que fueren necesarias para establecer como infracción criminal el acceso intencional sin autorización a la totalidad o parte de un sistema informático. Los Estados podrán requerir que el hecho sea cometido infringiendo medidas de seguridad o con la finalidad de obtener datos u otra finalidad deshonesta o, en relación con los sistemas informáticos, que se encuentren conectados a otros sistemas informáticos».*

Otra de las conductas típicas castigadas en el artículo 197.2 del CP, inciso 1.º, es la utilización (el uso o empleo) de datos reservados. Esta conducta se prevé, asimismo, en el inciso 2.º del artículo 197.2 del CP, aunque no se entiende de cuál es la razón de dicha reiteración o si, simplemente, se trata de un defecto de técnica legislativa.

Se castiga, asimismo, en el primer inciso del artículo 197.2 del CP, la modificación de datos reservados, mientras que en el inciso 2.º del artículo 197.2 del CP se castiga la alteración de datos, sin que se alcance fácilmente a ver qué diferencia hay entre una y otra conducta.

Véase SJP de Badajoz de 15 de febrero de 2006 (Ar. 46). GONZÁLEZ RUS, J.J.: «Los ilícitos en la red (I): hackers, crackers, cyperpunks, sniffers, denegación de servicio y otros comportamientos semejantes», en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, ROMEO CASABONA, C.M.ª (coord.), pp. 241 y ss.

18. MORÓN LERMA, E.: *Internet y Derecho Penal: hacking y otras conductas ilícitas en la Red*, Pamplona, 1999, pp. 42 y ss.; ORTS BERENGUER, E./ROIG TORRES, M.: *Delitos informáticos y delitos comunes cometidos a través de la informática*, Tirant lo Blanch, Valencia, 2001, p. 35; RUIZ MARCO, F.: *Los delitos contra la intimidad*, Colex, Madrid, 2001, pp. 26-27. Véase la SAP de Valencia de 2 de diciembre de 2005 sobre el acceso irregular a correo electrónico de profesor de Universidad (Ar. 24635).

19. HUERTA TOCILDO, S./ANDRÉS DOMÍNGUEZ, A.C.: «Intimidad e informática», *Revista de Derecho Penal*, 2002, pp. 11-71, 26.

2.3.2. Acceso, utilización o alteración por cualquier medio de datos reservados de carácter personal (artículo 197.2 del CP, inciso 2.º)

En el 2.º inciso del artículo 197.2 del CP se castiga:

— El **acceso** por cualquier medio a los datos reservados en perjuicio del titular de los datos o de un tercero [20].

— **La alteración o utilización** por cualquier medio a los datos reservados en perjuicio del titular de los datos o de un tercero.

El citado inciso se expresa en los siguientes términos:

> «*Iguales penas* [que las del inciso anterior] *se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos* [datos] *y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero».*

Ardua resulta la tarea de distinguir la conducta de apoderamiento de los datos (que, como se dijo antes, no ha de entenderse meramente en sentido de apoderamiento físico) de la de acceso a los mismos o la conducta de modificación de datos personales de la de alteración de los mismos.

En ocasiones, el acceso a los datos puede estar justificado, en cuyo caso la conducta no sería antijurídica. No siempre es fácil dilucidar cuándo la conducta está justificada. Se puede plantear, por ejemplo, el conflicto entre el deber de vigilancia del empresario y, por tanto, el derecho de éste a velar por el buen hacer de sus empleados y verificar el uso que hacen del ordenador de la empresa, y el derecho a la intimidad [21].

---

20. La SAP de Barcelona de 12 de diciembre de 2003 (Ar. 50) se pronunció sobre la conducta de quien accedió y utilizó el buzón electrónico de la víctima, dispuesto en la red informática de la Universidad en la que ésta estudiaba, llegando a abrir mensajes en él depositados y a utilizar sus claves de acceso para enviar desde la dirección de la víctima mensajes a terceros con obscenos y denigrantes contenidos. Véase SAP de Tarragona de 23 de julio de 2001 (Ar. 310139).

21. La SAP de Asturias de 29 de junio de 2005 (Ar. 175379) aprecia este delito en un caso en el que el acusado accede al correo electrónico de la víctima. GARCÍA GONZÁLEZ, J.: «Intervenciones de terceros en el correo electrónico. Especial referencia al ámbito laboral y policial», en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, ROMEO CASABONA, C.M.ª (coord.), pp. 297 y ss. Véase el AAP de Castellón de 30 de junio de 2005 (Ar.199356).

Véase la STEDH (Sección 4.ª), de 3 de abril de 2007, *Caso Copland contra Reino Unido*, dictada tras la demanda presentada ante el TEDH por una ciudadana británica contra el Reino Unido por el seguimiento de sus llamadas

Por otro lado, el acceso a mensajes de correo electrónico puede subsumirse en el apartado 1 del artículo 197 del CP, que castiga expresamente el apoderamiento de mensajes de correo electrónico. No obstante, puede entenderse que esta conducta encaja en el inciso 2.º del artículo 197.2 del CP, en tanto en cuanto constituye, asimismo, un acceso a datos de carácter personal.

El acceso a datos reservados concurre, frecuentemente, con el delito de daños informáticos del artículo 264.2 del CP (SJP de Valencia de 15 de junio de 2004 —Ar. 187091—, SJP de Valencia de 15 de junio de 2004 —Ar. 187091—, SAP de Málaga de 28 de enero de 2005 —Ar. 140119—) o contra la integridad moral (SAP de Barcelona de 12 de diciembre de 2003 —Ar. 50—).

2.4. OBJETO DEL DELITO: LOS DATOS RESERVADOS DE CARÁCTER PERSONAL O FAMILIAR

La acción descrita en el artículo 197.2 del CP ha de recaer sobre datos reservados de carácter personal o familiar de otro registrados en ficheros o so-

---

telefónicas, correo electrónico y navegación por Internet realizado por su centro de trabajo para comprobar si usaba estos medios con fines personales. El TEDH estima la demanda por violación del artículo 8 del Convenio. Véase la STC 98/2000, de 10 de abril, en cuyo FJ 6.º se declara que *«no puede descartarse que también en aquellos lugares de la empresa en los que se desarrolla la actividad laboral puedan producirse intromisiones ilegítimas por parte del empresario en el derecho a la intimidad de los trabajadores, como podría serlo la grabación de conversaciones entre un trabajador y un cliente, o entre los propios trabajadores, en las que se aborden cuestiones ajenas a la relación laboral que se integran en lo que hemos denominado propia esfera de desenvolvimiento del individuo (SSTC 231/1988, de 2 de diciembre, FJ 4.º y 197/1991, de 17 de octubre, FJ 3.º, por todas). En suma, habrá que atender no sólo al lugar del centro de trabajo en que se instalan por la empresa sistemas audiovisuales de control, sino también a otros elementos de juicio (si la instalación se hace o no indiscriminada y masivamente, si los sistemas son visibles o han sido instalados subrepticiamente, la finalidad real perseguida con la instalación de tales sistemas, si existen razones de seguridad, por el tipo de actividad que se desarrolla en el centro de trabajo de que se trate, que justifique la implantación de tales medios de control, etc.), para dilucidar en cada caso concreto si esos medios de vigilancia y control respetan el derecho a la intimidad de los trabajadores. Ciertamente, la instalación de tales medios en lugares de descanso o esparcimiento, vestuarios, aseos, comedores y análogos resulta, "a fortiori", lesiva en todo caso del derecho a la intimidad de los trabajadores, sin más consideraciones, por razones obvias (amén de que puede lesionar otros derechos fundamentales, como la libertad sindical, si la instalación se produce en los locales de los delegados de personal, del Comité de empresa o de las secciones sindicales). Pero ello no significa que esa lesión no pueda producirse en aquellos lugares donde se realiza la actividad laboral, si concurre alguna de las circunstancias expuestas que permita calificar la actuación empresarial como ilegítima intrusión en el derecho a la intimidad de los trabajadores. Habrá, pues, que atender a las circunstancias concurrentes en el supuesto concreto para determinar si existe o no vulneración del artículo 18.1 CE»* (FJ 6.º). RODRÍGUEZ ESCANCIANO, S.: «La potencialidad lesiva de la informática sobre los derechos de los trabajadores», *Revista Española de Protección de Datos*, 2, enero-junio de 2007, pp. 95-158.

portes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Las conductas que afecten a datos no registrados y pongan en peligro la intimidad informática pueden ser sancionadas conforme a la Ley Orgánica 15/1999, de 13 de diciembre (LOPD) [22].

Se ha mantenido por la doctrina que el concepto de *datos reservados* del artículo 197.2 del CP es un concepto normativo. En este sentido, se ha considerado que para la interpretación de qué sean *datos personales reservados* hay que tener en cuenta la LO 15/1999, de Protección de Datos de Carácter Personal, en cuyo artículo 3.a) se establece que se entenderá por datos de carácter personal *«cualquier información concerniente a personas físicas identificadas o identificables»* [23]. Sin embargo, otra opinión entiende que el artículo 197.2 del CP no es una ley penal en blanco [24], sino que entraña un concepto propio de *«datos reservados»*.

El artículo 197.2 del CP se refiere expresamente a los *datos reservados de carácter personal y familiar*. El término *«familiar»* no aparece en la LOPD ni en la Directiva 1995/46, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Parece tener su origen en el artículo 18.1 de la CE. El Tribunal Supremo niega que haya una *«intimidad familiar»* [25].

Reservados se entiende que son los datos de conocimiento limitado para terceros ajenos al fichero en el que se encuentran [26]. *Datos reservados* han de ser informaciones cuyo conocimiento está limitado a personas autorizadas o,

---

22. Véase el AAP de Guipúzcoa de 2 de marzo de 1998 —Ar. 1785— y de 21 de marzo de 2000, y el AAP de Lérida de 29 de julio de 1999 —Ar. 2715—. Véase el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, de 21 diciembre (BOE 19 de enero de 2008, núm. 17, p. 4.103).
23. Véase el AAP de Guipúzcoa de 2 de marzo de 1998 (Ar. 2152), el AAP de Lérida de 29 de julio de 1999 (Ar. 2715) y de 21 de marzo de 2000 (Ar. 59).
24. QUERALT JIMÉNEZ, J.J.: *Derecho Penal español. Parte especial*, Atelier, Barcelona, 2008, p. 266.
25. STS de 20 de junio de 2003 (Ar. 4359) y AAP de Ciudad Real de 9 de mayo de 2006 (Ar. 166119). Véase MIERES MIERES, L.J.: *Intimidad personal y familiar*. Prontuario de Jurisprudencia Constitucional, Aranzadi, 2002. Sobre la intimidad en la pareja, pueden verse: SSAP de Valencia de 20 de mayo de 2003 (Ar. 240374), de Navarra de 31 de julio de 2003 (Ar. 275626), de Cádiz de 29 de diciembre de 2003 (Ar. 110278), de Barcelona de 16 de enero de 2004 (Ar. 1478) y de Castellón de 12 de abril de 2004 (Ar. 323).
26. Véase sobre este concepto y, en general, sobre los delitos de descubrimiento y revelación de secretos, ROMEO CASABONA, C. M.ª: *Los delitos de descubrimiento y revelación de secretos*, Tirant lo Blanch, Valencia, 2004, p. 110.

lo que es lo mismo, han de ser datos no disponibles sin autorización y que incidan en la esfera personal o familiar [27].

La STS de 11 de junio de 2004 (Ar. 483614) declara que los datos relativos al lugar de trabajo y al domicilio de la empresa son datos reservados. No son reservados los datos *«destinados naturalmente al conocimiento público»* (STS de 20 de septiembre de 1999 —Ar. 51483—). Acerca de qué son *«datos reservados»* se pronuncia la STS de 18 de febrero de 1999 (Ar. 510), según la cual *«no todos los datos reservados de carácter personal o familiar pueden ser objeto del delito contra la libertad informática»* [28]. Los datos protegidos no son sólo los datos íntimos, sino todos aquellos datos personales cuyo empleo por terceros pueda afectar negativamente a los derechos de su titular (STC 292/2000, de 30 de noviembre). Datos que, en principio, pueden parecer inocuos, si se archivan e interrelacionan pueden dar lugar a información sensible o crear un auténtico perfil de la persona [29]. En este sentido, y para no ampliar en exceso el ámbito del tipo, debiera entenderse que los datos personales a los que se refiere el artículo 197.2 del CP son reservados en tanto en cuanto no son públicos y el titular de los mismos no desea que lo sean.

Es importante resaltar que los datos reservados protegidos en el artículo 197.2 del CP no pertenecen a lo que se ha dado en denominar el núcleo duro de la *privacy* (SSTS de 10 de diciembre de 2004 y 11 de julio de 2001, Ar. 1056), es decir, no son datos de los considerados *«sensibles».* Para MORALES PRATS el término *«reservados»* no tiene sentido porque todos los datos personales automatizados quedan protegidos por el artículo 197.2 del CP, dado que una vez introducidos en el fichero automatizado pueden ser manipulados [30].

---

27. CASTIÑEIRA PALOU, M.ª T.: *Lecciones…*, ob. cit., p. 132. LOZANO MIRALLES, J., en BAJO FERNÁNDEZ, M.: *Compendio de Derecho Penal, Parte Especial* (vol. II).

28. Véase STS de 18 de febrero de 1999 —Ar. 272511—, STS de 14 de septiembre de 2000 (Ar. 7942), SAP de Toledo de 17 de octubre de 2005 (Ar. 261533), FJ 1.º: *«no ha de interpretarse en el sentido estricto de "confidencial" sino en su aspecto relacionado con la intimidad de las personas, porque tal es el derecho que protege la norma penal».* [ATSJCV de 18 de febrero de 1999, FFJJ 3.º y 4.º (Ar. 1040)].

29. Así, HUERTA TOCILDO, S./ANDRÉS DOMÍNGUEZ, A.C.: «Intimidad e informática», *Revista de Derecho Penal*, 2002, pp. 11-71, 2002; HERRÁN ORTIZ, A.I.: *La violación de la intimidad en la protección de datos personales*, Dykinson, Madrid, 1999, p. 211. La SAP de Lérida de 28 de febrero de 2000 (Ar. 92375), considera que es suficiente la violación del continente, con independencia de su contenido (véase también la SAP de Ciudad Real de 25 de noviembre de 1999 —Ar. 4684—).

30. MORALES PRATS, F.: *Comentarios,* ob. cit., p. 422; JORGE BARREIRO, J.: *Comentarios,* ob. cit., pp. 129 y ss. Véase, en este sentido, la SAP de Ciudad Real de 23 de abril de 2001 (Ar. 443).

En mi opinión, yerra la STS de 18 de febrero de 1999 (Ar. 510) cuando declara:

> *«No es fácil precisar, "a priori" y en abstracto, cuándo el desvelamiento de un dato personal o familiar produce ese perjuicio. (…) 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 estricto, 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».*

Es equivocada, a mi juicio, la utilización que la mencionada sentencia hace del calificativo *«sensible».* Y ello, por dos razones: 1.ª) porque no hay datos sensibles. Sensible será, en todo caso, el titular de los datos; y 2.ª) porque *sensibles* son los datos relativos al núcleo duro de la *privacy*.

En la doctrina y en la jurisprudencia ha habido intentos por distinguir el concepto de *«secreto»* de la idea de *«intimidad».* Así, se ha entendido el secreto en un sentido formal (STC 114/1984). Sin embargo, frente a esta interpretación, se ha sostenido también que, por el contrario, el CP en su artículo 197 del CP *«asimila textualmente el descubrimiento de los secretos a la vulneración de la intimidad, puesto que sitúa las correspondientes conductas en un plano de equivalencia, al conectarlas mediante la conjunción "o"»* (STS de 19 de junio de 2006). Como señala esta sentencia en su FJ 4.º, *«la idea de secreto en el artículo 197.1.º del CPenal resulta conceptualmente indisociable de la de intimidad: ese "ámbito propio y reservado frente a la acción y el conocimiento de los demás" (SSTC 73/1982 y 57/1994, entre muchas)».* En este sentido, la STS de 4 de abril de 2001 (Ar. 2016) declara que por *secreto* ha de entenderse lo concerniente a la esfera de la intimidad, que es sólo conocido por su titular o por quien él determine.

Al respecto, puede consignarse que la STS de 19 de junio de 2006 fue absolutoria por considerar que la intimidad es un ámbito que *«no debe verse implicado en el desempeño habitual de actividades político-administrativas»* y que los acusados no pretendieron vulnerarla. Pero lo cierto es que los acusados estaban accediendo indebidamente a una cuenta de correo ajena y que el carácter delictivo o no de la conducta no se puede vincular exclusivamente a la naturaleza íntima o no de la información que se llega a obtener. Ello sería tanto como castigar las interceptaciones telefónicas sólo y exclusivamen-

te cuando el contenido de la conversación ilícitamente intervenida sea de carácter íntimo. Sin perjuicio de entender que los términos *«secreto»* e *«intimidad»* son sinónimos en muchas ocasiones y contextos, lo cierto es que el Derecho Penal debe proteger también el derecho a la libertad de las comunicaciones, con independencia del carácter de éstas, y un derecho al control de los datos o informaciones privadas, abstracción hecha de su carácter más o menos íntimo [31].

Objeto material del artículo 197.2 del CP podrá ser cualquier dato personal registrado, que no sea *sensible,* sea íntimo o no [32]. La determinación de qué son datos reservados, como se ha apuntado, no es pacífica. Así, por ejemplo, podemos plantearnos si algunas informaciones de carácter personal constituyen datos reservados a los efectos del artículo 197.2 del CP:

1) *La numeración de la tarjeta de crédito* [33].

2) *La dirección de correo electrónico.*

   Puede considerarse que la dirección de correo electrónico en sí misma no es información «secreta» pero es posible que el titular de la dirección no quiera que se conozca por temor a que le invadan el correo o porque crea que alguien puede utilizar su dirección con aviesas intenciones. La SAP de Madrid de 25 de febrero de 2002 (Ar. 149473) señala en su FJ 1.º:

   > *«la dirección de correo electrónico no es distinta de la dirección postal o del número de teléfono que utiliza una persona. En sí mismos no son más que la forma de individualizar un lugar para recepción de correspondencia postal o telegráfica, o una cifra que activa un teléfono determinado estableciendo comunicación con la persona que atienda la llamada o dejar mensajes en un dispositivo grabador.*

---

31. Véase la SAP de Burgos de 10 de diciembre de 2002 (Ar. 33300) sobre un caso en el que el acusado se apoderó de cartas que no entregó a sus destinatarios. La información contenida en las cartas no era susceptible de ser catalogada como *«secreto»* ni pertenecía a la esfera de intimidad más estricta de los destinatarios.

32. ORTS BERENGUER. E./ROIG TORRES, M.: *Delitos informáticos…,* ob. cit., pp. 32-33; CARBONELL MATEU/GONZÁLEZ CUSSAC: *Comentarios*, ob. cit., p. 1000.

33. SAP de Barcelona de 6 de noviembre de 2001 (Ar. 891) y SAP de Barcelona de 10 de marzo de 2006 (Ar. 510).

(…) Lo importante es el contenido, no el continente; y la dirección electrónica no es más que una referencia identificativa de un continente (…) allí donde se conservan los datos que pueden afectar a la intimidad de la persona.

El solo conocimiento de esa referencia identificativa no permite acceder a los datos conservados, ni manipularlos o transferirlos».

En los casos en que se usa una dirección de correo electrónico ajena para solicitar contactos con personas del mismo sexo sería posible apreciar un delito de injurias. Así lo reconoce el AAP de Tarragona de 24 de noviembre de 2003 (Ar. 109051), en su FJ 4.º:

«Difundir en un medio tan público como Internet no sólo los gustos sexuales de una persona, que además y por lo que querellante y querellado manifiestan no son los reales del querellante, sino también su promiscuidad al solicitar relaciones con terceros, dando una apariencia de verosimilitud al circunscribir tales relaciones en un determinado espacio y dando elementos de contacto reales (correo electrónico, teléfono y nombre de referencia), perfectamente puede constituir delito de injurias» [34].

3) El *número de teléfono* (móvil o fijo) también se considera un dato reservado [35].

4) *Listados de llamadas* [36].

---

34. La SAP de Madrid de 25 de febrero de 2002 (Ar.149473) absuelve al acusado de publicar un anuncio en tablón de empresa de prestación de servicios de telecomunicaciones en el que, sin el consentimiento de la interesada, se revelaba su correo electrónico junto con una solicitud de contactos para relaciones lésbicas, manteniendo oculta su identidad. Previamente, el Juzgado de lo Penal núm. 20 de Madrid había condenado al acusado.

35. SAP de Castellón de 26 de septiembre de 2005 (Ar. 274833).

36. SSTS de 7 de diciembre de 2001 (Ar. 2070), 22 de octubre (Ar. 7951) y 10 de diciembre de 2004 (Ar. 7917) y SAP de Gerona de 14 de noviembre de 2005 (Ar. 15). Cfr. Circular 1/1999, de 29 de diciembre, sobre intervención de las comunicaciones telefónicas en el seno de los procesos penales. Véase artículo 38.3 de la Ley 32/2003, General de Telecomunicaciones, de 3 de noviembre, y la Directiva 2002/58/CE, la cual prevé en su artículo 15.1 la posibilidad de limitar los derechos vinculados a la protección de datos personales cuando *«tal*

Los listados de llamadas realizados desde un determinado teléfono que un juzgado solicite de la compañía telefónica no vulnera el derecho al secreto de las comunicaciones ni el derecho a la intimidad (STS de 22 de marzo de 1999, Ar. 2947) (37).

5) Datos que circulan a través de programas informáticos para descargar archivos de Internet.

El Tribunal Supremo ha estimado en una reciente sentencia de 28 de mayo de 2008 (Ar. 222550) que los datos que circulan a través del programa «eMule» se convierten en públicos para los usuarios de Internet, que usan dicho programa y consienten en compartir archivos y no están protegidos por el derecho a la intimidad ni el derecho al secreto de las comunicaciones, por lo que la Policía puede acceder a ellos. Esta sentencia anula una anterior, de 2 de mayo de 2007, de la Audiencia Provincial de Tarragona (Ar. 185184), que había absuelto a una mujer, acusada de un delito de facilitación de material de pornografía infantil, por entender que se había lesionado gravemente su derecho fundamental al secreto de sus comunicaciones (38).

* * *

Ha de subrayarse que la protección penal se limita a la tutela de datos ya registrados o archivados y, por tanto, no se extiende a las fases de creación de los ficheros automatizados y de recogida de datos personales [FJ 3.º AAP de Guipúzcoa de 2 de marzo de 1998 (Ar. 1785)]. Queda excluida, asimismo, del ámbito penal la comisión por imprudencia de estas conductas, ya que todas las contempladas en el Título X del Libro II del CP deben ser do-

---

limitación constituya una medida necesaria, proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46». PRIETO ANDRÉS, A.: «La nueva Directiva europea sobre el tratamiento de datos personales y la protección de la intimidad en el sector de las telecomunicaciones», *LL* 2002-5, pp. 1710-1713.

37. GÓMEZ NAVAJAS, J.: «¿Tienen obligación los proveedores de servicios de facilitar datos de usuarios? (Comentario a la sentencia del Tribunal de Berlín de 25 de septiembre de 2006)», *Revista Española de Protección de Datos*, núm. 1, 2007, pp. 249-263.

38. GÓNZALEZ LÓPEZ, J.J.: *Los datos de tráfico de las comunicaciones electrónicas en el proceso penal,* La Ley, 2007.

losas, habida cuenta de que nuestro Código Penal no hace mención expresa a la imprudencia en estos delitos que afectan a los datos personales y, conforme al artículo 12 del CP, la imprudencia se rige por el sistema de *numerus clausus* (39).

Sí es posible apreciar el error de tipo (el error que recae sobre alguno de los elementos de cada uno de los tipos penales que estamos analizando) cuando se yerra sobre el carácter reservado de los datos o sobre la autorización para utilizarlos. A este respecto, la SAP de Madrid de 15 de abril de 1999 (Ar. 1762) declara:

> *«si bien el ciudadano sabe o tiene la obligación de saber que los datos relativos a la intimidad de una persona recogidos en un registro o archivo público no se pueden conocer ni difundir sin la autorización competente (conocería pues la prohibición), al inducírsele a error debido a la existencia de la autorización, acabó creyendo que los datos que se le proporcionaban no eran reservados (elemento del tipo penal) y que, por lo tanto, no incurría al utilizarlos en una conducta prohibida en el caso concreto. Este error resulta todavía más comprensible si se pondera que los datos facilitados no se refieren al ámbito más sustancial o restringido del derecho a la intimidad».*

En cuanto a si este error tiene naturaleza de error vencible o no, ha de decirse que es indiferente, a efectos de pena, puesto que en ambos casos la consecuencia es la impunidad. *«Y ello porque* —como señala el FJ 3.º de la SAP de Madrid de 15 de abril de 1999 (Ar. 1762)— *a tenor de lo dispuesto en el artículo 14.1, último inciso, del Código Penal, en la hipótesis de que consideráramos que el error tiene carácter de vencible, sólo cabría penar la conducta si se admitiera el tipo penal imprudente. Y como esa posibilidad queda descartada al no prever esa modalidad el tipo del artículo 197.2, que sólo tipifica la comisión dolosa, ha de calificarse, pues, la conducta en todo caso como atípica».*

Estamos también ante un *error de tipo* cuando el sujeto cree que cuenta con el consentimiento de la víctima. El artículo 197.2 del CP requiere que se ac-

---

39. Artículo 12 del CP: *«Las acciones u omisiones imprudentes sólo se castigarán cuando expresamente lo disponga la Ley».*

túe *«sin autorización»* (40). Hubiera podido decir *«sin consentimiento».* La autorización se entiende que equivale al consentimiento y que excluye la tipicidad. El consentimiento opera, pues, como causa de atipicidad (41).

3. LOS TIPOS AGRAVADOS DEL ARTÍCULO 197 DEL CP

3.1. DIFUSIÓN, REVELACIÓN O CESIÓN DE SECRETOS (ARTÍCULO 197.3 DEL CP)

En los tipos agravados que prevé el Código Penal es fácil identificar cuál es la razón o el fundamento de la agravación. Así, en el apartado 3 del artículo 197 del CP se prevé una pena más grave para el caso de que el sujeto que previamente se ha hecho con los datos los difunda, revele o ceda a un tercero, porque el daño causado al bien jurídico en este caso es mayor.

El artículo **197.3 del CP**, en su apartado primero, contiene un tipo agravado de los anteriores tipos básicos del artículo 197 del CP (apartados 1 y 2) para el supuesto en que el autor realice las anteriores conductas de descubrimiento —apoderamiento de datos o hechos descubiertos o imágenes— y, además, difunda, revele o ceda lo descubierto a terceras personas (42).

Se sobreentiende que el artículo 197.3 del CP queda restringido a aquellas infracciones más graves (AAP de Madrid de 23 de marzo de 1999 —Ar. 1465—, FJ único).

---

40. En parecidos términos está formulado el § 202 del Código Penal alemán. Cfr., por ejemplo, KINDHÄUSER, U.: *Strafgesetzbuch, Lehr - und Praxiskommentar,* 3.ª ed., Nomos, Baden-Baden, 2006, pp. 642 y ss. El citado parágrafo del StGB también exige que se actúe *«sin autorización» (unbefugt).*

41. RUIZ MARCO, F.: *Los delitos contra la intimidad*, 2001, ob. cit., p. 79; GÓMEZ NAVAJAS, J.: *La protección penal…*, ob. cit., 225. No obstante, hay quien considera que lo que excluye es la antijuridicidad. Véase QUERALT JIMÉNEZ, J.J.: *Derecho Penal español,* ob. cit., p. 267.

42. SSTS de 23 de octubre de 2000 (Ar. 8791) y 4 de abril de 2001 (Ar. 2016), SSAP de Madrid de 3 de julio de 2000 (Ar. 3384), de Ciudad Real de 23 de abril (Ar. 443), de Lugo de 29 de diciembre (Ar. 67917) y de Barcelona de 17 de octubre de 2001 (Ar. 16043), de Madrid de 11 de enero (Ar. 71184) y de 31 de julio de 2002 (Ar. 475).

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

Difundir es dar a conocer, poner al alcance de otros los datos personales de una persona, obtenidos ilícitamente [43].

Revelar y *divulgar* o difundir vienen a ser conductas similares, si bien se entiende que la revelación posee un ámbito más reducido que la difusión [44].

Ceder implica transmitir la información a la que se ha accedido o se ha recibido a una o varias personas.

Para que se aprecie la figura cualificada del art. 197.3 CP es necesario que previamente se haya realizado alguna de las conductas tipificadas en los números 1 y 2 del art. 197 CP: apoderamento de documentos o efectos personales, interceptación de telecomunicaciones, utilización de artificios tecnicos de escucha, transmisión, grabación o reproducción de sonido o imagen, apoderamiento, utilización, modificación de datos reservados de carácter personal o familiar o acceso a los mismos.

Un supuesto interesante es el que se plantea con la grabación realizada por cámaras ocultas y la posterior difusión de lo grabado [45]. Salvo que se considere que la difusión de lo grabado redunda en beneficio de la libertad de información, el eterno e inevitable conflicto entre ésta y el derecho a la intimidad se resolverá, por lo general, a favor de esta última.

---

43. El Auto de la AP de Madrid de 2 de septiembre de 2004 (Ar. 264877) reconoce en su FJ 1.º: *«Divulgar es la "acción de comunicar por cualquier medio, sin que se requiera que se realice a una pluralidad de personas, toda vez que la lesión al bien jurídico intimidad se produce con independencia del número de personas que tenga el conocimiento"».* STS de 10 de diciembre de 2004 (Ar. 7917).

44. Véase la SAP de Madrid de 25 de febrero de 2002 (Ar. 149473), el AAP de Sevilla de 4 de junio de 2004 (Ar. 263128), el AAP de Tarragona de 24 de noviembre de 2003 (Ar. 109051), las SSAP de Navarra de 30 de diciembre de 1998 (Ar. 5131) y de Madrid de 11 de julio de 2001 (Ar. 901), la AAP de Córdoba de 22 de julio de 1999 (Ar. 2444), la AAP de Madrid de 19 de octubre de 2004 (Ar. 639) y la SAP de Toledo de 17 de octubre de 2005 (Ar. 261533).

45. SSAP de Madrid de 15 de abril de 1999 (Ar. 1762), 21 de diciembre de 2003 y 1 de marzo de 2004, y STS de 18 de julio de 2005 (Ar. 9146).

El artículo 197.3 del CP, apartado segundo, contiene un tipo autónomo para castigar con pena de prisión de uno a tres años y multa de doce a veinticuatro meses al sujeto que, sin haber tomado parte en el descubrimiento de los datos, hechos o imágenes (por consiguiente, sin necesidad de realizar las conductas de los tipos básicos), pero con conocimiento de su origen ilícito, difunde, revela o cede a terceros datos, hechos o imágenes [46]. Se castiga aquí una conducta que se ha denominado *«receptación de datos íntimos»* y que constituye un tipo atenuado (SAP de Navarra de 30 de diciembre de 1998 —Ar. 5981—). Si quien procede a difundir los datos o las imágenes ignora el origen ilícito de los datos o imágenes, su conducta no será punible. En cambio, es suficiente con que sepa que el proceso de obtención ha sido ilegal. La SAP de La Rioja de 3 de diciembre de 1999 (Ar. 5447) castiga por el artículo 197.3 del CP en un caso en el que se procedió a la difusión de unas fotografías conociendo el origen ilícito de éstas, que habían sido robadas a la denunciante [47].

3.2. EL TIPO AGRAVADO EN FUNCIÓN DEL SUJETO ACTIVO: ARTÍCULO 197.4 DEL CP

El artículo **197.4 del CP** contiene un tipo agravado por la cualificación del autor, es decir, en atención a la condición profesional del sujeto activo del delito (encargado o responsable de ficheros o bancos de datos automatizados, archivos o registros), proyectable a los tipos básicos tipificados en los apartados 1 y 2 del precepto. Se trata de un *delito especial impropio*.

El fundamento de la agravación se basa, pues, en la condición profesional del sujeto activo, que tiene acceso autorizado a los datos pero que, precisamente por ello, está especialmente llamado a velar por la reserva de éstos. Ello limita considerablemente el ámbito de aplicación del tipo cualificado, pues esa persona debe tener encomendada esa responsabilidad, otorgándole una posición de garante de discreción con respecto a los archivos y registros en los cuales constan los datos reservados.

---

46. SSAP de La Rioja de 3 de diciembre de 1999 (Ar. 5447) y de Madrid de 31 de julio de 2002 (Ar. 475).
47. Véase también la SAP de Madrid de 11 de mayo de 2001 (Ar. 198207).

3.3. EL TIPO AGRAVADO EN FUNCIÓN DEL CARÁCTER SENSIBLE DE LOS DATOS Y DEL SUJETO PASIVO: ARTÍCULO 197.5 DEL CP

El artículo **197.5 del CP** contiene un tipo agravado por la cualificación del objeto o la víctima. Así, la pena se impone en su mitad superior cuando el descubrimiento o la revelación afectan *«a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual»* o cuando *«la víctima fuere un menor de edad o un incapaz»* [48].

Si los datos hacen referencia a la ideología, religión, creencias, salud [49], origen racial o vida sexual [50] se aplica el tipo agravado del artículo 197.5 del CP (SAP de Valladolid de 14 de julio de 1998 —Ar. 3221—: vulneración de la intimidad de los miembros de una Asociación de parapléjicos y minusválidos físicos). La pena es la prevista en cada caso para la infracción cometida en su mitad superior (STS de 10 de diciembre de 2004 —Ar. 7917— y 11 de julio de 2001 —Ar. 1056—).

Por su parte, la LOPD considera en su artículo 7.5 que son datos especialmente protegidos:

> *«Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras».*

La Ley 41/2002, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, de 14 de

---

48. STC de 29 de septiembre de 1997 (Ar. 151), SAP de Madrid de 15 de abril de 1999 (Ar. 1762), STS de 9 de octubre de 2000 (Ar. 8755), SSAP de Pontevedra de 18 de mayo de 2001 (Ar. 602), de Tarragona de 4 de febrero (Ar. 99644) y de Zaragoza de 19 de junio de 2002 (Ar. 482) y de 20 de junio de 2003 (Ar. 4359).

49. Véase el AAP de Barcelona de 24 de enero de 2000 (Ar. 958), que declara la atipicidad de la conducta de unos laboratorios que comunican a su cliente, una compañía aérea, el resultado de análisis de sangre y orina encargados por ella con respecto a una trabajadora, contando con la autorización de ésta y sin que conste la difusión a terceros del dato íntimo conocido. El AAP de Madrid de 19 de octubre de 2004 (Ar. 639) ve indicios delictivos en la conducta de proceder a la digitalización y publicación en Internet de una historia clínica del personado como acusación particular, sin autorización ni consentimiento de éste.

50. El Código Penal se refiere no sólo a los datos relativos a la orientación sexual sino a la vida sexual, en general.

noviembre, establece que el acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, investigación o docencia, se rige por la LO 15/1999, y añade que el acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, de modo que se asegure su anonimato, salvo que el propio paciente haya dado su consentimiento. La LOPD establece una regulación muy rigurosa cuando se trata de datos relativos a la salud (51).

Si el autor, además de acceder de forma ilícita a los datos, los difunde, revela o cede, se aplica el tipo agravado del artículo 197.3 del CP. Y, si actúa con fin lucrativo, el artículo 197.6 del CP (STS de 9 de octubre de 2000 —Ar. 8755—).

La SAP de Valladolid de 14 de julio de 1998 (Ar. 3221) apreció este delito en un caso de vulneración de la intimidad de los miembros de una Asociación de parapléjicos.

Otros datos de carácter personal, no especialmente protegidos pero que, sin duda alguna, merecen protección penal, son los relativos a antecedentes penales. A ellos se refiere el artículo136.4 del CP:

> *«4. Las inscripciones de antecedentes penales en las distintas Secciones del Registro Central de Penados y Rebeldes no serán públicas».*

En la actualidad se plantea la cuestión de si se deben hacer públicos los nombres de algunos delincuentes (maltratadores, pederastas…) (52). Dudo de la legitimidad y efectividad de esta medida.

---

51. SSAP de Toledo de 17 de octubre de 2005 (Ar. 261533) y SAP de Madrid de 3 de julio de 2000 (Ar. 3384). DE MIGUEL SÁNCHEZ, N.: «Intimidad e historia clínica en la nueva Ley 41/2004, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica», *Revista Española de Derecho Administrativo,* núm. 117, 2003, pp. 9-31; de la misma autora: *Tratamiento de datos personales en el ámbito sanitario: intimidad «versus» interés público (especial referencia al SIDA, técnicas de reproducción asistida e información genética,* Tirant lo Blanch, Valencia, 2004.

52. GÓMEZ NAVAJAS, J.: «Listas de delincuentes, ¿pena de escarnio público?», en MORILLAS CUEVA, L. (coord.), *Estudios Penales sobre violencia doméstica*, Edersa, Madrid, 2002, pp. 493-508. Crítico también con la medida de publicar listas de delincuentes se muestra ALFONSO LASO, Daniel de: «Intimidad y protección de datos…», ob. cit., pp. 71 y ss.

Es preciso llamar la atención acerca de la necesidad de proteger los datos personales de las víctimas. Así, no es infrecuente que en los medios de comunicación o en los repertorios de jurisprudencia aparezca el nombre completo, incluso, de la víctima de un delito, que a su condición de víctima y a la victimización secundaria que conlleva el proceso judicial, por lo general, añade el atentado a su intimidad que supone la publicación de las sentencias en algunos repertorios de jurisprudencia o bases de datos accesibles al público en general.

Por lo que a la violencia de género se refiere, la LO 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género, establece en su artículo 63:

> *«1. En las actuaciones y procedimientos relacionados con la violencia de género se protegerá la intimidad de las víctimas; en especial, sus datos personales, los de sus descendientes y los de cualquier otra persona que esté bajo su guarda o custodia.*
>
> *2. Los Jueces competentes podrán acordar, de oficio o a instancia de parte, que las vistas se desarrollen a puerta cerrada y que las actuaciones sean reservadas».*

Una cuestión interesante y problemática es la de la publicación de las sentencias, a la que se refieren los artículos 120 y 164.1 de la CE y 86 y 99 de la LOTC), sobre la que, por ejemplo, se ha pronunciado el Tribunal Constitucional en la discutible sentencia 114/2006, en la que estima que no se ve vulnerado el derecho al honor por la publicación de éstas, pero obvia que se puede ver afectado el derecho a la protección de los datos personales [53]. El Tribunal Constitucional se inclina por la publicación íntegra de las sentencias; sin embargo, este principio admite excepciones (artículo 266.1 de la LOPJ, STC 86/1982, FJ 2.º y ATC 425/2003, FJ 5.º).

Muy interesante resulta también todo lo relacionado con la creación de bases de datos genéticas. Debe atenderse a lo dispuesto en la Ley Orgánica

---

53. Crítica con la mencionada sentencia se muestra ARENAS RAMIRO, M.: *«Protección de datos persona˙les y sentencias del Tribunal Constitucional: a propósito de la sentencia del T˙ribunal Constitucional 114/2006», Revista Española de Protección de Datos*, núm. 1, pp. 235-250; GÓMEZ NAVAJAS, J.: *«Listas de delincuentes…»,* ob. cit., pp. 497 y ss.

10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN (54).

La STS de 14 de febrero de 2006 (Ar. 717) distingue en función de si las muestras de ADN son extraídas del cuerpo del acusado o si éstas han sido abandonadas o encontradas por el sospechoso en el lugar del delito. En este caso (conforme a la decisión de la Sala 2.ª del TS, en Pleno no jurisdiccional de 31 de enero de 2006), no se requiere autorización judicial (55).

3.4. EL TIPO AGRAVADO EN FUNCIÓN DE LA FINALIDAD LUCRATIVA: ARTÍCULO 197.6 DEL CP

El artículo **197.6 del CP** contiene un tipo agravado que contempla las anteriores conductas delictivas realizadas con fines lucrativos (56). No se requiere la efectiva obtención del lucro.

> *«6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 y 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 de prisión de cuatro a siete años.*

---

54. Véase MORA SÁNCHEZ, J.M.: *Aspectos sustantivos y procesales de la tecnología del ADN*, Fundación BBVA-Comares, Granada, 2001; ETXEBERRÍA GURIDI, J.F.: *Los análisis de ADN y su aplicación al proceso penal*, Comares, Granada, 2000.

55. Artículo 363 de la LECrim, párrafo 2.º: *«Siempre que concurran acreditadas razones que lo justifiquen, el Juez de Instrucción podrá acordar, en resolución motivada, la obtención de muestras biológicas del sospechoso que resulten indispensables para la determinación de su perfil de ADN. A tal fin, podrá decidir la práctica de aquellos actos de inspección, reconocimiento o intervención corporal que resulten adecuados a los principios de proporcionalidad y razonabilidad»*. Por su parte, el artículo 326 de la LECrim, párrafo 3.º, se pronuncia en los siguientes términos: *«Cuando se pusiera de manifiesto la existencia de huellas o vestigios cuyo análisis biológico pudiera contribuir al esclarecimiento del hecho investigado, el Juez de Instrucción adoptará u ordenará a la Policía Judicial o al médico forense que adopte las medidas necesarias para que la recogida, custodia y examen de aquellas muestras se verifique en condiciones que garanticen su autenticidad sin perjuicio de lo establecido en el artículo 282»*. Véase la STS 501/2005 (Ar. 4190), que consideró —con excesivo rigor, a juicio de algunos— que *«sin resolución judicial que ordenara o autorizara la prueba de ADN, estaríamos ante una prueba irregular, ilícitamente obtenida y, por tanto, sin ningún valor probatorio»*.

56. STS de 20 de junio de 2003 (Ar. 4359), SAP de Madrid de 31 de julio de 2002 (Ar. 475), STS de 9 de octubre de 2000 (Ar. 8755) y SAP de Pontevedra de 18 de mayo de 2001 (Ar. 602).

Ejemplo: Un sujeto se apodera de datos de carácter personal que revelaban el estado de salud y minusvalía física de los miembros de una asociación de parapléjicos y grandes inválidos físicos con el fin de utilizarlos para actividades de contactos, sexo o trabajos fraudulentos (STS 9 de octubre de 2000 —Ar. 8755—).

3.5. EL TIPO AGRAVADO EN FUNCIÓN DE LA CUALIDAD DE FUNCIONARIO DEL SUJETO ACTIVO: ARTÍCULO 198 DEL CP

El artículo **198 del CP** es un tipo agravado para el caso de que las conductas del anterior precepto las realice un funcionario o autoridad.

> *«La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaleciéndose 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 habilitación absoluta por tiempo de seis a doce años».*

Se trata de un *delito especial propio*, a juicio de un sector de la doctrina [57]. Otros autores, sin embargo, lo consideran como un delito especial impropio [58].

La condición de funcionario es de carácter normativo (artículo 24 del CP) y resulta determinante para fundamentar la agravación de la pena [59]. Además, el tipo exige que el sujeto activo actúe fuera del ámbito del ejercicio de la función pública; por ello, la descripción típica exige expresamente que la autoridad o funcionario proceda a realizar su comportamiento concurriendo alguna de las siguientes circunstancias:

---

57. RUIZ MARCO, F., en *Comentarios al Código Penal*, t. VII, Edersa, Madrid, 1999, p. 227.

58. Delito especial *propio* lo consideran RUIZ MARCO, F.: *Los delitos contra la intimidad*, ob. cit., p. 93; y GONZÁLEZ RUS, J.J.: *Derecho Penal Español*, Parte Especial, Dykinson, Madrid, 2005, pp. 341 y ss.; JORGE BARREIRO entiende que es un delito especial impropio, *Comentarios al Código Penal,* tomo VII, Edersa, Madrid, 1999, p. 217. Así, también, GÓMEZ NAVAJAS, J.: *La protección de los datos personales,* ob. cit., p. 396.

59. Véase las SSAP de Madrid de 26 de mayo de 1999 (caso CESID) (Ar. 3043), de Madrid de 19 de junio de 1999 (Ar. 3226), de Baleares de 28 de noviembre de 2000 (Ar. 2997), de Zaragoza de 26 de diciembre de 2002 (Ar. 848), de Albacete de 31 de julio de 2000 (Ar. 2849) y de Álava de 4 de abril de 2003 (Ar. 112624).

a) Fuera de los casos permitidos por la Ley.
b) Sin mediar causa legal por delito.
c) Prevaliéndose de su cargo público.

a) Fuera de los casos permitidos por la Ley.

El funcionario que se extralimita en sus funciones se comporta como un particular (SAP de Madrid de 19 de junio de 1999 —Ar. 3226—). Tiene acceso a los datos por su condición de funcionario público y se aprovecha de esta circunstancia para cometer el delito (SAP de Navarra de 27 de julio de 1999 —Ar. 2857—).

b) Sin mediar causa legal por delito.

Para que se aprecie el art. 198 CP, además de concurrir los demás elementos del tipo, el funcionario o autoridad debe actuar *«sin mediar causa legal por delito»*, a diferencia de lo que exigen los artículos 535 y 536 del CP, insertos en los delitos cometidos por los funcionarios públicos contra la inviolabilidad domiciliaria y demás garantías de la intimidad (dentro del Título XXI —«Delitos contra la Constitución»—, Capítulo V: «De los delitos cometidos por los funcionarios públicos contra la libertad individual»), en los que se requiere *que medie causa por delito*. Aun mediando causa por delito, la conducta deja de estar justificada si la intervención de las comunicaciones no era necesaria o no resulta motivada, proporcionada, ni sometida a la autorización y control judicial pertinentes [60].

La exigencia de que la conducta se realice *«sin mediar causa por delito»,* es decir, fuera del marco de unas diligencias judiciales de investigación, diferencia este delito de los contemplados en los artículos 535 y 536 CP entre los delitos cometidos por funcionarios contra las garantías de la intimidad, que son de mucha menor gravedad. No se ha previsto en el Código Penal una figura delicitiva que castigue los abusos informáticos contra datos reservados realizados por autoridad o funcionario mediante causa por delito. Es ésta una laguna legal que debe soslayarse en una necesaria reforma, lamentablemente aún no prevista.

---

60. GÓMEZ NAVAJAS, J.: «Espionaje telefónico: conculcación de un derecho fundamental», *La Ley* 1998, pp. 1647-1658; MARTÍNEZ MARTÍNEZ, R.: *Tecnologías de la información, policía y Constitución*, Tirant lo Blanch, Valencia, 2001.

Se aplicará el artículo 198 del CP si se atenta a la intimidad personal en el marco de una investigación penal por delito, cuando la intromisión en la intimidad sea gratuita e innecesaria para los fines de la investigación en curso y se realice, por tanto, al margen de ella [61]. En estos casos, no es que el funcionario en el curso de la investigación se extralimite en sus funciones y atribuciones, sino que lleva a cabo intromisiones en la intimidad ajena fuera de sus competencias.

c) Prevaliéndose de su cargo público.

El funcionario o autoridad utiliza su condición de tal para que le resulte más fácil la comisión del delito.

La revelación de secretos realizada por funcionario se castiga en el artículo 417 del CP [62]:

> *«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».*

Quedan castigadas en este precepto conductas tales como [63]:

— Suministrar información reservada contenida en archivos de la Seguridad Social a empresa dedicada a la gestión de cobro de impagados [64]. La

---

61. GONZÁLEZ RUS, J.J., en *Derecho Penal Español*, Parte Especial, ob. cit., p. 373.

62. SSTS de 18 de febrero de 1999 y de 9 de octubre de 2000 (Ar. 8755), SAP de Madrid de 5 de marzo de 2001 (Ar. 165870) y STS de 11 de julio de 2001 (Ar. 1056).

63. Véase GÓMEZ NAVAJAS, J., en ZUGALDÍA ESPINAR, J.M./MARÍN DE ESPINOSA, E.: *Derecho Penal. Parte Especial. Un estudio a través del sistema de casos,* Tirant lo Blanch, Valencia, 2007, pp. 345 y ss. Véanse: STS de 21 de mayo de 1993 (Ar. 4244), SSAP de Madrid de 19 de junio (Ar. 3226) y de Barcelona de 2 de noviembre de 1999 (Ar. 5244) y de Albacete de 31 de julio de 2000 (Ar. 2849), STS de 11 de julio de 2001 (Ar. 1056), SSAP de Zaragoza de 26 de diciembre de 2002 (Ar. 848) y de Madrid de 20 de enero de 2003 (Ar. 530), SSTS de 16 de mayo de 2003 (Ar. 4237), 11 de junio (Ar. 5625) y 7 de diciembre de 2004 (Ar. 469), SAP de Baleares de 19 de mayo de 2005 (Ar. 142755), SSTS de 18 de julio de 2005 (Ar. 9146) y 19 de junio de 2006 (Ar. 4929).

64. De un supuesto similar se ocupa la STS de 7 de diciembre de 2004 (Ar. 469). Véase también la SAP de Madrid de 20 de enero de 2003 (Ar. 530), que castigó a un funcionario del INSS que proporcionó datos personales contenidos en el sistema informático de la Seguridad Social relativos a particulares o empresas a cambio de una retribución económica.

SAP de Madrid de 31 de diciembre de 2003 (Ar. 643) castigó por delito continuado de cohecho en concurso ideal con otro delito continuado de descubrimiento y revelación de secretos, concurriendo la atenuante analógica de vulneración del derecho a un proceso sin dilaciones indebidas. El Tribunal Supremo estimó la atenuante como muy cualificada.

No cabe apreciar el error porque quien paga para obtener determinados datos que no puede obtener de otra manera lícita no ignora que se trata de objetos protegidos especialmente (SAP de Zaragoza de 26 de diciembre de 2002 —Ar. 848— y STS de 11 de junio de 2004 —Ar. 5625—).

— Informar a un amigo de antecedentes policiales de numerosas personas a cambio de precio, con el fin de valorar su contratación para la empresa de éste (SAP de Albacete de 31 de julio de 2000 —Ar. 2849— y STS de 16 de mayo de 2003 —Ar. 4237—).

— Obtener, usando las claves de otros compañeros, cerca de cuarenta hojas del padrón de distintas personas (STS de 11 de julio de 2001 —Ar. 1056— y SAP de Madrid de 19 de junio de 1999 —Ar. 3226—) [65].

Es muy frecuente que este delito concurra con el de cohecho (artículo 419 del CP). Sujeto pasivo será el titular de los datos personales (tercero) que, por regla general, será también perjudicado [66]. No es aplicable el perdón del ofendido (STS de 11 de junio de 2004 —Ar. 5625—).

4. LA PROTECCIÓN PENAL DE LOS DATOS DE LAS PERSONAS JURÍDICAS

El artículo **200 del CP** contempla una cláusula de extensión de la tutela penal de la intimidad a los datos reservados de las personas jurídicas:

---

65. La SAP de las Islas Baleares de 28 de noviembre de 2000 (Ar. 32071) castigó por un delito del artículo 198 del CP a un funcionario que para conocer el domicilio de una señora, con el fin de mandarle flores y declararle su amor, utilizó los datos de su domicilio obrantes en el Padrón Municipal de Habitantes. Lo noble del fin no justificó los medios.

66. HUERTA TOCILDO, S./ANDRÉS DOMÍNGUEZ, A.C.: «Intimidad e informática», ob. cit., p. 65; JORGE BARREIRO, A.: *Comentarios*, ob. cit., 1999, p. 128.

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

A pesar de que pudiera, en un principio, llamar la atención que se considere a las personas jurídicas como sujeto pasivo de los delitos contra la intimidad, el Tribunal Constitucional ya ha reconocido en diversas ocasiones derechos fundamentales a las personas jurídicas [(67)].

Los datos de las personas jurídicas se encuentran protegidos en el artículo 200 del CP, que no tutela información de contenido societario o empresarial [(68)]. Hay que interpretar que la tutela de los datos o informaciones de tipo societario o empresarial en sentido estricto no debe incluirse en este precepto, sino en los delitos relativos al mercado (artículos 278 y ss. del CP) [(69)].

La intimidad es un bien jurídico difícilmente predicable de las personas jurídicas. De ahí que MORALES PRATS entienda que lo que se protege en este precepto son datos de personas jurídicas con trascendencia en la intimidad de las personas físicas [(70)].

El AAP de Madrid de 28 de abril de 1999 (Ar. 1890) declara:

> *«Si bien pudiera plantearse alguna duda en relación con el artículo 200 del Código Penal al referirse ésta a "datos reservados de las personas jurídi-*

---

67. Véase, por ejemplo, la STC 214/1991, de 11 de noviembre (caso León Degrelle). Véase CARMONA SALGADO, C.: «El significado personalista del honor en la Constitución y su relación con algunos delitos del Código Penal», *CPC* 41 (1990), pp. 261-275; de la misma autora: «Conflicto entre la libertad de expresión y el derecho al honor. (Comentario a la sentencia del Tribunal Constitucional de 11 de noviembre de 1991)», *CPC* 47 (1992), pp. 573-580; LÓPEZ PEREGRÍN, C.: *La protección penal del honor de las personas jurídicas y los colectivos*, Tirant lo Blanch, Valencia, 2000. Esta autora reconoce a las personas jurídicas derecho a la intimidad en la medida en que *«tienen derecho tanto a controlar la información sobre sí mismas que circula en la sociedad como a disponer de un lugar en el que ejercer con libertad su actividad social sin injerencias y sin conocimiento por parte de terceras personas ajenas»* (ob. cit., p. 57).

68. SAP de Albacete de 31 de julio de 2000 (Ar. 2849), SSTS de 16 de mayo de 2003 (Ar. 4237) y 7 de diciembre de 2004 (Ar. 541756). En este caso, los datos eran relativos a altas y bajas en la Seguridad Social, prestaciones que percibían, deudas, domicilios particulares y laborales, categoría profesional; STS de 11 de julio de 2001 (Ar. 1056): obtener usando las claves de otros compañeros hojas del padrón correspondiente a diversas personas, cuyo destino final se ignora.

69. SAP de Alicante de 22 de marzo de 1999 (Ar. 612).

70. MORALES PRATS, F.: *Comentarios a la Parte Especial del Derecho Penal,* ob. cit.

cas", decir que aunque en este precepto el Código penal extienda la tutela brindada al derecho a la intimidad de las personas físicas a las jurídicas —frente a conducta de descubrimiento, revelación o cesión de datos reservados pertenecientes a estas últimas— se entiende que sólo es posible aplicar dicha cláusula extensiva cuando la conducta consistente en descubrir, divulgar o ceder los secretos o datos reservados pueda afectar a la intimidad personal de terceros o a los propios individuos que forman parte de la correspondiente asociación o fundación. Todo lo anterior se fundamenta en el entendimiento del derecho a la intimidad personal como un bien de naturaleza personal cuya titularidad corresponde exclusivamente a las personas físicas (SSTC 231/1988 y 139/1995) [71]*. En definitiva, no se trata en el artículo 200 del Código Penal de proteger aquellos secretos de empresa cuyo descubrimiento lesionaría otros bienes jurídicos distintos a la intimidad personal».*

Por consiguiente, se entiende, por lo general, que el artículo 200 del CP debe integrarse exclusivamente con aquellos datos reservados de las personas jurídicas que tengan trascendencia para la intimidad de las personas físicas (por ejemplo datos de los socios, directivos, empleados, etc.). Y es que, como indica el AAP de Madrid de 28 de abril de 1999 (Ar. 1880, FJ 1.º), *«se entiende que sólo es posible aplicar dicha cláusula extensiva cuando la conducta consistente en descubrir, divulgar o ceder los secretos o datos reservados pueda afectar a la intimidad personal de terceros o a los propios individuos que forman parte de la correspondiente asociación o fundación. Todo lo anterior se fundamenta en el entendimiento del derecho a la intimidad personal como un bien de naturaleza personal cuya titularidad corresponde exclusivamente a las personas físicas (SSTC 231/1988 y 139/1995)»*.

En la doctrina hay, sin embargo, quien sostiene que las personas jurídicas tienen intimidad (criterios de administración, control, aspectos contables, infracciones…). Sin embargo, estos aspectos más bien formarían parte del secreto de empresa, protegido, como se ha indicado, en el art. 278 CP. A juicio de

71. ATC 257/1985, de 17 de abril, FJ 2.º: *«el derecho a la intimidad que reconoce el artículo 18.1 de la CE por su propio contenido y naturaleza, se refiere a la vida privada de las personas individuales, en la que nadie puede inmiscuirse sin estar debidamente autorizado, y sin que, en principio, las personas jurídicas, como las sociedades mercantiles, puedan ser titulares del mismo»*. Véase, también, no obstante, la STC 137/1985, de 17 de octubre, en la que el Tribunal Constitucional reconoció el derecho fundamental a la inviolabilidad del domicilio.

RUIZ MARCO, el artículo 200 del CP tutela la intimidad de las personas físicas en supuestos en los que los datos estén bajo control de personas jurídicas. JORGE BARREIRO señala contundente:

> *«la intimidad personal, derecho de la personalidad y bien jurídico protegido en el Título X del Libro II del C.p., difícilmente se le podrá aplicar a las personas jurídicas y, por lo tanto, el ámbito de aplicación de la cláusula extensiva prevista en el artículo 200 del C.p. sólo podrá tener sentido y operatividad en cuanto a través de la conducta típica se pueda ver afectada la intimidad personal de terceros o personas físicas integrantes de la correspondiente persona jurídica. Otra cosa, bien distinta, es que, a la luz de las nuevas reflexiones del T.C. sobre el significado del derecho al honor y la inclusión de las personas jurídicas en su ámbito de protección (SS.TC. 139/1995 y 183/1995), se llegue a postular la posible aplicación a las personas jurídicas de un concepto amplio de intimidad»* (72).

Es posible, no obstante, defender que las personas jurídicas tienen derecho a mantener una esfera de reserva y confidencialidad y a preservar datos que les conciernan (y no constituyan estrictamente secreto de empresa). El objeto de protección del artículo 200 del CP está constituido por informaciones que no atañen directamente a las personas físicas que componen la persona jurídica (que es un ente autónomo y distinto de éstas) ni puede considerarse, propiamente, secreto empresarial (73). Y nada impide que puede considerarse a las personas jurídicas como titulares del derecho a la autodeterminación informativa.

El consentimiento opera como causa de atipicidad (74). La autorización o consentimiento han de ser concedidos por las personas físicas a las que afectan las conductas tipificadas en el Capítulo I del Título X Arts. 197 a 199 CP) (75).

---

72. JORGE BARREIRO, A.: «Artículo 200», *Comentarios al Código Penal*, t. VII, p. 278. Véase, a favor de un *forum internum* frente a intromisiones ilegítimas, ISENSEE: *Anwendung der Grundrechte auf juristische Personen*, ISENSEE/KIRCHHOF. Puede verse la STC 23/1989, de 2 de febrero, donde se reproduce el artículo 19.3 de la Ley Fundamental de Bonn (*Grundgesetz* o Constitución alemana): *«los derechos fundamentales rigen también para las personas jurídicas en la medida en que, por su naturaleza, resulten aplicables a ellas».*

73. GÓMEZ NAVAJAS, J.: *La protección de los datos personales,* ob. cit., pp. 167 y ss.

74. JORGE BARREIRO, A.: *Comentarios*, ob. cit., p. 279; CARBONELL/MATEU: *Comentarios* I, p. 1008; LÓPEZ BARJA/PÉREZ DEL VALLE: *Código Penal II*, p. 2334.

75. RUIZ MARCO, F.: *Comentarios al Código Penal*, t. VII, ob. cit., p. 288.

5. JUSTIFICACIÓN, CULPABILIDAD Y CIRCUNSTANCIAS

Las distintas conductas tipificadas en el art. 197 CP han de llevarse a cabo *sin la autorización del sujeto pasivo*. Actuar con autorización puede considerarse una especial causa de justificación, que excluye la antijuridicidad (RUIZ MARCO, 2001, 85) o un elemento negativo del tipo, que excluye la tipicidad (STS de 18 de febrero de 1999 —Ar. 510— y SAP de Madrid de 15 de abril de 1999 —Ar. 1762—) [(76)], lo cual tiene transcendencia a efectos de error.

Como opinan CARBONELL y GONZÁLEZ CUSSAC, se debe proteger la intimidad salvo que ésta entre en conflicto con otro bien jurídico preponderante (investigación de un delito, salud pública…) [(77)].

Puede, eventualmente, invocarse el ejercicio legítimo de un derecho, de modo tal que la conducta quede justificada por concurrir la causa de justificación del artículo 20.7 del CP (STS de 18 de febrero de 1999 —Ar. 510—) [(78)]. El derecho a comunicar libremente información veraz puede operar como causa de justificación [(79)] [artículo 20.7.º del CP, en relación con el artículo 20.1.d) de la CE, SAP de Madrid de 15 de abril de 1999 —Ar. 1762—). Se plantea un conflicto entre dos derechos fundamentales (el derecho a comunicar información veraz y el derecho a la autodeterminación informativa). El Tribunal Constitucional se ha ocupado en numerosas resoluciones del derecho fundamental a comunicar y recibir libremente información [(80)]. Es doctrina reiterada del Tribunal Constitucional que *«el derecho a la intimidad no es absoluto, como no es ninguno de los derechos fundamentales, pudiendo ceder ante intereses cons-*

---

76. STS de 18 de febrero de 1999, FJ 1.º, y SAP de Madrid de 15 de abril de 1999 (Ar. 1762). Así también JORGE BARREIRO, A., en *Comentarios*, RODRÍGUEZ MOURULLO (dir.), Civitas, p. 573.

77. No apreció esta eximente la SAP de Barcelona de 10 de marzo de 2006 (Ar. 510). Véase la SAP de Málaga de 2 de marzo de 1999 (Ar. 1163), en la que se utilizan datos económicos del ex marido para ejercer un derecho legítimo como es la obtención de gananciales, lo que motiva que la sentencia sea absolutoria y no aprecie un delito del artículo 197.3 del CP.

78. CARBONELL MATEU, J.C. y GONZÁLEZ CUSSAC, J.L., en AA.VV.: *Derecho Penal. Parte Especial,* ob. cit., pp. 324 y ss.

79. STS de 18 de febrero de 1999, que revocó la SAP de Las Palmas de 15 de noviembre de 1997, en la que se había absuelto al imputado por entender que no actuó con la especial intención de perjudicar que requiere el tipo; SAP de Madrid de 15 de abril de 1999 (Ar. 1762), SSTC 6/1998, de 21 de enero, 105/1983, de 23 de noviembre, STEDH *(caso Lingens)* de 8 de julio de 1996, 159/1986, 51/1989 y 20/1990, 85/1992, de 8 de junio.

80. SSTC 107/1988, 171/1990, 172/1990, 214/1991, 40/1992. 85/1992, 15/1993, 178/1993, 41/1994, 173/1995.

titucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho» (SSTC 57/1994, de 28 de febrero y 143/1994, de 9 de mayo; por todas, 2000/98, de 10 de abril).

La STS de 18 de febrero de 1999 (Ar. 510) apreció la **eximente incompleta de cumplimiento de un deber** en el caso de un periodista que publicó en un periódico unos datos obtenidos de archivo informático en los que se hacía constar que dos internos de un centro penitenciario padecían SIDA y trabajaban en la cocina.

Por lo que se refiere a la *culpabilidad,* y, en concreto, a la previa y necesaria comprobación de la imputabilidad del sujeto activo, es posible estimar la eximente de anomalía psíquica (STS de 18 de octubre de 2002 —Ar. 9128— y SAP de Barcelona, de 12 de diciembre de 2003 —Ar. 50—, 21.1.ª y 20.1.ª del CP).

Se desestima con frecuencia el **error de prohibición** (81). Así, la SAP de La Rioja de 3 de diciembre de 1999 (Ar. 5447), citada anteriormente, declara a este respecto:

> *«no existe error alguno de prohibición, ya que si bien podría desconocer el acusado los perfiles exactos de un tipo penal, o incluso su existencia como tal delito, no parece que pudiera desconocer, y por ello no se le exime de responsabilidad, que la conducta de mostrar una documentación tan comprometedora, a sabiendas de su origen ilícito, era una conducta que no mereciera reproche alguno y el mismo calificativo que se hace a su procedencia»* (FJ 1.º).

No es probable ni creíble que una persona invoque que desconocía la ilicitud de su conducta cuando de obtener datos reservados se trata. Cualquier persona con mediana inteligencia tendría conciencia de la ilicitud de dicho comportamiento. Si las conductas son realizadas por un detective (82), por regla general, no se aprecia el error de prohibición porque el detective, para llegar a serlo, ha debido obtener la Diplomatura de Criminología, lo que implica unos conocimientos en Derecho Penal que excluyen el error alegado.

---

81. SAP de Barcelona de 10 de marzo de 2006 (Ar. 510).

82. SSAP de Barcelona de 10 de marzo de 2006 (Ar. 510) y de Pontevedra de 18 de mayo de 2001 (Ar. 602).

Como circunstancia modificativa de la responsabilidad criminal se puede apreciar la atenuante analógica de ludopatía (SJP de Badajoz de 15 de febrero de 2006 —Ars. 46 y 193—). Alguna vez se ha apreciado la atenuante de arrepentimiento (SAP de Málaga de 28 de enero de 2005 —Ar. 140119— por haber procedido el culpable a desinfectar el ordenador. Procede en algunos casos aplicar al inculpado la atenuante 5.ª del artículo 21 del CP, al haber procedido a la inmediata devolución de la documentación [83].

No apreció la atenuante de arrebato u obcecación la SAP de Gerona de 14 de noviembre de 2005 (Ar. 15) al considerar que la separación matrimonial no es estímulo suficiente para justificar la conducta llevada a cabo por el acusado.

6. ¿DELITO DE TENDENCIA O DE RESULTADO?

La exigencia de que la conducta se realice *en perjuicio de tercero* se interpreta como un elemento subjetivo del injusto, junto al dolo [84]. Se entiende que es necesario que el sujeto actúe con ánimo de causar un perjuicio, pero no se requiere que éste se llegue a causar. El perjuicio puede ser de cualquier clase, aunque, en principio, se piense que se refiere al de índole económica. La SAP de Valladolid de 14 de julio de 1998 (FJ 1.º —Ar. 3221—) señala:

> *«Tampoco resulta obstáculo alguno para la aplicación del precepto, la alusión al perjuicio de tercero, del artículo 197.2, toda vez que ello no puede interpretarse como producción de un perjuicio económico o patrimonial concreto o determinado para con los interesados, sino que el perjuicio debe entenderse producido desde el momento en que con ello se invade la esfera de la intimidad personal o familiar, constitucionalmente protegida, para despenalizar, en su caso, los supuestos en que dicho apoderamiento, utilización o acceso, resulte inocuo o intrascendente para sus titulares en sus derechos de intimidad»* [85].

---

83. Conforme a las reglas para la individualización de la pena, en virtud del artículo 66.2.º del CP, procede imponer la pena en su grado mínimo.

84. MUÑOZ CONDE, F.: *Derecho Penal, Parte Especial*, Tirant lo Blanch, Valencia, 2007, p. 265.

85. SSTS de 18 de febrero de 1999, 9 de octubre de 2000 (Ar. 8755) y 11 de julio de 2001 (Ar. 1056).

La expresión *«en perjuicio de»* parece exigir un ánimo o especial intención de perjudicar al titular de los datos o a un tercero. El sujeto ha de realizar la conducta *«para descubrir»,* con la finalidad de conocer los secretos de otro o vulnerar su intimidad —*animus scienci*— (86). MORÓN ha criticado la exigencia de este elemento subjetivo. También la STS de 18 de febrero de 1999 (Ar. 510) entendió que esta expresión no implicaba una especial tendencia o motivación (87) sino que *perjuicio* se refiere al resultado de la acción (88). La acción debe ser idónea para lesionar la intimidad. También para algunos autores es un delito de resultado (89). Un sector de la doctrina interpreta el perjuicio como un elemento objetivo que debe ser abarcado por el dolo del autor y no como un elemento subjetivo del tipo que defina el móvil del autor, que no tiene por qué ser el de causar un perjuicio. Éste es interpretado como una exigencia objetiva compatible con el dolo eventual (90).

Es posible afirmar que *«el delito se consuma tan pronto el sujeto activo "accede" a los datos»* (STS de 18 de febrero de 1999, y AAP de Madrid de 2 de septiembre de 2004, FJ 1.º), pues sólo con eso se quebranta la reserva de éstos. Por tanto, no es necesaria la producción del perjuicio para entender consumado el delito (SAP de Valladolid de 14 de julio de 1998 —FJ 1.º, Ar. 3221—). Sin embargo, para la STS de 18 de febrero de 1999, como el delito se consuma tan pronto el sujeto conoce los datos y los tiene a su disposición, pues sólo con eso ha quebrantado la reserva, se debe entender que la norma requiere la existencia de un perjuicio añadido para que la violación de la reserva integre el tipo. Y este perjuicio puede afectar al titular de los datos o a un tercero. Esta sentencia reconoce que no es fácil determinar cuándo el desvelamiento de un dato personal produce ese perjuicio, pero apunta que puede entenderse producido siempre que se trate de un dato que el hombre medio de nuestra cultura considera *«sensible»* por ser inherente al ámbito de su intimidad más estricta, o sea, un dato perteneciente al reducto de los que

86. SSTS de 10 de septiembre de 1997 (Ar. 6375) y 29 de septiembre de 1998 (Ar. 6974), SSAP de Asturias de 27 de julio de 1998 (Ar. 4821) y de Alicante de 22 de marzo de 1999 (Ar. 612), STS de 9 de octubre de 2000 (Ar. 8755).

87. JAREÑO LEAL, Á./DOVAL PAÍS, A.: «Revelación de datos personales…», ob. cit., pp. 1490 y ss.

88. Véase la STS 14 de septiembre de 2000 (Ar. 7942). JAREÑO LEAL, Á./DOVAL PAÍS, A.: «Revelación de datos personales…», ob. cit.; JORGE BARREIRO, A.: *Comentarios*, ob. cit., 1999, p. 134.

89. QUERALT JIMÉNEZ, J.J.: *Derecho Penal español*, ob. cit., p. 267.

90. JORGE BARREIRO, A.: *Comentarios*, ob. cit., 1999, p. 136.

normalmente se pretende que no trasciendan fuera de la esfera en que se desenvuelve la privacidad de las personas y de su núcleo familiar.

En algunas sentencias se interpreta que el artículo 197.2 del CP es un delito doloso pero no de tendencia y, por tanto, basta con que el sujeto se represente la posibilidad de que cualquier persona pueda resultar afectada por la utilización de los datos, sin exigir un ánimo específico de perjudicar a tercero (SSTS de 18 de febrero de 1999 y 9 de octubre de 2000). El AAP de Madrid de 2 de septiembre de 2004 (Ar. 264877) en su FJ 1.º, reconoce, en un caso de acceso a cuenta de correo electrónico:

> *«respecto al "iter criminis", es una figura delictiva que se integra en la categoría de los delitos de intención, y en la modalidad de delito que incluye 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».*

Desde mi punto de vista, la presencia en el tipo de un elemento subjetivo restringe el ámbito de aplicación de la norma penal, en este caso del artículo 197.2 del CP. Y ello por la razón de que conductas que, de no exigirse dicho elemento o intención tendrían la consideración de delito quedan fuera de la cobertura del tipo penal si se exige por parte de éste una intención y la misma no concurre en el caso concreto. Este efecto, que puede interpretarse como positivo, en tanto que limita la intervención punitiva, tiene como contrapartidas: a) la difícil determinación de la concurrencia o no de la intención en cada caso (dificultad de prueba); b) la impunidad de las conductas en las que no se corrobore el ánimo de perjudicar a un tercero.

Se suele entender que la exigencia de una especial intencionalidad en el sujeto activo implica dolo directo, excluyéndose el dolo eventual [91]. Éste no debe excluirse, sin embargo, y considero que es posible cometer las conductas del artículo 197.2 CP a título de dolo eventual [92].

---

91. ORTS BERENGUER, E./ROIG TORRES, M.: *Delitos informáticos…,* ob. cit., p. 28.

92. Desde una teoría cognitiva del dolo no plantea dificultad alguna esta postura. Despojado del elemento volitivo, el dolo (directo o eventual) requiere, únicamente, el conocimiento de los elementos del tipo.

7. PENA CORRESPONDIENTE A LOS DELITOS QUE AFECTAN A DATOS PERSONALES

Las penas que el Código Penal prevé en el art. 197 para las conductas que atentan contra los datos personales son de uno a cuatro años de prisión y multa de 12 a 24 meses para las previstas en los números 1 y 2. Por lo que a los tipos agravados se refiere, las penas son las siguientes:

— Prisión de dos a cinco años si se difunden, revelan o ceden los datos (artículo 197.3 del CP).

— Multa de 12 a 24 meses si se difunden, revelan o ceden los datos con conocimiento de su origen ilícito pero sin haber tomado parte en su descubrimiento (artículo 197.3 del CP, párrafo 2.º).

— Prisión de tres a cinco años, si las conductas de los números 1 y 2 son realizadas por las personas encargadas o responsables de los ficheros; si se procede a la revelación por parte de éstos, la pena se impondrá en su mitad superior (artículo 197.4 del CP).

— Penas previstas en su mitad superior si los datos atañen a la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima es menor o incapaz (artículo 197.5 del CP).

— Penas previstas en su mitad superior si los hechos se realizan con fin lucrativo. Y si, además, afectan a datos de los protegidos en el número 5 del artículo 197 del CP, la pena será de prisión de cuatro a siete años.

— Si las conductas del artículo 197.2 del CP son llevadas a cabo por la autoridad o funcionario (art. 198 CP), la pena será la que corresponda, en función del tipo que haya cometido, en su mitad superior y la de inhabilitación absoluta por tiempo de seis a doce años.

8. CUESTIONES PROCESALES

8.1. PERSEGUIBILIDAD

Finalmente, el artículo 201 del CP establece las reglas para la perseguibilidad de estas conductas [93].

> *«1. Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquella sea menor de edad, incapaz o una persona desvalida [94], también podrá denunciar el Ministerio Fiscal.*
>
> *2. No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.*
>
> *3. El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal o la pena impuesta, sin perjuicio de lo dispuesto en el párrafo del número 4.º del artículo 130».*

Los delitos contenidos en el Capítulo I del Título X son delitos de los denominados delitos semi-privados, pues para proceder a su persecución es necesario un requisito procesal. En concreto, *estos delitos requieren la denuncia de la persona agraviada o de su representante legal.* Son, por tanto, delitos perseguibles a instancia de parte (como sucede en los artículos 191, 215 ó 228 del CP). Parece aconsejable, desde un punto de vista político-criminal, que estos delitos no estén sometidos a las reglas generales de perseguibilidad, ya que en muchos casos el titular del bien jurídico puede preferir no perseguir el delito ante la publicidad que conlleva el proceso penal. Además, la intimidad es un derecho de la personalidad disponible. No obstante, se prevén dos excepciones:

---

93. Sobre ésta y otras cuestiones procesales relacionadas con estos delitos véase GÓMEZ NAVAJAS, J.: *La protección de los datos personales,* ob. cit., pp. 431 y ss.

94. SAP de Pontevedra de 18 de mayo de 2001 (Ar. 602).

1.ª El artículo 201.2 del CP excluye del requisito de previa denuncia de la parte agraviada los delitos contra la intimidad cometidos por los funcionarios públicos, con prevalimiento de su cargo, esto es, los hechos descritos en el artículo 198 del CP, y

2.ª aquellos supuestos en los que el delito contra la intimidad afecte a los intereses generales o a una pluralidad de personas (véanse los artículos 287 y 296 del CP), por ejemplo, abusos informáticos sobre datos personales que afecten a una pluralidad de personas o fugas masivas de datos personales a «paraísos informáticos». Dadas las dimensiones que pueden adquirir este tipo de comportamientos, que afectan a la libertad informática (y a la intimidad) de una multitud de ciudadanos, es lógica esta previsión del artículo 201.2 del CP, que faculta al Ministerio Fiscal para proceder de oficio.

No obstante, la doctrina penal critica, con razón, estas cláusulas generales indeterminadas previstas por el legislador español, al referirse a la afectación de *«intereses generales»* o a *«una pluralidad de personas»,* porque esta técnica legislativa atenta contra las más elementales exigencias de seguridad jurídica, al tiempo que estima que tales cláusulas deben ser objeto de una interpretación doctrinal restrictiva [95].

8.2. EFICACIA DEL PERDÓN DEL OFENDIDO

Finalmente, el artículo 201.3 del CP prevé el perdón del ofendido [96]. En este delito el perdón del ofendido funciona como una causa de extinción de la responsabilidad criminal. Esta medida se adopta sin perjuicio de lo dispuesto en el artículo 130.5 del CP, apartado segundo, respecto a las garantías previstas para los casos en los que la víctima fuere un menor o incapaz. El art. 201 CP se remite por error al apartado 4.º del art. 130 CP cuando, en realidad, es el apartado 5 el que se refiere al perdón del ofendido.

---

95. JORGE BARREIRO, A.: «Artículo 200», *Comentarios,* ob. cit., p. 282. CARBONELL/GONZÁLEZ CUSSAC: *Comentarios*, I, p. 1011; LOZANO MIRALLES: *Compendio…*, Parte Especial II, p. 208; JORGE BARREIRO, A.: «El delito de revelación de secretos (profesionales y laborales)», *LL*, 1996, p. 1034.

96. STS de 9 de octubre de 2000 (Ar. 8755).

«5. Por el perdón del ofendido, cuando la Ley así lo prevea. El perdón habrá de ser otorgado de forma expresa antes de que se haya iniciado la ejecución de la pena impuesta. A tal efecto, declarada la firmeza de la sentencia, el Juez o Tribunal sentenciador oirá al ofendido por el delito antes de ordenar la ejecución de la pena.

En los delitos o faltas contra menores o incapacitados, los Jueces o Tribunales, oído el Ministerio Fiscal, podrán rechazar la eficacia del perdón otorgado por los representantes de aquellos, ordenando la continuación del procedimiento, con intervención del Ministerio Fiscal, o el cumplimiento de la condena.

Para rechazar el perdón a que se refiere el párrafo anterior, el Juez o Tribunal deberá oír nuevamente al representante del menor o incapaz».

La eficacia del perdón es coherente con el carácter disponible del bien jurídico *intimidad* pero plantea problemas cuando el bien jurídico se configura como público. También es dudosa la operatividad del perdón cuando el delito afecta a una pluralidad de personas (SAP de Valladolid de 14 de julio de 1998 —Ar. 3221—, FJ 1.º, y STS de 9 de octubre de 2000 —Ar. 8755—). La doctrina ha criticado la excesiva relevancia concedida al perdón en estos delitos, que puede otorgarse incluso después de haberse dictado sentencia condenatoria *«y cuya única justificación, una vez que el ofendido ha soportado las consecuencias gravosas del proceso penal para su intimidad, podrá encontrarse en motivos privados de responsabilidad civil, propiciando así el reprobable tráfico crematístico de los perdones dentro del proceso penal»* [97].

8.3. COMPETENCIA JUDICIAL

El artículo 14 de la LECrim considera como regla preferente para determinar qué juzgado es competente la del *locus delicti commisi*, es decir, el lugar geográfico en el que el delito se haya cometido. Si el lugar en el que se reali-

97. JORGE BARREIRO, A.: «Artículo 200», *Comentarios*, ob. cit., p. 283. SAP de Granada de 3 de abril de 2003 (Ar. 200106).

za la conducta no coincide con el lugar en el que se produce el efecto ilícito el Tribunal Supremo se inclina por considerar que el delito se perpetra en donde se produce el resultado (98).

8.4. UTILIZACIÓN PROCESAL DE PRUEBAS OBTENIDAS VULNERANDO LA INTIMIDAD

Siguiendo «*la doctrina de los frutos del árbol envenenado*», y conforme al artículo 11.1 de la LOPJ, serán nulas las pruebas obtenidas con vulneración de derechos fundamentales (99).

El artículo 579 de la LECrim es el único precepto que contiene una regulación —parca e insuficiente— acerca de la intervención de las comunicaciones (100), que no alude en absoluto a las comunicaciones electrónicas. No debe hacerse esperar por más tiempo una modificación de la ley procesal penal que haga referencia a éstas.

9. REFLEXIÓN FINAL: LOGROS Y DÉFICITS

Es un acierto que el Código Penal se ocupe de la protección de los datos de carácter personal. No podía ser de otro modo si se quieren atajar las conductas que constituyen un abuso de dichos datos y se quiere acompasar el Código Penal al desarrollo de las tecnologías, que representan nuevas vías de

---

98. ATSJ de Cataluña de 11 de diciembre de 2000 (Ar. 83425). Véase GUTIÉRREZ FRANCÉS, M.ª L.: «Problemas de aplicación de la ley penal en el espacio virtual», en *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, ROMEO CASABONA, C.M.ª (coord.), Comares, Granada, 2006, pp. 43 y ss.

99. SSAP de Barcelona de 29 de enero de 2004 (Ar.156554) y de Asturias de 29 de noviembre de 2004 (Ar. 704); AAP de Sevilla de 29 de abril de 2005 (Ar. 142959), SSAP de Madrid de 25 de mayo (Ar. 321) y de 7 de diciembre de 2005 (Ar. 70), y SAP de Barcelona de 10 de marzo de 2006 (Ar. 510).

100. MAGRO SERVET, V.: «La necesaria nueva regulación de las intervenciones telefónicas a raíz de la Jurisprudencia del TEDH, TC y TS», *La Ley* 2004-5, pp. 1564 y ss.; MAZA MARTÍN, J.M.: «La intervención judicial de las comunicaciones a través de Internet», *Cuadernos de Derecho Judicial*, Madrid, 2001, pp. 633 y ss.

comisión delictiva. Sin embargo, el artículo 197.2 del CP necesita de una reforma que clarifique el precepto y lo haga más operativo.

Induce a confusión, y a la consiguiente inseguridad jurídica, la falta de precisión en la descripción de las conductas típicas de la que adolece el artículo 197.2 del CP y la indeterminación acerca de qué se haya de entender por *tercero* y por *perjuicio*.

Igualmente, debería esclarecerse qué se ha de entender por *datos reservados de carácter personal*. Los datos relativos a la comisión de infracciones penales también deberían merecer especial protección y sería conveniente incluir una referencia expresa a los datos genéticos en el artículo 197.5 del CP, como datos merecedores de una protección reforzada, por ser *especialmente sensibles* (101) y por la importancia que están adquiriendo en la actualidad.

La pena prevista para las conductas del artículo 197.2 del CP tal vez debiera ser superior a las señaladas para las conductas del artículo 197.1 del CP, en atención al carácter insidioso de los medios empleados para obtener los datos (102).

Asimismo y como se ha expuesto, no se ha previsto en el ámbito de los delitos cometidos por los funcionarios públicos contra la inviolabilidad domiciliaria y demás garantías de la intimidad (artículos 534-536 del CP, Sección 2.ª, Capítulo V, Título XXI) una figura que castigue los abusos informáticos contra datos reservados realizados por funcionario mediando causa por delito.

Por otra parte, se hace cada vez más evidente y urgente la reforma de la LECrim, concretamente de su artículo 579, para regular la intervención de las comunicaciones electrónicas.

En definitiva: hace falta una mejora de la redacción y de la técnica legislativa de los preceptos con los que en nuestro actual Código Penal se preten-

---

101. GÓMEZ SÁNCHEZ, Y.: «Protección de datos genéticos: nuevos derechos para nuevas biotecnologías», *Revista Española de Protección de Datos*, 1, 2007, pp. 61-91; DE MIGUEL SÁNCHEZ, N.: «Investigación y protección de datos de carácter personal: Una aproximación a la Ley 14/2007, de 3 de julio, de investigación biomédica», *Revista Española de Protección de Datos*, 1, 2007, pp. 143-201.

102. Así opina MORALES PRATS, F.: *Comentarios…*, ob. cit., 6.ª ed., p. 416.

den proteger los datos personales. Esta reforma debería ir acompañada de otra de la LECrim para regular con precisión las intervenciones de las telecomunicaciones. Ello redundaría, sin duda, en una mejor tutela de los datos y en una mayor seguridad jurídica. Ambos objetivos merecen claramente el esfuerzo de emprender dichas reformas. De lo contrario, continuaremos teniendo la sensación de que el Código Penal castiga sólo parcialmente las conductas que atentan contra los datos personales y que sigue habiendo preocupantes vacíos legales y dificultades de persecución de estos delitos, lo que, en un ámbito tan delicado como éste, coloca a los ciudadanos en una situación de indefensión, y, con frecuencia, ante la imposibilidad de detener el impune manejo de datos que les conciernen y que son su baluarte, su misma esencia.