EGUZKILORE
Número 22.
San Sebastián
Diciembre 2008
89 - 115

LA INTIMIDAD Y LOS SECRETOS DE EMPRESA COMO OBJETOS DE ATAQUE POR MEDIOS INFORMÁTICOS[1]

Antonio DOVAL PAIS
Universidad de Alicante

Resumen: En el ámbito de los delitos contra la intimidad y el secreto de empresa, los conceptos de intimidad y secreto poseen puntos de contacto a pesar de referirse a esferas tan diferentes como la persona física y la empresa. A la vista de los pronunciamientos de los juzgados y tribunales en esta materia, se analizan las cuestiones más problemáticas que presentan en la práctica estos delitos, al objeto de poner de manifiesto las posibilidades que ofrece la regulación de estas conductas para la protección de los correspondientes bienes jurídicos frente a los ataques cometidos por medios informáticos, y aportar argumentos que puedan contribuir a esclarecer algunas de las dudas planteadas en este ámbito.

Laburpena: Intimitatea eta enpresa sekretuei buruzko delituen alorrean, bai intimitatea baita sekretuak ere ukitze puntuak dauzkate nahiz eta pertsona fisikoa eta enpresaren gainean mintzatu. Epaitegi eta auzitegiek gai honen inguruan erabaki dutena kontutan harturik, praktikak agertzen dituen arazo nagusienak aztertzen dira, portaera hauen erregulazioak sortzen dituen aukerak nabarmenduz, bai ondasun juridikoen babeserako baita informatika erabiliz egindako erasoen aurrean. Era berean, alor honetan sortzen diren zalantzak argitzen lagunduko duten argumentuak agertzen dira.

Résumé: Dans le domaine des infractions contre l'intimité et les secrets d'entreprise, les concepts d'intimité et du secret ont des points en commun, bien qu'ils se réfèrent à des sphères aussi différentes que la personne physique et l'entreprise. Étant donné les prononcés des tribunaux dans cette matière, on analyse les questions les plus problématiques que ces infractions présentent dans la pratique, afin de mettre en évidence les possibilités qui offre la régulation de ces conduites pour protéger les biens juridiques face aux attaques commises par des moyens informatiques, et apporter des arguments qui peuvent contribuer à éclaircir certains des doutes posés dans ce domaine.

Summary: In the field of crimes against privacy and company secrecy, the terms of intimacy and secrecy are linked in spite of refer to so different spheres like the physic person and the company. Considering the judicial pronouncements on this matter, we analyze the most controversial issues of these crimes in practice,

1. La presente contribución ha sido realizada al amparo de los Proyectos de investigación "Límites sobre la Protección jurídica de la intimidad (SEJ2006-06663/JURI), financiado por el Ministerio de Educación y Ciencia y "Nuevos Conflictos Sociales: el papel de la privacidad. Análisis jurídico, interdisciplinar y comparado" (SEJ2714/2007), financiado por la Consejería de Innovación Ciencia y Empresa de la Junta de Andalucía (véase: http://www.uv.es/limprot).

showing the possibilities that offer the regulation of this conducts to protect corresponding legal rights from computer attacks and, also, exposing arguments that contribute to elucidate the doubts of this field.

Palabras clave: Derecho penal, Criminología, Delitos contra la intimidad, Delitos de espionaje industrial, Descubrimiento y revelación de secretos.

Gako Hitzak: Zuzenbide penala, Kriminologia, Intimitatearen kontrako delituak, Industria espioitza delituak, Sekretuen ezagutza eta agerraraztea.

Mots clef: Droit pénal, Criminologie, Délits contre l'intimité, Délits d'espionnage industriel, Découverte et révélation de secrets.

Key words: Criminal law, Criminology, Privacy crimes, Industrial spying crimes, Discovery and disclosure of secrets.

I. INTRODUCCIÓN

Este trabajo tiene su origen en la participación en la Jornada de Derecho penal sobre los "Retos en la securización de los territorios digitales: delitos informáticos" (celebrada en la UPV/EHU, Leioa, en abril de 2007). El tema propuesto entonces, "Delitos contra la intimidad y el secreto de empresa: descubrimiento y revelación de secretos y espionaje industrial por medios informáticos", se presenta aquí bajo un título distinto. Pero conecta en todo caso dos conceptos, la intimidad y el secreto, que poseen interesantes puntos de contacto a pesar de referirse a esferas tan diferentes como la persona física, por un lado, y la empresa, por otro.

Se trata de conceptos que, aunque estamos acostumbrados a considerarlos muy vinculados entre sí (hablamos a menudo de "secretos de la intimidad" o de que algo pertenece a la intimidad aludiendo a su carácter reservado, sustraído al conocimiento de los demás), no son idénticos, sino que existen entre ellos importantes diferencias.

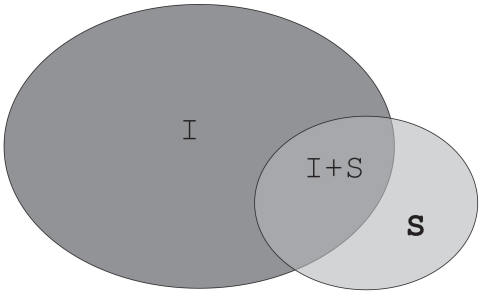
Si nos preguntáramos cuáles son los ámbitos propios de la intimidad y del secreto, podríamos estar de acuerdo en que la intimidad tiene como campo de referencia exclusivo la persona física. Así lo ha considerado también el Tribunal Constitucional desde sus primeros pronunciamientos. Aunque, como ha advertido, esto no significa que no exista un espacio reservado de las sociedades que merezca y deba ser resguardado, pero al margen de la intimidad personal.

¿Y el secreto? Su relación con la intimidad se pone de manifiesto observando el propio contenido (o las manifestaciones) de la intimidad. En efecto, ésta incluye tanto aspectos reservados relativos a la persona (deliberadamente reservados por el titular de la intimidad) como otros sencillamente no compartidos (aunque tampoco, propiamente, "secretos", en el sentido de intencionalmente ocultos). Estos últimos son los que tienen lugar en ámbitos, espacios u ocasiones no compartidos porque casi siempre su campo natural es el privado, y no por otra razón (como, por ejemplo, una conversación cualquiera en familia a la hora de comer u otras actividades cotidianas que se llevan a cabo normalmente en los hogares). Por eso, estas manifestaciones personales pertenecen a la esfera de la privacidad.

A diferencia de la intimidad, el secreto o lo secreto es algo simplemente conocido por alguien, o por algunos, pero desconocido por la mayoría porque está sustraído a su conocimiento (¡la mera ignorancia no hace a lo desconocido "secreto"!). Y puede ser un secreto de la intimidad (sobre aspectos reservados de –o sobre– uno) o un secreto

no relativo a la intimidad, como, por ejemplo, un secreto científico. En consecuencia, el secreto puede referirse a una persona física o jurídica.

De este modo, la relación entre las áreas de la intimidad y el secreto podría representarse mediante el diagrama siguiente:



Conforme a esta representación, existirían, pues, tres distintos ámbitos: uno, de "intimidad (no reservada)" (I), del que formarían parte las manifestaciones más comunes de la vida privada, otro, de "secretos de la intimidad" (I+S), que abarcaría aspectos escogidamente reservados de la vida personal; y, por último, el tercero, de "secretos no de la intimidad" (S) que albergaría aspectos reservados pero no referidos a la persona, y que podrían ser tanto de titularidad de la persona física como de la persona jurídica[2].

El primero y el segundo son claramente campos propios –aunque no exclusivos[3]– de los delitos del artículo 197 (descubrimiento y revelación de secretos, delitos contra la intimidad). Y el tercer sector, el de los secretos no relativos a la intimidad, si bien es claro que constituye el terreno de los delitos de los artículos 278 y siguientes (delitos de descubrimiento y revelación de secretos de empresa), ofrece inmediatamente algunas dudas con respecto a si es también el de ataques contemplados en el artículo 197 y, sobre todo, de los que recoge el artículo 200 del Código penal. Estas dudas se plantean, respectivamente, a raíz de las referencias legales al descubrimiento de *secretos*, en el artículo 197, como posible finalidad con la que se lleven a cabo las conductas, y a la *persona jurídica*, en el artículo 200, como titular (?) de los "datos reservados".

---

2. No obstante, debe tenerse en cuenta que, en realidad, la intersección de los dos círculos no viene delimitada por una línea, sino, más bien, por un trazo borroso en el que resulta discutible el carácter de secreto o no de ciertos elementos. Por ejemplo, el nombre de una persona que le ha dado una información a otra, nombre que éste trata de ocultar, es dudoso que constituya sólo un secreto o que afecte a la intimidad del receptor de la información; o que una carta de la Seguridad Social dirigida al cónyuge sea o no un secreto de la intimidad (al respecto, considerándolo, véase la STS de 23-10-2000).

3. Pues este ámbito también es materia, por ejemplo, de los delitos de allanamiento de morada y puede serlo, incluso, de delitos contra el honor.

Por una parte, la alusión al descubrimiento de secretos junto al móvil alternativo de vulnerar la intimidad en el artículo 197.1 enfrenta al intérprete al dilema de entender, bien que el tipo penal es redundante (es decir, considerando que los secretos no pueden ser –en este contexto– más que secretos de la intimidad), bien que permite como alternativa típica considerar los ataques dirigidos a conocer secretos desvinculados de la intimidad; esto es –como se especifica en la STS de 19 de junio de 2006–, ataques que tienen por objeto proyecciones de la persona o de la personalidad menos esenciales (que la intimidad) y situadas "en el espacio relativamente indiferenciado y más abierto de lo «privado»"[4].

Por otra parte, la aparición de la persona jurídica en el artículo 200 hace pensar de nuevo en la posibilidad de la protección penal de secretos desvinculados de la intimidad, al menos, bajo la premisa de que la persona jurídica haya de ser aquí la persona titular de los "datos reservados".

En todo caso, los contenidos y relaciones de la intimidad y el secreto constituyen en este ámbito elementos claves para la determinación del alcance típico de estos artículos[5].

Pues bien, en el contexto definido como de la "securización de los territorios digitales", el objeto de este trabajo es, precisamente, por un lado, poner de manifiesto las posibilidades que ofrecen los delitos contra la intimidad y los delitos relativos a los secretos de empresa para la protección de los correspondientes bienes jurídicos frente a ataques cometidos por medios informáticos y, por otro, aportar argumentos que puedan contribuir a esclarecer algunas de las dudas que se han enunciado.

Para ello, a partir de las posiciones asumidas, se analizarán las cuestiones más problemáticas que presentan en la práctica unos y otros delitos, a la vista, sobre todo, de los pronunciamientos de los juzgados y tribunales sobre los mismos.

---

4. Al respecto, no obstante, debe tenerse presente que la doctrina y la jurisprudencia mayoritarias consideran que en el contexto de los arts. 197 y ss. la referencia a los "secretos" no puede dejar de entenderse vinculada a la intimidad. Véanse en este sentido, por lo que se refiere a la doctrina, F. Morales Prats en Quintero Olivares, G.(Dir.)/Morales Prats, F. (Coord.): *Comentarios a la Parte especial del Derecho penal*, 5ª ed., Cizur Menor, 2005, pág. 411, A. Jorge Barreiro en Rodríguez Mourullo, G.(Dir.)/Jorge Barreiro, A.(Coord.): *Comentarios al Código penal*, Madrid, 1997, pág. 569, y, con toda contundencia y más referencias, Rueda Martín, Mª. A.: *Protección penal de la intimidad personal e informática (Los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código Penal)*, Barcelona, 2004, págs. 35 y 36. En cuanto a la jurisprudencia, pese a la línea mayoritaria (véase, por ejemplo, la doctrina recogida en la citada STS de 19-6-2006), las referencias a la intimidad y al secreto no dejan de resultar confusas y han dado lugar a que los tribunales hayan estimado que "el art. 197.1 tutela dos distintos bienes que son objeto de la protección jurídico-penal: la salvaguarda de los secretos propiamente dichos y, aparte, la intimidad de las personas, viniendo a representar este tipo penal una especie de desarrollo sancionador a las conductas que vulneren el derecho fundamental a la inviolabilidad de las comunicaciones consagrado en el art. 18 CE como parte integrante del derecho a la intimidad personal del individuo" (STS 23-10-2000, f. de D. segundo, y, siguiéndola, SAP de Albacete de 21-11-2002, f. de D. tercero y SAP de Cádiz de 29-12-2003, f. jco. tercero). Incluso, en alguna ocasión ha considerado que el carácter secreto de los documentos apoderados (agendas profesionales, expedientes, etc. de un despacho de abogados) basta para considerar cometido el delito del art. 197.1 (así, la STS de 14-9-2000, f. de D. tercero).

5. Tal como ha observado, con toda razón, Anarte Borrallo en "Consideraciones sobre los delitos de descubrimiento de secretos (I). En especial, el artículo 197.1 del Código penal", en *Jueces para la Democracia*, núm. 43, marzo de 2002, pág. 52.

II. LOS DELITOS CONTRA LA INTIMIDAD FRENTE A LOS ATAQUES POR MEDIOS INFORMÁTICOS

Los artículos 197 y siguientes del Código penal recogen una serie de conductas de las que se puede decir –simplificando mucho– que consisten bien en el apoderamiento de manifestaciones –o elementos– de intimidad (o secretos), bien en la revelación o difusión de datos o hechos de la intimidad (o secretos).

1. El artículo 197.1: conductas de apoderamiento de e-mails, interceptación de telecomunicaciones y utilización de artificios técnicos

De todos los comportamientos del artículo 197.1 que requieren "apoderamiento", interesan en este marco los tres siguientes: el apoderamiento de mensajes de correo electrónico, la interceptación de las telecomunicaciones y la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o la imagen.

El primero[6] no se refiere al apoderamiento de los e-mails ya impresos en papel (pues estos casos cabrían como "papeles" o "cartas" –y, desde luego, como "otros documentos"–, a los que también se refiere el mismo artículo), sino a los mensajes que se hallan en algún soporte digital (abiertos en la pantalla del ordenador, recogidos en un archivo informático, etc.).

De acuerdo con el sentido gramatical del verbo típico, para el apoderamiento no basta, desde luego, la mera visión del texto del mensaje[7], ni su simple lectura[8] o captación mental[9] directa de la pantalla del ordenador, sino que –también por exigencias de la interpretación sistemática[10]– es preceptivo que pueda afirmarse que el autor ha conseguido el mensaje para sí, utilizando para ello cualquier medio que se lo permita de un modo insidioso. Es decir, quebrantando algún resguardo del sistema para llegar al mensaje[11].

---

6. La referencia a los "mensajes de correo electrónico" en este precepto se debe a la enmienda (núm. 727) presentada al texto original del Proyecto del C.P. por el grupo parlamentario de Izquierda Unida-Iniciativa per Catalunya, que fue aceptada por la Ponencia sin discusión (BOCG, Congreso, Proyectos de Ley, núm. 77-8, pág. 461).

7. De acuerdo con Anarte Borrallo: "Consideraciones sobre los delitos de descubrimiento de secretos (I)", cit., pág. 54, y Jareño Leal, A.: *Intimidad e imagen: los límites de la protección penal*, Madrid, 2008, pág. 46.

8. Como afirma, sin embargo, R. Rebollo Vargas en Córdoba Roda, J./García Arán, M. (Dirs.): *Comentarios al Código penal. Parte especial*, Tomo I, Madrid-Barcelona, 2004, pág. 457.

9. Como considera un sector de la doctrina. Véase, por ejemplo, F. Morales Prats en Quintero Olivares/Morales Prats: *Comentarios a la Parte especial del Derecho penal*, cit., pág. 410, y A. Jorge Barreiro (en Rodríguez Mourullo/Jorge Barreiro: *Comentarios al Código penal*, cit., pág. 567). No obstante, la llamada "captación mental" o "intelectual" no parece que pueda ser algo distinto de la lectura directa del mensaje.

10. Comparando lo que para otros objetos del mismo delito representa la misma conducta (por ejemplo, para las cartas o papeles).

11. Así, Mata y Martín, R.M.: "La protección penal de datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías", en *Revista Penal*, núm. 18, julio 2006, pág. 224 y Jareño Leal: *Intimidad e imagen*, cit., pág. 46. Por ejemplo, consiguiendo por medio de un programa informático copias de los e-mails enviados por otra persona (caso de los hechos de la STS de 21-3-2007).

El Tribunal Supremo ha estimado que también existe apoderamiento, en general, en los casos que denomina de "aprehensión virtual", es decir, cuando el sujeto consigue el contenido del documento "de cualquier forma técnica que permita su reproducción posterior, como por ejemplo mediante su fotografiado" y, también, mediante su fotocopiado[12]. De esta afirmación interesa aquí, en particular, la referencia al fotografiado por su posible aplicación al mensaje de correo electrónico abierto en la pantalla. La diferencia de estos casos con la llamada "captación visual" o, incluso, con la "captación mental" (o "intelectual") inmediata se hallaría en que la imagen así obtenida resulta completamente fiel al documento original y puede merecer mayor credibilidad si se revelase, difundiese o cediese que una mera manifestación del mensaje que fue visto y retenido mentalmente. Pero considero que esto no es lo decisivo para la tipicidad de la conducta conforme al tipo básico, que requiere, más bien, que el apoderamiento sirva para el descubrimiento de los secretos o para vulnerar la intimidad de otro. Efectivamente, en estos casos, si el fotografiado es un medio aplicado por el intruso una vez conocido el contenido o la información relevante del mensaje de correo electrónico, la conducta no será típica. Pero si el empleo del instrumento fotográfico sirviera para conseguir el mensaje de un modo subrepticio y poder después acceder a su contenido, entiendo que la conducta sí reuniría la exigencia típica (como, por ejemplo, si mediante una cámara oculta situada en la mesa de trabajo de la víctima se capta el e-mail o si la rapidez de captación de la imagen por la cámara es decisiva para el apoderamiento). En definitiva, con esta interpretación, se trata de no equiparar las formas de captación no insidiosas de los mensajes con las llevadas a cabo de un modo subrepticio.

Las conductas que recaen sobre mensajes de correo electrónico se vienen presentando, sobre todo, en el ámbito –y la jurisdicción– laboral, a propósito de los controles que efectúan las empresas para verificar el uso de los medios puestos a disposición de los trabajadores (de cuyas constataciones derivan a menudo despidos); aunque por lo general se trata de conductas de acceso a los e-mails o de su interceptación y no de conductas de apoderamiento. Para decidir, tanto en el ámbito laboral como en el penal, sobre estos casos es absolutamente fundamental[13] conocer si el trabajador dio o no su consentimiento para dichos controles, porque en el ámbito en el que desempeña su trabajo no pierde, sin más, su intimidad. Cuando el trabajador dé su consentimiento en el contrato de trabajo para que la empresa realice los controles del uso del correo electrónico no habrá problema[14]. No obstante, la existencia de una normativa interna de la empresa que meramente prohíba su utilización con fines particulares opino que no puede dejar expedito el camino para que los responsables de la empresa puedan interceptar o reproducir libremente el

12. Sentencia de 14-9-2000, f. de D. tercero.

13. Deben considerarse, además, otras condiciones como las que requiere en general el Tribunal Constitucional en este contexto. Sobre ello véase Roqueta Buj, R.: *Uso y control de los medios tecnológicos de información y comunicación en la empresa*, Valencia, 2005, y "El uso de los sistemas de comunicación electrónica de las empresas. A propósito de la STC de 7 de noviembre de 2005", en *Actualidad laboral*, núm. 3, 2006, págs. 265-282. Además, con específica referencia a la plasmación de las exigencias constitucionales en grupos de casos concretos, en "La intimidad en el ámbito de la empresa", "*Actas del II Seminario Internacional sobre los Límites de la protección jurídica de la intimidad*" (Universidad de Valencia, 13 y 14 de junio de 2008).

14. En el mismo sentido, Jareño Leal: *Intimidad e imagen*, cit., pág. 72.

contenido de los mensajes enviados por los trabajadores[15]. En tales casos, considero que será necesario el consentimiento del trabajador para revisar el uso dado a esa aplicación informática para eludir el delito del artículo 197, porque ni la propiedad de los equipos informáticos, ni el lugar en el que se utilizan, ni el fin productivo de su aplicación, ni la propia relación laboral de dependencia del trabajador dotan al empresario de un derecho de acceso, apoderamiento o interceptación sin restricciones. Y la falta de pacto expreso de aquellos extremos que benefician al empresario (como el control del uso de los equipos informáticos) no puede servir para recortar los derechos de los trabajadores.

Por lo demás, la captación del mensaje ha de alcanzar total o parcialmente a su contenido (texto del cuerpo del mensaje) o a aquellos datos imprescindibles para su intelección o relevancia (como el destinatario, la fecha y hora de su emisión, el asunto, etc., incluso sin abrir ningún mensaje[16], según las circunstancias)[17]. Pero no puede consistir sólo en la captación de la dirección del correo electrónico[18].

Y, por último, en estrecha relación con los mensajes de correo electrónico cabría considerar también como posible objeto del apoderamiento típico los SMS (enviados comúnmente –aunque no sólo– por medio de teléfonos móviles) por su aptitud para ser considerados "documentos" conforme a su definición legal (art. 24 C.p.). Al igual que los archivos informáticos que incorporen texto, imagen o cualquier otra clase de información.

La segunda conducta (interceptación de las telecomunicaciones), que antes se limitaba en la práctica a las comunicaciones telefónicas y por radio, ha alcanzado con los medios informáticos nuevas posibilidades a través del difundidísimo uso de los programas específicos para la comunicación a distancia (como "Messenger" o "Skype") y, también, como consecuencia del envío de datos a través de Internet con el propósito de solicitar información sobre productos o servicios, o de adquirirlos. Con ocasión de estas comunicaciones son registradas informaciones o datos personales de gran interés comercial (o para la comisión de delitos) relativos a los hábitos y preferencias de consumo, a números de cuentas bancarias o de tarjetas de crédito, datos domiciliarios, etc.

---

15. Véase, en la misma línea, la STS, Sala de lo Social, de 26-9-2007, exigiendo en estos casos "informar a los trabajadores de que va a existir control y de los medios que van a aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso" (f. de D. cuarto).

16. Como afirma la SAP de Barcelona de 18-1-2008 (f. jco. cuarto).

17. Véase esta doctrina en relación con el secreto de las comunicaciones en la STEDDHH de 2-8-1984 (caso Malone). En España, La Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (de transposición de la Directiva 2006/24/CE), se refiere a la conservación de esta clase de datos por los operadores de telecomunicaciones y establece la necesidad de autorización judicial para la cesión de los mismos a los *agentes facultados* cuando se refieran a comunicaciones concretas (art. 6).

18. Como se afirmó en la SAP de Madrid de 25-2-2002, "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" (f. de D. primero). En idéntico sentido, el AAP de Toledo de 24-11-2003 (f. jco. tercero).

Algo muy semejante sucede con la figura descrita como la utilización de "artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación", desde la generalización del uso de "cámaras web", capaces de accionarse a distancia desde equipos informáticos que se encuentran en manos de terceros intrusos con el fin de captar imágenes y sonidos de un modo imprevisible (y a veces hasta imperceptible) para el usuario[19].

Cualquiera de las conductas anteriores puede ir seguida de la revelación, difusión o cesión a terceros de los hechos descubiertos o las imágenes captadas. De modo que aquello conocido mediante la conducta de apoderamiento puede ser, desde luego, mostrado o comunicado a otro u otros, divulgado en general o cedido a terceros. Y, siendo típico el apoderamiento, estas conductas serían igualmente delictivas (art. 197.3). De nuevo aquí los medios digitales han abierto grandes vías para afectar a la intimidad y a la propia imagen, potenciadas por la generalizada disponibilidad de medios técnicos para hacerlo con gran facilidad, rapidez y alcance; por ejemplo, mediante la posibilidad de subir al instante a Internet fotos captadas con el móvil[20].

Pero todos los comportamientos a los que se refiere el artículo 197.1 del Código penal para ser típicos han de ser realizados "para descubrir los secretos o vulnerar la intimidad de otro", sin su consentimiento. Y de esta exigencia derivan las siguientes consecuencias:

En primer lugar, que es imprescindible actuar con dicha intención y que es, además, suficiente desde el punto de vista subjetivo. Esto significa que no es necesario que el autor pretenda nada más allá, como por ejemplo, desvelar lo captado.

En segundo lugar, que no es necesario llegar a descubrir el secreto o vulnerar la intimidad, sino que la intervención penal puede producirse antes de que ello se produzca.

En tercer lugar, y como consecuencia de la observación anterior, si pese a la intención que mueve la conducta, y después de todo, no había secreto ni cosa alguna referida a la intimidad de otro, se podría también castigar como un delito consumado. Esta conclusión –que me parece obligada por el tenor literal del precepto–, lleva a interpretar esta figura como un delito de peligro. Pero su injusto puede resultar demasiado inerte (o abstracto) si no se exige que el comportamiento parta de una expectativa objetivamente fundada *ex ante* acerca de la existencia de

---

19. La SAP de Málaga de 28 de enero de 2005 se ocupó de uno de estos casos: un estudiante de ingeniería técnica informática, después de seleccionar al azar la dirección de correo electrónico de una mujer, se introdujo en su sistema informático mediante un virus *troyano* accediendo al disco duro, interceptando su correo electrónico y sus conversaciones mediante *chat* y observando imágenes de la víctima captadas por medio de la *webcam*. Otro caso así se dio a conocer en noviembre de 2006 cuando la Guardia civil detuvo a varias personas que también habían creado un virus de las mismas características para activar subrepticiamente las *webcams* de conocidos y compañeros del instituto y lograr imágenes íntimas. Una vez captadas, chantajeaban a sus víctimas exigiéndoles el pago de dinero para no difundir las imágenes por Internet o en centros docentes. Por este procedimiento consiguieron imágenes de unos cien jóvenes (véase Diario "El País", 16 de noviembre de 2006).

20. Véase en el Diario "El País" de 27 de febrero de 2008 el artículo titulado "El '*cibervoyeur*' te vigila y te graba".

algo secreto o íntimo (idoneidad objetiva)[21]. Es decir, no, por ejemplo, cuando signos externos apuntaran objetivamente de antemano otro contenido en el objeto de la conducta; como cuando se trata de mensajes claramente comerciales distribuidos de forma generalizada, o, en el caso de los mensajes de correo electrónico, reconocibles por el remitente o por la especificación del asunto. Y ello aunque después resulte que la apariencia del objeto constituía un ardid especialmente buscado para encubrir o disimular otro contenido. En estos supuestos, la intención de conocer el contenido del mensaje (por ejemplo, el de una promoción comercial de aparatos electrodomésticos) no incluye, en modo alguno, la voluntad de descubrir secretos o vulnerar la intimidad del destinatario del envío. Y esto es decisivo. En efecto, tal intención debe acompañar, como ya se ha indicado, a cualquiera de las modalidades del artículo para su tipicidad. Y, si en casos como el anterior no puede considerarse presente, en otros no puede considerarse ausente por el hecho de que el autor actúe con otra voluntad. Esto último se ha venido planteando en la práctica, sobre todo, cuando ante crisis matrimoniales uno de los cónyuges pretende obtener alguna prueba para demostrar la infidelidad o cualquier otra circunstancia que pueda ser relevante en los procedimientos de separación, nulidad o divorcio; aunque también cuando se ha tratado de conseguir pruebas con otros fines (como, por ejemplo, para el despido laboral de un trabajador[22]). En tales casos, esta intención que mueve toda la conducta no puede dejar de suponer que, al proceder así, muchas veces se hará teniendo que descubrir secretos o que vulnerar la intimidad del otro; es decir, si no de modo final, sí como una consecuencia necesaria del actuar del autor, que no le priva de la intencionalidad requerida por el tipo del art. 197.1[23].

---

21. Es cierto, sin embargo, que la referencia del art. 197.3 a que la conducta tenga por objeto "los datos o hechos descubiertos o las imágenes captadas" da lugar a pensar que el número 1 requeriría la efectiva captación, como apunta Anarte Borrallo en "Consideraciones sobre los delitos de descubrimiento de secretos (I)", cit., pág. 54. Pero esta conclusión no es, a mi juicio, necesaria porque la alusión a los "los datos o hechos descubiertos…" figura junto a otras conductas (la revelación, difusión o cesión, y no se refiere específica y directamente a la captación) y, además, porque precisamente para revelar, difundir o ceder, lo normal será haber "descubierto" lo que se desea transmitir, pero el hecho de que por lo general se hayan descubierto, no impide que en otros casos no haya descubrimiento. Por otra parte, podría suceder que los signos externos de un objeto simularan contener un contenido secreto, obedeciendo tal apariencia, sin embargo, sólo a motivos de índole comercial (como, por ejemplo, una carta con el rótulo de "confidencial", pero con fines de propaganda). En este caso, si alguien se apoderase de dicho objeto con la pretensión de descubrir los secretos del destinatario, podría apreciarse una tentativa inidónea (en realidad, un error inverso de tipo: el sujeto cree cometer un delito cuando su conducta resulta ex ante objetivamente inadecuada para ello). Por lo demás, como se ve, en el texto se propone una interpretación del delito como un delito de peligro de la clase de los de aptitud o idoneidad, en los términos que se señalan.

22. Hechos, por ejemplo, del Auto de la AP de Madrid, Sección 6ª, de 23-1-2004.

23. Sobre esto, específicamente, Boix Reig, J., Jareño Leal, A., Doval Pais, A.: "Protección penal de la intimidad y derecho de defensa en causas matrimoniales" (en *La Ley-Asociación Española de Abogados de Familia*, año VII, núm. 26, Madrid, 3 de octubre de 2002, págs. 2-20), a raíz del importante cambio jurisprudencial que supuso la STS de 14-5-2001. Expresamente, en el sentido señalado en el texto, véase la STS de 21-3-2007, f. de D. segundo. En la línea que se señala en el texto, se ha declarado, por ejemplo, que "el hecho de aportar a un procedimiento judicial unos datos ya supone la voluntad de revelación" (SAP de Segovia de 15-12-2005, f. de D. cuarto), en una abierta síntesis del proceder jurisprudencial en casos semejantes. La exigencia de dolo directo considero que resulta inevitable a la vista de la dicción legal. Sin embargo, alguna sentencia ha apreciado el delito con dolo eventual (SAP de Barcelona de 18-1-2008, f. jco. cuarto).

2. El artículo 197.2

Este precepto es el que contempla las figuras típicas más especialmente relacionadas con los medios digitales, al referirse a conductas que recaen siempre sobre "datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos".

Aunque no limita su alcance a registros informatizados, pues caben perfectamente otros ("o en cualquier otro tipo de archivo o registro"), los ilícitos que recoge se conocen generalmente como "delitos contra la intimidad –o la libertad– informática"[24]. Los hechos a los que se refiere este artículo son, al menos aparentemente, muy diversos: apoderamiento, utilización, modificación, alteración de datos reservados o acceso a los mismos, conductas a las que puede seguir, al igual que en los casos del artículo 197.1, la revelación, difusión o cesión de los datos, en cuyo caso se agravará también la pena (del art. 197.2, que es la misma que la del 197.1[25]) según lo que señala el artículo 197.3. Pero para llegar hasta aquí es necesario que la conducta-base (el apoderamiento, la utilización, la modificación o el acceso) sea típica, lo que sólo ocurrirá cuando se lleve a cabo "en perjuicio de tercero" o "en perjuicio del titular de los datos o de un tercero", como exige el 197.2, según los casos[26].

Este artículo requiere, desde luego, hacer algunas observaciones de carácter general y otras de carácter específico sobre las conductas que contempla.

Con carácter general, se ha criticado, con razón, su deficiente factura técnica, pues su redacción resulta compleja y confusa y desconcierta al intérprete como enseguida veremos al tratar de las conductas[27]. Dejando al margen su estructura defectuosa –o hasta dislocada– dos son los puntos más criticables del texto teniendo en cuenta su inmediata repercusión en el alcance de los delitos: la referencia a "*datos reservados de carácter personal o familiar*" y al perjuicio "*de tercero*" o "*del titular de los datos*".

2.1. Concepto de "datos reservados"

La alusión a un objeto material constituido por "*datos reservados*" desconcierta porque éstos no se definen en el Código penal, ni tampoco fuera de él. En particular, la Ley Orgánica 15/1999, de Protección de Datos Personales (en adelante, LOProDa) se

---

24. Aunque no todos los ataques por medios informáticos penalmente relevantes, ni siquiera necesariamente los más sofisticados, encuentran cabida aquí. Como se ha señalado en páginas anteriores, en el número 1 del art. 197 caben muy diversos supuestos de esta clase.

25. La previsión de una misma penalidad para conductas que sin duda poseen una distinta insidiosidad resulta cuestionable y ha sido cuestionada. Véase, a propósito, entre otros, F. Morales Prats en Quintero Olivares/Morales Prats: *Comentarios a la Parte especial del Derecho penal*, cit., págs. 428-429, R. Rebollo Vargas en Córdoba Roda/García Arán: *Comentarios al Código penal*, cit., pág. 466, y Jareño Leal, A. y Doval Pais, A.: "Revelación de datos personales, intimidad e informática (comentario a la STS 234/1999, de 18 de febrero)", en La Ley, núm. 4844, 21 de julio de 1999, pág. 3.

26. Véase la STS 11-7-2001, asimilando, al menos en cierto modo, la expresión *en* "*perjuicio de otro*" a la intención de "descubrir los secretos o vulnerar la intimidad de otro", del art. 197.1, teniendo en cuenta que "ambas infracciones penales tratan de proteger idénticos bienes jurídicos" (f. de D. 3, f).

27. También en el mismo sentido, Huerta Tocildo, S./Andrés Domínguez, A.C.: "Intimidad e informática", en *Revista de Derecho Penal*, 6, 2002, pág. 65. Efectivamente, "se aprecia la incomodidad del legislador con los materiales tecnológicos", como ha observado Anarte Borrallo (en "Consideraciones sobre los delitos de descubrimiento de secretos (I)", cit., pág. 52).

refiere, como se ve, a "*datos de carácter personal*" (en su propia rúbrica) o a "*datos especialmente protegidos*" (en su art. 7: ideología, religión, creencias, afiliación sindical, salud, vida sexual, origen racial o étnico), pero los datos de los que habla el Código penal no pueden identificarse ni con unos, los del rótulo de la Ley, porque, si bien son "personales", no son todos "reservados", ni con los otros, los del artículo 7, porque aluden a datos de naturaleza especialmente sensible a cuya especial protección se destina en el Código penal el subtipo agravado del número 5 del mismo artículo, abarcándolos casi todos[28]. Ante esta falta de referencias[29], el Tribunal Supremo ha sostenido líneas interpretativas de consecuencias bien distintas.

En virtud de la primera, con origen en la Sentencia de 18-2-1999, "debe entenderse que la norma requiere la existencia de un perjuicio añadido [*sc*. al mero conocimiento o quebranto de la reserva] para que la violación de la reserva integre el tipo, un perjuicio que puede afectar, como hemos visto, al titular de los datos o a un tercero. No es fácil precisar, «a priori» y en abstracto, cuándo el desvelamiento de un dato personal o familiar produce ese perjuicio. Baste ahora con decir que lo produce siempre que se trata de un dato que el hombre medio de nuestra cultura considera «sensible» por ser inherente al ámbito de su intimidad más estricta, dicho de otro modo, un dato perteneciente al reducto de los que, normalmente, se pretende no transciendan fuera de la esfera en que se desenvuelve la privacidad de la persona y de su núcleo familiar" (f. de d. 2º). Con esta interpretación el Tribunal Supremo pretendía, más que establecer las propiedades características de la expresión "datos reservados de carácter personal", determinar cuáles son los datos de carácter personal o familiar capaces de producir un perjuicio y, en consecuencia, quedar abarcados por la protección penal. Ésta es una vía material para la determinación del sentido "reservado" del dato en la medida en que se fija en el efecto que la intervención de un tercero puede producir sobre el ciudadano al que se refiere la información. Y, conforme a la Sentencia, lleva a que se trata de los datos "de la intimidad más estricta" de la persona física (aunque no se concretaron por el Tribunal en esta resolución)[30]. De este modo, la categoría de los "datos reservados" no definiría formalmente un sector de datos caracterizados por su especial naturaleza o contenido, sino por las circunstancias del sujeto al que se refiere. Efectivamente, por ejemplo, en aplicación de esta doctrina, se ha estimado que el número de teléfono puede constituir un dato reservado en determinadas circunstancias, aunque pueda no serlo en otras, por más que se trate de un dato de la misma clase[31].

---

28. De todos los "datos especialmente sensibles" de la LOProDa, el Código penal únicamente deja sin cobertura en el art. 197.5 los datos de "afiliación sindical" y los específicamente relativos al "origen étnico".

29. Que se confirma cuando se acude, incluso, a consultar fuentes internacionales en la materia, como la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24/10/1995, 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 (Diario Oficial núm. L 281, de 23/11/1995) y el Convenio del Consejo de Europa.

30. En una dirección parecida, Orts Berenguer y Roig Torres han señalado que son datos reservados los "datos más recónditos de la intimidad" (en *Delitos informáticos y delitos comunes cometidos a través de la informática*, Valencia, 2001, pág. 33).

31. La SAP de Castellón de 26-9-2005 consideró que el número correspondiente al teléfono móvil que la víctima precisamente había tenido que cambiar para que el acusado dejara de molestarla, constituía un "dato reservado". Sin embargo, el número de teléfono también se ha equiparado (por ejemplo, en la SAP de Madrid de 25-2-2002 y el AAP de Toledo de 24-11-2003, cits.) a una mera referencia identificativa de un contenido (éste sí relevante porque es donde se encuentran los datos que pueden afectar a la intimidad de una persona).

La segunda línea interpretativa se plasmó en la Sentencia de 11-7-2001. Allí la Sala consideró que: "no existen datos personales automatizados [*sic*] reservados y no reservados, por lo que debe interpretarse que todos los datos personales automatizados quedan protegidos por la conminación punitiva del artículo 197.2 C.P.". Éste es el significado que también propone un significativo sector de la doctrina[32], constituyendo un punto de vista bastante aceptado[33]. De este modo, aplicando un criterio netamente formal, se identificarían los "datos reservados" con los datos personales o familiares registrados; o sea, con los datos registrados relativos a las personas[34] o a sus familias, dejándose con esta interpretación el término "reservados" sin contenido material y ampliando, en consecuencia, el tipo. Pero el Tribunal Supremo ha exigido un poco más: que los datos sean "secretos", en el sentido de "no públicos" o conocidos ("que el sujeto activo no conozca, o no esté seguro de conocer y que el sujeto pasivo no desee que se conozca", f. de D. tercero, 7, de la misma Sentencia), acercando en lo posible las características del objeto material de estos delitos a las de los objetos del artículo 197.1. "Datos reservados" serían, pues, datos registrados y no públicos.

No obstante, aun con esta última restricción, realmente son muy pocos los datos que objetivamente escapan de la reserva: únicamente los que se encuentran al alcance de su consulta por cualquier interesado, como los datos que figuran en la guía telefónica, en el censo o en cualquier otra de las denominadas "fuentes accesibles al público" (que definen la LOProDa y su Reglamento[35])[36]. Sin embargo, como es obvio, no todas las informaciones sobre una persona, aunque no sean públicas, poseen la misma importancia en orden a la tutela de las condiciones básicas para desarrollar su vida[37].

---

32. F. Morales Prats (en Quintero Olivares/Morales Prats: *Comentarios a la Parte especial del Derecho penal*, cit., pág. 423: "todos los datos personales automatizados quedan protegidos por la conminación punitiva del art. 197.2 CP"). Siguéndole, A. Jorge Barreiro (en Rodríguez Mourullo/Jorge Barreiro: *Comentarios al Código penal*, cit., pág. 573), R. Rebollo Vargas (en Córdoba Roda/García Arán: *Comentarios al Código penal*, cit., pág. 467) y Huerta Tocildo/Andrés Domínguez: "Intimidad e informática", cit., pág. 59. En contra, Jareño Leal: *Intimidad e imagen*, cit., pág. 63, a mi juicio con razón teniendo en cuenta los argumentos que se recogen más adelante en el texto.

33. Véanse las referencias en este sentido de Mata y Martín en "La protección penal de datos como tutela de la intimidad de las personas", cit., pág. 229.

34. Los "datos de carácter personal" se definen en la LOProDa como "cualquier información concerniente a personas físicas identificadas o identificables" y en el art. 5.1, f del Reglamento de desarrollo de la misma Ley como "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables".

35. R.D. 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOProDa. Dichas fuentes son: el censo promocional (es decir, el formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral, art. 31.1 LOProDa, una de las más importantes novedades de la Ley), las guías de servicios de comunicaciones electrónicas, las listas de personas pertenecientes a grupos de profesionales, los diarios y boletines oficiales y los medios de comunicación social (arts. 2.3.j de la LOProDa y 7 del Reglamento).

36. Véase, por ejemplo, la SAP de Barcelona de 2 de noviembre de 1999 desestimando la consideración de algunas informaciones como secretos o datos reservados por haber sido publicados en el Boletín Oficial de la Provincia y ser, en consecuencia, "ya del dominio público".

37. Ésta es la perspectiva fundamental que considero que dota de contenido material esencial a la intimidad como objeto de protección (y, sobre todo, como objeto de protección jurídico-penal), como más adelante referiré en el texto.

Pues bien, las consecuencias de una u otra interpretación son claras: si se sigue una interpretación material del carácter reservado del dato, las conductas recogidas en el artículo 197.2 para ser típicas deberán recaer sobre datos de la intimidad más estricta[38]. Sin embargo, si se opta por una interpretación formal de los "datos reservados", dichas conductas deberán afectar a datos registrados y no públicos, con independencia de su contenido y relevancia.

La opción por una u otra interpretación depende directamente, pues, del bien jurídico protegido por el precepto. Y es que, como se ve, la intimidad no resultaría siempre afectada en ambos casos, sino solamente en el primero; es decir, si se considerase que los datos reservados son de la intimidad más estricta. Si, por el contrario, se considera que los datos reservados basta que estén registrados, entonces, ocurrirá que habrá conductas típicas que no afectarán a la intimidad, teniendo en cuenta la naturaleza y las características del dato afectado; aunque sí, obviamente, a los propios datos.

En mi opinión, por "datos reservados de carácter personal o familiar" debe entenderse "cualquier información concerniente a personas físicas identificadas o identificables" –siguiendo el art. 3.a LOProDa–. Estos datos, como objeto material del delito del artículo 197.2, habrán de encontrarse ya "registrados" en el momento de realizar el delito, pues así lo exige el precepto (y, en consecuencia, resultan excluidas las conductas de recogida de datos personales para su informatización o la creación clandestina de ficheros o bancos de datos personales, que varios grupos parlamentarios propusieron introducir durante la tramitación del Código penal[39]). Y han de referirse a la intimidad.

Esta última considero que es una exigencia indispensable en este contexto jurídico-penal para excluir los datos reservados que son de carácter personal, pero no íntimos[40]. Se trata de aquellos datos cuyo titular desea que no se conozcan por cualquiera (desde este punto de vista serían próximos a secretos) pero que no afectan a la intimidad del sujeto. Esta interpretación, que se fija en la diferente entidad de la información que encierran los datos personales, permite situar el foco de la intervención penal sobre los casos que verdaderamente inciden en el derecho fundamental y repercuten en las posibilidades de realización del individuo. Se trata, como se ve, de una concepción instrumental de la intimidad en virtud de la cual debe distinguirse la gravedad de los ataques que padece atendiendo a su mayor o menor incidencia en la esfera de libertad –e, incluso, seguridad– del sujeto, como ha propugnado Boix[41].

---

38. Aunque no sobre los datos sensibles del art. 197.5 (véase el texto, *supra*).

39. Propuestas del Grupo Popular (enmienda núm. 343) y de Izquierda Unida-Iniciativa per Catalunya (enmienda núm. 729), BOCG, Congreso, Proyectos de Ley, núm. 77-6, págs. 194 y 290, respectivamente.

40. En esta distinción ha incidido razonablemente Jareño Leal en *Intimidad e imagen*, cit., págs. 63-67.

41. En "Protección jurídico-penal de la intimidad e informática", en *Poder Judicial*, núm. especial IX, 1988, pág. 19. En la misma dirección, Huerta Tocildo, S./Andrés Domínguez, A.C.: "Intimidad e informática", cit., pág. 60. Con este modo de entender la intimidad conecta la propia definición de este derecho que maneja el Tribunal Constitucional poniendo de manifiesto su importancia "para mantener una mínima calidad de vida humana" (STC 231/1988, f. jco. 3º y en adelante).

Y, en la práctica, no puede dejar de requerir un examen circunstancial en el caso concreto, lo que resulta, por lo demás, perfectamente acorde con la perseguibilidad privada de estos delitos (art. 201 C.p.). Sin embargo, no es ésta la interpretación que se sigue siempre por los juzgados y tribunales, ni tampoco resulta unánime en la doctrina[42].

2.2. La expresión "en perjuicio"

Con la exigencia de que las conductas de apoderamiento, utilización o modificación de los datos se realicen "*en perjuicio de tercero*" parecen configurarse unas figuras para las que no bastaría la intención de apoderarse, de utilizar o modificar datos, sino que se necesitaría, además, que se llevasen a cabo con un ánimo especial. ¿Tiene esto sentido? En mi opinión, sí lo tiene cuando se trata de comportamientos que pueden no suponer un perjuicio para la intimidad *per se*, pero no en otro caso. Es decir, esa condición legal debe su sentido a la limitación del alcance del tipo, de modo que si, al margen de esta cláusula, considerando los componentes objetivos y subjetivos de la conducta, ésta no puede dejar de suponer por sí que se ha actuado "en perjuicio de tercero", no cabrá exigir nada más. Éste considero que es el caso del "acceso"[43].

Por lo demás, dicha exigencia legal, aunque se interprete como un elemento subjetivo, no impide la concurrencia de otros ánimos, como por ejemplo el ánimo de obtener un beneficio económico como consecuencia directa de la conducta (casos de tráfico de datos) o el mero ánimo de quebrantar los sistemas de seguridad que protegen los datos (casos de *hackers*)[44].

---

42. La STS de 11-6-2004 ha señalado que "el dato referente al lugar de trabajo de una persona contenido en los archivos de la Seguridad Social […] es un dato de carácter personal en el sentido del art. 197.2 CP, pues se refiere a uno de los ámbitos en los que una persona desarrolla y realiza su personalidad […] No son datos que están a disposición de cualquier solicitante" (f. de D. segundo). En esta misma línea, de la que discrepo, Romeo Casabona considera que el bien jurídico protegido en el delito del art. 197.2 son los datos reservados de carácter personal o familiar de otro "sin que hayan de ser necesariamente íntimos" (en *Los delitos de descubrimiento y revelación de secretos*, Valencia, 2004, págs. 103 y 110). También críticamente, Rueda Martín: *Protección penal de la intimidad personal e informática*, cit., pág. 30.

43. Sugiriéndolo, también, la SAP de Barcelona de 18-1-2008, f. de D. cuarto. Véase, con más detalle, Jareño Leal y Doval Pais: "Revelación de datos personales, intimidad e informática", cit., pág. 4. La STS de 18-2-1999 (f. de D. segundo) abordó directamente esta cuestión, que fue el objeto del citado trabajo. Sosteniendo otras opiniones, entre otros autores, Orts Berenguer y Roig Torres: *Delitos informáticos*, cit., págs. 37-41, Mata y Martín: "La protección penal de datos como tutela de la intimidad de las personas", cit., pág. 231, y Gómez Lanz, J.: *La interpretación de la expresión en perjuicio de en el Código penal*, Madrid, 2006, págs.: 254 y ss.

44. Coincido en esto con Huerta Tocildo/Andrés Domínguez: "Intimidad e informática", cit., pág. 26. El Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, de 2006 (BOCG, Congreso, 119-1, de 15 de enero de 2007), previó la incorporación al art. 197 de un nuevo apartado para castigar con pena de prisión de seis meses a dos años al 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". A la necesidad de esta nueva disposición se refería la Exposición de Motivos, apelando a que "crecen los riesgos […] a causa de las intrincadas vías tecnológicas que permiten violar la privacidad o reserva de datos contenidos en sistemas informáticos" y señalando que se trata de una "preocupante laguna, que pueden aprovechar los llamados *hackers*" que debe eliminarse "cumpliendo con obligaciones específicas sobre la materia plasmadas en la Decisión Marco 2005/222/JAI de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información". Los defectos sistemáticos y de contenido de la disposición prevista saltan a la vista y algunos de ellos fueron puestos de manifiesto por el Consejo General del Poder Judicial en su correspondiente informe sobre el Texto, diciendo, …

Todavía en relación con la referencia de la ley a que los comportamientos se realicen "en perjuicio", se debe poner de manifiesto que es muy confusa la alusión al "tercero" junto al "titular de los datos", al decir, en el último inciso del artículo 197.2 "en perjuicio del titular de los datos o de un tercero"[45]; y lo es, incluso, a la vista de la Ley de Protección de Datos y su Reglamento[46]. El Tribunal Supremo ha interpretado, al menos en una ocasión, que tal expresión alcanza tanto al afectado en su intimidad (es decir, al titular de los datos) como a "cualquier persona que pudiera resultar afectada por el apoderamiento, utilización o modificación de los datos registrados" (STS de 9-10-2000, f. de D. 9º). Pero esta interpretación deja abiertas muchas preguntas; por ejemplo, con respecto a la clase de daño que se requiere, porque si es de la intimidad será porque los datos son suyos (y, entonces, sobraría una de las referencias legales) y, si no afecta a la intimidad, habría que preguntar qué importan aquí los daños ocasionados a otros bienes jurídicos.

Estas dificultades llevan a pensar que la alusión al perjuicio del "titular de los datos o de un tercero", más bien, busca una correspondencia con la previsión del tipo de que las conductas recaigan, por un lado, sobre datos reservados de carácter "personal" o, por otro, sobre datos de carácter "familiar"; de modo que cuando afecten a datos "de carácter personal", es necesario que se obre "en perjuicio del titular de los datos" y cuando se trate de datos de carácter "familiar" es preciso que se actúe en perjuicio "de un tercero". Así, pues, las actuaciones sobre datos de terceros registrados (o deducibles a partir de los registrados) a nombre de otro, también son típicas si son realizadas en perjuicio del tercero. Éste puede ser, por ejemplo, el caso del acceso a datos de un hijo registrados a nombre de sus padres[47].

…
en resumen: "el Consejo recomienda que se evite el solapamiento de la nueva figura con las previstas en el artículo 197 CP. En este sentido, el enfoque que da la Decisión Marco a su propuesta armonizadora, que busca de forma directa el aseguramiento de una tutela penal eficiente de la seguridad de los sistemas de información con abstracción de la naturaleza y contenido de los datos comprendidos en los mismos y de la intencionalidad que guíe al culpable, aconseja la ubicación sistemática del nuevo tipo fuera del artículo 197 CP, en un precepto autónomo en el que se sancione la conducta de quien no estando comprendido en ninguno de los supuestos del artículo 197 CP, acceda intencionadamente y sin autorización a un sistema de información ajeno transgrediendo las medidas de seguridad que lo protegen. Una descripción típica de este tenor permitiría cerrar el círculo de protección penal de conductas atentatorias de la intimidad informática, abarcando la incriminación de las conductas de los denominados *hacker* que en muchas ocasiones se inmiscuyen en sistemas ajenos sin una finalidad específica de perjuicio o de violación de la intimidad, guiados únicamente por el propósito de demostrar su pericia técnica o por un puro afán recreativo." Desde luego, la intervención penal ante estas conductas ha sido también planteada desde la doctrina (así, aunque insistiendo en la necesidad de reflexión político-criminal al respecto, Romeo Casabona: "Los datos de carácter personal como bienes jurídicos penalmente protegidos", cit., pág. 189) y seguramente será inevitable en un futuro próximo como consecuencia de la imparable –pero inútil y contraproducente– escalada del Derecho penal hacia el "riesgo cero".

45. La inclusión en el artículo de esta exigencia se debió a una enmienda (núm. 49) presentada por el grupo parlamentario del PNV-Grupo Mixto, que fue aceptada por la Ponencia sin discusión (BOCG, Congreso, Proyectos de Ley, núm. 77-8, pág. 461).

46. Efectivamente, el art. 3 de la Ley y el art. 5.1 del R.D. 1720/2007 definen como "afectado o interesado" a la "persona física titular de los datos que sean objeto de tratamiento". Expresamente, no se considera "afectado", ni siquiera "interesado", el "tercero" según la definición que ofrece en el apdo. r) del mismo artículo el citado Reglamento.

47. Coincido así con una de las posibilidades residuales que plantean Huerta Tocildo y Andrés Domínguez en "Intimidad e informática", cit., pág. 65.

2.3. Breve referencia al "acceso"

Con respecto a las conductas en particular, la más problemática es, sin duda, la del "acceso" a los datos[48]. En un sentido muy amplio se podría entender que alcanza el mero conocimiento de los datos, pero considerando que el sentido del verbo típico utilizado (¡que no es "conocer"!) supone gramaticalmente "entrar", debe exigirse más. En concreto, una acción mediante la cual se supere alguna barrera (aunque sea mínima) de resguardo de los datos (idea de la "ruptura directa" por parte del agente[49]). Y no es necesario que se actúe con ánimo de divulgar, revelar o ceder la información obtenida, pese a lo declarado en alguna sentencia[50].

2.4. El especial entorno de Internet

En este contexto, no se pueden dejar de considerar los datos que pueden conocerse de muchas personas a través de Internet. Esta posibilidad ha convertido a la red en un auténtico registro de datos "público", en el sentido de que está dotado de la mayor publicidad potencial posible, pues cualquiera puede acceder a datos personales muy diversos desde cualquier lugar del mundo y en todo momento y ponerlos a su entera disposición. Las características de la red y, en particular, las posibilidades que ofrecen los conocidos "buscadores" plantean, desde luego, serios retos a la tutela de los datos e imágenes personales, aunque no sólo se plantean en estos casos[51]. No obstante, al mismo tiempo que dificultan la protección de la intimidad personal, dichas características pueden relativizar también los ataques a la misma considerando que cualquiera puede acceder libremente a los contenidos publicados y manipularlos, razón por la que los referidos datos pueden generar una menor confianza en su autenticidad.

Pero, dejando a un lado las importantes dificultades que en la práctica plantea Internet dadas sus peculiaridades (dificultades para el descubrimiento de los hechos, para la averiguación del lugar de su comisión[52], para la imputación de responsabili-

---

48. Sobre este verbo típico, específicamente, la SAP de Barcelona de 18-1-2008, f. jco. cuarto.

49. Más ampliamente, Jareño Leal y Doval Pais: "Revelación de datos personales, intimidad e informática", cit., pág. 3.

50. Véase la SAP de Tarragona de 23-7-2001, en la que se afirma que "no es de hallar en la voluntad de los acusados […] un animus desvelandi de la información informática obtenida irregularmente, pese a que ha de reconocerse que simplemente una sutil variación con respecto a la forma de valorar la prueba podría llevarnos a una conclusión condenatoria, por cuanto es claro y diáfano que el proceder de los acusados discurrió en la línea fronteriza entre lo relevante o no penalmente […] Más bien cabe considerar la actitud de los acusados como un reto personal de obtener información sin fin, esto es, como una voluntad de auto competición enmarcada en un contexto que vulgarmente podríamos calificar de «chafarderío informático»" (f. de D. segundo). Los acusados habían accedido mediante un programa informático *ad hoc* a códigos de usuarios y contraseñas de profesores de un centro universitario, a sistemas informáticos de Universidades, habían copiado palabras de paso de más de dos mil alumnos, habían accedido a cuentas de correo electrónico de profesores, etc.

51. Por ejemplo, la STS de 9-5-2008 ha considerado que "quien utiliza un programa P2P, en nuestro caso EMULE, asume que muchos de los datos se convierten en públicos para los usuarios de Internet, circunstancia que conocen o deben conocer los internautas y tales datos […] no se hallan protegidos por el art. 18.1 ni por el 18.3 CE" (f. de D. segundo).

52. La práctica ubicuidad de la red plantea serias dificultades para la persecución penal de los delitos cometidos por este medio. Sobre ello véase Sánchez García de Paz, I./Blanco Cordero, I.: "Problemas de Derecho penal internacional en la persecución de delitos cometidos a través de Internet", en *Actualidad Penal,* núm. 7, 11 a 17 febrero 2002.

dades a los proveedores de los servicios y a otros facilitadores del acceso a los datos o imágenes[53], etc.), el régimen jurídico-penal de las actuaciones sobre los datos personales no debe presentar diferencias con respecto al tratamiento de los comportamientos que tienen lugar en otros entornos diferentes: las conductas de simple consulta o visionado de los datos ilícitamente consignados en la red son atípicas (por falta de "acceso"); pero no las de su divulgación, revelación o cesión, a sabiendas de su origen ilícito (art. 197.3.II)[54], como tampoco, por supuesto, aquellas a las que se deba, precisamente, la aparición de la información personal reservada en Internet (conductas de divulgación, revelación o cesión típicas previstas en el art. 197.3.I).

3. El extraño artículo 200 del Código penal

En el contexto de los delitos contra la intimidad llama la atención hallar un precepto, como el artículo 200, que extiende lo dispuesto en el capítulo del Código dedicado a los delitos de descubrimiento y revelación de secretos "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". Lo llamativo resulta concretamente que se aluda a "datos reservados de personas jurídicas"[55], teniendo en cuenta que nos encontramos en el ámbito sistemático de la protección penal de la intimidad, que es un derecho fundamental de titularidad exclusivamente individual. En consecuencia, se suscita inmediatamente la pregunta acerca de cuál puede ser el sentido de este artículo y, al respecto, existen diversas posibilidades:

La primera la ofrece su interpretación más literal: que se refiera, efectivamente, a conductas que tengan por objeto datos reservados referidos a personas jurídicas; es decir, datos concernientes a aspectos como su organización o estructura, particularidades de la financiación y desarrollo de su actividad, planes y estrategias, etc., que se quieren resguardar del conocimiento de terceros. Un interesante indicio para vincular

---

53. Véase Gómez Tomillo, M.: *Responsabilidad penal y civil por delitos cometidos a través de Internet. Especial consideración del caso de los proveedores de contenidos, servicio, acceso y enlaces,* Ed. Aranzadi, Cizur Menor, 2004.

54. Aunque en algunos supuestos habría que plantear si, materialmente, el hacer llegar la información a una(s) persona(s) más supondría o no alguna perturbación más para el bien jurídico protegido. A propósito de esta cuestión, recientemente, un magnate británico, protagonista de unas escenas de contenido sexual subrepticiamente captadas en vídeo, no pudo conseguir de los jueces una resolución para que impidieran que continuara su difusión en Internet porque se consideró "que hubiera sido «fútil» prohibirlo cuando ya había recibido –en sólo dos días- cerca de un millón y medio de visitas" (de ello da cuenta M. Vargas Llosa en su artículo de opinión titulado "Traseros irritados", publicado en el Diario "El País" de 20 de abril de 2008, pág. 37; sobre ello, también, el mismo diario el 13 de julio de 2008, en su sección "El País Domingo", págs. 6 y 7, afirmando que para esta fecha habría sido visto ya por tres millones y medio de personas). Este asunto plantea la interesante pregunta de si, en ciertos casos, la exposición de lo íntimo *una vez más* no constituye, en realidad, *ninguna vez más*. Y pone de manifiesto la dificultad de resolver estos casos pues si, en efecto, la difusión del video entre unas (o muchas) personas más, no supone en tal caso una lesión significativamente mayor de la intimidad del afectado, sí puede suponer un evidente riesgo para su honor en el caso de que alguien que conozca a la víctima vea las imágenes a partir de entonces.

55. La LOProDa se refiere a "ficheros de titularidad pública" (arts. 20 y ss.) y a "ficheros de titularidad privada que contengan datos de carácter personal" (art. 25), pero no a "datos". Y su Reglamento establece expresamente que "no será aplicable a los tratamientos de datos referidos a personas jurídicas" (art. 2.2 R.D. 1720/2007).

directamente los datos con las personas jurídicas se hallaría en que ya no se habla aquí de datos reservados *de carácter personal* (como en el art. 197.2), sino de "datos reservados", a secas. Al que hay que añadir otro indicio más: que el consentimiento de los representantes de la persona jurídica levanta el delito, lo que significa que los representantes de la persona jurídica pueden disponer de los datos y confirma cuál es la titularidad de los mismos.

Sin embargo, esta primera opción interpretativa choca con algunos problemas. Además de la dificultad sistemática que plantea el encaje del artículo 200 entre los delitos contra la intimidad, ofrece el problema del deslinde de la figura en cuestión de los delitos de descubrimiento y revelación de secretos de empresa (arts. 278 y ss.), con los que el artículo 200 se solaparía en la mayoría de los casos[56]. Aunque no en todos. En efecto, no se produciría ninguna duplicidad cuando la persona jurídica no fuera una "empresa", sino una asociación, una fundación u otra clase de entidad con personalidad jurídica y de naturaleza no mercantil. De ser así, el problema únicamente se reduciría a conciliar la ubicación del precepto con este contexto sistemático dedicado a la tutela de la intimidad.

La segunda posibilidad es que el artículo 200 aluda a datos reservados de personas físicas que se encuentran registrados en manos de personas jurídicas porque son necesarios para el desarrollo de su actividad (por ejemplo, datos de clientes de productos o servicios). Pero, entonces, la previsión legal de este precepto sería innecesaria porque bastarían las de los artículos 197.1, 2 y 3 (los ataques que tuvieran por objeto los datos de las personas jurídicas serían, en fin, ataques contra la intimidad de personas físicas)[57].

Sin embargo, aún sería posible exprimir algo más este modo de interpretar el artículo 200 y entender que el legislador ha querido establecer aquí una cláusula –como de recogida– para aquellos supuestos en los que, por las características del ataque, resulta difícil determinar el número de las personas afectadas y la intensidad de la afección de cada una. Casos, por ejemplo, en los que se ha accedido a los archivos de la persona jurídica y se han descubierto datos de algunas (o muchas) personas físicas, se han revelado o cedido a terceros los de otras (o las mismas) personas, etc., sin poderse llegar a comprobar, o precisar con certeza, la extensión real que alcanzó la intromisión[58]. La vaguedad, la cierta indeterminación, que tendrían estos ataques explicaría, por lo demás, que la pena correspondiente fuera la misma que la prevista para cada uno de los casos de los artículos anteriores (¡con los que, por

56. La proximidad a los delitos de descubrimiento y revelación de secretos de empresa está muy presente en el artículo. Por ello, precisamente, remite de forma implícita a los mismos al decir "…salvo lo dispuesto en otros preceptos de este Código", indicando que el art. 200 deberá ceder ante otros más específicos o por otra razón más adecuados, como lo serán en muchos casos los artículos que recogen los delitos de descubrimiento y revelación de secretos de empresa.

57. En el mismo sentido, Anarte Borrallo: "Consideraciones sobre los delitos de descubrimiento de secretos (I)", cit., pág. 60.

58. Un caso de estas características puede ser, por ejemplo, el apoderamiento de documentos (agendas profesionales, expedientes, etc., con diferentes datos de diversos clientes y otras personas relacionadas) de un despacho de abogados (similar a aquel del que entendió la STS de 14-9-2000, *véase supra*).

cierto, no guarda un absoluto paralelismo![59]), a las que se remite el propio artículo 200; en consecuencia, quedaría en cada caso el correspondiente intervalo de la pena para el ajuste de la sanción aplicable conforme a las características del hecho y del autor[60]. No obstante, el propio artículo 200 cierra la puerta a esta interpretación, que choca de nuevo con la eficacia que se reconoce al consentimiento de los representantes de la persona jurídica para enervar el delito.

Por último, otra alternativa, próxima a la anterior, es que la alusión que nos ocupa se refiera a datos que en efecto son de la persona jurídica pero que afecten a la intimidad de las personas físicas *en* la persona jurídica (por ejemplo, de los socios, directivos o empleados de la misma o datos cuyo titular es una asociación cultural o política que afecta a los afiliados o socios), como apuntó Morales Prats dando al precepto una "extensión instrumental de la tutela de la intimidad"[61]. Ésta es la interpretación del artículo 200 que parece que va prevaleciendo en el panorama jurisprudencial[62].

Algunas resoluciones de Audiencias, adscribiéndose a esta lectura, consideran también posible que la conducta afecte a la intimidad personal de terceros[63]. Y también un sector de la doctrina asume esta posibilidad[64]. Pero, con esta interpretación, volvería a resultar redundante el precepto con respecto al artículo 197.

En suma, el artículo 200 no deja de resultar extraño y en la práctica propicia algunas raras afirmaciones además de algunas aplicaciones que me parecen desenfocadas. Como ejemplo de las primeras, la SJP_7 de Palma de Mallorca de 14-3-2001, incidió en la idea de la extensión de la tutela de la intimidad a los datos reservados de las personas jurídicas afirmando incluso que las personas jurídicas tienen derecho a la intimidad si

---

59. Las conductas del art. 200 se limitan al descubrimiento, la revelación y la cesión de datos, dejando al margen otras conductas referidas en los artículos anteriores, como el apoderamiento, la utilización, la modificación o la alteración de los datos. Véase al respecto, críticamente, Romeo Casabona: *Los delitos de descubrimiento y revelación de secretos*, cit., pág. 213.

60. Ante hechos como los descritos, el Tribunal Supremo recurre al delito continuado (art. 74), aunque en relación con el artículo 197.1 (y no con el art. 200), como en la STS de 19-12-2005, en un caso en que el acusado, funcionario de Hacienda, extrajo y facilitó a terceros durante un periodo de tiempo de más de dos años "numerosa documentación relativa a personas físicas y personas jurídicas". También, en un caso muy similar de *tráfico de datos*, la STS de 18-7-2005.

61. "La protección penal de la intimidad frente al uso ilícito de la informática en el Código penal de 1995", en C.G.P.J., *Cuadernos de Derecho Judicial*, "Delitos contra la libertad y la seguridad", Madrid, 1996, pág. 192. También en Quintero Olivares/Morales Prats: *Comentarios a la Parte especial del Derecho penal*, cit., pág. 454. A esta extensión le ha dotado el mismo autor de una importante virtualidad práctica a efectos de la persecución del delito, conforme a lo establecido en el artículo 201 del Código penal, al legitimar a las personas jurídicas para hacerlo en cuanto persona agraviada. Véase también Huerta Tocildo/Andrés Domínguez: "Intimidad e informática", cit., pág. 70.

62. Véanse, entre otras, la SJP_7 de Palma de Mallorca de 14-3-2001, la SAP de Sevilla de 15-2-2002 (caso de apoderamiento de datos de la vida laboral de un trabajador de los que disponía una empresa en el que se condenó por el art. 200), la SAP de Asturias de 14-7-2003 y el AAP de Barcelona de 17-3-2006.

63. Así, por ejemplo, los Autos de la AP de Madrid de 28-4-1999 (f. de D. Primero) y de la AP de Barcelona de 22-10-2004 (razonamiento jurídico segundo).

64. Por ejemplo, A. Jorge Barreiro en Rodríguez Mourullo/Jorge Barreiro: *Comentarios al Código penal*, cit., pág. 591.

"el quebranto de su intimidad [*sic]* repercute en o trasciende a las personas físicas que les representan" (f. de D. 2º). Y, como muestra de las segundas, la SAP de Alicante de 23-3-1999 justificó la aplicación del precepto en un caso de apoderamiento de un documento interno de una Caja de Ahorros referente a una sociedad mercantil en el que "se recogía respecto de ésta la situación de activo y pasivo o de riesgo tanto de operaciones actuales como fallidas" en que "tales datos reservados o secretos pertenecían a la Caja de Ahorros" (f. de D. primero). Esta sentencia fue luego confirmada sin más comentarios por el Tribunal Supremo (S. de 21-3-2001), pese a que los hechos afectaban a una mercantil en aspectos relacionados con su explotación.

Estas han sido algunas de las resoluciones más desvinculadas de la intimidad que se encuentran en la escasa jurisprudencia habida sobre el particular hasta la fecha. Y constituyen en todo caso una excepción, porque, como señalé, la línea que se va imponiendo y se reafirma es que el artículo 200 solamente puede aplicarse "cuando la conducta consistente en descubrir, divulgar o ceder los datos reservados de personas jurídicas pueda afectar a la intimidad de terceros o a los propios individuos que forman parte de aquellas de forma que la alusión a los datos reservados de las personas jurídicas se proyecta sobre datos, en principio de personas jurídicas, pero con trascendencia en la intimidad de las personas físicas" (AAP de Madrid de 28-4-1999, f. de D. primero)[65].

Sin embargo, la línea dominante, aunque comprensible, no puede convencer por las razones que ya han sido señaladas. Realmente, en el difícil contexto creado por la presencia del artículo 200, ninguna opción interpretativa resulta impecable, pero en mi opinión la alternativa más convincente es la de entender que la Ley se refiere, en efecto, exactamente, a "datos reservados de personas jurídicas"[66]. Siguiendo un modelo paralelo al plasmado en los delitos de allanamiento de morada, domicilio de personas jurídicas y establecimientos abiertos al público (arts. 202-204, ubicados bajo el mismo Título de los delitos contra la intimidad), parece que este precepto tiene por objeto la protección de personas jurídicas (no mercantiles: asociaciones, fundaciones u otras) frente a comportamientos que puedan dañarlas en su actividad mediante el descubrimiento, la revelación o la cesión de sus datos reservados. De este modo, se trataría de un precepto que cumpliría en el ámbito de las personas jurídicas no mercantiles una función semejante a aquella que desempeñan los artículos 278 a 280 en el terreno de las empresas, considerando que también las personas jurídicas no mercantiles desempeñan importantes funciones que pueden ser seriamente afectadas por conductas como las que recoge el artículo 200, que pueden dañar su capacidad ejecutiva en su correspondiente ámbito de actividad. Por ejemplo, el caso de la revelación o cesión de datos (socios, estrategias, acciones previstas, contactos, etc.) de una ONG[67].

---

65. Véanse, en la misma línea, las resoluciones citadas en la nota 62.

66. Próximo, Romeo Casabona ha afirmado que "Las personas jurídicas sí gozan de una confidencialidad o reserva propia y autónoma de la de sus miembros, o con mayor, precisión, de una protección de *datos reservados*, que es el bien jurídico protegido, con independencia del contenido o valor económico que puedan ostentar estos datos"(en *Los delitos de descubrimiento y revelación de secretos*, cit., pág. 210).

67. Cabría pensar, incluso, en las personas jurídicas mercantiles por lo que se refiera a datos reservados sobre aspectos que no comprometen directamente su ventaja competitiva, pero que les afecten de otro modo, como, por ejemplo, actuaciones incoherentes desde el punto de vista ético que desean mantenerse ocultas (por ejemplo, una empresa de alimentos ecológicos que posea plantaciones de cultivos transgénicos, una empresa de alimentos infantiles cuyos proveedores se sirvan del trabajo infantil o un laboratorio farmacéutico que utiliza para probar sus fármacos a personas pobres de países subdesarrollados, etc.).

Sin embargo, si ésta no es una lectura incorrecta, considero que la opción político-criminal así plasmada debe ser criticada. Efectivamente, además de por las razones sistemáticas que ya se han señalado y que se refieren a la fricción de la protección penal de los datos secretos de las personas jurídicas con el rótulo legal del Título de los "delitos contra la intimidad", debe ponerse de manifiesto que la actuación del Derecho penal resulta en este caso completamente desproporcionada desde el punto de vista de su necesidad, considerando que el Derecho penal es aquí la *unica ratio legis*, puesto que fuera del Derecho penal no existen otros ilícitos con los que se pretenda contener tales conductas.

III. LOS DELITOS DE ESPIONAJE INDUSTRIAL (DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS DE EMPRESA)

Los artículos 278 a 280 del Código penal recogen los delitos relacionados con el llamado "espionaje industrial", aunque albergan conductas que no se ajustan a esta denominación porque no se dirigen a obtener datos secretos (sino, por ejemplo, que ya se poseen legítimamente) o no se refieren estrictamente a una actividad industrial (sino, más bien, empresarial). Por estas razones se conocen como "delitos de descubrimiento y revelación de secretos de empresa", utilizándose una denominación análoga a la que el Código penal aplica a los delitos de los artículos 197 a 201. Esta designación resume muy bien, además, las clases principales de las conductas que se recogen (efectivamente, sobre todo, de descubrimiento y de revelación de secretos) y resulta muy oportuna teniendo en cuenta que la estructura de este grupo de artículos responde al mismo esquema del 197.1 y 3, lo que permite, incluso, la remisión expresa a éste desde el 278.1 para completar alguna de sus referencias típicas. De modo que la diferencia fundamental entre aquellos y estos delitos se halla en el objeto que se pretende proteger, el secreto de empresa, desde el que se debe dotar de contenido a los datos, documentos, comunicaciones, etc. a los que aparecen vinculadas las conductas típicas.

1. Concepto de "secreto de empresa"

El concepto de secreto de empresa alude a cualquier información reservada (incluso, naturalmente[68]) por la empresa debido a la importancia de su conocimiento en exclusividad para dotarle de una ventaja competitiva en el mercado. Esta ventaja procede del conocimiento determinado (*know-how*) que aporta sobre ideas, productos, servicios, modo de organización de la empresa, procedimientos productivos, estrategias de mercado, etc., relevantes para la actividad empresarial de que se trate[69]. Aunque, eso sí: deben ser cono-

68. Véase la nota 76.

69. Aunque la interpretación doctrinal y jurisprudencial absolutamente dominantes relacionan el valor del secreto de empresa con la ventaja competitiva que le proporciona (por lo que se refiere a la doctrina, véase, por todos, sobre esto, y en general sobre el secreto de empresa, Carrasco Andrino, M.: *La protección penal del secreto de empresa*, Barcelona, 1998, págs. 139-140 y Morón Lerma, E.: *El secreto de empresa: Protección penal y retos que plantea ante las Nuevas Tecnologías*, Cizur Menor, 2002, págs. 128 y ss.; con más referencias, Martínez-Buján Pérez, C.: *Derecho penal económico y de la empresa. Parte especial*, 2ª ed., Valencia, 2005, págs. 212 y 215; y, en cuanto a la jurisprudencia véanse, también sólo a título de ejemplo, las resoluciones siguientes: AAP de Madrid de 28-4-1999, SAP de Lleida de 12-2-2001, SAP de Barcelona de 30-12-2002, SAP de Asturias de 14-7-2003, SAP de Córdoba de 20-10-2004, …

cimientos cuya explotación pueda proporcionar una ventaja actuando en el mercado conforme a las reglas del "*fair play*"; esto es, cuya utilidad no se obtenga (o no se obtenga exclusivamente) como consecuencia de su aplicación en o por medio de comportamientos ilícitos (algo que, desde luego, es muy vago y difícil de concretar en la práctica). De este modo, se pretende evitar que el Derecho penal sirva para tutelar medios o instrumentos destinados a ser aplicados con fines gravemente desleales en el mercado o, incluso, fraudulentos o de otro modo peligrosos para los consumidores y usuarios de los productos y servicios. Por lo tanto, y en suma, "no cualquier dato, por ser de la empresa, ha de entenderse como secreto" (SAP de Guipúzcoa, 30-12-1998, f. de D. quinto).

Bajo las restricciones anteriores, los secretos de empresa pueden ser relativos a conocimientos sobre la producción (descubrimientos científicos, invenciones, modelos de utilidad, dibujos y modelos industriales, etc.), la distribución y comercialización de los productos o servicios (el llamado "*trade secret*", que incluye listas de clientes y proveedores, tablas o tarifas de precios, márgenes comerciales, etc.) o de gestión (es decir, conocimientos sobre la organización y administración de la empresa, relativos a aspectos financieros, a la planificación de la actividad, etc., a menudo incluidos entre los "secretos comerciales", expresión que se utiliza como una clase residual). Pero no existen clases enteras de informaciones que constituyan invariablemente, en todos los casos, materia propia de un secreto de empresa (por ejemplo, no siempre lo serán los proyectos[70] y estudios, ni las listas de clientes[71], proveedores, precios, etc.), sino

---

…
AAP de Barcelona 17-3-2006, SAP de Granada de 2-2-2007, AAP de Guipúzcoa de 19-2-2007, SAP de Guipúzcoa de 15-5-2007), la SAP de Sevilla de 19-10-2007 ha afirmado, apoyándose en argumentos extraídos, fundamentalmente, de la regulación penal precedente y del Proyecto de 1992, que "no resulta conceptualmente necesario que los datos reservados tengan precisamente un interés económico […] dentro de la expresión «secreto de empresa» hemos de entender comprendido cualquier dato que la empresa tenga intención de preservar del conocimiento público, sin que esté necesariamente relacionado con una ventaja competitiva o con un interés exclusivamente económico. Ciertamente, ha de estar relacionado con el tráfico mercantil propio de la actividad de la empresa en cuestión, pues de otro modo no sería calificable de «secreto de empresa», pero fuera de esta especificación el tipo penal no exige ninguna otra" (f. de D. tercero). Los hechos de los que entendió esta sentencia consistieron en el apoderamiento y publicación en Internet de un listado que contenía miles de fichas de clientes de una clínica de tratamientos de estética que recogían con respecto a cada uno –solamente– un código numérico y su nombre de pila, además de las fotografías del médico director y de otra médica empleada. Para la calificación jurídico-penal de estos hechos, la Audiencia Provincial encontró –obviamente– una importante dificultad en la interpretación generalizada del secreto de empresa y tuvo que forzar del modo indicado el concepto al uso del "secreto de empresa", en el que llegó a considerar que quedarían "absorbidos" (!) los demás hechos (la publicación de las fotografías de los médicos).

70. Por ejemplo, porque carezcan de entidad o valor suficiente para que la información que incorporan pueda ser considerada una información relevante. Tal fue el caso de "los programas de actividades y de actos lúdicos" ("campamentos de recreo, jornadas de convivencia, campañas de Navidad, campeonatos de fútbol, día de la madre en centros comerciales, actividades de animación, fiestas de carnaval, de disfraces o de San Valentín, certámenes musicales o de otra naturaleza"), su horario, la infraestructura y los medios precisos para su desarrollo, a los que se refieren los hechos de la SAP de Burgos de 26-1-2004.

71. Éstas suelen considerarse por los juzgados y tribunales generalmente aptas para integrar el secreto de empresa, aunque en alguna sentencia se ha señalado su improcedencia (por ejemplo, en la SAP de Barcelona de 18-1-2001, f. de D. segundo, diciendo: "se protege […] el secreto empresarial mediante la descripción de unas figuras típicas que lesionan la seguridad que para la posición de la empresa en el mercado supone el conocimiento exclusivo de determinados datos internos y relativos a su actividad, quedando fuera por tanto de su ámbito de cobertura aquellos datos, como el listado de clientes, en modo alguno calificables de secreto empresarial"; también, en la STS de 29-10-1999, f. jco. 2º, citada por Morón Lerma en *El secreto de empresa*, cit., pág. 292.).

que dependerá de las circunstancias de la empresa concreta y del sector de actividad en el que opere[72], y nunca sólo de la voluntad del empresario de considerar que es un "secreto" una determinada información sin condiciones objetivas para poderlo ser[73]. También puede depender del tratamiento que la empresa haya hecho de una información que era accesible para terceros ajenos a la empresa (o sea, no secreta) pero cuyo resultado sí resulta valioso para la explotación[74].

2. Conductas típicas

Sobre la clase de conocimientos que se han descrito, o mejor dicho, sobre los soportes y objetos que los recogen, plasman o transmiten, recaen unas conductas típicas tan variadas como las del artículo 197, y en una buena parte análogas a aquéllas: de apoderamiento de objetos, de interceptación de las telecomunicaciones, de empleo de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, de revelación, difusión o cesión a terceros de los secretos conocidos o descubiertos o, por último, de utilización del secreto legítimamente conocido en provecho propio.

Aunque estos comportamientos no requieren el empleo de medios informáticos en todos los casos, todos ellos resultan aptos para ser cometidos mediante instrumentos de esa naturaleza (programas informáticos, equipos periféricos y terminales, etc.), en cuyo caso los riesgos para el bien jurídico inherentes al empleo de estos medios pueden, efectivamente, ser más graves en el caso concreto (peligro derivado de la mayor facilidad para su captación o de la mayor facilidad de difusión de los datos o conocimientos obtenidos). Pero, aparte de esto, prácticamente, la única referencia expresa que se encuentra en estos artículos a los medios o instrumentos informáticos es la que se hace al apoderamiento "de soportes informáticos u otros objetos que se refieran al mismo" (art. 278.1[75]).

Dado el paralelismo de las conductas típicas de los artículos 278 a 201 con las del artículo 197.1 y 3, muy pocas son las particularidades que aquí se presentan (salvando, naturalmente, las que imponen los distintos objetos a los que están orientadas

---

72. Véase, a propósito, el AAP de Madrid de 13-5-2004, con referencia a unos hechos en los que estas características desempeñaban un papel fundamental para negar su tipicidad, diciendo: "difícilmente se puede predicar tal condición [sc. de secretos] del listado de clientes de la empresa [...] precisamente en relación a la distribución de un producto restringido a un mercado muy concreto, el de transportistas, donde las empresas son escasas y perfectamente conocidas por todas las personas que operan en el sector" (f. de D. primero).

73. Así, la SAP de Barcelona de 30-12-2002 (f. de D. cuarto) y, en idéntico sentido, la SAP de Burgos de 26-1-2004 (f. de D. primero). También, la SAP de Tarragona de 4-4-2003 (f. de D. segundo).

74. En esta dirección, la SAP de Alicante de 19-12-1998 dio el tratamiento de "secreto de empresa" a "datos cognoscibles que, aunque no se reputen un secreto, implica el ahorro de un inmenso trabajo de captación y contraste de técnicas y criterios de ventas (sobre todo precios), que hicieron que de inmediato comenzase a funcionar el negocio con el consiguiente perjuicio para la empresa propietaria que los había pacientemente elaborado". Es decir, que los datos que se utilizaron "podían pacientemente ser averiguados, por la nueva empresa, aunque le hubiera costado algún tiempo" (f. de D. primero). Esta resolución, que había condenado al procesado por un delito del artículo 278.1, fue casada por el Tribunal Supremo en Sentencia de 16-2-2001, aunque por razones que no tienen que ver con las afirmaciones anteriores.

75. Véase también la alusión a los "soportes informáticos" en su número 3.

las conductas en unos y otros delitos). Pero sí hay algunas que son muy relevantes y que derivan de la clase de secretos de que se trata.

La primera es la que ofrece la figura que consiste en la difusión, revelación, cesión o utilización del secreto en provecho propio llevada a cabo por quien tuviere legal o contractualmente obligación de guardar reserva (art. 279). A la vista de esta disposición, solamente puede cometer el delito quien tuvo un acceso legítimo a la información reservada por razón de su empleo en la empresa (es, pues, un delito especial que solamente pueden cometer los directivos o los trabajadores de la empresa). Se trata de sujetos que es preciso que conozcan o manejen datos o conocimientos para el desempeño de su trabajo en la empresa, información que la empresa desea mantener en exclusiva para sí por razones competitivas. Teniendo en cuenta la posición de confidentes necesarios que ocupan los directivos o los trabajadores en estos casos, estas personas pueden tener por ley o por contrato un deber expreso y específico de sigilo con respecto a los datos, informaciones o conocimientos que manejan o poseen con el fin de preservar la posición de la empresa en el mercado.

Pues bien, cuando así sea, podrán plantearse dudas sobre el alcance temporal de la obligación pero no, obviamente, sobre si dichos sujetos están obligados, o no, a mantener la reserva. Efectivamente, en supuestos así, la pregunta fundamental es si la obligación de secreto persiste después de cesar en el empleo y, en caso afirmativo, si entonces persiste ilimitadamente. Esta cuestión surge, evidentemente, en los casos en los que no se ha previsto específicamente este extremo junto a la cláusula de confidencialidad (o no concurrencia), pero también la suscita la ley cuando se establece dicha obligación sin límite alguno (caso de la Ley de Sociedades Anónimas y la Ley de Sociedades de Responsabilidad Limitada), pues de este modo extiende desmesuradamente la reserva.

Sin embargo, en otros casos que ofrece la práctica la duda es si existía en absoluto aquella obligación de mantener el sigilo, aunque la ley no disponga nada y pese a no haberse previsto en el contrato. La premisa fundamental sobre la que necesita apoyarse esta cuestión es una interpretación de la obligación de guardar reserva a la que alude el artículo 279 en términos puramente materiales; es decir, como si se refiriese a que en los casos en los que dada la (evidente) importancia de la información de la empresa su carácter secreto resulta "natural" y no deberá difundirse, revelarse, etc.[76].

Al respecto, es doctrina común de los tribunales que "la obligación de guardar reserva, si es expresa, convierte al sujeto en garante de protección, pero si es genérica –la derivada de la buena fe y de la diligencia a la que alude al art. 5 a) del Estatuto de los Trabajadores– sólo dará lugar a una infracción de deberes genéricos originadora, en su caso, de una responsabilidad civil"[77].

---

76. Las SSAP de Granada de 24-10-2005 y 2-2-2007 han reconocido la posibilidad de que exista información "naturalmente reservada" en aquellos casos en los que posea un indudable interés económico "por incidir en la capacidad competitiva de la empresa" (en ambas, f. de D. segundo). Pero lo normal es que a los jueces y tribunales les baste para desestimar el castigo con constatar que no se pactó y que no existía una norma especial que impusiera el deber de reserva al trabajador (véase así, por ejemplo, la SAP B 7-6-1999).

77. AAP de Madrid de 28-4-1999 (f. de D. 2º), SAP de Barcelona de 7-6-1999 (f. de D. tercero), SAP de León de 21-2-2007 (f. de D. tercero, con más referencias), AAP de Guipúzcoa de 19-2-2007 (razonamiento jco. quinto)

Con todo, en la práctica, resulta en muchos casos imposible de distinguir el "secreto de empresa" de los conocimientos que los directivos o los empleados han adquirido de un modo u otro con su trabajo en la empresa, bien porque dichos conocimientos son el resultado de informaciones elaboradas por los mismos sujetos en la empresa[78] o porque proceden del desarrollo de habilidades propias con ocasión del mismo. Por ejemplo, en determinados casos, el trabajo con los clientes durante unos años hace que no se tenga que sustraer ningún documento para conocer quiénes son o poder comunicar con ellos[79]. En estos supuestos, el manejo de la información que se posee solamente puede limitarse mediante cláusulas expresas legales o convencionales, que serán las que terminarán definiendo el ámbito de las posibles conductas típicas a la vista de la remisión del artículo 279. De manera que el abandono de la empresa anterior para la creación de una propia dedicada a la misma actividad constituirá en otro caso el mero ejercicio de la libertad de empresa[80].

La segunda referencia típica que merece, dada su singularidad, un breve comentario en el contexto en el que se inscriben estas líneas es la que alude a la "utilización del secreto en provecho propio". Se contempla en el mismo artículo 279, también con respecto a quien se encuentra en una relación legítima con el secreto (y está obligado a guardar reserva). Se trata de un supuesto para el que la ley aminora la pena prevista para las conductas de difusión, revelación o cesión del secreto, pese a que su utilización supone su puesta en obra, su efectiva aplicación. Esto, que puede llamar la atención en un primer momento, desde el punto de vista del injusto a que da lugar tiene una explicación: aquéllas conductas pueden resultar más peligrosas para la posición de la empresa en el mercado que la aplicación del secreto por un competidor determinado[81].

---

78. Considerando que este hecho es muy relevante véanse, por ejemplo, la SAP de Burgos de 26-1-2004 (f. de D. primero) y la SAP de Córdoba de 12-3-2007 (f. de D. quinto). Sin embargo, la SAP de Guipúzcoa de 30-12-1997 advirtió, con razón, que aunque unos determinados datos se hayan obtenido con el propio trabajo del empleado, no por eso los datos dejan de ser de la empresa por y para la que se trabaje.

79. Así, el AAP de Madrid de 12-5-2003 (f. de D. primero), la SAP de Córdoba de 20-10-2004 (f. de D. sexto: "ni apoderamiento ni aprovechamiento, simplemente utilización de los conocimientos que por su cargo tenía"), el AAP de Guipúzcoa de 12-5-2006 (razonamiento jco. primero) o el AAP de Castellón de 15-5-2006 (razonamiento jco. tercero). Al igual que el AAP de Madrid de 12-5-2003, citado, la SAP de Córdoba de 12-3-2007, además de reproducir esta misma idea, indica que en estos casos lo único que hubiera podido obstaculizar jurídicamente la utilización de la información habría sido un pacto de no concurrencia (f. de D. quinto).

80. Así, la SAP de Barcelona de 18-1-2001 (f. de D. primero).

81. Véase, sin embargo, con interesantes matices, Morón Lerma: *El secreto de empresa*, cit., págs. 386 y 387. Y, con referencias, Anarte Borrallo, E.: "Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información", en *Derecho y Conocimiento. Anuario Jurídico sobre la sociedad de la información*, Vol. I, Huelva, 2001, pág. 242 y nota 315. De un caso de estas características entendió la SAP de Zaragoza de 3-12-1999, castigando a los procesados a las penas mínimas (un año de prisión y multa de doce meses) conforme al art. 280 (y no por el 279) por no constar cómo pudo haber llegado la lista antigua de clientes que poseía uno de ellos, ex trabajador de otra empresa del mismo sector, que aplicó para las ventas de un producto similar. Debe ponerse de manifiesto que, pese a que el límite inferior de la pena de prisión del art. 280 es menor para estos casos (un año) que el de la misma pena en el art. 279 (dos años), no lo es el superior (3 años en ambos casos), perdiéndose la simetría con la gravedad de una y otra conducta en este extremo.

3. Relaciones concursales

En cuanto a las relaciones concursales de estos delitos, el artículo 278.3 contempla una innecesaria y distorsionada cláusula referida a "las penas que puedan corresponder por el apoderamiento o destrucción de los soportes informáticos". Pese a la previsión de las reglas de los artículos 73 y siguientes del Código, no son extrañas algunas de estas reiteraciones en la parte especial del Código que, si bien no contribuyen a la economía legislativa, pueden acaso cumplir alguna (débil) función preventivo-general o de otro tipo, pero siempre a riesgo de comportar algún coste. Aquí, el de la duda que plantea su falta de referencia a las mismas conductas que recaigan sobre soportes no informáticos de los secretos.

También en el terreno de los concursos se debe hacer en este contexto una observación sobre la posible concurrencia de los delitos de descubrimiento y revelación de secretos de empresa con alguna de las figuras del delito de descodificación y facilitación de la señal de acceso a servicios restringidos de radiodifusión sonora o televisiva u otros, del nuevo artículo 286 del Código penal, obra de una de las reformas de 2003 (L.O. 15/2003). Esta observación es debida, sobre todo, a la vista de la interpretación de la SAP de Barcelona de 4-11-2002, que, a falta de este nuevo precepto –de penalidad más leve– en los momentos de enjuiciamiento del hecho, condenó a los autores por un delito de descubrimiento y revelación de secretos de empresa por fabricar, vender y distribuir tarjetas aptas para la decodificación de una señal de televisión emitida de un modo exclusivo para sus abonados. En este caso, la Audiencia consideró que los códigos desencriptadores grabados por los acusados tenían el carácter de secretos de empresa (por ser confidenciales, exclusivos y claves para el mantenimiento de la actividad de la empresa propietaria "al punto de que su mantenimiento fuera del conocimiento y alcance del público en general constituye un presupuesto necesario para la pervivencia de la empresa propietaria de los códigos", f. de D. décimo[82]). No obstante, una argumentación hecha, fundamentalmente, en clave de injusto, como la de esta resolución no es suficiente para considerar cometido el delito de descubrimiento y revelación de secretos. Efectivamente, la Sentencia argumentó, sobre todo, acerca de la lesividad de la conducta para la empresa suministradora del servicio y propietaria de los códigos encriptados (lesividad que está fuera de toda duda), pero no fundamentó tanto el asiento típico del comportamiento en el art. 278.2, base de la imputación de este delito. En mi opinión, la difusión y cesión a terceros en soportes tarjeta "de unos determinados códigos desencriptadores de otros" pone de manifiesto el quebranto de unos códigos, pero esto no equivale al descubrimiento de un secreto de empresa; es decir, seguramente, los autores ni siquiera llegaron a tener que conocer los códigos encriptados para quebrantarlos. Y, si lo que averiguaron fueron las vías para hacerlo (por ejemplo, el tipo de códigos a aplicar) a partir de los propios decodificadores legítimos, no podríamos hablar de apoderamiento de un secreto de empresa del art. 278 del Código penal.

4. Rasgos característicos de la jurisprudencia en materia de secretos de empresa y perspectivas

Por último, un breve comentario sobre lo que manifiestan las resoluciones de los juzgados y tribunales sobre estos delitos. Sus rasgos más característicos son los siguientes:

---

82. Véase, reproduciendo esta misma doctrina, la SJP_1 de León de 9-2-2004, f. de D. Tercero, que no obstante absolvió al procesado ante la falta de prueba de que hubiera difundido, revelado o cedido "el secreto de empresa".

Se trata de una jurisprudencia que no ha sido abundante hasta fechas recientes, pero cuyo volumen ha ido aumentando considerablemente en estos últimos años[83]. Las cuestiones más litigiosas que se plantean son, en primer lugar, las que se refieren a la relevancia de la información para dotar a la empresa afectada de una verdadera ventaja competitiva y, en segundo lugar, las que examinan la mayor o menor dificultad para la obtención de la información (o, dicho de otro modo, la disponibilidad, o no, de la información por terceros ajenos a la empresa –y, en consecuencia, el carácter efectivamente "secreto" de la información).

La mayoría de los hechos de los que entienden las sentencias tienen que ver con las listas de clientes de las empresas. Generalmente, además, son sentencias que terminan con la absolución de los procesados, bien por la falta de prueba del apoderamiento o del conocimiento del origen ilícito del documento u objeto[84] o de la aplicación o uso del secreto, bien porque, en efecto, se demuestra que la información podría haberse obtenido de otro modo (lícito) al alcance de cualquiera o, incluso, era ya conocida[85].

En conclusión, en este sector de delitos se aprecia una notable indefinición de conceptos que son absolutamente fundamentales, empezando por el propio "secreto de empresa". El examen detenido de la jurisprudencia pone de manifiesto que quizá el término "secreto" puede distorsionar en la práctica la característica que ha de poseer el objeto de las conductas en relación con el bien jurídico: lo principal es que la información sea valiosa, pero no sólo por ser secreta, sino por ser exclusiva, por ser propia de la empresa por haber sido obtenida, tratada de una determinada manera o, incluso, recopilada o elaborada según un procedimiento que la hace importante en términos empresariales y que ha requerido la aplicación de una inversión de dinero y de tiempo. Es ésta, pues, una idea más próxima a la propiedad industrial cuyas posibilidades puede ser interesante explorar a la vista de las limitaciones que se ponen de manifiesto cuando se observa el *Derecho real* que rige en esta materia.

---

83. En correspondencia con el crecimiento del espionaje industrial. En particular, el "ciberespionaje" industrial creció un 18% en España en 2007 (véase http://www.elpais.com/articulo/red/ciberespionaje/industrial).

84. Así, por ejemplo, las siguientes resoluciones: SAP de Madrid de 30-12-1999, AAP de Madrid de 28-4-1999, SAP de Barcelona de 11-2-2000 y la SAP de Asturias de 14-7-2003.

85. SSAAPP de Asturias de 14-7-2003 y de Córdoba de 20-10-2004.