La protección penal de datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías

Ricardo M. Mata *Profesor Titular de Derecho Penal Universidad de Valladolid*
rimata@der.uva.es

SUMARIO: I. Introducción. 1. Tutela de datos y su protección penal. 2. Dirección de ataque de los hechos contrarios a la tutela datos. II. Dimensiones de la protección de datos personales. III. Panorama general de la regulación de protección de datos. IV. Relevancia penal de la protección de datos personales y familiares. 1. Principios constitutivos del Derecho penal como presupuestos general. 2. Regulación penal: comportamientos típicos. V. Conductas punibles. 1. Protección de secretos documentales. 2. Interceptación de telecomunicaciones y control audiovisual clandestino. 3. Tutela penal de datos recogidos en ficheros, archivos o registros electrónicos.

I. Introducción

1. Tutela de datos y su protección penal

La tutela de datos tiene que ver con la regulación legal que dispensa protección a los datos en el sentido de unidad relevante de información, frente a intromisiones ilegítimas que los descubran, modifiquen, destruyan o hagan públicos. Sin embargo, los datos protegidos pueden tener un carácter y finalidad muy diversa. Pueden poseer una naturaleza económica o comercial, bien puede tratarse de datos personales o bien pueden concernir a la defensa nacional. Debido a este amplio espectro de los datos, en realidad la tutela penal de los mismos no es una realidad unívoca[1], pues no poseen una conexión exclusiva o unitaria directa, sino que la regulación penal relativa a datos puede vincularse a distintos bienes jurídicos. En el Código penal español los datos económicos o comerciales se vinculan a los delitos contra el mercado, los que afectan a la seguridad nacional a los delitos relativos a la defensa nacional, o los datos de carácter personal tienen que ver con los delitos que atacan la intimidad. Así se contienen en otros preceptos y lugares sistemáticos del Código penal lo relativo al descubrimiento y revelación de secreto de empresa o comerciales (arts. 278 y ss. CP) o al descubrimiento y revelación de secretos laborales y profesionales (art. 199 CP), procesales (art. 446 CP), o los relativos a la defensa nacional (arts. 598 y ss. CP).

Nosotros vamos a tratar exclusivamente la protección penal de datos desde el ángulo de la intimidad de las personas, es decir, la protección penal de datos personales. Se trata de un acercamiento a aquellas conductas vinculadas a la transgresión de la intimidad de otro, en especial al quebrantamiento de la esfera íntima relativa a datos contenidos en soporte electrónico, que alcanzan relevancia jurídico-penal. El desarrollo de las comunicaciones ha llevado necesariamente a evidenciar nuevos riesgos para la intimidad de las personas, hasta el punto que puede decirse que "la protección de datos personales en el ámbito general de las comunicaciones electrónicas constituye el desafío más evidente de la sociedad tecnológica"[2].

Como se ha mencionado vamos a realizar una aproximación general al sistema y a las conductas punibles que afectan a la intimidad de las personas, particularmente en aquellos casos en los que se conculca por el autor la intimidad informática –habeas data–[3]. Desde el punto de vista indicado, las conductas toman como referencia la inti-

1 Cfr. HAMM, R. *Der strafrechtliche Schutz personenbezogener Daten in Gegenwart und Zukunft. El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Tomo I. Valencia 2003, pág. 57.

2 BALLESTEROS MOFFA, L.A. *La privacidad electrónica. Internet en el centro de protección*. Tirant lo Blanch/Agencia Española de protección de datos. Valencia 2005, pág. 139.

3 Materia de la que ya nos hemos ocupado en *Delincuencia informática y Derecho penal*. Edisofer, Madrid 2001, págs. 125 y ss. También en "Criminalidad informática: una introducción al Cibercrimen". *Temas de Direito da informática e da Internet*, Coimbra Editora, 2004, págs. 207 y ss.

midad de las personas. El concepto general de intimidad se refiere al "ámbito personal donde cada uno, preservado del mundo exterior, encuentra las posibilidades de desarrollo y fomento de su personalidad" (BAJO)[4]. Si en el complejo mundo actual este espacio reservado de las personas podía ya ser objeto de múltiples ataques, la aparición de las Nuevas Tecnologías ha supuesto un enorme ensanchamiento de estos riesgos. El objeto de la exposición es entonces la tutela penal de esos datos personales y familiares que conciernen a la intimidad de una persona, por lo que a la tutela de otro tipo de datos no vamos a prestar atención en este momento. Como se verá la regulación penal española también diferencia los ámbitos a los que pertenecen los datos que pueden ser objeto de tutela penal.

2. Dirección de ataque de los hechos contrarios a la tutela de datos

La creciente dependencia de todos los sectores de la vida social de su conexión a procedimientos automatizados e informatizados hace que los hechos irregulares e ilícitos que puedan ser cometidos a través o sobre este tipo de sistemas alcancen progresivamente una mayor trascendencia. Los servicios públicos (sanidad, regulación del tráfico rodado, aéreo o marítimo, etc.), la producción industrial, el comercio, la defensa de un país o la enseñanza, van integrándose inexorablemente en el entramado de las tecnologías de la información y telecomunicaciones. Junto a las indudables aportaciones y beneficios que proporcionan al ser humano, las Nuevas Tecnologías también engendran nuevos riesgos y ocasiones para la realización de hechos ilícitos. Con la eclosión de las nuevas tecnologías el ámbito de la privacidad de las personas se ha visto sometido a riesgos más intensos, debido a la capacidad lesiva de estos nuevos medios que permiten almacenar grandes cantidades de datos e informaciones relativas a personas, así como un tratamiento automatizado de los mismos a gran velocidad[5]. Por ello también el Ordenamiento Jurídico ha respondido con medidas específicas relativas a la tutela de la privacidad informática.

En el ataque a la intimidad materializado en los datos personales existe una nueva dimensión que aporta un cambio cualitativo. Y esta nueva dimensión hace referencia a la posibilidad de que sea el propio ser humano el objeto de ataque de una manera hasta ahora cualitativamente desconocida. Las posibilidades abiertas por los nuevos sistemas de almacenamiento y tratamiento de información personal, de acceso y descubrimiento de un conjunto amplio de datos de toda índole, hacen que estos hechos adquieran una significación añadida. Por su propia naturaleza los sistemas informáticos permiten contener una ingente cantidad de información sobre un número elevadísimo de personas, un tratamiento automatizado y a gran velocidad de esa misma información, así como una gran capacidad de adaptación a las exigencias actuales del hombre. Estas características técnicas de los sistemas de almacenamiento y tratamiento automatizado de datos viene a cubrir una necesidad de las sociedades más avanzadas, cada vez más complejas y que ofrecen una más amplia prestación de servicios de todo género. Las sociedades modernas requieren, por su propio dinamismo y complejidad, la existencia de sistemas de información de una amplia gama de datos personales (sanitarios, fiscales, financieros, profesionales, de prestación de servicios, etc.). Se ha destacado, además, como valor más innovador de las nuevas tecnologías el que la información haya pasado a constituir un valor económico de primera magnitud. Los procedimientos informáticos representan desde esta perspectiva la capacidad de acceso a la información, la posibilidad de información sobre la información.

Pero con todo ello lo que sucede es que se genera la posibilidad no sólo de acceder y manejar aspectos de la privacidad de las personas, sino que potencia la construcción

4 "Protección del honor y de la intimidad". *Comentarios a la Legislación Penal*, Tomo I, Edersa 1982, pág. 101.

5 Pueden verse al respecto las interesantes observaciones que, sobre el aumento de la capacidad de vigilancia se produce con las Nuevas Tecnologías, hace David LYON, *El ojo electrónico. El auge de la sociedad de la vigilancia*. Alianza Editorial. Madrid 1995, págs. 130 y ss. Como señala este autor en realidad el control sobre la información no es nuevo, el cambio que se produce es el de la "informatización de la información", pasando de la vigilancia de papel a la vigilancia electrónica, de forma que la combinación del poder informático y de las redes de telecomunicación (tecnologías de la información) lo que consiguen es "hacer más eficaces, más extendidos y simultáneamente menos visibles muchos procesos que ya estaban en marcha" (págs. 65-8). Las nuevas tecnologías lo que han producido es un aumento de la capacidad de vigilancia y de procesamiento de la información recibida. En primer lugar el volumen de información ha aumentado, con ficheros más precisos y discriminativos. Además la amplitud de las redes y sus conexiones hacen más difícil la posibilidad de sustraerse a la eficacia de los sistemas de vigilancia. Por otra parte la velocidad de flujo de los datos ha aumentado espectacularmente con base en los avances en telecomunicaciones, lo que permite respuestas más rápidas de los sistemas ante cualquier circunstancia. Finalmente la capacidad de vigilancia de los sistemas se ve incrementada por el mayor número de puntos de contacto entre los sistemas de vigilancia y los sujetos, permitiendo en mayor medida la verificación externa de la información, el sistema de referencias cruzadas, los perfiles y el cotejo de información, logrando un amplio grado de transparencia del sujeto (págs. 79-82). Las nuevas tecnologías incrementan las visibilidad de los datos identificativos de los sujetos, al tiempo que los procesos de vigilancia se vuelven más silenciosos. "A medida que se amplía el alcance de identificación documental, mayores son las posibilidades de saber cosas sobre alguien sin preguntarle (autoidentificación), sino comprobando directamente otros ficheros" (pág. 133). Se consuma así lo que se podría llamar el panóptico global, como metáfora atrayente para la comprensión de la vigilancia electrónica (págs. 106-7).

o, mejor, la reconstrucción de la personalidad en su conjunto de un hombre o de una mujer. Son los llamados perfiles personales que pueden ser objeto de utilización con fines comerciales, políticos o puramente personales[6]. Esto nos puede convertir en lo que se conoce como "ciudadanos transparentes"[7], hasta el punto de llegar a dudarse si en una sociedad computerizada tiene cabida la intimidad[8], situación en la que en realidad lo que quiebran son los presupuestos para un actuar libre en la vida social[9]. Efectivamente "las posibilidades de almacenamiento, tratamiento y control de la información que ofrece la Informática la convierten con frecuencia en un instrumento de presión y control social que amenaza la libertad del individuo"[10]. El Tribunal Constitucional español en desarrollo del art. 18.4 del texto fundamental ha señalado su conexión e incidencia de la libertad informática y habeas data en la libertad de las personas. Así las SSTC de 20 de julio de 1993 y de 9 de mayo de 1994 afirman la existencia de un nuevo Derecho o Libertad Fundamental "frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama la informática".

II. Dimensiones de la protección de datos personales

En el contexto general de la protección penal de la intimidad ROMEO[11] ha señalado tres grandes ámbitos a través de los cuales se dispensa protección a este bien jurídico. En primer término estaría la intimidad como reducto de la personalidad en la vida privada. Se trata de la tutela de ciertos ámbitos en los que el interesado puede manifestar su oposición frente a injerencias no deseadas, como ámbito tradicional de la intimidad. Aquí se incluirían los delitos relativos a la protección del secreto y de captación de imágenes y sonidos. En segundo lugar se encuentra la intimidad en su manifestación de confidencialidad compartida. Se trata de sectores en los que intervienen terceros pero a los cuales se les obliga a guardar reserva. De ahí deriva el deber de secreto de los trabajadores, de los profesionales y de las autoridades y funcionarios públicos. Finalmente estaría la intimidad en relación con el procesamiento y comunicación de datos a través de las modernas tecnologías de la información y de la comunicación. Este último caso se refiere a la tutela de las informaciones de carácter reservado que han sido almacenadas o procesadas en un fichero o archivo, es la tutela penal de datos.

Del mero rechazo de intromisiones ilegítimas como poder jurídico clásico del titular del derecho a la intimidad, se ha pasado a otorgar más amplias facultades para la tutela de la intimidad frente a los modernos medios tecnológicos por la especial capacidad de intromisión que generan. La dimensión pasiva de la tutela de datos se identifica con la facultad del sujeto para rechazar intromisiones no consentidas en ámbitos privados. Se trata de la facultad clásica en la protección de la intimidad, vinculada a la categoría tradicional de "secreto" (algo a lo que no se puede acceder sin consentimiento del titular, del interesado). La dimensión jurídica propia de la protección de datos se ha visto ampliada con la aparición de las nuevas tecnologías. Para este concreto campo la emergencia de la necesidad

6 La recopilación masiva de información sobre personas y la formación de expedientes tras unos adecuados cruces de información se produce sobre la base de la información registrada por grupos privados o por las Administraciones públicas. Existen agencias privadas especializadas en la recogida de datos personales y en la elaboración de dossier con distintas finalidades (GÓMEZ NAVAJAS, J. *La protección de los datos personales*. Thomson/Civitas, Madrid 2005, págs 40). También los poderes públicos poseen una ingente cantidad de información –obtenidos y con fines lícitos– tanto en los archivos de los organismos de seguridad como en el conjunto de las Administraciones Públicas. En la perspectiva internacional es muy conocido el caso de la red ECHELON. Puede verse al respecto LOSANO, M. "privacidad y seguridad en la era del terrorismo: el deber del jurista informático". *Derecho informático*. Fundación de cultura universitaria, 2005, págs. 127 y ss.

7 ROMEO CASABONA, C. *Poder Informático y seguridad Jurídica*, Fundesco, Madrid 1987, pág. 16.

8 SIMITIS, S. "Chancen un Gefahren der elektronischen Datenverarbeitung", *Neue Juristische Wochenscchrift* 1981, pág. 675. En un sentido semejante también se dice que "proteger la vida privada en la era del ordenador es como intentar cambiar una rueda de un coche en movimiento". Expresión recogida en BALLESTEROS MOFFA, L.A. *La privacidad electrónica. Internet en el centro de protección*. Tirant lo Blanch/Agencia Española de protección de datos. Valencia 2005, pág. 48.

9 Como se había indicado en MATA Y MARTÍN, R.M. *Delincuencia informática y Derecho Penal*, Ed. Hispamer, Managua 2003, págs. 18-9. En todo caso se está haciendo referencia a la libertad del ser humano en el sentido más amplio y no como un auténtico bien jurídico-penal.

10 GÓMEZ NAVAJAS J. *La protección de los datos personales*. Thomson/Civitas, Madrid 2005, pág. 33. Esta autora indica cómo tanto desde instancias públicas como privadas se produce esta acumulación de información. Señala como más agudo el riesgo proveniente del sector público pues es donde se concentra una gran cantidad de información. Esta actuación confiere a los poderes públicos una enorme capacidad de fiscalización política y de control de la ciudadanía, "cobrando fuerza la imagen de una dictadura tecnológica que reduce a los individuos a meras cifras" (pág. 37). Pero también la utilización de datos personales por las empresas privadas también representa un peligro para la intimidad de los ciudadanos. De manera que existen agencias privadas especializadas en la recogida de datos personales y en la elaboración de dossier (pág. 40).

11 *Comentarios al Código penal, Parte Especial II*. DÍEZ RIPOLLES/ROMEO CASABONA (coordinadores). Tirant lo Blanch, Valencia 2004, págs. 692 y ss.

de tutela por el Ordenamiento Jurídico en las últimas décadas ha llevado en un progresivo desarrollo por la jurisprudencia del Tribunal Constitucional hasta la afirmación de un auténtico y específico Derecho Fundamental.

Esta evolución se ha manifestado en el reconocimiento de la tutela de datos y las facultades atribuidas al titular de los mismos. Con la llamada dimensión activa se produce la afirmación de la propia libertad frente a los riesgos de la sociedad tecnológica. Surge, por tanto, vinculada a la aparición de las nuevas tecnologías inicialmente en el mundo anglosajón, y es de aplicación para el caso de los ficheros automatizados de datos. Suponen la atribución de facultades de control, de posibilidades de actuación positiva, de los datos por su titular (derechos de acceso, modificación, cancelación de tales datos y de consentimiento). La doctrina del Tribunal Constitucional español ha insistido en la afirmación de esa nueva esfera de actuación para el ciudadano en defensa de su intimidad pues "el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos" (STC 292/2000 de 30 de noviembre, FJ 6.º)[12].

La determinación de esta nueva posición jurídica de los ciudadanos contaba con antecedentes directos en el derecho comparado. Ya en el año 1983 el Tribunal Constitucional Federal Alemán declaró el derecho a la autodeterminación informativa en el sentido del reconocimiento del nuevo ámbito de la intimidad de las personas y de las necesidades complementarias para el titular de los datos[13]. Esta construcción, en definitiva, conduce a un nuevo desarrollo de los derechos y libertades fundamentales de las personas, hablándose de derechos y libertades de tercera generación, ya que supera las categoría de derechos individuales y de derechos sociales acuñados con anterioridad. En última instancia estaríamos ante una actualización de los derechos y bienes de la personalidad para hacer frente a las necesidades, erosiones y contaminación de las libertades en la sociedad tecnológica (*liberties pollution*)[14].

III. Panorama general de la regulación de protección de datos

El desarrollo inicial en Estados Unidos de la protección de datos se produce con la *Privacy Act* de 1974[15], y en la actual Unión Europea cobra un fuerte impulso en su desarrollo en relación al fenómeno de la inmigración en la década de los años 80[16]. En realidad la experiencia muestra que la aparición inicial de la regulación legal de datos, en algunos casos, es consecuencia de algún asunto público de importancia, de manera que la producción de algún acontecimiento estimula la redacción y aprobación de estas leyes (llámese el Watergate en Estados Unidos, la inmigración y el sistema Schengen en la Unión Europea o la inquietud ante el censo de población en Suecia)[17].

La tutela de datos concierne a todo el Ordenamiento Jurídico. Por eso su regulación se manifiesta a lo largo de un amplio elenco de normas pertenecientes a distintos sectores jurídicos. En España, ya en la cúspide misma del Ordenamiento jurídico –o en la base según se quiera expresar– se recoge la tutela dispensada por las normas jurídicas a la información contenida en datos, ahora desde la perspectiva de la intimidad de las personas y del secreto de las comunicaciones[18]. Efectivamente la propia Constitución en su art. 18 establece en primer lugar el deber de garantizar el derecho a la intimidad: "Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen" (art. 18.1). Después se pasa a determinar la necesidad de respeto a la libertad de todo tipo de comunicaciones que deben permanecer inmunes a cualquier intromisión no consentida: "Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial" (art. 18.3). Finalmente el texto constitucional se refiere de forma ya concreta a la tutela de la intimidad de las personas en el ámbito de la informática ante la evidencia de que se trata de un espacio en el que ese derecho resulta especialmente vulnerable. El precepto establece que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" (art. 18.4).

El Tribunal Constitucional español en el desarrollo del reconocimiento constitucional de la libertad informática y la protección de datos personales ha llegado a considerarlo como un Derecho Fundamental autónomo por su especial conexión con otros Derechos Funda-

12 Lo que a veces se denomina de diferentes formas: puede llamarse autodeterminación informativa, libertad informática, intimidad informática, habeas data, etc. Estas diferentes denominaciones pueden verse en GÓMEZ NAVAJAS J. *La protección de los datos personales*. Thomson/Civitas, Madrid 2005, pág. 129.

13 Cfr. ROMEO CASABONA, C.M. *Comentarios al Código penal, Parte Especial II*. DÍEZ RIPOLLÉS/ROMEO CASABONA (coordinadores). Tirant lo Blanch, Valencia 2004, pág. 696.

14 Cfr. RUEDA MARTÍN, M.ª.A. *Protección penal de la intimidad personal e informática*. Atelier, Barcelona 2004, pág. 33.

15 TÉLLEZ AGUILERA, A. *La protección de datos en la Unión Europea*. Edisofer 2002, págs. 21 y ss.

16 Cfr. RUIZ CARRILLO, A. *Manual práctico de protección de datos*. Bosch, 2005, págs. 11-2.

17 Cfr. LYON, D. *El ojo electrónico. El auge de la sociedad de la vigilancia*. Alianza Editorial. Madrid 1995, pág. 236.

18 En las Constituciones Europeas suele ser habitual el reconocimiento expreso de la tutela de la intimidad de las personas. En otros casos, ante la ausencia de una formulación directa caben otra alternativas. Así ha sucedido en el Uruguay, donde la no declaración de la Constitución no ha impedido un reconocimiento tácito entre los derechos inherentes a la persona del art. 72 del Texto Fundamental, según la propuesta de DELPIAZZO.

mentales[19]. De esta manera se configura la protección de datos personales como presupuesto necesario de la tutela del libre desarrollo de la personalidad y de la misma dignidad y libertad de las personas, reconocidos como Derechos Fundamentales de los ciudadanos y como fundamento del orden político y de la paz social en el art. 10 CE. En definitiva el Tribunal Constitucional establece un nuevo derecho que se cualifica respecto al más genérico de la intimidad: "el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobres sus datos personales" (STC 292/2000 de 30 de noviembre, FJ 6.º)[20].

Fuera ya del texto constitucional la primera norma que refleja la protección de datos es la Ley Orgánica de Protección de Datos (LOPD), LO 15/1999 de 13 de diciembre[21]. La misma "tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar" (art. 1). De esta forma se vincula a la protección del honor y la intimidad de las personas, sobre la base del tratamiento de datos de carácter personal almacenados en ficheros. Los datos consisten en "cualquier información concerniente a personas físicas identificadas o identificables". Por fichero entiende la ley "todo conjunto organizado de datos de carácter personal, cualquiera que se la forma o modalidad de su creación, almacenamiento, organización y acceso".

Las conductas ilícitas, contra las que la ley establece su amparo, hacen referencia a un tratamiento de los datos desviado de los admitidos. Por tratamiento de estos datos debemos entender las "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogidas, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias". Como se ve la nueva LOPD prescinde del soporte en el que se encuentren los datos (papel o electrónico) para la protección de los Derechos Fundamentales (el soporte ha pasado a ser una anécdota). Es decir la protección de los datos, conforme a la regulación de la ley, se extiende a los contenidos en cualquier tipo de soporte, tanto los tradicionales como los electrónicos o informáticos, Sin embargo, los reglamentos todavía no se han reformado y siguen haciendo referencia exclusivamente a los ficheros automatizados.

Esta norma únicamente contiene infracciones y sanciones administrativas para el caso de hechos lesivos a los derechos tutelados, pero en ningún caso incluye delitos y penas en esta materia. Estas infracciones se refieren fundamentalmente a los hechos ilícitos cometidos desde dentro de la cúspide de la organización del fichero en el tratamiento de los datos. Por eso adquieren especial relevancia las figuras del responsable de los ficheros y del encargado del tratamiento de los datos.

La regulación de los datos como se ha dicho posee distintas perspectivas en el Ordenamiento Jurídico. De manera que cuando los datos entran en red se ocupa de ellos la Ley General de Telecomunicaciones (arts. 44 y ss). En este caso los datos también se manifiestan en la prestación de servicios en las redes de telecomunicaciones. Por otra parte si los datos son objeto de contratación telemática se regulan por lo previsto en la llamada abreviadamente Ley de Servicios de la Sociedad de la Información LSSI. Finalmente la protección de datos también aparece en el Código Penal. Determinadas conductas, especialmente graves, que afectan a la intimidad y a la protección de datos de las personas alcanzan relevancia jurídico penal, por lo que a los infractores en estos casos se les imponen sanciones criminales que pasamos a ver a continuación.

IV. Relevancia penal de la protección de datos personales y familiares

1. Principios constitutivos del Derecho Penal como presupuesto general

Como hemos visto la protección jurídica de datos se produce ya con anterioridad a la legislación penal. El último recurso de los poderes del Estado que constituye el *ius puniendi* puede intervenir en la tutela de determinados bienes jurídicos, para los hechos que revistan mayor gravedad y una vez constatada la insuficiencia de otros instrumentos jurídicos, pero siempre de acuerdo a sus princi-

19 ANARTE BORRALLO, E. "Sobre los límites de la protección penal de datos". *Derecho y conocimiento*, vol. 2, 2004, pág. 235. También en http://www.uhu.es/derechoyconocimiento/DyC02/DYC002. En sentido semejante GÓMEZ NAVAJAS, J. *La protección de los datos personales*. Thomson/Civitas, Madrid 2005, págs. 106 y ss. También BALLESTEROS MOFFA, L.A. *La privacidad electrónica. Internet en el centro de protección*. Tirant lo Blanch/Agencia Española de protección de datos. Valencia 2005, págs. 78 y ss., quien habla de un "derecho constitucional de configuración legal" (pág. 79).

20 Señala BALLESTEROS MOFFA que se trata del pronunciamiento más importante en esta materia ya que hasta el mismo no se había reconocido en plenitud la autonomía y singularidad de este derecho fundamental partiendo de la diferente función que representan la intimidad y la libertad informática. *La privacidad electrónica. Internet en el centro de protección*. Tirant lo Blanch/Agencia Española de protección de datos. Valencia 2005, págs. 92-3.

21 Sobre esta norma existe un amplísimo listado bibliográfico. Por todos puede verse TÉLLEZ AGUILERA, A. *Nuevas tecnologías. Intimidad y protección de datos. Estudio Sistemático de la Ley Orgánica 15/1999*. Edisofer, Madrid 2001.

pios constitutivos que legitiman la intervención penal en un moderno sistema penal.

Por tanto, los principios generales del Derecho penal tienen aplicación también a la protección de datos. Se estima por el legislador penal que los datos, en conexión a determinados bienes jurídicos –entre ellos la intimidad– representan un interés jurídico a los que deben dispensar protección. Sin embargo, no todos los hechos socialmente reprochables ni todos los hechos ilícitos relativos a la protección de datos resultan jurídico-penalmente relevantes, de acuerdo al principio de subsidiariedad o intervención mínima. Desde ambas perspectivas se produce una selección de las conductas que tendrán acogida en la regulación penal. Tal principio de intervención mínima supone que el Derecho Penal únicamente actúa cuando las medidas disponibles desde otros sectores y disciplinas del ordenamiento jurídico no resulten adecuadas para su tutela. Téngase en cuenta que la legislación administrativa ya prevé sanciones de esta naturaleza para algunas conductas y que, por tanto, debe establecerse una relación coherente de las infracciones administrativas de la LOPD con las infracciones penales (delitos), que además no viole el principio *non bis in idem*.

El Principio de lesividad es otro de los que vertebran los sistemas penales contemporáneos. Desde esta óptica el recurso al Derecho penal únicamente se legitima cuando la conducta afecte a intereses fundamentales de la persona o la sociedad, a los que conocemos como bienes jurídicos. No cabe duda que la intimidad de las personas representa en las modernas sociedades de nuestro entorno cultural un interés fundamental para la convivencia libre de los ciudadanos, como lo manifiestan los textos constitucionales más modernos. En este sentido ya hemos visto cómo el art. 18 de la Constitución española de 1978 proclama su vigencia y se constituye como uno de los Derechos Fundamentales de los que son titulares los ciudadanos. Este último principio debe combinarse con el de fragmentariedad. Como la tutela penal lo es frente a los casos más intolerables para la convivencia, no se protegerá al bien jurídico –intimidad informática en nuestro caso– en todos los supuestos en los que se vea amenazado, sino exclusivamente en aquéllos más graves, que serán los que recoja el tipo penal. Finalmente el principio de legalidad debe ser tenido en consideración, como no puede ser de otra forma. Básicamente tiene la consecuencia de que únicamente se lleva a cabo la tutela penal de acuerdo a las previsiones legales para tales casos.

2. Regulación penal: comportamientos típicos

Admitida la intimidad informática de las personas como un interés de tan alto rango que en los casos más graves se legitime la intervención con medidas penales, el legislador penal debe actuar para construir las figuras delictivas que prohíban y sancionen las conductas que menoscaben la misma. Entre ellas deberán incluirse aquellas que se dirigen contra la intimidad mediante los procedimientos a los que ha dado lugar la sociedad de la información.

La ubicación sistemática de las conductas punibles se realizará entre el grupo de delitos contarios a la intimidad (Título X del Libro II del Código Penal). Los comportamientos típicos que incluye el legislador español de 1995, y que como veremos en todos ellos las Nuevas Tecnologías poseen incidencia, desde el ángulo de la intimidad son diversos. En primer lugar están las acciones relativas al descubrimiento de secretos documentales (art. 197.1 CP). Además, se incluyen acciones conocidas como de interceptación de telecomunicaciones (art. 197.1 CP). En último lugar se encuentran las acciones sobre datos en bases de datos o archivos, electrónicos o no (art. 197.2), apartado este en el que se quiere situar la protección de la intimidad informática o habeas data en sentido estricto, aunque realmente esta afirmación necesite –como se hará posteriormente– cuando menos algunas precisiones. En definitiva, en estos distintos ámbitos se presenta la nota común de protegerse la voluntad de una persona de que no sean conocidos determinados hechos[22].

V. Conductas punibles

Como se ha mencionado, el análisis se dirige al estudio de los delitos contra la intimidad de las personas mediante el uso de la informática, comprendiéndose el acceso o manipulación de datos reservados registrados en soportes informáticos. La regulación penal podría atender de forma general al ciclo operativo de los bancos datos automatizados, aunque en la práctica únicamente se recogen conductas punibles sobre la base de datos ya registrados, no alcanzando relevancia penal por tanto otras conductas previas como las de recogida fraudulenta de datos o la creación clandestina de ficheros[23], así como otras, habría que añadir, posteriores, referentes a la conservación de los datos por el titular del banco.

Para la incriminación se ha empleado la técnica codificadora desechando la alternativa de la ley especial, lo que plantea problemas en la coordinación con la regulación extrapenal (LOPD), que provoca falta de precisión técnica y de correspondencia con las previsiones de tal regulación[24]. En otros ámbitos la técnica legislativa elegida para la protección penal del habeas data ha sido la ley especial, es decir, la regulación de la materia no en el texto penal general del Código, sino que desde una perspectiva total del Ordenamiento Jurídico se reúne en una sola norma todo lo concerniente a tal sector, incluidas las nor-

22 MUÑOZ CONDE, F. *Derecho Penal, Parte Especial*. Tirant lo Blanch, Valencia 2002, pág. 248.
23 MORALES PRATS, F. *Comentarios a la Parte Especial del Derecho Penal* (QUINTERO director). Aranzadi, 2005, págs. 419-20.
24 MORALES PRATS, F. *Comentarios a la Parte Especial del Derecho Penal* (QUINTERO director). Aranzadi, 2005, pág. 420.

mas penales que crean delitos y sus sanciones criminales. Ésta ha sido la vía seleccionada por Argentina mediante la Ley 25.326 de Protección de los Datos Personales de 4 de octubre de 2000. La mencionada norma además del desarrollo de la materia incluye las infracciones y sanciones administrativas (art. 31), así las infracciones de carácter penal y las penas correspondientes (art. 32). El caso de Uruguay es algo distinto, pues pese a aprobarse una ley sectorial, la Ley 17.838, de protección de Datos personales y Habeas Data, de 24 de septiembre de 2004, su conculcación no resulta respondida con ningún género de infracciones y sanciones, sino que se produce una remisión a los procedimientos generales (art. 19). En otros casos, como el austríaco, el sistema resulta intermedio. Por una parte la Ley de Protección de datos (*Datenschutzgesetz* 2000, DSG 200) crea algunos tipos penales en el parágrafo 51, relativos a la utilización de datos con la intención de causar un daño o buscar un enriquecimiento. Junto a ello el texto del Código penal mantiene también otros supuestos punibles, en los parágrafos 126a y 148a[25]. En la legislación italiana se diversifica la regulación efectuada por el Código penal de protección de la intimidad en cuanto reserva de las comunicaciones (reforma introducida en el Código por la Ley 547/1993) de la relativa al tratamiento automatizado de datos personales mediante ley especial 675/1996 de 31 de diciembre[26].

Pese a que habitualmente se señala como precepto receptor de la tutela penal del habeas data el art. 197 en su número segundo, como vamos a comprobar también en los diversos supuestos del art. 197, en su número primero, tienen cabida en la incriminación llevada a cabo por el legislador hechos vinculados a la intimidad informática, singularmente los relativos al correo electrónico.

1. Protección de secretos documentales (primer inciso art. 197.1)

Nos vamos a referir aquí en concreto al apoderamiento de los mensajes de correo electrónico (y otros documentos) con la finalidad de descubrir un secreto de otro o vulnerar su intimidad. La acción prevista con carácter general debe recaer sobre documentos u otros efectos personales (papeles, cartas) entre los que se cita los mensajes de correo electrónico. En el contexto del Capítulo I del Título X se castigan las acciones de apoderamiento de documentos o efectos personales llevados a cabo por el autor para descubrir los secretos o vulnerar la intimidad de otro. Entre los posibles objetos de apoderamiento que pueden lesionar la intimidad del sujeto pasivo se menciona expresamente por el legislador los mensajes de correo electrónico. La incorporación de este particular objeto fue consecuencia de una enmienda del Grupo Parlamentario de CiU en la tramitación parlamentaria del Proyecto de Código Penal, sumándose a los otros objetos ya enumerados, con la justificación de "Proteger el cada vez más extendido correo electrónico"[27].

La perspectiva de este primer inciso del art. 197 es la de la tutela de aspectos de la intimidad recogidos documentalmente o en efectos personales[28]. Así el legislador ejemplifica con "papeles, cartas, mensajes de correo electrónico" y finaliza la referencia al objeto material del delito con una fórmula genérica de recogida –"o cualesquiera otros documentos o efectos personales"– en la que se manifiesta la concreta dimensión de la intimidad a la que afecta la conducta punible. En realidad como manifiesta MORALES son aptos todos aquellos objetos que permitan una proyección espacial de la intimidad acotada a la materialidad de los documentos o de objetos personales[29].

La acción del sujeto activo sobre los elementos documentales o personales que guardan relación con la intimidad se describe como un apoderamiento. De acuerdo a las características de los elementos y documentos como el correo electrónico resulta complejo una absoluta identificación de esta conducta con la de los clásicos delitos de apoderamiento en el campo patrimonial[30]. Hay que tener en cuenta que –dada la naturaleza de los elementos informáticos fácilmente repetibles y virtuales– no siempre se producirá la desposesión del titular del mensaje o documento en sentido físico, lo que no es óbice alguno pues el bien jurídico no es la propiedad sino la intimidad, que ya resulta menoscabada o puesta en riesgo con la aprehensión del objeto. En el ámbito de los delitos contra la propiedad

25 *Datenschutz. Rechtsgrundlagen*. Weka-Verlag, 1999, págs. 398. Respecto a esta protección penal de datos en el derecho austriaco y otros aspectos del derecho penal informático puede verse JAVATO MARTÍN, A. "La protección penal del consumidor en el comercio electrónico en del derecho austriaco", *Cuadernos de Política Criminal* 2006 (en prensa). Para el caso suizo puede consultarse JAVATO MARTÍN, A. "La tutela penal del consumidor en el comercio electrónico en el derecho suizo". *Revista Electrónica de Ciencia Penal y Criminología* 7/2005, págs. 2 y ss, y 4 y ss.

26 Cfr. PICA, G. *Diritto penale delle technologie informatiche*, Utet, Torino 1999, págs. 281 y ss.

27 *Ley Orgánica del Código Penal. Trabajos Parlamentarios, vol I*, Cortes Generales 1996, pág. 299.

28 Ésta es la forma clásica de protección de los secretos en el ámbito penal, a veces presente de forma única en las legislaciones penales. Así el CP Uruguayo, en su Título XI, Capítulo IV (arts. 296 y ss.) se refiere al descubrimiento y revelación de secretos, basados en la idea de secreto documental. En la legislación argentina por medio de la Ley 25.326 se incorporan al Código Penal (arts. 117 bis y 157 bis) otras formas de agresión a la intimidad no vinculadas al secreto documental.

29 *Comentarios a la Parte Especial del Derecho Penal* (QUINTERO director). Aranzadi, 2005, pág. 410.

30 Sobre estos aspectos MATA y MARTIN, R.M. *El delito de robo con fuerza en las cosas*, Tirant lo Blanch 1995, págs. 198 y ss. y 140 y ss.

la desposesión viene demandada por el hecho de que la lesión del bien jurídico consiste en la privación al titular del conjunto de facultades jurídico-económicas que el Ordenamiento Jurídico le atribuye sobre el objeto. Sin tal desposesión queda claro que no puede darse el menoscabo efectivo del bien jurídico. En lo concerniente a la intimidad, sin embargo, basta con la apropiación del contenido para que la misma se vea amenazada.

Pese a lo que se acaba de señalar la inserción del apoderamiento del correo electrónico en este particular ámbito nos llevará a establecer algunas variantes. Lo que sí parece requerir en definitiva el apoderamiento en este campo de la intimidad es algún tipo de materialización instrumental del mensaje de correo electrónico o del objeto de que se trate, de forma que permita al autor la aprehensión del mismo. Con ello se excluyen del ámbito de la tipicidad las conductas que no lleven asociadas algún tipo de materialización y su correlativo apoderamiento por el sujeto activo[31]. De forma que es el propio autor del hecho punible el que debe llevar a cabo la materialización y posterior aprehensión, como acción que permite superar la barrera –tangible o intangible– que rodea y protege a la intimidad de la víctima. Sin embargo, no resultará necesario ya el desplazamiento físico del objeto, puesto que como se ha puesto de relieve la conducta es idónea en ese momento para amenazar al bien jurídico y ha cumplido con las exigencias típicas.

Sobre este problema de los requisitos de la acción de apoderamiento en general y en concreto para el caso del correo electrónico, ROMEO[32] realiza una detenida y matizada exposición. Considera que la acción de traslación física se entiende como suficiente en el sentido típico por cuanto permite al sujeto activo acceder al contenido del objeto material. Pero considera también que, conforme al proceso de espiritualización del acto de apoderamiento es posible asimilar distintas formas actuales de materialización que incorporan un objeto que cabe apreciar como distinto al original (fotografiar, fotocopiar) y que permiten el acceso al contenido. Estas admisiones se producen teniendo en cuenta el carácter instrumental de la acción de apoderamiento y la idoneidad de la acción para atacar el bien jurídico. Se incluirían en el ámbito típico las conductas de traslación física del soporte pero también las de reproducción de éste junto con el contenido que incorpora o únicamente del contenido, siempre que haya un comportamiento previo que facilite el acceso al objeto (trasladar virtualmente un mensaje de correo electrónico almacenado en un determinado ordenador actuando desde ese mismo terminal o desde otro).

Esta última ampliación para el caso de los mensajes de correo electrónico tendría su base en que el estado natural de los mismos es el virtual, sin que ningún soporte material los contenga y porque si la acción se limitase a las de desplazamiento físico del objeto estarían ya cubiertas a través del resto de objetos materiales mencionados en la descripción típica. En último extremo no se puede estar más de acuerdo con el autor "en el desacierto de mantener la expresión legal comentada –apoderarse–, puesto que ofrece un rendimiento muy trabajoso para lograr cubrir la variedad de aspectos –nuevos y no tan nuevos– mediante los cuales puede presentarse la acción en la vida real"[33]. Quizás la alternativa fuese incorporar los supuestos relativos al correo electrónico a otro tipo penal.

Cabe señalar, sin embargo, que desde la perspectiva de este primer inciso del número primero del art. 197, el de los secretos o aspectos de la intimidad documentalmente recogidos, resulta coherente la exigencia de un plus en la acción delictiva, representado por la apropiación del documento o efecto personal. Este plus, que puede entenderse como el desvalor de acción específico del comportamiento, se correspondería con el exigido en el caso del control audiovisual ilícito (art. 197.2 segundo inciso), cuando se requiere legalmente el empleo de medios técnicos en las conductas relativas al sonido o imagen ajenos. Por ello no puede incluirse en el tipo que estamos analizando los comportamientos de mera captación intelectual del mensaje de correo electrónico, visualizado en pantalla, como –sin embargo– si admiten MORALES[34] y SEGRELLES[35]. Paralelamente en el supuesto ya indicado del control audiovisual punible tampoco resulta típico el escuchar una conversación privada parapetado detrás de una puerta[36]. En ambos casos estas exigencias manifiestan el umbral mínimo del ilícito penal conforme a los principios de subsidiariedad e intervención mínima.

Sí que resultan abarcadas por el tipo, para las conductas que en concreto nos interesan, la impresión del mensaje de correo electrónico, apoderándose el autor del contenido mediante esa conversión a papel del mensaje. También puede considerarse incluida la grabación del mensaje en un disquete que le permita posteriormente al autor acceder a su contenido. En ambos casos se produce esa cierta materialización del contenido que exigiría la acción de apo-

31 En sentido semejante LOZANO MIRALLES, J. En BAJO FERNÁNDEZ (Director), *Compendio de Derecho penal (parte especial), Volumen II*. Editorial Centro de Estudios Ramón Areces, SA. Madrid 1998, pág. 210.

32 *Comentarios al Código Penal, Parte Especial II*. DÍEZ RIPOLLÉS/ROMEO CASABONA (coordinadores). Tirant lo Blanch, Valencia 2004, págs. 727 y ss.

33 ROMEO CASABONA, CM. *Comentarios al Código Penal, Parte Especial II*. DÍEZ RIPOLLÉS/ROMEO CASABONA (coordinadores). Tirant lo Blanch, Valencia 2004, pág. 736.

34 En *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi 1999, págs. 339.

35 SEGRELLES DE ARENAZA, I. En *Compendio de Derecho Penal Español (Parte Especial)*, Marcial Pons 2000, pág. 275.

36 Así MUÑOZ CONDE, F. *Derecho Penal, Parte Especial,* Tirant lo Blanch 1999, pág. 247.

deramiento documental en este primer inciso del art. 197.1.

Por tanto, y con base en el tipo de objetos con los que se encuentra regulado (todos los demás son documentos materiales), resultará necesaria la acción de apoderamiento en el sentido indicado. Ése era el sentido de la regulación a la que, si se quiere incoherentemente, se añade en la tramitación parlamentaria el correo electrónico. La conclusión resulta necesaria, en cuanto a la interpretación de la acción de apoderamiento, para establecer un desvalor semejante de la acción respecto a cada uno de los objetos, ya que para los de carácter material no sería suficiente un acceso a su contenido facilitado con tenerlos a la vista sin que al autor haya llevado a cabo algún tipo de conducta sobre el mismo. Pese a que para algunos supuestos relativos al correo electrónico –su interceptación– será posible aplicar otros supuestos del art. 197, su apoderamiento en este caso exigiría la impresión en papel y su sustracción o la grabación en otro soporte informático. Inicialmente en esta misma dirección se pronuncia MORALES[37], de manera que indica debe limitarse a las conductas de apoderamiento con desplazamiento físico de los mensajes, haciendo un encaje general de las conductas acorde con los presupuestos generales de la tutela de secretos contenidos en documentos materiales, pero luego, sin embargo –no coherentemente– para el caso de los mensajes de correo electrónico admite los supuestos de visión en pantalla.

Entiendo que realizan una interpretación en buena medida coincidente con la aquí mantenida, y defendida ya anteriormente[38], ORTS/ROIG[39] sobre la base del significado de los verbos empleados por el legislador y del diferente desvalor procedente de un tipo de conductas y de las otras. Señalan estos autores que "el verbo apoderarse expresa, en general, la acción de adueñarse de algo..., de modo que el apoderamiento de mensajes de correo electrónico comprenderá tanto la aprehensión de los ya impresos como su obtención mediante la entrada en el ordenador en el que se encuentren registrados. Debemos significar que para que concurra este delito es necesario que el autor realice una acción física dirigida a obtener los datos secretos. De lo contrario se llegaría a soluciones tan inverosímiles como la posibilidad de aplicar una pena de prisión de hasta cuatro años a quien se limitase a leer mensajes, cartas, etc., que el interesado hubiese dejado al alcance de terceros (por ejemplo, al olvidar cerrar un e-mail). Desde esta óptica, la visualización y retención en la memoria de la correspondencia privada no será punible si no va precedida de una actuación positiva del autor dirigida a apropiarse del contenido de la misma...".

Por otra parte, los documentos deben contener hechos que quepa calificar como secretos o afecten a la intimidad. Naturalmente el apoderamiento de mensajes de correo electrónico, en el sentido indicado, debe hacer referencia a mensajes con contenido secreto o que recojan referencias a la intimidad de las personas para que puedan estimarse como objeto material de este hecho punible. Finalmente será precisa la concurrencia de un elemento no objetivo. En sentido subjetivo, además, el tipo precisa que el autor que se apodera del objeto en el que determinados contenidos afectan a la intimidad, debe actuar con la intención de descubrir tales secretos o vulnerar la intimidad. Otros fines perseguidos por el autor dejan fuera de la tipicidad esta clase de apoderamientos de mensajes de correo electrónico o de cualquier otro documento, incluso aunque desde el punto de vista objetivo, dado el contenido, puedan peligrar o lesionar los secretos o la intimidad de alguien.

En todo caso, pese a la finalidad exigida al autor, sin embargo, no se requiere desde el punto de vista objetivo que efectivamente se lesione la intimidad o se descubran determinados secretos. Es decir, se produce la consumación de la conducta del art. 197.1 con la acción de apoderamiento del documento o efecto personal en el que se contienen datos secretos o íntimos, sin necesidad de ulteriores consecuencias como la de una auténtica vulneración de la intimidad o real descubrimiento del secreto, de acuerdo a lo previsto en su descripción típica. O lo que es lo mismo, la consumación se produce sin que sea preceptivo que el sujeto activo llegue al conocimiento del contenido del mensaje o documento. Por eso cabe calificar estos hechos delictivos como delitos de peligro, pues no exigen sino la amenaza –apoderamiento del objeto– al bien jurídico y no el menoscabo real y efectivo –acceso al contenido con la consiguiente lesión de la intimidad– que puede producirse pero no aparece como una auténtica exigencia típica. Ahora bien como el tipo exige el apoderamiento previo la acción se desenvuelve en una zona ya próxima e inmediata al bien jurídico intimidad informática por lo que habría que calificar el tipo como de peligro concreto. El peligro abstracto para el bien jurídico se ha sobrepasado desde el momento en el que se produce el apoderamiento que sitúa la conducta en las inmediaciones de la afectación real del bien jurídico[40]. Éste sería el caso, por ejemplo, de quien se apodera de un mensaje de correo

37 *Comentarios a la Parte Especial del Derecho Penal* (QUINTERO director). Aranzadi, 2005, págs 413.

38 En mi monografía *Delincuencia informática y Derecho penal*. Edisofer, Madrid 2001, págs. 127 y ss.

39 *Delitos informáticos y delitos comunes cometidos a través de la informática*. Tirant lo Blanch, Valencia 2001, págs. 25-6.

40 Otros autores prefieren hablar de peligro abstracto, como es el caso de RUEDA MARTÍN, M.ª A. *Protección penal de la intimidad personal e informática*. Atelier, Barcelona 2004, pág. 48. Sin embargo, ya he señalado que por el estado avanzado de la acción, que por necesidades típicas ha debido llegar al apoderamiento del objeto en el que se contiene el secreto o aspectos de la intimidad de la víctima, el riesgo es elevado y muy cercano al conocimiento del secreto o a la vulneración de la intimidad, es decir, la conducta se sitúa en el momento inmediatamente previo a la lesión misma. Con anterioridad ya había señalado la calificación del tipo como delito de peligro pero sin mayores precisiones en mi obra *Delincuencia informática y Derecho penal*, Edisofer, Madrid 2001, pág. 129.

electrónico cifrado por lo que finalmente no puede llegar a conocer lo contenido en el mismo. El delito ha rebasado la mera tentativa y ha llegado a la fase de consumación pues se ha producido el peligro para la intimidad requerido por el tipo. Menos aún resulta necesario que, una vez conocido el contenido íntimo o secreto, tales aspectos se difundan o trasladen a terceros. Esta situación es objeto de un plus punitivo conforme a lo previsto en el número tercero del art. 197 del CP: "Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos…".

2. Interceptación de telecomunicaciones y control audiovisual clandestino (inciso segundo art. 197.1)

En un segundo momento de la descripción de las conductas punibles en el art. 197.1 se prohíbe y castiga la interceptación de telecomunicaciones[41]. También la intimidad puede verse quebrantada mediante la intromisión ilegítima en los modernos medios de telecomunicación, entre los que se pueden incluir los informáticos, como el correo electrónico. En realidad, en esta segunda modalidad, están presentes dos conductas alternativas. Por una parte la de interceptación de las telecomunicaciones propiamente, relativa a acciones en las que se accede ilegítimamente al contenido de la comunicación y que debe distinguirse de las acciones que realmente consistan en la mera obstrucción de la señal de telecomunicación. Hoy en este ámbito se incluye cualquier tipo de emisión ("cualquier otra señal de comunicación"). Pero además se regulan las conductas de percepción, grabación o reproducción del sonido o la imagen. Se trata básicamente, como veremos de la captación de sonido o imagen de forma ilícita para descubrir secretos o vulnerar la intimidad.

a) Elementos comunes a las dos conductas

La interceptación, en cuanto acción típica, se entiende en este ámbito como acceso ilícito al contenido de la comunicación en tránsito. No se trata, como impone una interpretación teleológica en atención al bien jurídico, de una obstaculización de la comunicación –que nada tiene que ver con la tutela de la intimidad–. Como señala POLAINO estamos ante una interceptación de indiscreción y no ante una interceptación de obstrucción. Dada la naturaleza de los medios tecnológicos empleados en las modernas telecomunicaciones se presenta como presupuesto necesario el empleo por el autor de medios técnicos que permitan el acceso al contenido de tales comunicaciones. Aun cuando la profusa redacción del número primero del art. 197 pudiera hacer pensar que la exigencia de utilización de "artificios técnicos" únicamente se refiere a las conductas de control ilícito del sonido o imagen, sin embargo, resulta incuestionable la presencia de los mecanismos de acceso a las telecomunicaciones en la conducta punible, aunque sólo fuera como presupuesto fáctico.

En contra de entender el empleo de instrumental técnico como una exigencia típica se ha manifestado SEGRELLES[42], incluso para el supuesto de captación o reproducción de imágenes o sonidos. El problema está –según este autor– en la confusión entre la intimidad en sí con la percepción de la misma por terceros, lo que se realiza a través de señales. El legislador protege la intimidad, cualquiera sea la señal por la que se pueda manifestar. Entiende que el último inciso del art. 197.1 admite la punición de la percepción de comunicaciones sin ayuda de medios técnicos.

Es verdad que, como señala este autor, el legislador protege la intimidad propia de cualquier tipo de comunicación, por lo que no exige que ésta se produzca a través de medios técnicos –al menos en algunos de los supuestos–. Otra cosa es que sí se exija que el autor en la conducta de ataque a la intimidad penalmente relevante emplee medios técnicos para el acceso al contenido de la comunicación o la captación de imágenes o sonidos. Para algunos supuestos resulta una exigencia típica expresa y para otros un presupuesto fáctico ineludible, como ya se ha indicado. En todos los casos la utilización de mecanismo técnico manifiesta un específico desvalor de acción en la conducta del autor, coherente con principios básicos del Derecho Penal como el principio de intervención mínima y el principio de fragmentariedad. La necesidad de empleo de instrumental técnico o de apoderamiento documental impone un umbral mínimo para las conductas penalmente relevantes, que se corresponde con la misión propia del Derecho penal y que evita que posea trascendencia penal el hecho de escuchar detrás de una puerta una conversación que también pueda afectar a secretos o la intimidad de determinadas personas, distinguiéndose la responsabilidad penal de las meras faltas de educación o los ilícitos exclusivamente civiles, por graves que puedan ser[43].

41 Tradicionalmente los comportamientos punibles relativos a la interceptación de las comunicaciones ha estado vinculada a las de carácter postal y telegráfico, a las que se añadiría posteriormente la de telefonía. De esta manera el art. 297 del CP Uruguayo se refiere exclusivamente a las comunicaciones postales, telegráficas y telefónicas.

42 En *Compendio de Derecho Penal Español (Parte Especial)*, Marcial Pons 2000, pág. 280.

43 Téngase en cuenta el carácter fragmentario de la tutela penal de los bienes jurídicos, como ya se ha mencionado, de manera que como expresa LOZANO MIRALLES "El Estado no puede asumir la tarea de proteger al individuo contra todo ataque a su esfera íntima. Es el particular el que debe poner los obstáculos pertinentes para mantener en sigilo aquello que puede afectar a sus intereses. El derecho penal sólo entra en juego cuando el comportamiento desvelador del secreto o conculcador de la intimidad se presenta especialmente intolerable". BAJO FERNÁNDEZ (Director). *Compendio de Derecho penal (parte especial, Volumen II*. Editorial Centro de Estudios Ramón Areces, S.A. Madrid 1998, pág. 194.

Ya se ha señalado que este supuesto afecta a cualquier tipo de señal empleada en la telecomunicación. En este sentido hay que indicar que la redacción original, vinculada a las comunicaciones telefónicas, se ha modificado desde 1994, ampliándose a "cualquier otra señal de comunicación", con lo que el tipo abarca todo tipo de telecomunicaciones. Pero la calificación del comportamiento como interceptación y la tipificación de algunas conductas en el primer inciso del art. 197.1 parece restringir las conductas relevantes penalmente a un determinado momento. Al hablarse de interceptación se está sugiriendo ya que la comunicación –al menos desde el punto de vista técnico– se está produciendo en ese momento, es decir, se trata de mensajes en tránsito. Igualmente el que antes se haya incriminado el apoderamiento documental –entre los que se encuentra el correo electrónico– sitúa nuevamente el segundo inciso del número primero del art. 197 –interceptación de las telecomunicaciones– fuera de las fases de recepción y almacenamiento de los mensajes. La exigencia de apoderamiento, con la consiguiente materialización del mensaje ya vista, en las anteriores conductas, harían referencia justamente a los momentos de recepción y almacenamiento. Con ello también se establece una correspondencia con la diferenciación procesal según el momento en el que se encuentre la comunicación para los casos de vigilancia o control ilícito de las telecomunicaciones por las autoridades[44].

Para esta conducta se reproducen el conjunto de elementos necesarios para la relevancia típica de la conducta del supuesto anterior. Así es necesario que el autor del hecho persiga con su conducta de interceptación de las telecomunicaciones el descubrir secretos o vulnerar la intimidad de otro. Bien entendido que esto no supone la producción de un menoscabo efectivo de la intimidad o descubrimiento real de algún tipo de secreto. Sin embargo, la consumación delictiva si que precisa que, según las circunstancias del caso concreto, el autor, de acuerdo a los medios técnicos empleados, llegue a interceptar de manera efectiva las telecomunicaciones. Es decir, si que resulta preceptivo, conforme a la estructura del tipo establecida, la instalación de los instrumentos técnicos y la interceptación o captación de la señal, pero no que efectivamente se llegue a descubrir el secreto o lesionar la intimidad. Interceptada la comunicación pero no descubierto secreto alguno o sin violación de la intimidad, el hecho punible está completo en su descripción típica. También aquí el supuesto toma como punto de referencia el descubrimiento de secretos o vulneración de la intimidad, como tendencia en la conducta del autor, y no lo referente a la posterior revelación o difusión de los datos que constituyen el secreto o afectan a la intimidad que, como ya se ha mencionado, se castigan independientemente y de forma más severa según las previsiones del número tercero del art. 197.

3. Tutela penal de datos recogidos en ficheros, archivos o registros electrónicos

En el número segundo del art. 197 encontramos lo que puede considerarse la regulación penal más completa de la intimidad informática. En el contexto del Título X (que cabe considerar como el lugar sistemático de la tutela de la intimidad) se contiene en el precepto indicado las conductas punibles relacionadas con datos reservados contenidos en ficheros automatizados. En realidad, se refiere no sólo a los datos electrónicos sino a cualquier otro fichero, por lo que no tiene su exclusivo asiento la tutela penal de la privacidad informática en el sentido específico del habeas data. Ya hemos visto algunas otras conductas vinculadas a la informática de agresión a la intimidad contenidas en el número primero del art. 197 y que, por tanto, deben excluirse del ámbito de este número segundo. A la hora de desarrollar este campo vamos a tratar separadamente los elementos distintos típicos y, por otro lado, las conductas en sentido estricto. En realidad vamos a comprobar que guardan una estrecha relación –especialmente en algún caso– y no sólo porque, naturalmente, la punibilidad dependa de la concurrencia del conjunto de requisitos típicos.

a) Autoría y participación

Los supuestos del art. 197.2 pueden ser cometidos –en principio– por cualquiera, es decir, se trata de delitos comunes, en cuanto al círculo posible de autores, puesto que el legislador nada determina ni restringe respecto a los posibles sujetos activos de los hechos. Pero en realidad las penas establecidas para los mismos están dirigidas a aquellas personas que actúan desde fuera de la estructura de responsabilidad del fichero o banco de datos. La pena de prisión de uno a cuatro años y multa de doce a veinticuatro meses es de aplicación a los sujetos externos al ámbito de decisión del fichero, archivo o registro. Y esta conclusión resulta evidente tras una interpretación sistemática de la total regulación del art. 197, en el que existe una previsión específica para los hechos llevados a cabo "por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros". Si los sujetos que cometen las conductas del 197.2 (e incluso las del 197.1) resultan ser tales encargados o responsables de los ficheros la pena se eleva hasta la prisión de tres a cinco años. Se configura así por el legislador un tipo agravado, si los autores actúan con la facilidad que le proporciona su posición en la organización

44 En este sentido el Documento de la UE sobre "Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos" de 26 de enero de 2001.

del fichero con una especie de abuso de confianza, el art. 197.4. Estos sujetos por la posición profesional que ocupan se sitúan en un ámbito de mayor cercanía y vulnerabilidad para el bien jurídico tutelado[45]. Este supuesto constituye un delito especial y además especial impropio, pues la misma conducta puede ser desarrollada por otros sujetos ajenos a su condición de encargados o responsables del fichero pero la misma se castiga en otro momento de la regulación. En todo caso la referencia a los encargados o responsables del fichero no excluye como posibles autores de la conductas del número segundo a otras personas que trabajen en el fichero pero que en el organigrama no se consideren como tales[46].

Para determinar más en concreto quiénes sean estos encargados o responsables de los ficheros la doctrina suele acudir a la regulación de la LOPD en la que se establecen algunas precisiones[47]. Así esta normativa entiende por responsable del fichero o tratamiento a la "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento". Por otra parte el encargado del tratamiento resulta "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento" (ambas definiciones en el art. 3 de la mencionada ley, letras d y g respectivamente). El contraste entre las definiciones señaladas y la regulación penal hace nacer algunas dudas. Inicialmente no hay una perfecta coincidencia entre los sujetos mencionados, pues la regulación penal incluye a las "personas encargadas o responsables de los ficheros", mientras las definiciones administrativas se refieren a "responsable del fichero o tratamiento" y al "encargado del tratamiento", distinguiendo la LOPD entre las responsabilidades referentes al fichero y las relativas al tratamiento de datos, cosa que no hace la regulación penal. Por otra parte la regulación administrativa permite que tales responsables o encargados lo sean junto a las personas físicas las jurídicas. Esto conduce en el terreno penal al intrincado problema de la responsabilidad de las personas jurídicas[48].

Todavía respecto a la autoría penal quedaría pendiente el problema de la participación de extraños –en los que no concurren las cualidades exigidas para el autor: encargado o responsable– en lo que es un delito especial restringido para ciertos sujetos[49]. En realidad el problema puede no ser tal si consideramos que el supuesto del art. 197.4 no deja de ser un tipo agravado –meramente modificado o dependiente– de los dos tipos básico del art. 197.1. En ese caso no hay inconveniente en castigar al partícipe en el que no concurre la cualidad de encargado o responsable del fichero por el supuesto recogido en el número primero y al autor –éste si es encargado o responsable del fichero– por el supuesto agravado del número cuarto. No se produce problema alguno pues por tratarse de tipos dependientes se está respetando el principio de unidad del título de imputación para autor y partícipes en el mismo hecho. Otra cosa sería si no se entendiera el número cuarto como tipo modificado del número primero –cosa difícil–. Bajo esos nuevos presupuestos si se quiere respetar la unidad del título de imputación al tercero no encargado ni responsable del fichero deberemos castigarle por el mismo delito que al autor, en este caso el tipo agravado del art. 197.4. Si se estima que en realidad en el tercero no concurren las cualidades exigidas por la ley para este tipo agravado, aplicándose el supuesto básico del art. 197.2, se aplica una pena menor a costa de quebrantar el principio de unidad del título de imputación que rige la participación criminal.

b) La naturaleza de los datos protegidos

Un aspecto decisivo se refiere al objeto material de este hecho punible contra la intimidad. La acción delictiva prevista en el número segundo del art. 197 debe recaer sobre "datos reservados de carácter personal o familiar de otro". Esta determinación legislativa del concreto objeto material del delito no deja de presentar varias dificultades[50]. Así la calificación de los datos que constituyen este objeto de la conducta punible como "reservados" produce cierto desconcierto en la doctrina. Primero por que tal calificación no coincide con la denominación usual en el ámbito de la protección de datos personales. Así la LOPDP habla de datos de carácter personal, que son todos los objetos de la mencionada regulación. Para los datos

45 RUEDA MARTÍN, M.ª.A. *Protección penal de la intimidad personal e informática*. Atelier, Barcelona 2004, págs. 99-100. LOZANO MIRALLES indica que "El fundamento de la agravación hay que buscarlo en un mayor desvalor de injusto, por la infracción de los deberes profesionales de quien lleva a cabo la vulneración de la esfera íntima y en una mayor peligrosidad, por cuanto la conducta del encargado o responsable de los ficheros puede amplificar la lesión del derecho a la intimidad". En BAJO FERNÁNDEZ (Director), *Compendio de Derecho penal (parte especial), Volumen II*. Editorial Centro de Estudios Ramón Areces, SA. Madrid 1998, pág. 218.

46 Como pone de manifiesto ROMEO CASANBONA, C.M. *Comentarios al Código penal, Parte Especial II*. DÍEZ RIPOLLÉS/ROMEO CASABONA (coordinadores). Tirant lo Blanch, Valencia 2004, pág. 746.

47 RUEDA MARTÍN, M.ª.A. *Protección penal de la intimidad personal e informática*. Atelier, Barcelona 2004, págs. 101-2.

48 Aspecto tratado por GÓMEZ NAVAJAS, J. *La protección de los datos personales*. Thomson/Civitas 2005, págs. 270 y ss.

49 Véase respecto a este problema lo señalado por RUEDA MARTÍN, Mª A. *Protección penal de la intimidad personal e informática*. Atelier, Barcelona 2004, pág. 103.

50 Véase también sobre estos aspectos PICA, G. *Diritto penale delle technologie informatiche*, Utet, Torino 1999, págs. 296 y ss.

que se entienden forman parte del núcleo de la intimidad de las personas, la mencionada LOPDP (art. 7) se refiere a "datos especialmente protegidos" con un régimen cualificadamente garantista.

No hay por tanto coincidencia en las denominaciones de estos dos órdenes jurídicos, lo que tampoco debe considerarse definitivamente un inconveniente. Pero es verdad que la calificación como reservados podría llevar a entender que sólo determinados datos personales son abarcados por la regulación penal que estamos viendo, quedando el resto fuera de la tutela jurídico-penal. En este sentido se han pronunciado algunas resoluciones judiciales. Así la Sentencia del Tribunal Supremo de 18 de febrero de 1999 (Ar. 510) entiende que se trata de "aquellos datos que el hombre medio de nuestra cultura considera sensibles por ser inherentes a su intimidad más estricta, o dicho de otro modo, los datos pertenecientes al reducto de los que, normalmente, se pretende no trasciendan fuera de la esfera en que se desenvuelve la privacidad de la persona y su núcleo familiar". En realidad con esta argumentación no se consigue una mayor precisión e incluso hace necesario volver a determinar qué se entiende por datos sensibles[51]. Según esta fórmula de aproximación al concepto deberían considerarse reservados aquéllos más estrechamente vinculados al ámbito de la intimidad de las personas, es decir, los referentes a la ideología, religión, creencias, afiliación sindical, origen racial, vida sexual, salud, todos ellos incluidos en el régimen particular establecido para los "datos especialmente protegidos" del art. 7 LOPD. Cabe entender que siguiendo esta opción más restrictiva se sitúan ORTS/ROIG[52] cuando tras la referencia a la sentencia indicada señalan que "el calificativo reservados encuentra su sentido en la exclusión de esta norma de aquellas acciones recayentes sobre datos individuales que, aun siendo personales, no pueden considerarse reflejo de la intimidad más estricta".

Esta posibilidad ha sido acertadamente descartada por MORALES[53] al confrontarla con las previsiones del número quinto del art. 197 CP. El tipo agravado del número quinto del art. 197 eleva las penas cuando los hechos "afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual…". Si se aceptase la interpretación propuesta sobre la calificación como reservados de los datos protegidos, obligaría a dejar total o sustancialmente vacío de contenido el tipo del número segundo del art. 197 CP. Así es, la previsión del n.º 5 del art. 197 como supuesto cualificado para los hechos cometidos sobre aquellos que forman el núcleo de la intimidad (ideología, religión,...), impide entender que sean estos los que se consideren "reservados" frente a otros.

Por otra parte, es conocido que no existen datos sin interés y menos, si como resulta correcto y realista, se valoran los mismos en una visión dinámica (interrelación o combinaciones entre los mismos, etc.) y no desde una óptica puramente estática[54]. En efecto para MORALES carece de sentido la calificación, pues todos son sensibles, ya que datos que aisladamente pueden considerarse inocuos, pero una vez introducidos en el fichero automatizado permiten la obtención de mayor información por inferencia.

Todo ello hace que exista un cierto acuerdo en estimar que no puede entenderse que la tutela penal se dirige únicamente a determinados datos, es decir, que cabe concebir, en principio, todos los incorporados a un fichero automatizado como reservados a efectos penales[55]. Esto puede justificarse no sólo por la lesividad potencial para el bien jurídico de cualquier dato personal incluido en un tratamiento automatizado, sino también porque el carácter de reservados puede entenderse en un sentido descriptivo[56], como aquellos para los que no se posee un acceso libre por cualquiera. Es decir, se excluirían únicamente los datos contenidos en ficheros de consulta libre por cualquier persona, como las denominadas "fuentes accesibles al público" en el art. 3j de la LOPDP, aunque no sólo éstas, dadas las exclusiones de determinados ficheros públicos del ámbito de la mencionada ley. De manera que por reservados deba quizá entenderse como no públicos, que no sean o puedan ser de conocimiento público (fuentes de acceso público, los recogidos en guías telefónicas o comerciales, los facilitados por los Registros Públicos, etc.). Dicho de forma inversa, pero creo que básicamente coincidente, se trata de los "datos que son de conocimiento limitado para terceros ajenos al fichero en que se encuentran registrados y archivados"[57]. En sentido semejante se indica que "probablemente con el calificativo reservados

51 Sobre ello GÓMEZ NAVAJAS J. *La protección de los datos personales*. Thomson/Civitas, Madrid 2005, págs. 187.

52 *Delitos informáticos y delitos cometidos a través de la informática*. Tirant lo Blanch, Valencia 2001, pág. 33.

53 En *Comentarios a la Parte Especial del Derecho Penal* (QUINTERO director). Aranzadi, 2005, pág. *423.*

54 MARCHENA GÓMEZ, M. "Intimidad e informática: la protección jurisdiccional del habeas data*". Boletín de Información. Ministerio de Justicia e Interior nº 1768 (1996)*, pág. 752. En este punto, pese a su apoyo a la concepción más restrictiva de los datos reservados, ORTS/ROIG sí que reconocen que la combinación de datos que inicialmente puedan parecer intrascendentes puede conducir a informaciones relevantes. *Delitos informáticos y delitos cometidos a través de la informática*. Tirant lo Blanch, Valencia 2001, pág. 17.

55 En este sentido MARCHENA GÓMEZ, M. "Intimidad e informática: la protección jurisdiccional del habeas data*". Boletín de Información. Ministerio de Justicia e Interior nº 1768 (1996)*, págs. 753-4.

56 Así SEGRELLES DE ARENAZA, I. En *Compendio de Derecho Penal Español (Parte Especial)*, Marcial Pons 2000, pág. 285.

57 RUEDA MARTÍN, M.ª.A. *Protección penal de la intimidad personal e informática*. Atelier, Barcelona 2004, págs. 71-2.

se quiera significar que los datos son conocidos por un círculo restringido de personas"[58].

También produce alguna dificultad la referencia a datos no sólo personales sino incluso familiares, probablemente por el peso de la declaración constitucional reconociendo el derecho a la "intimidad personal y familiar" (art. 18.1 CE). Igualmente esta diferencia con la regulación de la LOPDP causa una inicial incerteza, aunque en la práctica lo más probable es que no tenga gran importancia. Como señala SEGRELLES[59] lo familiar es al final también personal. Los datos familiares poseen significación para la intimidad de los miembros de ese grupo familiar. Quizás la dificultad real estribe en determinar qué grado de parentesco resulta comprendido en el objeto material.

De manera que existe un cierto acuerdo doctrinal sobre la noción de "datos reservados de carácter personal o familiar" que viene a expresar lo manifestado por ROMEO[60] para este tema. Mantiene que poseen una cierta naturaleza singular aunque sin desconexión con la normativa general. Consisten primariamente en informaciones pertenecientes al ámbito personal o familiar, en cuanto persona individual o como conjunto familiar, dualidad conectada a la declaración del art. 18 de la Constitución. De manera que ha de tratarse de informaciones relativas a personas físicas o de carácter familiar identificadas o identificables, lo que excluye aquellos casos en los que han sido anonimizados mediante un proceso de disgregación o disociación entren la identidad de la persona y la información a ella referida, siempre que tal disociación no sea reversible[61]. El carácter de reservados para los datos penalmente protegidos impone una restricción pues indica a su vez la existencia de otros datos no reservados y que hay que vincular con la posición de ultima ratio y de intervención mínima del Derecho penal. "Por reservados habrá que entender aquellos datos personales que son de acceso o conocimiento limitado para terceros ajenos al fichero en el que se hallan registrados y archivados"[62].

En todo caso, se trata siempre de datos reservados ya registrados en un determinado fichero. El Derecho penal ha renunciado a admitir como hechos relevantes momentos anteriores a la existencia del fichero. Toda la fase anterior, en el ciclo total de un fichero, la fase de formación del mismo (obtención irregular de datos, constitución del mismo fichero[63]), pero también de otro tipo de hechos (recuperación ilícita de datos, conservación de los mismos confines ilícitos por tiempo mayor del permitido, ausencia de medidas legales de seguridad, violación del principio del consentimiento[64]) quedaría al margen de los hechos penalmente relevantes[65]. Particular interés puede poseer la formación misma del fichero al margen de la regulación legal prevista para ello, que pudiendo ser considerada atípica[66], puede dar lugar, sin embargo, a conductas punibles

58 GÓMEZ NAVAJAS J. *La protección de los datos personales*. Thomson/Civitas, Madrid 2005, pág. 188.

59 En *Compendio de Derecho Penal Español (Parte Especial)*, Marcial Pons 2000, pág. 286.

60 *Comentarios al Código penal, Parte Especial II*. DÍEZ RIPOLLÉS/ROMEO CASABONA (coordinadores). Tirant lo Blanch, Valencia 2004, págs. 747 y ss.

61 ROMEO CASABONA, C.M. *Comentarios al Código penal, Parte Especial II*. DÍEZ RIPOLLÉS/ROMEO CASABONA (coordinadores). Tirant lo Blanch, Valencia 2004, pág. 749.

62 ROMEO CASABONA, C.M. *Comentarios al Código penal, Parte Especial II*. DÍEZ RIPOLLÉS/ROMEO CASABONA (coordinadores). Tirant lo Blanch, Valencia 2004, pág. 750. ROMEO insiste además en que los datos no necesariamente deben ser íntimos en sentido estricto, aspecto este en el que ya no se produciría el acuerdo básico respecto a la noción de datos reservados. Pese a la ausencia de un elemento subjetivo específico, a diferencia de lo que sucede en el art. 197.1, que imponga claramente la dirección de la conducta –al menos desde la perspectiva del autor– existen otros argumentos que avalarían la conexión con la intimidad de este supuesto. Por una parte la conducta o conductas se inscriben en el marco normativo general de la tutela penal de la intimidad (Título X del Libro II del CP). Por otra parte el propio carácter reservado de los datos manifiesta su vinculación con el ámbito de la intimidad de las personas. Por ello los datos de conocimiento o acceso público no resultan protegidos, sino que sólo se incluyen los de acceso limitado. El resto de ámbitos penales en los que se protege los datos poseen un sentido distinto (secreto profesional, secreto de empresa, defensa nacional), por lo que únicamente entre estos delitos contra diferentes aspectos de la intimidad tienen cabida. Quizá el dato más perturbador sea el que el Tribunal Constitucional en el desarrollo de la doctrina sobre la protección de datos haya afirmado un Derecho Fundamental específico para la tutela de datos personales. Pero en realidad la presencia de un Derecho Fundamental específico no desvirtúa la tutela de la intimidad, pues por una parte el bien jurídico-penal no tiene por qué ser plenamente identificado con el Derecho Fundamental y aun así no dejaría de percibirse su conexión con la intimidad de las personas. Incluso la referencia a los datos personales y familiares del Código Penal, que el propio ROMEO reconoce deriva de la declaración del art. 18 de la Constitución, siempre lo es –por dos veces– en el texto constitucional a "la intimidad personal y familiar". El propio ROMEO describe tres ámbitos de la tutela penal de la intimidad entre los que incluye la protección de datos.

63 La constitución clandestina de un fichero, sin embargo, constituye específicamente en la legislación francesa un hecho punible en esta materia. Véase PANSIER, F.J/JEZ, E. *La criminalité sur lÍnternet*, PUF 2000, pág. 70.

64 GÓMEZ NAVAJAS J. *La protección de los datos personales*. Thomson/Civitas, Madrid 2005, págs. 133-4.

65 MARCHENA GÓMEZ, M. "Intimidad e informática: la protección jurisdiccional del habeas data*". Boletin de Información. Ministerio de Justicia e Interior n.º 1768 (1996)*, pág. 756. MORALES PRATS, F. En *Comentarios a la Parte Especial del Derecho Penal*, Aranzadi 2005, págs. 416 y ss.

66 En ese sentido MARCHENA GÓMEZ, M. "Intimidad e informática: la protección jurisdiccional del habeas data*". Boletín de Información. Ministerio de Justicia e Interior nº 1768 (1996)*, pág. 757.

sobre la base de los datos obrantes en el mismo. En todo caso su exclusión del ámbito penal no evita su ilicitud y su consideración como infracción administrativa.

c) La actuación en perjuicio de tercero y sin autorización

En las dos secuencias típicas del número segundo del art. 197 CP se hace una mención al perjuicio que deben causar estas conductas. Así en el primer inciso (apoderamiento, utilización o modificación de los datos) se exige que el autor obre "en perjuicio de tercero". Para el segundo ámbito típico (acceso, alteración o utilización) nuevamente el sujeto activo sólo actúa en el sentido requerido por la tipicidad si lo hace "en perjuicio del titular de los datos o de un tercero". Quedan, sin embargo, por determinar múltiples aspectos relativos a este elemento, como su naturaleza objetiva o subjetiva, los sujetos a los que en concreto se refiere el mismo o cómo debe sustanciarse en el ámbito de la conducta típica. Además resulta que todas estas preguntas se encuentran interrelacionadas entre sí. En definitiva tenemos un precepto y unos supuestos, los del art. 197.2, que generan en la doctrina una auténtica desorientación a la hora de aclarar su sentido. Esto queda claro, la más que deficiente técnica legislativa empleada para redactar el precepto, ante las innumerables y diversas propuestas interpretativas a que da lugar.

En ocasiones este elemento se entiende desde la perspectiva subjetiva "como un elemento subjetivo del injusto equivalente a que el acto se lleve a cabo para descubrir o vulnerar la intimidad de otro"[67]. Esta comprensión subjetiva no resulta necesaria pero además cabe preguntarse, de haber sido tal la pretensión del legislador, por qué no utilizó la misma fórmula que en los supuestos del art. 197.1 para introducir un elemento subjetivo. La exigencia típica de perjuicio puede ser entendida, como sucede generalmente en los numerosos hechos punibles en los que se plantea de igual manera, bien en sentido subjetivo o bien en sentido objetivo. Si se estima que es un elemento subjetivo, como un particular elemento subjetivo del injusto, se viene a requerir que el autor actúe con la tendencia interna de perjudicar, con ánimo de causar perjuicio. Ello comporta las dificultades propias de todos los elementos de naturaleza subjetiva.

Entre las distintas posibilidades JAREÑO/DOVAL[68] entienden que se trata de un elemento objetivo, siguiendo la tesis del TS en la sentencia de 18 de febrero de 1999, por las dificultades que entrañan los elementos subjetivos y por no añadir nada a la conducta específica de acceso que queda fijada ya con su mera consideración objetiva. Consideran que la perspectiva objetiva obliga a entender este elemento como resultado lesivo abarcado por el dolo. La perspectiva objetiva parece acertada, no así su comprensión como resultado lesivo, no congruente con la estructura del tipo ni necesario desde el punto de vista gramatical.

De otra manera, en sentido objetivo, cabe vincularlo a la tendencia de la conducta externa del autor, como idoneidad objetiva de la misma para causar un perjuicio. La conducta desarrollada por el sujeto debe reunir condiciones apropiadas para lesionar la intimidad de la víctima, aun cuando no llegue a producirse tal lesión. Esta opción permite descartar aquellos hechos que no pudieran originar perjuicio alguno para el bien jurídico. Pero además, de acuerdo a la estructura del delito aquí mantenida, resulta acertado exigir una idoneidad objetiva de la acción para lesionar el bien jurídico, precisamente porque la consumación del delito no va a precisar que de manera efectiva se menoscabe la intimidad. Parece más acertada esta versión, que además conecta con los postulados de la moderna teoría de la imputación objetiva y con la consideración de este supuesto como delito de resultado, en relación al acceso a los datos, que no como lesión de la intimidad.

Como se ha dicho, el legislador incluye este elemento del perjuicio en dos momentos distintos. En un primer momento se refiere a la actuación "en perjuicio de tercero" y en un segundo inciso la referencia lo es al comportamiento "en perjuicio del titular de los datos o de un tercero". Como en el primer caso únicamente se menciona al tercero, éste tiene que coincidir necesariamente con el titular del bien jurídico (intimidad), quien ve afectada su intimidad por el comportamiento sobre los datos reservados. No es posible entender que quien se ve afectado en su intimidad sólo se proteja en el segundo inciso. La denominación de tercero responde entonces a su consideración desde el punto de vista del autor de los hechos.

En el segundo momento regulativo el legislador se refiere no sólo al tercero sino también al titular de los datos. Lo que, según la interpretación propuesta, debe corresponder con el titular de la gestión de los datos, es decir, con el titular del fichero o del conjunto de datos cuyo tratamiento está automatizado. En este sentido MARCHENA[69] entiende que en este caso se protege a tal titular frente a un posible desapoderamiento o utilización inconsentida de los datos desde la perspectiva patrimonial. Con ello se decide también el último aspecto concerniente a la

67 En este sentido MORALES. *Comentarios a la Parte Especial del Derecho Penal* (QUINTERO director). Aranzadi, 2005, pág. 424.

68 "Revelación de datos personales, intimidad e informática*". El nuevo Derecho Penal Español. Estudios Penales en Memoria del Profesor José Manuel Valle Muñiz*, Aranzadi 2001, págs. 1486-90.

69 MARCHENA GÓMEZ, M. "Intimidad e informática: la protección jurisdiccional del habeas data*". Boletin de Información. Ministerio de Justicia e Interior nº 1768 (1996)*, pág. 756. Sobre estos aspectos en la legislación Suiza SCHMID, N. *Computer- sowie Check- und Kreditkartenkriminalität*, Zürich 1994, págs. 34 y ss.

naturaleza del perjuicio. Para el denominado tercero se protege la intimidad y para el llamado "titular de los datos" lo relevante es el aspecto patrimonial, cuya inclusión en este ámbito sistemático puede considerarse una incongruencia[70]. De todas las maneras, la necesidad político-criminal de una reorganización del precepto se hace ineludible como se hace todavía más patente al analizar más adelante las concretas conductas descritas en el tipo.

Las conductas realizadas sobre datos reservados obrantes en ficheros automatizados deben realizarse por el sujeto activo "sin estar autorizado". Es decir, se criminalizan las conductas previstas en este número segundo del art. 197 que no cuenten con la anuencia del interesado o interesados. Teniendo en cuenta que el sistema de protección de datos se ha formulado legalmente como sistema de registro pero no de autorización previa de los bancos de datos no es posible entender que se refiera el legislador a tal autorización para la creación del banco. Por ello deberá entenderse como autorización del titular de los datos respecto a la inclusión en el fichero.

Se trata pues de un ámbito en el que el legislador admite la disponibilidad del bien jurídico tutelado por su titular. Como al referirnos a los sujetos perjudicados hemos distinguido entre el tercero y el titular, nuevamente aquí debe aplicarse la distinción a los efectos de determinar quien debe prestar el consentimiento válido. La forma concreta de prestación del consentimiento deberá ser aquella en la que quede determinado de manera incuestionable la auténtica voluntad del interesado con relación a la conducta a realizar sobre los datos reservados.

d) Las conductas punibles de ataque a la protección de datos

Se ha indicado ya que las conductas relativas al habeas data penal en sentido estricto, desenvueltas por el autor del hecho punible vienen recogidas en el número segundo del art. 197 en dos momentos sucesivos. En un primer inciso el legislador incrimina "al que, sin estar autorizado, se apodere, utilice o modifique" los datos registrados en ficheros. Ya en el segundo inciso prevé las mismas penas para "quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice".

El apoderamiento debe entenderse en el sentido señalado, como aprehensión de algún tipo de materialización de los datos contenidos en el fichero. Ahora se trata de datos consignados en un fichero automatizado y no de los datos recogidos documentalmente (según la previsión del número primero del art. 197 en su primer inciso). La descripción de la misma conducta dos veces distintas pudiera hacer surgir problemas concursales, pero la distinción se produce no tanto por la acción misma sino por el objeto del apoderamiento, en un caso de carácter documental y en otro sobre datos registrados en ficheros. La utilización de los datos se entiende como cualquier comportamiento de aprovechamiento posterior de los mismos. La modificación supone el cambio o transformación de los datos almacenados en el fichero. Modificación y alteración son conductas equivalentes a pesar de que el legislador emplee términos diversos. Con el acceso se produce la captación intelectual de la información almacenada en el sistema informático[71].

ORTS/ROIG[72] entienden, que las conductas del número segundo del art. 197 configuran un delito de resultado, en cuanto para su consumación requieren el apoderamiento (en el sentido de acceso) de los datos secretos. Es verdad que para todos los supuestos se requerirá al menos el acceso al dato registrado en un fichero –como límite mínimo–, pero es posible que como tipo mixto alternativo se produzcan otros resultados diversos admitidos por el tipo: al menos los de modificación y utilización, que van más allá del mero acceso al dato personal. Esto nos pone sobre la pista de alguna diferencia entre los supuestos del art. 197. En principio las conductas del 197.1 y del 197.2 coinciden en la exigencia de un resultado, el apoderamiento para el inciso primero del 197.1, la interceptación o captación de la comunicación en el inciso segundo y el acceso a los datos o su modificación o utilización para los supuestos del 197.2 (al menos la conducta debe llegar al estadio de acceso a los datos). Pues bien, con base en la diferencia de objetos materiales sobre los que recae la conducta la afectación del bien jurídico tutelado será diversa. En el ámbito del 197.1 el apoderamiento de los objetos o la interceptación de la comunicación no genera automáticamente un conocimiento de los datos por lo que el bien jurídico únicamente ha sido amenazado o puesto en riesgo (delito de peligro). Pero para el supuesto de los da-

70 MARCHENA GÓMEZ, M. "Intimidad e informática: la protección jurisdiccional del habeas data*". Boletín de Información. Ministerio de Justicia e Interior nº 1768 (1996)*, págs. 756.

71 Conducta ésta de acceso que no debe confundirse nunca con la de intrusismo informático o acceso no consentido, pues en esta última no se produce el acceso a los datos sino al sistema mismo. Esta diversidad de conductas puede verse extensamente en GÓMEZ NAVAJAS, J. *La protección de los datos personales*. Thomson/Civitas, Madrid 2005, págs. 135 y ss. Se hace referencia a cada una de estas conductas además en CARBONELL/G.CUSSAC. *Comentarios al Código penal de 1995*, vol I, págs. 1000 y ss. También de los mismos autores en *Derecho Penal. Parte Especial*, Tirant lo Blanch 1999, págs. 290-2.

72 *Delitos informáticos y delitos cometidos a través de la informática*. Tirant lo Blanch, Valencia 2001, pág. 31. Esta acertada calificación pone de relieve una diferencia con los supuestos del número primero del art. 197. En principio las conductas del 197.1 y del 197.3 coinciden en la exigencia de un resultado, el apoderamiento para el inciso primero del 197.1, la interceptación o captación de la comunicación en el inciso segundo y el acceso a los datos para los supuestos del 197.2.

tos personales cuyas modalidades de ejecución deben consistir por lo menos en el acceso a los mismos (o bien, todavía en estadios más avanzados su modificación o utilización), este acceso se identifica ya con el conocimiento del mismo dato y su contenido por lo que el bien tutelado de la intimidad informática o habeas data ha sido conculcado de manera efectiva (delito de lesión). Hay que descartar que las conductas de modificación o alteración se entiendan de forma equivalente al delito de daños[73], pues en ese ámbito normativo existe una incriminación específica y aquí nos situamos en el sector de tutela de la intimidad. Desde este punto de vista la modificación o alteración idónea para lesionar la intimidad de otra persona debe presuponer el acceso.

Por tanto las conductas típicas incluyen comportamientos que se sitúan en dos segmentos distintos del ciclo total de un fichero automatizado de datos. Por una parte, se incriminan conductas realizadas sobre los datos existentes en el fichero (acceso, modificación y alteración) y, por otra, conductas posteriores cuando el dato ha sido obtenido ya del fichero (utilización). Sin embargo, nada obliga a que quien obtiene el dato del fichero y quien lo utiliza posteriormente sean los mismos sujetos. No se recogen otros supuestos distintos, por lo que quedan excluidos de la zona penalmente prohibida momentos previos a la incorporación del dato al fichero (recogida ilícita de datos o formación misma del fichero).

No deja de señalarse por la doctrina la diferenciación legislativa a la hora de incriminar las conductas punibles, en dos momentos sucesivos, empleando los mismos o equivalentes términos, con lo que se llega a una situación de confusión. Se ha producido algún intento de explicar las divergencias de las dos secuencias típicas. Así CARBONELL/G. CUSSAC[74] sitúan la distinción en torno al objeto de las conductas. De este modo el primer inciso (apoderamiento, utilización o modificación) se proyectaría sobre los datos reservados, mientras el segundo momento lo haría sobre los ficheros o soportes informáticos, electrónicos o telemáticos. De manera que CARBONELL/G. CUSSAC entienden por tanto el segundo inciso como protección de los ficheros o soportes mismos y no de los datos en ellos incluidos. MORALES señala varios inconvenientes para esta interpretación, como el definitivo de que la intimidad que es el objeto de protección no se contiene en los soportes sino en los datos. Este autor ha rechazado acertadamente esta posibilidad al desenfocar teleológicamente la regulación, pues la protección de la intimidad hace relación a los datos personales y no se persigue la tutela de los ficheros o sistemas informáticos por sí mismos. Además, señala otras disfunciones como la de adelantar el momento de protección de los ficheros y retrasar la línea de intervención penal para los datos personales, auténtico objeto material del bien jurídico intimidad[75].

Quizás otra forma de señalar la distinción entre ambos incisos legislativos pudiera correr mejor suerte. Puede entenderse que la distinción responde no al objeto material sino a los sujetos que pueden recibir el perjuicio (potencial) exigido por la regulación. Conforme a lo desarrollado antes para el elemento del perjuicio se ha señalado ya como en un primer momento su destinatario es únicamente el tercero y en el segundo momento también el titular de los datos. Así las conductas de apoderamiento, utilización o modificación se vinculan al sujeto pasivo tercero, entendido como el afectado en su intimidad por las conductas realizadas sobre los datos reservados.

La segunda secuencia típica se refiere al acceso, alteración o utilización, pero para éstas se señala como sujeto pasivo no sólo el tercero, sino también "el titular de los datos" entendido como el propietario del fichero que vería lesionado su poder de disposición sobre el conjunto de datos y organización que constituyen el fichero, archivo o registro. La diferencia está únicamente en la conducta de acceso, no prevista en el primer inciso, como si se quisiera expresar que la misma no constituye atentado a la intimidad y sí de carácter patrimonial para el titular del fichero. De ser esta la concepción que subyace tras la regulación, ésta constituye un excelente ejemplo de deficiente técnica legislativa.

En el sentido indicado ROMEO[76] señala que el primero supuesto puede ser cometido por el propio titular de los datos en perjuicio de un tercero, lo que ya no tendría cabida en el segundo ámbito al incluirse el perjuicio del titular de los datos o de un tercero, de manera que debe ser otro el que perjudique necesariamente al titular. Se apunta así una interpretación relativa a los intervinientes en los hechos y quienes sufran el perjuicio, aun siendo conscientes de la confusión descriptiva y del solapamiento de conductas.

En realidad el texto del número segundo del art. 197 es fruto de un particular modo de legislar. La redacción definitiva del precepto tiene su origen en una superposición descoordinada de enmiendas sobre la base del texto del proyecto de Código Penal de 1994, sin tener en cuenta lo que cada una de ellas modificaba del sentido del texto. El Proyecto únicamente incluía la acción de apoderamiento

73 Cfr. GÓMEZ NAVAJAS J. *La protección de los datos personales*. Thomson/Civitas, Madrid 2005, págs. 139-40.

74 *Comentarios al Código penal de 1995*, vol I, pág. 1001.

75 En *Comentarios a la Parte Especial del Derecho Penal* (QUINTERO director). Aranzadi, 2005, págs. 426-7. De la misma manera rechaza esta posibilidad GÓMEZ NAVAJAS J. *La protección de los datos personales*. Thomson/Civitas, Madrid 2005, págs. 144-5.

76 *Comentarios al Código penal, Parte Especial II*. DÍEZ RIPOLLÉS/ROMEO CASABONA (coordinadores). Tirant lo Blanch, Valencia 2004, págs. 754 y ss.

de los datos reservados (art. 188)[77]. La enmienda número 606 del GS había incorporado las conductas de utilización o modificación del finalmente primer inciso que debía producirse "en perjuicio de otro"[78]. La número 728 del Grupo Federal IU-IC añadía la posibilidad de incluir los soportes electrónicos o telemáticos y, finalmente, la conducta por la que se "accediese por cualquier medio a los mismos sin la citada autorización"[79]. La enmienda número 49 del GPV añadía al final "y a quien los alterase o utilizare en perjuicio del titular de los datos o de un tercero"[80]. Con alguna reforma de matiz y estilo, ésta fue la redacción definitiva, como conjunción de distintas enmiendas que aisladamente poseían cierta coherencia, pero que sumadas todas ellas creaban una gran confusión y desdibujaban el sentido de la regulación.

e) El Convenio de Cibercrimen: el problema del mero intrusismo informático

Además de la legislación española en una materia como la de la delincuencia informática se hace necesario la creación de instrumentos jurídicos internacionales. La exigencia de cooperación internacional para el caso de estos delitos que traspasan con gran facilidad los límites nacionales se hace evidente. Por ello, distintos grupos de trabajo dirigen sus esfuerzos a lograr instrumentos internacionales aptos para la lucha contra una forma de delincuencia claramente transnacional. El Convenio de Cibercrimen del año 2001 (Budapest 23.11.01), redactado en el marco de la actividad del Consejo de Europa –pero abierto a la firma de cualquier país, de manera que lo fueron países como Estados Unidos o Canadá– representa por el momento el instrumento internacional más válido frente a la cibercriminalidad. Pese a estar firmado por más de una treintena de países, sin embargo, no cuenta en este momento con un número elevado de ratificaciones. Aun así debe ser objeto de atención en las distintas materias en las que aborda, entre ellas la de la armonización de los hechos punibles vinculados a la informática que deben estar penalizados en los países firmantes. El Convenio de Cibercrimen propone entonces en esta materia varias infracciones que deberán ser incorporadas a las legislaciones nacionales y que clasifica en cuatro grandes grupos de ilícitos penales.

Un primer grupo de infracciones lo constituyen los hechos contrarios a la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos. Como se verá se trata de hechos infractores poco congruentes con la regulación penal española pues no poseen una correspondencia unitaria con las previsiones de nuestro Código Penal. Dentro de este grupo se incluyen, en primer lugar, las conductas de acceso ilegal injustificado a todo o parte de un sistema informático (art. 2). La legislación penal española actual –a diferencia de lo que sucede en otros países, como Portugal– no conoce una auténtica infracción de mero acceso o mero intrusismo informático[81]. Se entiende como tales conductas las de acceso no autorizado de forma subrepticia a cualquier sistema informático o red de comunicación electrónica de datos. Extensivamente se puede incluir las conductas de interferencia del sistema o de utilización no consentida del mismo o con exceso respecto a lo autorizado[82]. En algunos casos los autores se deciden claramente por el castigo de estas conductas, llegando a mostrarse tan favorables a la incriminación que llegan a decir que "Uno de los defectos de la regulación de los delitos informáticos en nuestro Código Penal (CP) es la ausencia de tipificación del acceso no autorizado o ilegítimo"[83]. Otros autores, de forma mucho más matizada, no dejan de reconocer las dificultades para su castigo, empezando por la de determinar el bien jurídico atacado –que no se sabe bien cuál sea y que sería preciso crear–, así como la necesidad de recurrir a la técnica de los delitos de peligro, de manera que se concluye que "la sanción administrativa se desvela como el instrumento y reproche

77 *Ley Orgánica del Código Penal. Trabajos Parlamentarios, vol I*, Cortes Generales 1996, pág. 36.

78 *Ley Orgánica del Código Penal. Trabajos Parlamentarios, vol I*, Cortes Generales 1996, pág. 272.

79 *Ley Orgánica del Código Penal. Trabajos Parlamentarios, vol I*, Cortes Generales 1996, pág. 299.

80 *Ley Orgánica del Código Penal. Trabajos Parlamentarios, vol I*, Cortes Generales 1996, págs. 124-4. Esta enmienda se redactaba como añadido al apartado 2 de la anterior enmienda 606 del GS.

81 Sobre la problemática del acceso ilegal en nuestro sistema penal puede verse RODRÍGUEZ MOURULLO/ALONSO GALLO/LASCURAIN SÁNCHEZ, "Derecho penal e Internet". Régimen Jurídico de Internet, La Ley 2002, págs. 266 y ss. También MORÓN LERMA, E. *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la Red*, Aranzadi 2002, págs. 46 y ss

82 Sobre el concepto de intrusismo informático GUTIÉRREZ FRANCÉS, M.ª.L. "Delincuencia económica e informática en el nuevo Código Penal", *Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial*, CGPJ, Madrid 1996, págs. 299-300. También MORÓN LERMA, E. *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la Red*, Aranzadi 2002, págs. 50 y ss.

83 RODRÍGUEZ MOURULLO/ALONSO GALLO/LASCURAIN SÁNCHEZ, "Derecho penal e Internet". *Régimen Jurídico de Internet*, La Ley 2002, pág. 269. Estos autores entiende que con el mero acceso se ha lesionado ya la confidencialidad del sistema y que el mismo va a suponer inevitablemente algún tipo de modificación de los datos y que frecuentemente los hackers realizan alteraciones de dichos datos para intentar borrar los rastros que pudieran identificarles. En realidad este tipo de argumentación lo que hace es poner en cuestión el concepto de intrusismo sobre el que estamos discutiendo, pues si se da por comprendida algún tipo de alteración de los datos la valoración jurídico penal de estos hechos debe ser bien distinta de una compresión del intrusismo como mero acceso inconsentido sin que afecte a datos concretos.

idóneo frente a los riesgos generados por los accesos inconsentidos"[84].

Efectivamente hay que señalar que el mero intrusismo o acceso inconsentido –sin otros añadidos o resultados ulteriores– en todo caso no es propiamente un hecho contrario a la intimidad informática de las personas pues no se trata de acceso a los datos sino al sistema informático mismo. De forma que quienes se inclinan por su recepción en el sistema penal se ven obligados a construir un nuevo bien jurídico cuyo contorno no puede perfilarse suficientemente ni se corresponde con las categorías existentes. En este sentido para GUTIÉRREZ FRANCÉS[85] las conductas de intrusismo podrían afectar a un nuevo interés consistente en la seguridad de los sistemas informáticos o bien la confianza en el funcionamiento de los sistemas de procesamiento de datos. Para RODRÍGUEZ MOURULLO/ALONSO/LASCURAIN[86] en todos los casos de acceso no autorizado y al margen de los resultados e intenciones ulteriores del sujeto, se ha producido ya una lesión de la confidencialidad y de la integridad del sistema informático atacado. Pero además de las dificultades evidentes para construir un nuevo bien jurídico, desde el ángulo del principio de lesividad, tampoco parece que tal comportamiento sea equiparable a otros propios de la delincuencia informática como los daños informáticos, la causación de perjuicios económicos mediante manipulaciones informáticas o el acceso y modificación de datos concretos y relevantes de las personas, desde la perspectiva del principio de proporcionalidad. De hecho el Consejo de Europa entre las Recomendaciones relativas a la delincuencia por ordenador de los años 1989/90 no incluyó este supuesto en la lista de "mininum" que los Estados deberían convertir en supuestos punibles, sino en la lista opcional para su incriminación, debido a la inseguridad sobre su merecimiento de sanción criminal y la falta de acuerdo necesario entre los negociadores[87].

El Convenio permite que las partes firmantes modulen la incriminación de este supuesto mediante diferentes formas. Así es posible vincular la punibilidad de este hecho a la violación de medidas de seguridad, la existencia en el autor de determinadas intenciones a la hora de realizar el hecho o la presencia de conexión entre distintos sistemas informáticos. También se abarcan los supuestos de interceptación ilegal de comunicaciones entre sistemas informáticos o en el interior de un mismo sistema, mediante el empleo de medios técnicos (art. 3). En el art. 4 se sitúan los atentados a la integridad de los datos, consistentes en el daño, borrado, deterioro, alteración o supresión intencional de datos informáticos. Este supuesto se puede condicionar a la producción de daños de carácter grave.

Después de haber realizado este recorrido por la tutela penal de la libertad informática y especialmente del habeas data penal, conviene recordar que la regulación penal, la imposición e sanciones criminales para el caso de conculcación de los derechos relativos a esa libertad informática de los individuos, no es más que el último eslabón –frente a los casos más graves y amenazadores– de la protección jurídica de datos. Pero es que el hacer realidad el respeto a los datos personales depende no sólo de un adecuado régimen legal, sino de un debate más amplio en el que se incluya, al menos, la conexión con la organización política, la historia del control social y la sociología de la tecnología. El Derecho, en este caso de forma más evidente que en otros, posee límites sin duda y no representa por sí solo una salvaguardia suficiente frente a los riesgos. Únicamente desde esta comprensión más totalizadora puede emprenderse el rumbo en el que las personas puedan verse como ciudadanos de sus datos y no como meros súbditos de la información concerniente a sí mismos.

84 MORÓN LERMA, E. *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la Red*, Aranzadi 2002, págs. 74 y ss

85 "Notas sobre la delincuencia informática: atentados contra la información como valor económico de la empresa". En ARROYO ZAPATERO/TIEDEMANN (eds.). *Estudios de Derecho Penal Económico*. Ediciones de la Universidad de Castilla La Mancha, Cuenca 1994, pág. 206.

86 "Derecho penal e Internet". *Régimen Jurídico de Internet*, La Ley 2002, pág. 269.

87 Cfr. MORÓN LERMA, E. *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la Red*, Aranzadi 2002, pág. 51.