Doctrina

Vías para la tipificación del acceso ilegal a los sistemas informáticos (y II)[1]

Nuria Matellanes Rodríguez

Profesora de Derecho Penal
Universidad de Salamanca

Revista Penal, n.º 23.—Enero 2009

***RESUMEN**: El trabajo se ocupa de la polémica acerca de la necesidad del delito de intrusismo informático. Ante la existencia de una previsión europea de incorporar a los códigos penales dicho delito, dada la inadecuación de los tipos vigentes en nuestro ordenamiento y la previsión de reforma del Código Penal, con la incorporación de un tipo autónomo y específico en esta materia, el trabajo estudia el contenido esencial que se asignaría el delito previsto, valorando sus lagunas y su idoneidad.*

***PALABRAS CLAVE**: delincuencia informática, intrusismo, derecho europeo, intimidad, secreto.*

***SUMMARY:** This article is focused about the need of a specific hacking crime. There is a prevision, in european law, of including such a crime in the criminals codes. In our country, the existing crimes aren´t able to include these kinds of behaviours, so in prevision of a reform in this aspect, this research analyses the main lines of the upcoming crime, valuing its flaws and its ability.*

***KEY WORDS**: computer crime, hacking, european law, intimacy, secret.*

5. Nuevos términos del debate: la reforma del artículo 197. 3 del código penal

5.1. La previsión del derecho positivo

Tanto la solución a la que se llega doctrinalmente de entender que los tipos penales vigentes en nuestro país no son idóneos apara albergar bajo su esquema típico las conductas de acceso no consentido a los sistema informáticos[2], así como los argumentos a favor o en contra de la necesidad de su punición específica me parecen, con carácter general, irreprochables. En particular, dichos argumentos a favor o en contra de la necesidad de la incriminación específica, encuentran su razón de ser en las diferentes opciones de polí-

1. Este trabajo constituye la segunda parte del publicado, con el mismo título en *Revista Penal*, nº 22, julio 2008.

2. Por ejemplo, GONZÁLEZ RUS, J.J.: «Los ilícitos en la red (I): *hackers*, *crackers, cyberpunks*, *sniffers*, denegación de servicio y otros comportamientos semejantes», *El Cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales* (ROMEO CASABONA, Coord.), Comares, Granada, 2006, pág. 248; MIR PUIG, C.: «Sobre algunas cuestiones relevantes del Derecho

tica-criminal en esta materia, vinculadas a la valoración que merezca el actual discurrir del Derecho penal caracterizado, como decíamos, por una tendencia (ya casi inercia) a la contención de riesgos de gran magnitud y a la incriminación de las más diversas manifestaciones de inseguridad: inseguridad ciudadana, inseguridad terrorista, inseguridad en el ámbito de la salud, inseguridad ante los avances médicos…, e inseguridad ante los avances de la tecnología informática, como sucedería en este caso. La asunción de que la seguridad de los sistemas informáticos o el pacífico uso y disfrute de esta vía de comunicación sea elevada a la consideración de interés penalmente relevante conecta con la preocupación acerca de si realmente nos hallamos ante auténticos bienes jurídicos o más bien ante la tutela de lo que se ha denominado «metáforas o abstracciones conceptuales»[3], que representan el envoltorio penal de lo que es la protección de meros intereses funcionales o instrumentales, en línea con las concepciones sociológico-funcionalistas del bien jurídico. Y decantarse acerca de si es legítima esta tendencia expansiva del Derecho penal hacia la tutela de funciones sociales o espacios de control tradicionalmente residenciados en las instancias públicas determina, también, un posicionamiento en torno a la pérdida de nitidez de los límites entre un concepto de bien jurídico, propio del derecho penal liberal, es decir, como referente axiológico de orientación o delimitación de la selección penal[4], y un concepto de bien jurídico en el que prime su función promocional[5]. Finalmente, todo ello se traduce en la aceptación o el rechazo de la denominada «administrativización del Derecho penal», fenómeno que nos coloca ante el modelo de Estado más intervencionista de los conocidos hasta la fecha, y que se ha denominado Estado de prevención[6].

Pero excede con mucho las pretensiones que nos habíamos trazado para este trabajo el realizar un pronunciamiento acerca de esta evolución que está sufriendo el Derecho penal y la incidencia de este proceso en la revisión de las garantías penales[7]. Por eso, no he entrado a valorar personalmente las opiniones vertidas acerca de si existe o no un nuevo bien jurídico de relevancia penal, si efectivamente es necesario o no un nuevo tipo, o si hace falta un delito de peligro abstracto en esta materia. La omisión es consciente, toda vez que lo único que se ha pretendido ha sido presentar el estado de la cuestión de lo que hasta el momento han sido respuestas diversas planteadas en un *contexto de lege ferenda* ante las distintas opciones de política criminal en materia de ilícitos cometidos mediante la informática o a través de la informática.

Ahora bien, así contextualizado el debate y aceptada su corrección, hay que tener en cuenta que lo es desde la *hipótesis de partida desde la que se formulan los argumentos anteriores: que el comportamiento de hacking puro no es nada más que el acceso al sistema sin entrar en contacto con nada más, porque desde el momento que ya se pasa a un contacto directo con los datos, a una interceptación de los mismos, ya hay algo más que hacking*.

Y como anteriormente manifestaba, lo subrayan con empeño los autores que han analizado el tema con profundidad: MÓRON LERMA, que afirma que cuando hay «interceptación, ya no es por definición un *mero* acceso inconsentido»[8]; similares son las palabras de MATA Y MARTÍN, según quien «el mero intrusismo (…) no se trata de acceso a los datos, sino al sistema informático mismo»[9], o de LÓPEZ ORTEGA, sostiene que «si hay acceso a datos ya no hay un simple acceso inconsentido, sin algo más que el mero intrusismo informático»[10].

Semejante caracterización de la conducta es en sí misma acertada y no merece objeción, puesto que se formula a través de un doble análisis: sistemático-legislativo, ya que toma como referencia el contenido específico de otras conductas punibles con las que el intrusismo pudiera tener algo de proximidad, pero destacando el rasgo que le peculiariza (el mero acceso no autorizado a un sistema ajeno, sin buscar otros fines ni afectar otros intereses específicos) y un análisis criminológico, que pone de manifiesto la existencia de conductas de este tipo. Pero siendo estos los presupuestos de los que se ha partido, *los argumentos vertidos acerca de la aptitud de un tipo penal para incorporar en la órbita de su prohibición esta clase de comportamiento o la conveniencia o no de realizar una tipificación explícita de ella no puede calificarse sino como especulación teórica* acerca del *hipotético* contenido, alcance y estructura típica que tendría un eventual tipo de *hacking* concebido bajo ese estereotipo de conducta.

penal en Internet», *Internet y Derecho penal*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2001, pág. 299; LÓPEZ ORTEGA, J.J.: «Intimidad informática y Derecho penal», *Derecho a la intimidad y nuevas tecnologías*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2004, pp. 118 y ss.

3. HASSEMER, W.: «Lineamientos para una teoría personal del bien jurídico», *Doctrina Penal*, nº 46, 1989, pág. 275.

4. MÉNDEZ RODRÍGUEZ, C.: *Los delitos de peligro y sus técnicas de tipificación*, Universidad Complutense de Madrid, Madrid, 1993, pág. 6 y pp. 154 y ss.

5. SÁNCHEZ GARCÍA DE PAZ, I.: *El moderno Derecho penal y la anticipación de la tutela penal*, *op. cit.*, pág. 74, con abundantes referencias bibliográficas.

6. BARATTA, A.: «Funciones instrumentales y simbólicas del Derecho penal: una discusión desde la perspectiva de la criminología crítica», *Pena* y *Estado*, nº 1, 1991, pág. 43.

7. GRACIA MARTÍN, L.: *Prolegómenos para la lucha por la modernización y expansión del Derecho penal y para la crítica del discurso de resistencia*, Tirant lo Blanch, Valencia, 2003, pp. 127 y ss.

8. MORÓN LERMA, E.: *Internet y Derecho penal: hacking y otras conductas ilícitas en la red*, Aranzadi, Pamplona, 2002, pág. 60.

9. MATA Y MARTÍN, R.: «La protección penal de datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías», *Revista Penal*, nº 18, julio 2006, pág. 235.

10. LÓPEZ ORTEGA, J.J.: «Intimidad informática y Derecho penal», *op. cit.*, pág. 119.

Sin embargo, *a los efectos de este estudio, lo interesante no es seguir elucubrando acerca de la conveniencia o no de la incriminación de un hacking informático definido en esos términos, sino valorar el lineamiento ya apuntado por el legislador penal ante este fenómeno.* La anunciada reforma del Código Penal en este punto nos ofrece una posición legislativa concreta. Salimos del terreno de las especulaciones y opiniones sobre lo que sería una hipotética conformación del Derecho penal en este punto para situarnos ante una opción específica en torno a las conductas de intrusismo informático.

Y ésta es la presentación del problema que hace el propio legislador en la Exposición de motivos del Proyecto de Ley Orgánica de 15 de enero de 2007, por la que se modifica la LO 10/1995 de 23 de noviembre del Código Penal:

Exposición de Motivos:

La tutela penal de la intimidad y de los secretos ha sido tradicionalmente fragmentaria, y condicionada a la realización de conductas de apoderamiento de papeles, cartas o mensajes, o de instalación de aparatos de captación de imagen o sonido, pero a la vez que la importancia fundamental de ese bien jurídico exige cada vez mayor atención y medidas legales, como son esencialmente las recogidas en la legislación sobre protección de datos, crecen los riesgos que lo rodean, a causa de las intrincadas vías tecnológicas que permiten violar la privacidad o reserva de datos contenidos en sistemas informáticos. Esa preocupante laguna, que pueden aprovechar los llamados hackers ha aconsejado, cumpliendo con obligaciones específicas sobre la materia plasmadas en la Decisión Marco 2005/222/JAI de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información, incorporar al art. 197 del Código Penal un nuevo apartado que castiga a quien por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático.

Art. 197.3:

«3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo, será castigado con pena de prisión de seis meses a dos años.»

La pregunta que ahora surge es: ¿ha dado respuesta el legislador a una conducta de *hacking* en el sentido que hemos descrito, como puro acceso al sistema sin otro contenido objetivo o subjetivo ulterior, o se castiga algo diferente? Cercano, pero distinto. El propio legislador habla de manera expresa de la actuación de los «*hackers»,* pero directamente apunta a que el sentido de estas intromisiones ilícitas se destina, y cito palabras textuales tomadas de la Exposición de motivos antes transcrita, a la «tutela penal de la intimidad y de los secretos», «la privacidad o reserva de los datos contenidos en sistemas informáticos». En efecto: el tipo previsto exige que el intruso *acceda a datos*. *El legislador no se detiene en ese solo acceso al sistema que caracteriza al hacking puro*, *sino que avanza en las exigencias típicas hacia una captación de los datos almacenados* en el sistema.

A la vista de ello, la primera impresión que delata esta nueva tipicidad relativa al *hacking* es que va a tener «cierta» conexión con la intimidad y que más que tutelar de manera directa y específica la seguridad de los sistemas informáticos o el pacífico funcionamiento de los mismos, que a su vez, representa una situación de riesgo para una variedad de bienes jurídicos (intimidad, patrimonio, seguridad nacional, competitividad económica de la empresa, etc.), el interés jurídico se centra en dar protección, con la finalidad de cubrir «una preocupante laguna» (según palabras del propio legislador), a formas de ataque a la intimidad que no estarían cubiertas por el art. 197, ya que en éste dicha tutela «ha sido (…) condicionada a la realización de conductas de apoderamiento de papeles, cartas o mensajes, o de instalación de aparatos de captación de imagen o sonido».

El desplazamiento de los términos de debate, por lo tanto, está servido: por principio no parece que el genérico intrusismo informático o «*hacking* puro» sea el contenido en el nuevo tipo o, al menos no solo, sino que en él también se da cabida una nueva forma de ataque a la intimidad personal. Ahora bien, lo que se intuye desde una primera lectura del precepto y de la voluntad del legislador manifestada en la Exposición de motivos del Proyecto de Ley de reforma del Código Penal requiere una profundización y un detenimiento detallado, al que nos dedicaremos a continuación. En lo que sigue, por lo tanto, este trabajo se dedicará a identificar con mayor precisión el objeto tutelado en el tipo del art. 197.3 y su alcance, concretando, de este modo, la clase de *hacking* que pasará al catálogo de conductas típicas.

5.2. Los sistemas informáticos como ámbito de comisión y la diversa dimensión atribuible al tipo

El carácter de «delito informático» del nuevo delito contenido en el art. 197.3 del Proyecto de Código Penal está fuera de toda duda. En un momento anterior se ha apuntado que la categoría de delito informático era una categoría de uso criminológico y de contenido funcional que permitía incorporar a la misma aquellas conductas en las que se apreciara un factor de abuso o extralimitación de las funciones propias que los sistemas informáticos; abuso que podía consistir en atentar directamente contra ellas, o bien en utilizarlas como sede de vulneración de algún interés. En este caso, la comisión directa de la conducta directamente sobre el sistema, abusando de las legítimas posibilidades de utilización del mismo es clave para encajar al *hacking* como un caso más dentro de la variada tipología de «delincuencia informática»[11].

11. Sea bien entendido que la calificación de esta conducta como «delito» está supeditada a su definitiva incorporación al Código Penal; no sería, por tanto, en este momento, un «delito» en sentido técnico, dado su estadio de propuesta *de lege ferenda*.

El origen del párrafo tercero del art. 197 previsto en el Proyecto de Código Penal está en la Decisión-Marco ya comentada. Y en ella, en la exposición de motivos o «*considerandos»* se insiste en una clara voluntad de armonización, que llega incluso a concertarse en la del empleo de un lenguaje común, seguro que ante la consciencia de que el mundo informático está altamente tecnificado, lleno de matices que pueden entorpecer ese objetivo unificador en caso de que los conceptos se entiendan de manera diferente y, por lo tanto, se les dote de distinto alcance. Por eso, se confiesa la voluntad, y cito palabras textuales del décimo «considerando», de utilizar unas «*definiciones comunes en este ámbito, más concretamente de los sistemas de información y los datos informáticos, son importantes para garantizar la aplicación coherente de la presente Decisión marco en los Estados miembros*». Así que, se ha de tomar de la Decisión-marco el significado de aquellos términos que ella misma defina. Y en este punto nos interesa la definición de «sistemas informáticos» y «datos informáticos» (art. 1).

— sistema informático es «*todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento*».

— dato informático es «*toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función*».

Por principio, cabe hacer varias observaciones: a) que el sistema informático requiere de aparatos conectados, formando un sistema o red informática, lo cual excluye los aparatos informáticos absolutamente autónomos o desconectados de una red; ellos no van a ser sede de las conductas típicas de intrusismo; b) que se extiende el concepto de sistema a los datos contenidos en el mismo[12]; y c) que los programas se entienden como una modalidad de datos informáticos.

Este último inciso aconseja una precisión interpretativa previa: y es que dada la similitud conceptual, a los efectos de la Decisión-marco y de los tipos penales derivados de ella, habrá que extender esa misma similitud en el art. 197.3, por lo que la distinción entre «*datos*» y «*programas*» es inútil, pues jurídicamente representan lo mismo. Ello justifica que en este trabajo a veces se prescinda de aludir a los dos objetos, datos y programas, y en muchas ocasiones solo se mencione a los primeros.

Ahora bien, lo que ya no distingue la Decisión-marco es el tipo de sistema informático en el que se actúa. Entiendo que éste no es un dato que haya de pasar desapercibido; *antes al contrario, que el tipo de sistema informático en el que se actúe, su orientación, la utilidad para al que se le destina, o si se quiere, el tipo de información que almacena, va a tener relevancia a la hora de identificar el alcance del tipo y su objeto de protección*.

No es lo mismo que el sistema al que se accede, sea un *sistema informático de uso absolutamente personal o particular*, restringido al ámbito de uso privado de una/s persona, como es el caso de un ordenador privado —que tenemos conectado a una red telemática, como puede ser Internet—; que un sistema informático, aún de titularidad privada, por ejemplo de una empresa, que esté *destinado al almacenamiento de datos o de programas sin carácter personal* alguno y específicamente destinados al uso del público (con sus más variadas orientaciones, por ejemplo, una web que contenga una base de datos de legislación o de jurisprudencia, o de música, o una web de ocio, viajes…); o, en tercer lugar, que un sistema informático de una empresa, pública o privada, entidad bancaria, institución oficial, etc., cuyo uso no es público, pero sí restringido al servicio de esa empresa o entidad. *Según nos hallemos ante sistemas informáticos «de uso privado», de «uso público» o de uso no privado pero «restringido», considero que es diferente la dimensión tuitiva del tipo respecto a la conducta de acceso a los datos, programas, es decir, información, que en ellos se almacena*.

A nivel de hipótesis, mi planteamiento es que no va a tener la misma trascendencia ni va a protegerse lo mismo cuando se entra subrepticiamente en un ordenador personal y se accede a sus informaciones, que cuando se entra del mismo modo en una base de datos jurisprudencial y se accede a una sentencia, por poner dos ejemplos diferentes de conductas, encajables en el tenor literal del tipo, pero con distinta repercusión. Ya de manera intuitiva, en el primer caso la intimidad parece hacer acto de presencia; no así en el segundo[13]. *En lo que sigue trataré de justificar esta diversidad.*

6. La intromisión en sistemas informáticos destinados al almacenamiento de datos o programas de uso personal

6.1. La influencia de la informática en la evolución del concepto de intimidad

Se entiende por intimidad el reducto privado en el que se desenvuelven algunas de las actividades más vincula-

12. A nuestros efectos de interpretación del 197.3, semejante equiparación resulta absolutamente absurda, pues turba la más elemental lógica, ya que si el precepto se refiere a los datos contenidos en un sistema, el tipo podría leerse como de acceso a los datos contenidos en otros datos.

13. No lo ve así GONZÁLEZ RUS, J.J.: «Los ilícitos en la red (I)…», *op. cit.*, pág. 247, para quien todo acceso no autorizado entraña una vulneración de la intimidad.

das a la naturaleza del ser humano. Desde sus creencias hasta determinadas relaciones personales, pasando por sus atributos (identidad, imagen, orientación sexual, salud, etc.). Desde ese ámbito vital, manifestado en numerosas vertientes y actividades (imágenes, conversaciones, relaciones, etc.) y objetos físicos (cartas, agendas, bases de datos, etc.), se le ha reconocido a la persona un derecho a excluir a los demás. Nadie puede entrar en ese reducto personal llamado intimidad[14]. El derecho a la intimidad, así concebido, se presenta como un derecho a la exclusión de terceros respecto a aspectos, datos o situaciones que el titular de los mismos ha decidido mantener bajo su ámbito de dominio. En palabras de MUÑOZ CONDE, «un derecho a la exclusión de los demás de determinados aspectos de la vida privada que pueden calificarse de secretos». En términos muy gráficos, esta dimensión se ha calificado como un derecho a ser dejado en paz, derecho a estar solo y a no inmiscuirse en lo secreto, es decir, en los hechos o datos de una persona que «solo son conocidos por ella o por un círculo reducido de personas»[15]. La sociabilidad del derecho es «cero»[16].

Pero en los últimos tiempos, como ya hemos reiterado en varias ocasiones, la implantación generalizada de la informática se ha convertido en un signo distintivo de la sociedad, de la que dimanan una serie de ventajas en tanto que procura una considerable celeridad y eficacia en la obtención de toda clase de necesidades humanas y sociales (desde las más básicas hasta las de nueva implantación, léase formas de ocio o facilidad en los viajes, por poner simples ejemplos) pero también, y es importante no olvidarlo, ciertos riesgos para el individuo tanto en lo relativo a su participación en la vida política, económica o social, como en su esfera privada. La sociedad de la información facilita el fluir de los datos, entre ellos de los datos personales y a la vez alumbra nuevos instrumentos o medios (dispositivos de captación y reproducción de sonido o de la imagen, redes interconectadas, etc.) capaces de acceder, controlar y transmitir los datos más allá de cualquier barrera tradicional que le pudiera oponer el individuo[17]. Riesgos que derivados de fenómenos tales como la acumulación ingente de información, el de la posibilidad de almacenamiento en bancos de datos, el de su circulación a través de un sistema comunicativo escasamente vigilado y regulado, el de la facilidad de acceso a la información por parte de personas no autorizadas y el del consiguiente peligro de interceptación y manipulación de la misma, han hecho saltar todas las alarmas en lo tocante a la falta de seguridad que para ciertos bienes jurídicos[18] y en especial, aunque no únicamente, para la intimidad personal y familiar, representa la llamada revolución de las comunicaciones sobre todo a partir de la espectacular extensión de las mismas vía Internet.

Resulta incontrovertible que las actuales concepciones y relaciones sociales han ido mermando paulatinamente el reducto de lo que antes era propio de la esfera privada. No es por ello de extrañar que las exigencias características de un modelo socio-político en el que se concede un margen cada vez mayor al intervencionismo estatal, unidas a las inherentes a un adecuado ejercicio de las libertades públicas en el marco del Estado social y democrático de Derecho hayan traído a primer plano la necesidad de conferir legitimidad a la progresiva captación por parte de los poderes públicos de datos sobre aspectos más o menos reservados o íntimos de los ciudadanos; todo ello con el objetivo de alcanzar mayor eficacia en el cumplimiento de sus funciones y en la prestación de sus servicios[19]. Esta misma tendencia es también observable en el sector privado, en el que la posesión de información, o la mera posibilidad de acceder a la misma, constituye un presupuesto necesario para la realización con éxito de numerosas actividades, por más que no se ignore que ello puede tener un alto precio para algunos derechos individuales[20].

Es por ello que el seno de la sociedad postindustrial y tecnológica ha sido necesaria una redefinición de lo privado[21] que ha determinado que junto a la mencionada dimensión *negativa o excluyente* de la intimidad (relativa a impedir la injerencia no consentida de terceros) que ha constituido el bastión tradicional de la intimidad, estruc-

14. RUIZ MARCO, F.: *Los delitos contra la intimidad. Especial referencia a los ataques cometidos a través de la informática*, Colex, Madrid, 2001, pág. 45.

15. MUÑOZ CONDE, F.: *Derecho penal. Parte especial*, Tirant lo Blanch, Valencia, 2004, pág. 256.

16. MORALES PRATS, F.: «Protección penal de la intimidad frente al uso ilícito de la informática en el Código Penal de 1995», *Delitos contra la libertad y la seguridad*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 1996, pág. 156.

17. RUIZ MARCO, F.: *Los delitos contra la intimidad…*, *op. cit.*, pág. 46.

18. FOUCAULT, M.: «Nuevo orden interior y control social», *El Viejo Topo*, nº 7, 1992, pp. 5 y ss.

19. MADRID CONESA, F.: *Derecho a la intimidad informática y Estado de Derecho*, Universidad de Valencia, Valencia, 1984, pp. 42 y ss.

20. HUERTA TOCILDO, S./ANDRÉS DOMÍNGUEZ, A.C.: «Intimidad e informática», *Revista de Derecho Penal*, nº 6, mayo 2002, pág. 13; ROMEO CASABONA, C. M.ª: «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», *Poder Judicial*, nº 31, 1993, pág. 164.

Advirtiendo de esta necesidad de recogida de datos por parte de los sectores público y privado, pero advirtiendo del riesgo que genera esta acumulación de información, GÓMEZ NAVAJAS, J.: *La protección de los datos personales*, Thomson-Civitas, Madrid, 2005, pp. 37 y ss.

21. MORALES PRATS, F.: «*Privacy* y reforma penal: la propuesta de anteproyecto de nuevo Código Penal», *Documentación Jurídica*, Vol. I, 1983, pp. 577-578.

turado en torno a la noción de *secreto*[22], se reconozca la existencia y gran pujanza de una *faceta positiva*, relativa a la concesión de unas posibilidades de actuación efectiva para el titular de la intimidad y que se concreta en las *facultades reconocidas a la persona para controlar el uso que de sus datos personales hagan los terceros*[23]. Un «derecho a perseguir los datos personales, a conocer el camino que seguirán para vigilar la utilización correcta y lícita de los mismos en relación con los fines para los que se obtuvieron»[24]. *Así, la intimidad adquiere la consideración de espacio de libertad individual, relativa a su decisión acerca del alcance que individualmente quiera asignarse a la participación en las relaciones sociales. La intimidad, vinculada directamente al ejercicio de la libertad personal, da lugar a la denominada «libertad informática», que ofrece una perspectiva social o externa al derecho a la intimidad*[25].

Es lo que se ha denominado en la cultura anglosajona la protección de la *privacy*, que supone el reconocimiento de una *vida social* de la *intimidad* que ya no está solo asilada tras los muros del secreto. De esta manera, la visión de la intimidad entendida como una libertad negativa es superada en pro de una conceptualización «como un bien jurídico positivo, proyectado socialmente, del que derivan facultades de control sobre los datos e informaciones del individuo en la sociedad tecnológica»[26]. La intimidad se identifica, así, con la capacidad de control de las informaciones que sobre uno mismo puedan tener otras personas o, más exactamente, con la posibilidad de autodeterminarse en el ámbito informativo, es decir, con la capacidad de determinar cómo, cuándo y en qué medida se comunica información a otros. Es, como ha señalado MORALES PRATS, una manifestación de la superación de la tradicional dicotomía entre derechos individuales (libertades-límite) y derechos social-participativos que, su vez, es producto de la crisis de la esquemática dicotomía entre lo público y lo privado. Se habla así de derechos y libertades de «tercera generación», que vendrían a constituir nuevas garantías del individuo frente a la contaminación o erosión de las libertades en la sociedad tecnológica[27].

Y ello para impedir que los terceros, sean los poderes públicos o los particulares, puedan acceder al reducto interno del ciudadano (llegar incluso a conocer su personalidad) a partir del cruce de datos que se albergan en las innumerables bases informatizadas. El acceso no sujeto a un riguroso control legal a la información sensible permite a quien lo consigue disponer de las características personales de cualquier ser humano, desde su domicilio, cuenta bancaria, estado financiero, estado civil, número de hijos, origen familiar, profesión, hábitos de compra, etc.); todo lo cual puede ser usado con los más variados fines, desde el marketing, hasta el control de la disidencia política (y como dice LANDROVE DÍAZ, «convertirnos en ciudadanos transparentes en una vieja aspiración del totalitarismo, más o menos encubierto»[28]), pasando por la mera curiosidad de «cotillear».

De modo que, a cada momento histórico, en función del nivel de desarrollo tecnológico, le corresponden nuevas formas de control que de manera progresiva han ido transformando la noción jurídica de intimidad[29]. Si en un principio la intimidad era considerada como un derecho a la soledad y al aislamiento, identificada con el secreto y el reconocimiento a su titular de facultades de exclusión, el desarrollo de las tecnologías informáticas de control y vigilancia ha llevado a extender el concepto de intimidad con la idea de control de esos datos que indefectiblemente salen del reducto del secreto y la incomunicación y se ubican en redes informáticas a merced de las necesidades del tráfico social y económico[30]. Si en un primer momento, la clave de la intimidad se resumía en la facultad ne-

22. MORALES PRATS, F.: «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», *Comentarios a la Parte Especial del Derecho Penal* (QUINTERO OLIVARES, Dir.), Thomson-Aranzadi, Pamplona, 2005, pág. 1029; HUERTA TOCILDO, S./ANDRÉS DOMÍNGUEZ, A.C.: «Intimidad e informática», *op. cit.*, pág. 15.

23. Detalladamente, sobre el contenido de estas facultades, HERRÁN ORTIZ, A.I.: *El derecho a la intimidad en la nueva Ley Orgánica de protección de datos personales,* Dykinson, Madrid, 2002, pp. 246 y ss.

24. HERRÁN ORTIZ, A.I.: *La violación de la intimidad en la protección de datos personales*, Dykinson, Madrid, 1999, pág. 91.

25. En general, sobre las facultades integrantes de esta libertad, *vid.* RUIZ MARCO, F.: *Los delitos contra la intimidad…*, *op. cit.*, pp. 47-48.

Detalladamente, sobre la implantación de este concepto, *vid.* MORALES PRATS, F.: *La tutela penal de la intimidad: privacy e informática*, *op. cit.*, pp. 45 y ss.; «Problemática jurídico penal de las libertades informáticas en España, tras diez años de vigencia de la Constitución de 1978», *Estudios Penales y Criminológicos*, T. XII, 1989, pp. 308 y ss.

26. MORALES PRATS, F.: «Protección penal de la intimidad frente al uso ilícito de la informática…», *op. cit.*, pág. 154; «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», *op. cit.*, pág. 1029.

27. MORALES PRATS, F.: «La protección penal de la intimidad frente al uso ilícito de la informática…», *op. cit.*, pp. 155-156.

28. LANDROVE DÍAZ, G.: «Delincuencia informática», *Temas Penales*, P.P.U., Barcelona, 1994, pág. 164.

29. Pone de manifiesto MARTÍN-CASALLO LÓPEZ, J.J.: «La protección de los datos personales: aspectos penales de la protección de datos», *Problemática jurídica en torno al fenómeno de Internet*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2002, pág. 18, que la intimidad y la informática existen de manera independiente, de manera que la intimidad no ha necesitado de la informática para su afirmación como bien jurídico pero que el mundo cibernético ha evidenciado un potencial lesivo para la intimidad.

30. LÓPEZ ORTEGA, J.J.: «Intimidad informática y Derecho penal», *op. cit.*, pág. 110.

gativa o de exclusión del titular de la intimidad, el desarrollo técnico de la sociedad ha operado una profunda transformación en su concepción y una redefinición de su contenido. La «práctica» social consistente en la acumulación de datos personales para múltiples fines (sanitarios, análisis de solvencia para solicitar un préstamo, laborales, publicitarios, etc.), multiplicándose también los soportes en los que se archivan esos datos y los medios a través de los cuales se pueden transmitir y difundir (redes telemáticas, por ejemplo) ha acabado por romper el viejo reducto de la intimidad, circunscrito antes casi a un concreto espacio físico, el domicilio, sacándola al exterior, situando los datos personales en cualquier lugar de la geografía. Lo íntimo y personal ya no está solo en casa y en unas pocas cartas o documentos, sino que la intimidad puede estar en el disco duro de cualquier ordenador y al alcance de cualquiera que tenga acceso al mismo[31]. Ante esta realidad, el Derecho ha incorporado al concepto de intimidad, nuevas facultades (positivas) consistentes en el reconocimiento a la persona del derecho de control de sus datos y sobre el uso que de ellos puedan hacer los demás[32].

A día de hoy podemos aventurar que el continuo y agigantado avance de la tecnología de la comunicación sigue propiciando posibilidades de intromisión en la intimidad que hasta hace bien poco eran desconocidas: hoy es posible acceder desde cualquier punto del planeta a un ordenador que esté conectado a la red de Internet, y captar los datos e informaciones que en él se contengan y, aún más, una vez así obtenidos es posible difundirlos en pocos segundos. La conexión del ordenador a la red pone el contenido de sus archivos casi a disposición de quien quiera acceder a ellos; y es más, el propio funcionamiento del sistema de red de Internet permite que cada vez que el usuario realiza una conexión, queden registradas estas «huellas», que van a permitir al servidor hacer una radiografía de las características personales del usuario[33]. De manera que ya no es solo que los datos incorporados previamente, y voluntariamente, a un sistema informático tengan que estar protegidos jurídicamente, reconociéndose a su titular una *habeas* para su control, y dotándose de relevancia penal la vulneración de este poder de control, es que ahora los datos se encuentran al eventual alcance de todo aquel que con algún conocimiento quiera acceder a ellos. El mero hecho de que toda conexión a Internet va dejando «huellas» que permiten «monitorizar las conductas de los usuarios», creando perfiles personales mediante el tratamiento de los datos obtenidos en la comunicación[34] alerta de nuevas formas de intromisión en la intimidad.

6.2. La protección de la intimidad en la Constitución Española

La posición de la Constitución Española en lo tocante a la intimidad refleja esta evolución hacia su «socialización» que en las líneas precedentes hemos descrito a grandes rasgos. El art. 18 de la Constitución Española establece que:

> «*1.— Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
>
> *2.— El domicilio es inviolable. Ninguna entrada o registro podrá hacerse sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.*
>
> *3.— Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*
>
> *4.— La ley limitará el uso de la informática para garantizar el derecho al honor a la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*»

El art. 18 de la Constitución acoge un concepto amplio de intimidad omnicomprensivo de las diferentes facetas que hemos descrito. Junto a la declaración general de positivización del derecho a la intimidad, se reconoce el derecho a la intimidad domiciliaria y a la libertad y confidencialidad de las comunicaciones privadas (tradicionalmente denominadas «secreto de comunicaciones»), para acabar con la constitucionalización de la faceta informática de la intimidad, aspecto este último en el que viene a cuajar el carácter institucional de garantía-presupuesto del ejercicio de otros derechos constitucionales (asociación, libertad ideológica, derecho a la no discriminación, derecho al trabajo, etc.) que la «privacy» adopta frente a los peligros de la informática. No se detiene en tutela de una capacidad de exclusión frente a terceros (aspecto éste que sí se contiene en los tres primeros párrafos del art. 18 de la Norma Fundamental) y que constituía el núcleo más tradicional de la intimidad, de entronque directo con el modelo más liberalista y asbtencionista de Estado de Derecho[35]. La norma constitu-

31. Es la finalización de la «edad del papel», en palabras de QUINTANO RIPOLLÉS, A.: *Tratado de la parte especial del Derecho penal, T.I., V.II,* Revista de Derecho Privado, Madrid, 1992, pág. 1008.

32. 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.

33. CASTILLO JIMÉNEZ, C.: «Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información», *Derecho y Conocimiento*, nº 1, 2001, pág. 37.

34. LÓPEZ ORTEGA, J.J.: «Intimidad informática y Derecho penal», *op. cit.*, pág. 109.

35. Y que se corresponden con los primeros pronunciamientos del Tribunal Constitucional sobre esta materia, cuando vinculaba la intimidad como un reducto restringido de la persona, vedado al acceso por parte de otros, pero sin reconocer efectos o relaciones para la libertad de actuar del sujeto. Se configuraba como un derecho de defensa; así, Sentencia del Tribunal Constitucional 73/1982, de 2 de diciembre.

cional avanza, y en su último inciso, párrafo 4, da entrada a la dimensión positiva de la intimidad, consistente en un derecho a la autodeterminación informativa, convertida en «libertad informática», que básicamente constituye un derecho del individuo de control (facultades jurídicas positivas) sobre los datos personales que circulan en la sociedad informatizada, derecho que se manifiesta y se ejercita a través de lo que se ha venido en denominar el «habeas data» (expresión representativa del conjunto de prerrogativas que permiten el ejercicio de esa facultad: derechos de información, de acceso, de rectificación y de cancelación de datos)[36].

Esta interpretación del art. 18.4 de la Constitución ha sido confirmada por el Tribunal Constitucional a través de diferentes Sentencias. Es sumamente clara la Sentencia 254/1993, de 20 de julio, cuando reconocía que la disposición consagrada en el párrafo 4 del art. 18 supone que se «incorpora una nueva garantía constitucional, como forma de de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso, estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a 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 Española llama «la informática». Una nueva garantía, una nueva manifestación del alcance constitucional de control de la intimidad que en algunas ocasiones ha dado la sensación de que tenía capacidad suficiente como para «volar sola», como garantía autónoma, desvinculada de la intimidad en sentido estricto tradicional, entendida como capacidad de exclusión.

Justamente así lo sugiere esta Sentencia (también otras con pronunciamientos semejantes, como por ejemplo, la Sentencia 11/1998, de 13 de enero[37]), cuando en ella se deja ver que la autonomía entre intimidad y libertad informática radica en los diferencias de función y objeto que caracterizan a cada uno de los dos derechos. Así la función del derecho a la intimidad estricto, sería la de proteger frente a cualquier invasión que pueda realizarse en aquél ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (se correspondería con una «reserva de datos»); en cambio, la libertad informática, entendida como derecho al control de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito. En cuanto al objeto de protección del derecho al control de datos, no se reduce solo a la protección de datos íntimos de a persona, sino a cualquier tipo de dato personal, íntimo o no, cuyo conocimiento o empleo por terceros puede afectar a sus derechos, sean o no fundamentales, porque su objeto no es propiamente la intimidad individual, que para ello está la atención que el art. 18.1 le otorga, sino los datos de carácter personal[38].

Sin embargo, en los propios pronunciamientos del Tribunal Constitucional, esta tajante separación y vida autónoma del «habeas data» informático respecto a la intimidad, no resulta tan evidente. En otras resoluciones, y cito la Sentencia 94/1998, de 4 de mayo, se afirma que «la garantía de la intimidad adopta hoy un entendimiento positivo que se aduce en un derecho de control sobre los datos relativos a la propia persona». Así que, si está reconociendo un derecho que adopta una faceta positiva, o una perspectiva de control, parece coherente que queda probado que el propio Tribunal dibuja un derecho en el que cabe otro «entendimiento», esta vez, de carácter negativo, consistente en una faculta de exclusión. *O lo que es lo mismo, que ambas dimensiones lo son de una misma realidad*[39] *que es el derecho a la intimidad, que es la ratio común a todas las puntualizaciones del art. 18,* pero que se manifiestan en aspectos diversos: básicamente reconducibles a lo siguiente: a) derecho a controlar los datos relativos a su persona que circulan porque previamente su titular los ha sacado al exterior; b) derecho a mantener excluido del conocimiento de terceras personas sus datos personales; c) derecho a mantener un circuito de comunicación, oral o escrita, cerrado a quienes no forman parte del mismo (relación privada interlocutor-receptor); y d) derecho a impedir la entrada en el domicilio a sujetos no autorizados, por ser el domicilio sede y marco de referencia de actividades privadas[40].

36. HUERTA TOCILDO, S./ ANDRÉS DOMÍNGUEZ, C.: «Intimidad e informática», *op. cit.*, pág. 17.

37. Que sostiene que el artículo 18.4 «consagra un derecho autónomo dirigido a controlar el flujo de informaciones que conciernen a cada persona, pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos, evitando que la informatización de los datos personales propicie comportamientos discriminatorios…».

Y en la mima línea, la Sentencia 292/2000, de 30 de noviembre.

38. ORTS BERENGUER, E./ROIG TORRES, M.: «Delitos contra la intimidad, utilización fraudulenta de tarjetas de crédito y falsedad en documento electrónico: análisis de casos», *Incorporación de las nuevas tecnologías en el comercio: aspectos legales*, Estudios de Derecho Judicial, Consejo General de Poder Judicial, Madrid, 2006, pp. 90-91.

39. RIQUERT, M.A.: *Protección penal de la intimidad en el espacio virtual,* Ediar, Buenos Aires, 2003, pp. 62-63.

40. PAREJO ALFONSO, L.: «El derecho fundamental a la intimidad y sus restricciones», *Perfiles del derecho constitucional la vida privada y familiar*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 1999, pp. 19-30; HUERTA TOCILDO, S./ ANDRÉS DOMÍNGUEZ, C.: «Intimidad e informática», *op. cit.*, pág. 19.

6.3. La tutela de la intimidad en el Código Penal

La protección del derecho a la intimidad al catálogo de los bienes jurídicos individuales necesitados de tutela penal ha visto un reflejo de la evolución reseñada en el Código Penal de 1995[41]. A diferencia del Código Penal anterior en el que las conductas típicas tuteladoras de la intimidad aparecían organizadas en torno a la idea de exclusión del conocimiento de terceros o secreto, y que además estaban dispersas a lo largo del articulado (como mucho reconducidas al epígrafe de los delitos contra la libertad y la seguridad), el texto vigente abre un Título dedicado *ex profeso* a la protección de la intimidad. A la intimidad como un todo, pero con variadas facetas, en concreto, la negativa o de exclusión, y la positiva, social, externa o de control.

Dejando aparte los posibles inconvenientes que una excesiva peculiarización del mismo, mediante las referencias a la propia imagen y la inviolabilidad del domicilio ha merecido a la doctrina, lo cierto es que en los tipos que en él se contienen se refleja sin duda esta doble dimensión de la intimidad: como secreto y como libertad informática. Muy sintéticamente, en el art. 197.1 se tutela básicamente la capacidad del titular de la intimidad de excluir del alcance de terceros el conocimiento de cuestiones personales que guarda en secreto, prohibiendo el apoderamiento de los soportes en los que éstos se guardan o la captación de las comunicaciones privadas, que también se incorporan a este concepto (secreto de las comunicaciones); por su parte, el 197.2, protege la dimensión más externa de la intimidad, puesto que parte del dato de que el sujeto ha colocado sus datos personales en bases de datos, archivos o ficheros y la tutela va referida a la capacidad de controlar el destino y el uso de esa información por parte del titular de los datos[42].

El resto de las conductas contenidas en el art. 197 se construyen sobre la base de estas dos formas de conculcar la intimidad, y básicamente constituyen tipos agravados en los que se castiga el mayor desvalor que a estas dos vías de intromisión ilegítima a la intimidad se le pudieran proferir: por ejemplo cuando los datos son además de interceptados, divulgados; cuando el autor de estas conductas es un sujeto «garante» de la indemnidad de los datos incorporados al registro, o cuando los datos personales sean integrantes de la parcela más íntima el sujeto.

Pues bien, la reforma del Código Penal, mediante la introducción de un nuevo art. 197.3 en el que *se castiga el acceso a datos o programas protegidos por medidas de seguridad contenidos en un sistema informático* parece colocarnos ante una nueva manifestación de vulneración de la intimidad que el legislador considera especialmente disvaliosa. Se trata de la posibilidad de acceder desde cualquier punto del planeta a un ordenador que esté conectado a una red telemática y captar los datos e informaciones que en él se contengan (y, aún más, una vez así obtenidos es posible difundirlos en pocos segundos). La conexión del ordenador a la red pone el contenido de sus archivos casi a disposición de quien quiera acceder a ellos (y como digo, el propio funcionamiento del sistema de red de Internet permite que cada vez que el usuario realiza una conexión, queden registradas «huellas» que permiten «monitorizar las conductas de los usuarios», creando perfiles personales mediante el tratamiento de los datos obtenidos en la comunicación[43], lo cual alerta de un nuevo frente de vulneración de la intimidad[44]).

De manera que ya no es solo que los datos incorporados previamente, y voluntariamente, a un sistema informático tengan que estar protegidos penalmente, reconociéndose a su titular un *habeas* para su control, es que los datos se encuentran al eventual alcance de todo aquel que con algún conocimiento quiera acceder a ellos.

El art. 197.3 del Proyecto se hace eco de esta nueva perspectiva de vulneración de la intimidad, que adquiere una dimensión cada vez más espiritualizada y más intangible, en la misma medida que lo es el espacio en el que se desarrolla. El ciberespacio. La configuración de este medio como el nuevo espacio de desarrollo personal y de ejercicio de vida cotidiana que, además, cada vez es más amplio, entiendo que conforman una nueva perspectiva de la intimidad, que ya no solo se aloja en espacios físicos, la morada, o en puntos aprehensibles, los datos aportados voluntariamente a sistemas informáticos, sino que también tiene su particular reducto en los sistemas informáticos de uso privado en los que «guardamos y hacemos buena parte de nuestra vida», convirtiéndose, de este modo, esos sistemas informáticos, en una suerte de «morada informática». Veamos desarrolladamente esta opción.

41. HUERTA TOCILDO, S./ ANDRÉS DOMÍNGUEZ, C.: «Intimidad e informática», *op. cit.*, pág. 54: «La opción a favor de proteger la intimidad en función de las modalidades de ataque a la misma, y no como bien jurídico merecedor de una protección penal autónoma, ha dado lugar históricamente a una continua labor de complementación legislativa al compás de las nuevas modalidades de ataque de las que podía ser objeto».

42. CARBONELL MATEU, J.C./GONZÁLEZ CUSSAC, J.L.: «Comentarios a los artículos 197 a 204 del Código Penal», *Comentarios al Código Penal de 1995*, Vol. I, Tirant lo Blanch, Valencia, 1999, pág. 999.

43. LÓPEZ ORTEGA, J.J.: «Intimidad informática y Derecho penal», *op. cit.*, pág. 109.

44. Para una explicación detallada y técnica de cómo adentrarse en la intimidad a través de los datos volcados en un ordenador por parte de su usuario, *vid.* PAYERAS CAPELLA Mª.M./FERRER GOMILA, J.L.: «Explicación técnica de las amenazas de las TIC a la intimidad», en *Derecho a la intimidad y nuevas tecnologías,* Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2004, pp. 77 y ss.

6.4. El alcance de la protección de la intimidad en el art. 197.3 del Proyecto de Código Penal

Entender que el solo acceso a unos datos contenidos en un SISTEMA INFORMÁTICO PERSONAL representa una vulneración de la intimidad con relevancia penal parece resultar por principio, contrario con las exigencias de lesividad y de intervención mínima. Porque hay que reparar en un aspecto: y es que el dato al que se refiere el tipo penal *puede ser cualquiera, no necesariamente un dato personal o un dato que denote un aspecto íntimo de la persona*; en el tipo se da cabida, bajo la noción de «*dato*» desde un trabajo académico enviado por un alumno, a un listado de celebraciones familiares, desde un archivo de música, a un fichero con la compra semanal. Es decir, en el tipo caben datos claramente «despersonalizados» o inocuos desde el plano estricto de la intimidad. Es más, la impersonalización llega al extremo de que el tipo selecciona como objeto de protección a los «*programas*» informáticos, en los que de manera obvia cabe concluir que en nada definen a la intimidad personal.

Sin embargo, también bajo los auspicios del principio de fragmentariedad del Derecho penal, en tanto que mecanismo seleccionador de las formas de ataque a los bienes jurídicos que se van considerando socialmente más graves, cabe admitir la existencia de un flanco de vulnerabilidad para la intimidad que se había venido denunciando: el que propicia la incorporación de gran parte de nuestra información, sea o no personal, en un sistema informático de uso personal y privado. El ordenador, hoy funciona para miles (millones) de usuarios, como una especie de agenda o de diario en el que se van «colgando» todos y cada uno de los pasos diarios, de cualquier índole, desde nuestras comunicaciones personales, hasta nuestro trabajo, pasando por nuestras formas de ocio, etc. El ordenador comporta hoy día un nuevo espacio en el que desarrollar nuestra vida personal, *constituyendo una especie de «morada informática» en la medida en que en él se realiza y a él va a para una buena parte de nuestra actividad cotidiana, de manera que los datos e informaciones contenidas, programas manejados, etc., pueden permitir a quien acceda a ellos, adentrarse en un espacio de desarrollo personal, de ejercicio de libertad*[45].

Esta exposición de nuestra «vida informática», que hoy seguramente ocupa un volumen importantísimo de nuestros movimientos, a eventuales inmisiones ajenas ha derivado en la selección por parte del legislador penal de una forma de vulneración de este reducto de actividad privada, la que consiste en un contacto con nuestros datos o programas instalados en un sistema informático. A día de hoy, por medio del acceso al contenido de un ordenador o un sistema informático es posible llegar a obtener una radiografía de su usuario: sus preferencias, sus gustos, sus actividades, etc. Datos aparentemente inconexos o irrelevantes, y por ello inocuos, pueden transformarse en informaciones fuertemente reveladoras de la personalidad de un individuo[46]. A este respecto, me resultan particularmente acertadas las palabras de MORALES PRATS cuando afirma que el acceso a los datos de un ordenador es una forma de «control certero, sistemático, penetrante e invisible sobre la persona»[47], pues subrayan de manera precisa el carácter, en mi opinión, inexcusablemente lesivo de la intimidad de las conductas de intromisión en un ordenador y contacto con *todo* aquello que en él se archiva y resguarda de intromisiones no consentidas. Mediante ese acceso se pueden descubrir facetas de la personalidad del individuo que, aisladamente consideradas pueden carecer de significado intrínseco, pero que si fueran coherentemente enlazadas entre sí, arrojarían como precipitado un retrato de al personalidad del individuo que éste tiene derecho a mantener reservado[48].

Del párrafo 3 del art. 197 del Proyecto de Código Penal, se ha dicho, lo dice el propio legislador, que es una punición expresa del *hacking*. Pues bien, realmente resulta ser una figura de castigo de acceso subrepticio, sí, pero no tan «blanco» o tan «puro», en el sentido de no afectar a otro bien jurídico, como la intimidad, pues hay ingredientes suficientes como para descubrir en él una forma específica de intromisión en una parte de la intimidad: la que «colgamos» de nuestro ordenador personal. Esos ingredientes son:

— primero, el ya mencionado ámbito «privado» en el que se desarrollan los hechos (el sistema informático de carácter «particular»). Cuando la comisión de esta conducta se realiza en un sistema informático de carácter «personal» o «propio» se justifica la consideración de que hay una nueva dimensión de la intimidad personal-informática que está siendo atacada por este tipo de intrusismo.

— segundo, que la conducta típica consiste en un «acceso a datos o programas» protegidos mediante «*medidas de seguridad*», es decir, *no es solo la penetración en un*

45. Sobre esta reclamación de la consideración del ordenador como una «morada informática o domicilio informático», MORALES GARCÍA, O.: «Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre el Cibercrimen», *Delincuencia Informática. Problemas de Responsabilidad*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2002, *op. cit.*, pág. 28.

46. HUERTA TOCILDO, S./ANDRÉS DOMÍNGUEZ, C.: «Intimidad e informática», *op. cit.*, pág. 14.

47. MORALES PRATS, F.: «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», *op. cit.*, pág. 1029.

48. SÁNCHEZ CARAZO, C.: *La intimidad y el secreto médico*, Díaz de Santos, Madrid, 2000, pág. 16, haciéndose eco de las palabras de la Exposición de Motivos de la anterior Ley Orgánica 5/1992, de 29 de octubre, de tratamiento automatizado de datos de carácter personal.

sistema informático, sino la captación de la información personal en él incorporada y que el titular de la misma no necesariamente quiere poner a disposición de terceros.

— tercero, la propia ubicación sistemática del precepto, que aunque veremos resulta desafortunada cuando se refiere al acceso a sistemas informáticos «no personales»[49], sí encuentra su sede sistemática natural en este caso de entrada en sistemas particulares. Si el precepto se sitúa en el ámbito de los delitos contra la intimidad personal, bajo una rúbrica relativa a la protección del secreto (y lo hace claramente, dada su incrustación en el propio art. 197.3, hasta el punto de llegar a desplazar la numeración) parece evidente que la conducta descrita en el mismo, debería tener alguna la repercusión en la intimidad. Y es más, en la propia exposición de motivos de la reforma el legislador justifica la creación del nuevo tipo en la «*importancia fundamental de este bien jurídico*» y en la necesidad de proscribir los riesgos de vulnerar la «privacidad o reserva de datos contenidos en un sistema informático». Es decir, en la tutela de la intimidad.

Por eso, como más detalladamente justificaremos a continuación, el previsto art. 197.3 del Código Penal encuentra su justificación en la protección de la protección de la intimidad en su faceta más férrea, la del «*secreto*» o facultad de exclusión de conocimiento respecto a los demás. Se trata de una noción de intimidad a la que se había considerado obsoleta[50], pero que adquiere nueva vida debido a la existencia de nuevas formas especialmente graves de atacarla; a la existencia de una nueva posibilidad de inmiscuirse en un espacio propio y separado del contacto externo. Veamos detalladamente estas consideraciones.

6.4.1. La redefinición del concepto de «secreto»

A) Concepto de secreto

La tutela penal del secreto, es decir, de la dimensión excluyente de la intimidad, ha tenido básicamente su sede tradicional en los últimos tiempos en el art. 197 .1 del Código Penal. La fijación de su contenido ha sido objeto de pronunciamiento por parte de la doctrina y la jurisprudencia y, con carácter general, el resultado ha sido el de dotar a este concepto un contenido más amplio que el que en principio cabría inferir del contacto con el bien jurídico intimidad, al que sirve de base[51].

Así, ha manifestado PRATS CANUT que se «trata de una cualidad que se predica de un dato, un hecho, una información, que tiene un soporte físico, cualidad que por otra parte es mutable en función de las decisiones del titular, de tal suerte que la condición de secreto no es predicable *a priori*»[52]. En este mismo sentido, advierten CARBONELL MATEU/GONZÁLEZ CUSSAC que la intimidad se plasma en todo conocimiento reservado, que el sujeto activo no conozca, o no esté seguro de conocer, «y que el sujeto pasivo no quiera que se conozca»[53]. Por su parte MUÑOZ CONDE, sostiene que la consumación del delito no exige que los datos a los que se accede tengan el carácter de dato personal desconocido, señalando el ilustrativo ejemplo de que «encontrarse una carta cerrada y leerla constituye delito, aún cuando lo que en ella se diga no pueda considerarse secreto»[54].

En esta misma línea, la jurisprudencia del Tribunal Constitucional, en Sentencia 123/2002, de 20 de mayo (en línea con lo ya manifestado en la Sentencia 114/1984, siguiendo la jurisprudencia del Tribunal Europeo de Derechos Humanos de 2 de agosto de 1984, *caso Malone*) atiende a una visión del secreto en la que lo decisivo es la tutela del hecho comunicativo «sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado».

De manera que se puede llegar a sostener que la noción de «secreto» *viene determinada por aquello que el sujeto excluye de los demás*. Que no hace partícipe de su contenido a terceras personas, que o él mismo decide a quién se lo traslada. Se trata de una noción de carácter subjetivo; un concepto que marca una barrera de entrada en lo privado, barrera que «establece el legítimo titular del soporte en que aquél se asienta»[55]. *No es directamente relevante el contenido de la información, en el sentido de que tenga que aludir necesariamente a cuestiones privadas, sino que lo que le confiere el carácter de secreto a un dato o información es su ubicación aislada o precintada de accesos no autorizados por parte de terceras personas*[56]. Por ello, la noción de secreto, aparece instrumentalizada al servicio de múltiples intereses que pueden verse repercutidos en caso de que se sea traspasada esa barrera de ais-

49. *Vid. infra* epígrafe 7, ***7***.2.- *La configuración dogmática del tipo*.

50. MORALES PRATS, F.: «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», *op. cit.*, pág. 1029.

51. Recoge algunas soluciones jurisprudenciales alternativas, FERNÁNDEZ TERUELO, J.G.: *Cibercrimen: los delitos cometidos a través de Internet*, Constitutio Criminalis Carolina, Oviedo, 2007, pp. 127-128.

52. PRATS CANUT, J.M.: «Descubrimiento y revelación de secretos en el nuevo Código Penal», *Delitos contra la libertad y la seguridad*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 1996, pág. 254.

53. CARBONELL MATEU, J.C./GONZÁLEZ CUSAC, J.L.: «Comentarios a los artículos 197 a 204 del Código Penal», *op. cit.*, pág. 1002.

54. MUÑOZ CONDE, F.: *Derecho penal. Parte especial*, *op. cit.*, pág. 260.

55. POLAINO NAVARRETE, M.: *Curso de Derecho penal español*, Vol. I, Marcial Pons, Madrid, 1996, pág. 399.

56. RUEDA MARTÍN, Mª.A.: *Protección penal de la intimidad personal e informática*, Atelier, Barcelona, 2004, pp. 71-71.

lamiento que establece su titular y los datos o información fueran alcanzados por quienes no tienen autorización para conocerlos (intimidad, seguridad nacional, capacidad competitiva de la empresa, el patrimonio, el patrimonio, etc.)[57].

En suma, ambos ingredientes: instrumentalidad del concepto y exclusión de la información decidida por su titular componen las señas de identidad de la noción de secreto. Sobre esta base, corresponde analizar su presencia en el párrafo 3 del 197 y su posible conexión a la intimidad.

B) La relevancia para la intimidad de la conducta descrita en el párrafo 3 del art. 197 del Proyecto de Código Penal

En la posible redacción del art. 197.3, el objeto sobre el que recae la acción de intromisión no consentida, es decir, el objeto material, son los datos o programas informáticos contenidos en un sistema informático, a los que se accede «*vulnerando las medidas de seguridad establecidas»* para impedir dicho acceso**.** El precepto se detiene en la mera indicación de que son «datos o programas», sin calificativos que apunten a la repercusión sobre la intimidad personal. *Es decir, por principio, cualquier dato tiene cabida en este tipo de conducta, sean datos de carácter íntimo, familiar, profesional, laboral, económico, o incluso datos absolutamente intranscendentes desde el punto de vista de la esfera nuclear de la intimidad*.

En todo caso, la redacción de lo que ocuparía un nuevo párrafo 6 no excluye la posibilidad de que se trate de datos privados o personales, porque directamente los utiliza para construir un especial desvalor de resultado sobre la intimidad cuando establece que «*cuando los hechos descritos en los apartados anteriores*» afecten a datos «del núcleo duro» y específicamente íntimo de la intimidad, como son los datos ideológicos, religiosos, de salud, origen racial o vida sexual, la pena se eleva.

Pues bien, haciendo uso de ese carácter instrumental que se le confiere a la idea de secreto, considero que *si el tipo abarca a toda suerte de datos, incluidos aquellos que no tengan nada que ver ni con lo personal ni con lo privado, lo que hace que la conducta de acceso a los mismos en un sistema informático personal conecte con la intimidad viene definido por la especial situación en la que se encuentran esos datos o programas: protegidos por medidas de seguridad establecidas para impedir el acceso a ellos*. Las medidas de seguridad determinan un espacio de exclusión frente a terceros que *convierte al dato accedido en un dato «secreto» y, consiguientemente, hacen del acceso al mismo una forma de penetración en la intimidad.*

De esta manera, el nuevo 197.3 significa una liberación de los elementos subjetivos como medios de selección de las formas de ataque a la intimidad con relevancia penal y gravedad, tal y como la doctrina ha venido reclamado, para facilitar así el arrinconamiento de un modelo de incriminación que prima la actitud interna del sujeto**,** en favor de una objetivización en la articulación de la tutela de la intimidad, construida en torno al objeto sobre el que ésta se proyecta y en la forma comisiva, forma tuitiva más acorde con los principios de ofensividad y lesividad, nucleares en un Derecho penal anudado a la determinación de a responsabilidad por el hecho[58]**.** De la misma manera que romper una cerradura de una casa ajena para acceder a ella, da lugar a la comisión de un delito de allanamiento de morada, por tratarse de una externalización de la inmisión en un reducto de intimidad, la morada ajena[59], así también romper las barreras de protección de los datos y programas contenidos en un sistema informático personal, identifica la directa voluntad de adentrarse en

57. BAJO FERNÁNDEZ, M./BACIGALUPO, S.: *Derecho penal económico*, Centro de Estudios Ramón Areces, Madrid, 2001; igualmente, MORALES PRATS, F.: «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», *op. cit.*, pág. 1034.

58. MORÓN LERMA, E.: «Intención del agresor y ataque a la intimidad», en El nuevo Derecho penal español. Estudios penales en memoria del Prof. J. M. VALLE MUÑIZ (QUINTERO OLIVARES, Dir.; MORALES PRATS, Coord.), Aranzadi, Pamplona, 2001, pp. 1617, 1619-1620.

59. JORGE BARREIRO, A.: *El allanamiento de morada*, Tecnos, Madrid, 1987, pág. 67.

Sobre este particular existe una dilatada opción jurisprudencial que considera que el empleo de formas de fuerza en las cosas, como puede ser ésta, comporta un caso de empleo de la violencia que constituye la forma agravada de allanamiento de morada; sin embargo, este parecer es rechazado de forma mayoritaria por la doctrina, que circunscribe la violencia a la realizada sobre las personas, de cuerdo con el criterio de rechazo de la interpretación extensiva, contraria al reo; coherentemente esta tesis doctrinal entiende que la ruptura de las cerraduras no da lugar a la forma agravada, sino que es expresiva de la conducta incisiva de la intimidad, realizada sin autorización del morador, tal cual exige el tipo básico del artículo 202; sobre esta cuestión, *vid*. JORGE BARREIRO, A.: *El allanamiento de morada*, *op. cit.*, pp. 79 y ss; RUIZ MIGUEL, C. /SANZ MORÁN, A.: «Algunas observaciones sobre el delito de allanamiento de morada», *Estudios de Derecho penal y criminología. Libro homenaje al Prof. RODRÍGUEZ DEVESA,* UNED, Madrid, 1989; MORALES PRATS, F.: «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», *op. cit.*, pág. 1078.

Para DE ALFONSO LASO, D.: «El *hackering* blanco. Una conducta ¿punible o no punible?», en *Internet y Derecho Penal*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2001, pág. 518, la conducta se semeja a la violencia espiritualizada el robo.

un espacio particular excluido a los demás[60]. O lo que es lo mismo, supone adentrarse en el ámbito de un dato «secreto», porque el titular del sistema lo ha asilado de su alcance a los demás. Así lo subraya LÓPEZ ORTEGA, cuando destaca que la opción mantenida por el legislador español «restringe la incriminación de las conductas de intrusismo a aquellos casos en que el titular ha hecho patente su voluntad de impedir el acceso a terceros mediante la interposición de medidas de seguridad que limiten el acceso al sistema (…) de tal marea que lo que se protege es el interés en la conservación del secreto frente a quien no está autorizado»[61].

En el futuro o hipotético delito de acceso a datos informáticos protegidos por medidas de seguridad, lo que le confiere el carácter gravemente vulnerador de la intimidad es el hecho de que el dato está cobijado de cualquier contacto externo no aceptado por el titular del mismo por la existencia de «medidas de seguridad *establecidas* para impedir ese acceso al dato», lo cual permite al legislador prescindir de cualquier referencia a la voluntad (ánimo de descubrir un secreto o vulnerar la intimidad) para sostener la trascendencia de estas conductas respecto a la intimidad. El tipo se vale de un elemento externo a través del que se revela la decisión de hacer secreta la información[62]. Lo que confiere al delito el carácter de comportamiento perturbador de la intimidad y necesitado de tutela penal es el hecho de que se trata de datos que cuentan con una barrera que les protege de inmisiones externas.

De modo similar al art. 197.2, en que la vulneración de la intimidad no viene directamente determinada por el carácter íntimo del dato (pues también da cabida a otros datos personales pero que en sí mismos pueden ser externos[63]), sino por la vulneración del poder de control y exclusión frente a terceros del titular de dicha información personal, también en el eventual párrafo 3, la intromisión en la intimidad *no se determina por el contenido de lo que se incluye en la información a la que se llega, sino por la forma en que esa información se presenta, aislada de los demás, lo cual revela una decisión de su titular de mantener ese dato bajo su espera de dominio particular.*

Por todo ello, el previsto párrafo 3 del art. 197 constituye un nuevo eslabón hacia la espiritualización de la concepción jurídico-penal de intimidad que han venido propiciando las nuevas tecnologías. Ya señalábamos que a cada etapa de desarrollo tecnológico le corresponden nuevas formas de control que de manera progresiva han ido transformando la noción jurídica de intimidad[64]. Primero fue la concesión de capacidades de control sobre los datos personales exteriorizados en ficheros o registros informatizados, a la vista de la facilidad de manipulación de éstos, la que determinó una extensión del bien jurídico-penal intimidad a cualquier dato concerniente a persona física identificada o identificable[65], dato que, aunque inicialmente inocuo, el mero hecho informático de su introducción en una red lo convertía en dato sensible o reservado[66] (pues esa incorporación del dato al sistema informático, en virtud de combinaciones alfanuméricas, pueden ser objeto de manipulación y permitir información por inferencia[67]); *ahora, va a ser la realidad de la interconexión informática la que justifica la consideración de que hay un nuevo modo peligroso de colarse en una dimensión privada, que no viene determinada por el contenido de los datos que se conocen, sino por el dónde y cómo se encuentran y conocen esos datos*. Cabe descubrir, pues, una *orientación cada vez más espiritualizada de la noción jurídico-penal de intimidad, que alcanza a todo aquello que un sujeto custodie en su sistema informático de carácter personal y excluya de intromisiones mediante el establecimiento de barreras*.

60. La vinculación del acceso no consentido con los delitos contra la inviolabilidad del domicilio es la opción directamente adoptada por el legislador italiano, en su artículo 615 *ter*, ubicado en el contexto de los «los delitos contra la libertad individual» del Capítulo III del Título XII (Delitos contra la persona), dentro de la sección 4ª, sobre «Los delitos contra la inviolabilidad del domicilio»; *vid. supra* epígrafe 3, 3.2.2.- Breve referencia a la regulación penal de algunos países de nuestro entorno, A) Italia; en *Vías para la tipificación del acceso ilegal a los sistemas informáticos (I)*, publicado en el número anterior; PICA, G.: *Diritto penale delle tecnologie infomatique*, Utet, Turín, 1999, pp. 61 y ss.

61. LÓPEZ ORTEGA, J.J.: «Intimidad informática y Derecho penal…», *op. cit.*, pág. 121.

62. Sobre esta particular de incriminación de una forma de intrusismo informático vulnerador de la intimidad, ya habría reclamado MORALES PRATS la necesidad de abordar «el correspondiente juicio de inferencias fundamentador de la intención de vulnerar la intimidad-libertad informática ajena, y en la base de ese juicio de inferencias está la valoración de datos objetivos», MORALES PRATS, F.: «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», *op. cit.*, pág. 1046.

63. MARCHENA GÓMEZ, M.: «Intimidad e informática: la protección jurisdiccional del *habeas data*», *Boletín de información del Ministerio de Justicia* e *Interior*, nº 1768, 1996, pág. 752, que destaca la visión dinámica y no estática de la intimidad a la que atiende el 197.2.

64. LÓPEZ ORTEGA, J.J.: «Intimidad informática y Derecho penal…», *op. cit.*, pág. 110.

65. MORALES PRATS, F.: «La protección penal de la intimidad frente al uso ilícito de la informática…», *op. cit.*, pág. 171.

66. MORALES PRATS, F.: «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», *op. cit.*, pág. 1044, apunta a lo superfluo del término «reservado», pues el mero hecho de introducir datos personales en un fichero informatizado los convierte en datos sensibles y objeto de protección en el artículo 197.2.

67. CASTILLO JIMÉNEZ, C.: «Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información», *op. cit.*, pág. 37.

La fijación de tales barreras o mecanismos de seguridad establecidas para impedir su acceso configuran un signo externo de exclusividad de la información almacenada por el sujeto particular y, por tanto, constituyen la clave demostrativa de que en una buena parte, la que viene determinada por el espacio de comisión delictiva (es decir, el sistema informático de uso personal), el previsible tipo penal que incorporará el art. 197.3 se orienta a la protección de un espacio específico de intimidad. *Las medidas de seguridad, de este modo, pasan a configurarse como el elemento externo que identifica la presencia de un espacio de un «secreto», en el sentido de exclusión negativa tradicionalmente mantenido* y una forma particularmente grave de vulneración de la intimidad, la que consiste en el acceso al reducto informático personal.

La solución española se sitúa en línea con la opción alemana que a la que apuntó en la primera parte de este trabajo[68]. El legislador alemán ha tenido reparos en castigar la mera penetración como tal en un sistema informático ajeno, limitándose solo a recoger en el parágrafo 202 a) el espionaje de datos, que reza: «*el que ilegítimamente se procurare a sí mismo o a otro datos que no están destinados a él y que se hallan especialmente protegidos contra el acceso no autorizado, será castigado con la pena de…*». Se castiga, pues, el acceso a los datos que están «especialmente asegurados» (por ejemplo, mediante los dispositivos lógicos de seguridad y notas de cierre, palabras clave y precintos, contraseñas, números de identificación personal, los dispositivos e reconocimiento de la voz, la criptografía de datos, etc.) Lo que se protege es un interés formal en la conservación del secreto de la persona autorizada a disponer sobre el almacenado y transmisión de datos no directamente perceptibles, que pone de manifiesto tal interés mediante el aseguramiento[69].

En definitiva, ante el panorama técnico descrito parece claro que el arsenal de instrumentos lesivos de la intimidad ha corrido parejo al desarrollo tecnológico, posibilitando nuevas formas de control del ciudadano más penetrantes y eficaces. El bien jurídico intimidad se ha vuelto más vulnerable frente al cada vez más amplio elenco de medios y formas de agresión; todo lo cual propicia esta nueva reacción del Derecho penal a través de la selección fragmentaria de una conducta que se concibe como específicamente lesiva de aquélla.

6.4.2. La vulneración de las medidas de seguridad: valor dogmático

Una vez afirmada la consideración de que la intimidad encuentra una nueva forma de lesión a través de las intromisiones subrepticias en los datos informáticos protegidos contenidos en un sistema informático de tipo personal, corresponde ahora ahondar en el papel que desempeña el requisito típico de la vulneración de las medidas de seguridad. El presupuesto del que hemos partido es la estimación de que esas medidas de protección son el instrumento que denota la presencia de un espacio particularmente relevante de intimidad, en el sentido de que indican la exclusión a terceros no autorizados de la información contenida en el sistema.

A) Aclaración interpretativa

Primeramente hay que proceder a una aclaración interpretativa, que incide en la especificación de lo que se vislumbra como objeto material del delito: las medidas de seguridad son presupuesto objetivo, sin cuya existencia la conducta deviene impune por atípica. El tenor literal no deja lugar a dudas, cuando indica que se trata de «*medidas de seguridad establecidas para impedirlo*» (se entiende que para impedir el acceso al dato o programa). Así que el tipo se reduce como objeto material, a los datos protegidos. Lo que resulta cuestionable es si la protección se tiene que realizar directamente de los datos (aunque lógicamente no tiene por qué ser cada dato individualmente protegido) o si basta una protección del sistema. Creo razonable esta segunda opción y encajable en el tenor literal del precepto pues el término «*impedirlo*» bien cabe referirlo respecto al acceso a los datos o al acceso al propio programa, lo cual no obsta para aceptar que además de la protección del sistema se hayan establecido medidas adicionales de protección de la información. Lo cierto es que en cualquiera de los dos supuestos, es precisa una labor previa de protección, quedando excluidas del alcance típico aquellas conductas de entrada sobre sistemas, datos o programas que no hayan sido objeto de protección expresa y directa.

Esta expresa exigencia de «*establecimiento de medidas*», que implica una previa actividad positiva de protección requiere, por tanto, plegar el contenido de estas medidas a la *instalación de elementos lógicos* (*passwords*, claves…) que sellen el dato, programa o sistema de contactos externos e impide considerar que sea el propio ordenador en sí mismo una medida de seguridad. Además, ello cuenta con un argumento de interpretación sistemática, que es el deslinde de este tipo respecto a otras conductas en las que la forma comisiva también consiste en la vulneración o destrucción, en el sentido de que si el propio ordenador fuera entendido como barrera y hubiera que vulnerarlo para cometer el delito, estaríamos ante una conducta de daños del art. 264.

B) La relevante lesividad para la intimidad

Como antes señalaba, el quebranto de esas barreras de protección constituye la manifestación concreta y tangible

68. *Vid. supra* epígrafe 3, 3.2.2.- Breve referencia a la regulación penal de algunos países de nuestro entorno, C) Alemania; en *Vías para la tipificación del acceso ilegal a los sistemas informáticos (I)*, publicado en el número anterior.

69. MIR PUIG, C.: «Sobre algunas cuestiones relevantes del Derecho penal en Internet», *op. cit.*, pág. 300.

de que los datos están excluidos del contacto con terceros, que no se ponen disposición de ellos y en ese sentido forman parte de los «secretos» del titular de ese sistema informático particular.

Ante esto, la pregunta que surge seguidamente es: ¿qué pasa con los datos, programas o sistemas que no están protegidos por específicas medidas de seguridad? Según el tenor del tipo, que requiere que se hayan establecido específicamente dichas medidas, quedaría fuera del ámbito típico el acceso a esos datos, en lo que entiendo traduce un correcto un ejercicio de selección de las conductas más graves para la intimidad y por ello consideradas merecedoras de atención por el Derecho penal. *Se podría haber optado por no haber exigido este quebranto de los mecanismos de protección, y que bastara el acceso no autorizado a los mismos. Y también habría una cierta repercusión en la intimidad, pues, subrayo, se trata de la entrada en un reducto de vida personal. Sin embargo, de ser así, entiendo que se generaría un doble problema*:

— Un primer inconveniente, en sede de principios, de legítima intervención penal, sería el relativo a la escasa entidad de las conductas incorporadas al tipo respecto a la incidencia en la intimidad, como ya hemos advertido previamente[70]. Recuerdo que entender que es perturbador de la intimidad el solo hecho de tomar contacto con datos insertos en un ordenador, datos que no necesariamente han de ser personales, representa un exceso de intervención punitiva, de similar calado al que representaría leer cartas privadas que quedan encima de la mesa y que están concientemente abiertas o mirar la pantalla del ordenador del compañero.

Vinculado a lo anterior, la estructura típica adolecería de un fuerte déficit de lesividad. En efecto, si el tipo se hubiera estructurado en base exclusivamente al acceso a los datos o programas contenidos en el ordenador personal, habida cuenta del posible carácter «impersonal» de los mismos, que en sí nada dicen de cuestiones personales, y que todo lo más posibilita, eventualmente, la obtención de un «retrato» de la persona, daría lugar a la conformación de un delito de peligro abstracto respecto a la intimidad, configurado en base a una presunción de descubrimiento de aspectos personales de la persona a través de la inferencia y o traducción a lo personal de esos datos. Realmente la lesividad queda lejos.

— Igualmente, no es desdeñable un problema probatorio que restaría eficacia al tipo, pues habría una enorme dificultad en la identificación de lo que el titular considera excluido de accesos a terceros, porque, ¿cómo identificar la falta de autorización, la voluntad excluyente? A diferencia del mundo físico en el que la voluntad contraria a la intromisión en una morada se puede obtener a través de datos implícitos-externos, pero claramente indicativos de una real voluntad del morador contraria a la entrada (comunicaciones verbales, cierre de la puerta con medidas físicas de protección, etc.), en el cibermundo esa voluntad excluyente, a salvo de expresa y específica autorización, es difícil de comprobar.

De modo que, si el tipo se detuviera en el solo acceso al dato o programa contenido en un sistema informático particular y ajeno, ya que no se precisa ninguna característica externa que denote «intimidad» en el dato, ni ninguna voluntad especial de conocer un dato íntimo por parte del sujeto activo, *estimo que un tipo así concebido, en sede de ataque a la intimidad, resultaría escasamente ofensivo de las exigencias del principio de intervención mínima*[71]. La selección de una forma relevante de ataque a la intimidad desarrollada en el espacio cibernético se vale de este componente identificador del carácter excluyente del contenido de un sistema informático (dimensión negativa de la intimidad)[72]. *En suma, el requisito de la vulneración de las medidas de seguridad integra un modo comisivo que revela la específica y relevante lesividad respecto a la intimidad de la conducta de acceso a los datos o programas contenidos en un sistema informático. Es lo que eleva esta conducta a la categoría de especialmente grave y disvaliosa para la intimidad personal*.

Por ello, la perturbación a la intimidad se produce desde el momento en que son rebasadas las medidas que protegen al dato o programa y éste queda al descubierto, sin que sea necesario llegar a tener conocimiento del contenido exacto de esos datos, que pueden resultar ininteligibles o indescifrables para el intruso[73]. En consecuencia, la imperfecta ejecución, la imputación a título de tentativa respecto a la intimidad, sería predicable de aquellos casos en que no se logra la destrucción de las barreras de protección.

Pero además, esa vulneración supone, al mismo tiempo, la perturbación de la seguridad y estabilidad conferida al sistema informático. Matizaré el alcance de este concepto, pero se verá a continuación al analizar el caso de acceso en sistemas informáticos que he denominado «no personales», que el quebrantamiento de estas medidas representa la forma exter-

70. Así lo entiende GONZÁLEZ RUS, J.J.: «Los ilícitos en la red (I)…», *op. cit.*, pág. 247, aunque entiende que la falta de esas medidas no supone necesariamente una presunción de ausencia de voluntad de que el sistema no sea invadido por terceros.

71. Una interpretación semejante acerca del 197.2, en BOIX REIG, J.: «Protección jurídico-penal de la intimidad e informática», *Poder Judicial*, nº especial IX, 1988, pág. 22.

72. GALÁN MUÑOZ, A.: «Ataques contra sistemas informáticos. Informe sobre la transposición a la normativa penal española de la Decisión-Marco 2005/222/JAI relativa a los ataques contra los sistemas de información», *Boletín de Información del Ministerio de Justicia*, *La armonización del Derecho Penal español: una evaluación legislativa*, año LX suplemento al número 2015, 15 de junio de 2006, pág. 229.

73. En línea con la interpretación que se ha atribuido a las conductas de apoderamiento o acceso a datos personales del artículo 197. 1 y 2; *vid.* MUÑOZ CONDE, F.: *Derecho penal. Parte especial*, *op. cit.*, pág. 259; DE ALFONSO LASO, D.: «El *hackering* blanco. Una conducta ¿punible o impune?», *op. cit.*, pág. 517.

na de lesión efectiva y objetiva de una concreta seguridad de uso del sistema informático. Pues bien, entiendo que la vulneración de esa seguridad o confianza en la estabilidad del sistema informático, también existe cuando el salto de las barreras que lo protegen se configura como el medio comisivo para acceder a datos o programas contenidos en un sistema de uso exclusivamente personal. La vulneración de los mecanismos articulados para aislar a un programa denota un perjuicio para la confianza, estabilidad y seguridad que el usuario tiene en que su peculiar sistema informático y los datos que en él deposita están libres de «entrometidos».

Nos hallamos, por lo tanto, ante un delito con un doble contenido de desvalor, el que representa la afección a la intimidad y la también directa lesión de la seguridad informática. La relación entre ambos es una relación instrumental en el sentido de que el quebranto de la seguridad informática está en relación de medio a fin para entrar en contacto con esa intimidad informática que representan los datos o programas custodiados por dicho mecanismo de protección. O, si se quiere, configura el bien jurídico intermedio que cristaliza en una tutela de la intimidad.

7. La intromisión en sistemas informáticos destinados al almacenamiento de datos o programas de de uso no personal

7.1. El objeto de protección jurídica

Ya hemos advertido en reiteradas ocasiones que llama la atención el hecho de que en la eventual redacción del art. 197.3 haya una ausencia de calificativo acerca de qué tipo de dato o de programa accedido constituyen el objeto del delito. Sobre todo es llamativo si se tiene en cuenta que en los párrafos precedentes se ha cuidado mucho el legislador de identificar el carecer personal o reservado de esos datos. La ausencia, por ello, parece a todas luces consciente. Y lo es más observando que tampoco el legislador se ocupa de definir el tipo de sistema informático en el que se desenvuelve la acción.

Justamente, hay sistemas informáticos cuyo destino es diametralmente opuesto al que hemos analizado antes (contener y sistematizar información de uso personal o privado) sino que directamente se crean con una pretensión de suministro público de la información que almacenan. Se trata de lo que aquí he clasificado como sistemas informáticos *de uso público* directamente creados para el acceso a su información por parte del público, como es el caso de los sistemas informáticos, de acceso vía *web* o Intranets, con contenidos plurales, destinados a diferentes usuarios; desde interesados el accesos a datos jurisprudenciales, legales, ocio, meteorología…, etc. (piénsese en los diversísimos contenidos de las Redes telemáticas).

Y hay sistemas informáticos, que pertenecen a una empresa, pública o privada, entidad bancaria, institución oficial, etc., *no a un particular*, *cuyo uso no es público, pero sí restringido*, al propio fin de esa empresa o entidad, en donde se almacenan datos acerca de dicha entidad. En ellos se contienen datos, informaciones de dicha entidad o empresa o institución, que no se refieren a sujetos particulares[74] integrantes de esa empresa, sino que interesan a la propia empresa o entidad, como por ejemplo, sus datos contables, su patrimonio, su calendario de actuaciones o programación de actividades,… Por supuesto que si se tratara de acceder a los datos personales que han sido insertos por su titular en un archivo o registro informático de esa entidad, estaríamos claramente en el caso del art. 197.2; si se tratara de datos con trascendencia para la intimidad de las personas físicas que la integran (nóminas, expediente académico personal, currículo, hoja de servicios), estaríamos ante el caso del art. 200[75]; y en caso de que el dato o información accedido tuviera la consideración de «secreto de empresa», por referirse a procesos industriales, comerciales, etc. propios de la empresa y cuyo conocimiento afecte a su capacidad competitiva, el delito aplicables sería el 278.

En todos estos casos, «colarse» en el sistema y tomar ese dato ajeno a un individuo queda francamente lejos cualquier vulneración con una intimidad personal, que no asoma por ninguno de los costados de la conducta típica.

74. Si se tratara de acceder a los datos personales que han sido insertos en un archivo o registro informático de esa entidad, estaríamos claramente en el caso del artículo 197-2; y si se tratara de otra suerte de datos con trascendencia para la intimidad de las personas físicas que la integran (nóminas, expediente académico personal, currículo, hoja de servicios), estaríamos ante el caso del artículo 200; ANARTE BORRRALLO, E.: «Consideraciones sobre los delitos de descubrimiento de secretos (I). En especial el artículo 197.1 del Código Penal», *Jueces para la Democracia*, nº 43, 2002, pág. 60; MORALES PRATS, F.: «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», *op. cit.*, pág. 1070.

75. La cuestión acerca de la atribución del derecho a la intimidad a personas jurídicas encuentra un rechazo considerable entre la doctrina y la jurisprudencia, que con carácter general rechazan esta posibilidad, «debido a que se trata de un derecho que se deriva de la idea de dignidad humana y está, por consiguiente, estrictamente vinculado a la personalidad, por lo que no pueden ser titulares del mismo las personas jurídicas» (Auto del Tribunal Constitucional 257/1985); *vid.* PAREJO ALFONSO, L.: «El derecho fundamental a la intimidad y sus restricciones», *op. cit.*, pp. 30-32; HUERTA TOCILDO, S./ANDRÉS DOMÍNGUEZ, A.C.: «Intimidad e informática», *op. cit.*, pág. 20.

A diferencia de lo que está sucediendo con el derecho al honor, en donde la STC 214/1991 de 11 de noviembre o la STC 135/1995, de 14 de octubre, apuntan a la atribución de este derecho a las mismas; sobre ello, *vid.* LÓPEZ PEREGRIN, C.: *La protección penal del honor de las personas jurídicas y los colectivos*, Tirant lo Blanch, Valencia, 2000, pp. 176 y ss.; LÓPEZ DÍAZ, E.: «El derecho al honor de las personas jurídicas. Nuevas tendencias en jurisprudencia», *La Ley*, nº 7, 2001, pp. 1392 y ss.; VIDAL MARÍN, T.: «Derecho al honor, personas jurídicas y Tribunal Constitucional», *InDret.com,* enero, 2007.

O para ser más exactos, las últimas tendencias relativas a la evolución del concepto jurídico de intimidad a consecuencia del influjo de las tecnologías de la comunicación apuntan a la idea de protección del anonimato, es decir, asegurar el desconocimiento de la identidad del sujeto que circula por Internet, y señalan como gran problema para la elevación de este contenido a sede jurídica el de su confrontación con la necesidad de descubrir al autor de muchos ilícitos que se cometen en la Red (y el que analizamos es uno de ellos)[76].

El interés jurídico parece ir por otro camino, pese a la citada disposición del delito en el ámbito de los que protegen la intimidad. Y si el tipo de datos y su ubicación en sistemas informáticos «neutrales para la intimidad», excluye a ésta de las posibilidades de tutela, no queda otro criterio para identificarlo que el de la situación en la que se encuentran los datos: ajenos al libre acceso o captación del mismo en virtud de la existencia de medidas de seguridad. La conducta típica no se detiene en el puro acceso no consentido a datos o programas, que acabamos de identificar como «impersonales», sino que *requiere que el intruso acceda a los datos o programas vulnerando las medidas de seguridad establecidas para impedirlo, es decir, que tome contacto con informaciones de cuyo alcance está excluido*: el intruso ha de acceder a datos que se pueden calificar de «secretos», pues las medidas de seguridad están ahí colocadas para impedir su acceso y ponen de manifiesto la voluntad del titular de que la información que se contiene en los mismos no sea conocida más que por quienes estén autorizados a ello[77].

De nuevo cabe reproducir aquí las precisiones vertidas acerca de lo que denota este blindaje del dato o programa, que lo aparta de contactos no autorizados, y que acerca su contenido a un contenido «secreto», excluido frente a terceros. Decíamos más arriba que el concepto de secreto era un *concepto instrumental, una técnica formal* que puede estar al servicio de múltiples intereses o bienes jurídicos (intimidad, seguridad nacional, capacidad competitiva de la empresa, el patrimonio, el patrimonio, etc.)[78]. Así como en el caso anterior, la ubicación «privada» del dato y la ruptura de esas medidas de seguridad, permitían deducir una orientación hacia la protección de la intimidad, en este caso, solo *contamos con el hecho de que el dato está protegido por las medidas de seguridad* que manifiestan la voluntad de no permitir el acceso a la información.

Y ahora sí, ya que trata de datos que se almacenan en sistemas informáticos que nada tienen que ver con un espacio de ejercicio privado de la personalidad (es decir, que son datos inocuos en clave de intimidad), su carácter de dato protegido, excluido o «secreto», hace resurgir aquéllas opiniones que habían mantenido que la intromisión ilegítima en un sistema informático, mediante la vulneración de los mecanismos específicamente creados para su protección y la de sus contenidos, indica la existencia un nuevo interés jurídico, de carácter colectivo o difuso, que podría denominarse «seguridad de los sistemas informáticos». En suma, que su condición de datos «secretos» en el sentido de «restringidos» a extraños, es el instrumento para dar luz a la presencia en el Código Penal de un nuevo interés objeto de tutela, *que es esta seguridad del sistema informático o confianza en la no vulnerabilidad del mismo y su contenido*[79].

7.2. La configuración dogmática del tipo

Se ha mantenido doctrinalmente, y lo destacaba al abordar el tratamiento doctrinal de esta cuestión[80], que la seguridad en los sistemas informáticos entendida como objeto de tutela *per se* constituiría un bien jurídico de carácter colectivo o difuso en el que la necesidad de su protección penal vendría dada en atención a su utilidad preventiva, en tanto que con su atención penal, se crearía un obstáculo para evitar agresiones a otros bienes jurídicos de carácter individual (como pudiera ser, el caso de la intimidad). El delito creado para garantizar dicha estabilidad en el uso del sistema informático se configuraría, por tanto, como un delito obstáculo para evitar ulteriores perturbaciones a variados y específicos bienes jurídicos. Dicho carácter da como efecto un tipo penal de naturaleza de peligro (abstracto) respecto a los más variados bienes jurídicos, que encaja a la perfección con la definición de *hacking* puro: recuerdo, el acceso subrepticio a un sistema informático, sin ninguna finalidad específica más allá del mero paseo por un sistema ajeno y sin acceder a nada, porque si se accede o intercepta algo, ya no hay un simple y «blanco» *hacking*, sino «algo más», como ha señalado LÓPEZ ORTEGA[81].

Sin embargo, en este caso, ha quedado ya dicho en varias ocasiones que el tipo no se ha detenido en un simple castigo de la ingerencia en el sistema ajeno, *sino que configura la acción típica como «acceder» a los datos contenidos en sistema informático, tras una desprotección de los mismos*, conducta que supone un contacto directo con el dato, y una voluntad clara de llegar al mismo**,** no un puro paseo por el sistema. El delito selecciona como objeto material no todo

76. LÓPEZ ORTEGA, J.J.: «Intimidad informática y Derecho penal», *op. cit.*, pp. 112-113.

77. DE ALFONSO LASO, D.: «El *hackering* blanco. Una conducta ¿punible o no punible?», *op. cit.*, pp. 513-514.

78. BAJO FERNÁNDEZ, M./BACIGALUPO, S.: *Derecho penal económico*, Centro de Estudios Ramón Areces, Madrid, 2001.

79. Realmente su inmaterialidad dificulta un lenguaje preciso; GUTIÉRREZ FRANCÉS, M: «Intrusismo informático (*hacking*). ¿Represión penal autónoma?, *Informática y Derecho*, nº 12-15, 1994, pág. 1183.

80. *Vid. supra* epígrafe 4; 4.2.1.-Razones de tipo dogmático; A) ¿Un nuevo bien jurídico? ¿Necesidad de protección penal?, en *Vías para la tipificación del acceso ilegal a los sistemas informáticos (I)*, publicado en el número anterior.

81. LÓPEZ ORTEGA, J.J.: «Intimidad informática y Derecho penal», *op. cit.*, pág. 119.

dato o sistema informático, sino los específicamente protegidos, de manera que *esa seguridad tiene un referente concreto en el dato o sistema al que guarda.*

Éste es el motivo por el que entiendo que el tipo se aleja de una tutela de la tranquilidad informática o pacífico disfrute de las redes, en abstracto, como característica de funcionamiento a la que según había mantenido un sector de la doctrina[82] se le debía elevar al rango de interés con relevancia penal. *Por el contrario, el legislador se queda con una visión de la seguridad bastante más restringida y objetivada:* la que *efectivamente se construye en torno a un sistema informático concreto* y cuya vulneración supone una forma comisiva traducible en una concreta aptitud riesgosa de la conducta, que desplaza la conformación dogmática del tipo hacia la naturaleza de «delito de peligro concreto» respecto a un determinado bien jurídico y al bien jurídico seguridad informática como un bien jurídico «intermedio»[83]. Dicho en otros términos: no se trata de una inseguridad o tranquilidad informática colectiva o difusa, como sucedería con el *hacking* puro, sino de una vulneración de la *específica, concreta o determinada seguridad* del sistema.

Por eso, la pregunta que ahora queda por atender es: ¿peligro respecto a qué? Porque el problema es que el carácter «impersonal», y por lo tanto plural, diverso del mismo hace que la *identificación del bien jurídico colocado en riesgo resulte francamente impredecible*[84], ya que, como ya he comentado en otro momento, el tipo ni siquiera apunta a algún elemento subjetivo que identifique la orientación de la conducta del intruso. Por este motivo, y pese a la dificultad de este elemento en clave probatoria, su especificación al menos habría servido para identificar la orientación del peligro, que entiendo inherente al hecho de que el *hacker* no se conforma con pasear por el sistema, sino que llega a una «captación intelectual»[85] del dato. Veamos, a título de muestra, algunas posibilidades:

— Podría tratarse del acceso a la información supeditada a los legítimos usuarios que obtienen, a cambio de una contraprestación económica las claves de acceso al dato (caso de acceso a bases *on-line* de jurisprudencia, legislación, música, etc.). En este caso, el interés afectado sería el patrimonio del servidor o titular del sistema, que realiza un «acto de disposición» sin obtener una prestación económica. Sería una figura de posible encaje en la estafa, ya que el intruso consigue la disposición de un bien de valor económico, y causa un perjuicio patrimonial por el valor de lo alcanzado. En el caso de que no hubiera que pagar por acceder al dato (supuesto de las «descargas» gratuitas), en donde el mantenimiento del sistema informático se logra a base de contratos publicitarios, entiendo que también el patrimonio del titular de la información estaría en peligro ante el evidente riesgo de que deje de recibir fondos de los que depende.

— Podría tratarse del acceso a los datos de un banco o de una empresa, que manifiestan su situación económica, sus activos o patrimonio, en cuyo caso, cabe percibir una situación de riesgo respecto a la situación patrimonial de la misma, que el *hacker* puede alterar por la vía de la manipulación de dichos datos, dándose lugar a una forma de estafa informática del art. 248.2 en grado de tentativa en tanto en cuanto la manipulación no se llegue a realizar.

— Podría ser que el solo acceso a los datos representase un riesgo para la propia integridad de los mismos, pues el intruso puede afectarlos a alterarlos. Estaríamos ante un caso de riesgo a una propiedad ajena, aunque incluible en el delito de daños informáticos del art. 264[86], también en tentativa[87] si no se produce la acción dañosa.

82. GUTIÉRREZ FRANCÉS, M.: «Intrusismo informático (*hacking*)…», *op. cit.*, pág. 1183; ROMEO CASABONA, C.Mª.: «La protección penal de la intimidad y de los datos personales en sistemas informáticos», *Estudios Jurídicos del Ministerio Fiscal*, 2001, pág. 290; «Los datos de carácter personal como bienes jurídicos penalmente protegibles», *El Cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales* (ROMEO CASABONA, Coord.), Comares, Granada, 2006, pág. 220.

83. *Vid.* MATA Y MARTÍN, R.M.: *Bienes jurídicos intermedios y delitos de peligro*, Comares, Granada, 1997, pág. 24.

84. PUENTE ABA, L.M.ª: «Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos», en *Nuevos retos del Derecho penal en la era de la globalización*, AA.VV. (FARALDO CABANA, Dir.,), Tirant lo Blanch, Valencia, 2004, pág. 401.

85. MATA Y MARTÍN, R.M.: *Delincuencia informática y Derecho penal*, *op. cit.*, pág. 139.

86. Un artículo que también se vería reformado para referirse a todos los casos de sabotaje informático, y en el que se diferenciaría entre daños directos sobre los datos y la perturbación del propio sistema.

«1. El que sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos o programas informáticos ajenos, será castigado, en consideración a la gravedad del hecho, con la pena de prisión de seis meses a dos años.

2. El que sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema de información ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, será castigado, atendiendo a la gravedad del hecho, con la pena de prisión de seis meses a tres años.

3. Se impondrán las penas superiores en grado a las respectivamente señaladas en los dos apartados anteriores y, en todo caso, la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

1.º Se hubiese cometido en el marco de una organización criminal (…).»

87. GONZÁLEZ RUS, J.J.: «El *cracking* y otros supuestos de sabotaje informático», en *Estudios Jurídicos del Ministerio Fiscal*, II-2003, Ministerio de Justicia, Madrid, 2003, pp. 247-248; «Protección penal de sistemas elementos, datos y programas informáticos», *Revista Electrónica de Ciencia penal y Criminología*, nº 1, 1991, pág. 7.

— Podría ser un acceso a datos relativos a la seguridad nacional o la defensa, lo cual supone una conducta de riesgo para la paz y seguridad nacional, encardinable en los arts. 584 ó 598.

Es decir, el delito, se comporta como una forma de lesión efectiva para la seguridad del sistema informático, dada la vulneración de las medidas de seguridad, pero, al propio tiempo, el acceso al dato que este quebranto implica deja paso a una afección, por lo menos en grado de tentativa, y por lo tanto como riesgo concreto[88]*, respecto a otros bienes jurídicos individuales, ya tutelados en otros delitos en función del ánimo inherente a la acción del sujeto*. Consecuentemente, se daría como efecto «un solapamiento y convergencia normativa con otros preceptos»[89], es decir, un concurso de normas a resolver por la regla de la especialidad en el caso de que el intruso manifestara el particular dolo que cada uno de ellos requiere. Esta reiteración típica, con la consiguiente necesidad de dar una respuesta a lo que técnicamente constituye un concurso de normas, hace surgir de nuevo la sombra de la duda de si no estaríamos ante una solución contraria a las exigencias de una intervención penal reducida a lo indispensable[90], pues no hacen sino delatar que el legislador erró al incorporar un precepto que ya existía dejando al descubierto una irreflexiva ansia punitiva.

El resultado de todo ello es que *el tipo quedaría circunscrito a los casos en que no se pudiera probar un específico dolo del intruso que accede al dato relevante para la seguridad, patrimonio, etc., o cuando el acceso al dato no representara ningún riesgo o lesión para otro bien jurídico* (piénsese, por ejemplo, en el acceso a datos protegidos de una biblioteca pública).

De modo que, al final, de esta particular naturaleza se desprende que el delito del 197.3, *operaría como una fórmula residual o de cierre respecto a otros delitos informáticos* cuya modalidad comisiva contemple situaciones de intromisión no legítima en un sistema informático ajeno. Y la consecuencia de todo ello *en clave de crítica formal al precepto es su inadecuada ubicación en un título dedicado a la protección de la «intimidad», con la que, en estos casos, nada tiene que ver*[91].

8. Resultado sobre el alcance protector del delito del artículo 197.3 del proyecto de Código Penal y propuesta

— El debate doctrinal acerca de si debía castigarse o no el acceso no consentido a un sistema informático ajeno, por el mero ánimo de retar al sistema informático, pero sin pretender ningún otro objetivo (acceder a datos personales, defraudar económicamente, etc.) ha quedado muy atrás, dada la forma específica que finalmente ha adquirido el delito de intrusismo informático, con lo cual aquellas críticas y contracríticas sobre las que abstractamente se polemizaba han quedado en buena parte superadas.

— Y ello porque la solución positiva ha derivado en una especie de *tertium genus* a caballo entre lo que se ha considerado un puro intrusismo «blanco» y una forma de ataque directo a otros bienes jurídicos concretos. Se incrimina el acceso a un sistema informático, pero se exige acceder a los datos y programas que en él se contienen y que se han protegido de tales accesos mediante el establecimiento de medidas de seguridad.

— El hecho de que la conducta requiera un acceso al dato o programa informático «rebasa» la mera intromisión en el sistema informático y nos sitúa ante una posibilidad de vulneración efectiva de un bien jurídico específico respecto al que el dato es su objeto material. Pero ello requiere la diferenciación según el según el ámbito «informático-espacial» en el que se actúa y se ubica el dato o programa accedido.

— Si se trata de datos contenidos en un «sistema informático de uso exclusivamente particular», que además el usuario ha blindado mediante medidas, cabe aceptar que los datos captados son datos secretos y de uso personal, en línea paralela con lo que serían sus objetos personales, situados en un espacio físico donde el sujeto desarrolla su vida, o sus cartas cerradas. Además, la consciente ruptura de los mecanismos protectores muestra objetivamente una voluntad vulneradora del espacio informático de intimidad o de intromisión en un espacio personal y privado. En este sentido, es admisible la ubicación de esa forma de intrusismo como una nueva manifestación de vulneración de la intimidad y en esa medida, de correcto encaje sistemático en el art. 197 del Código penal. Y diría más, de adecuada situación detrás de la forma más graves de ataque a la intimidad personas, inserta en el párrafo precedente. El inferior perjuicio para la intimidad, derivado del carácter no reservado de los datos justifica que la pena sea inferior.

— La respuesta legislativa de atender al *hacking* informático se ha traducido en una particular forma de tutela de la intimidad proyectada y ejercida en lo que hoy es un lugar cotidiano y habitual de relación social y desarrollo personal, el medio informático. Es lo que he calificado como una manifestación de la progresiva spiritualización/ am-

88. Con lo que se rebajarían las críticas acerca de la configuración del *hacking* como un delito de peligro abstracto que vimos al tratar *supra* epígrafe 4; 4.2.1.-Razones de tipo dogmático; B) Estructura típica para dar respuesta a ese bien jurídico: el peligro abstracto, en *Vías para la tipificación del acceso ilegal a los sistemas informáticos (I)*, publicado en el número anterior.

89. MORÓN LERMA, E.: *Internet y Derecho penal*…, *op. cit.*, pág. 82.

90. MIR PUIG, S.: *Derecho penal. Parte general*, *op. cit.*, pág. 651.

91. Parcialmente, GALÁN MUÑOZ, A.: «Ataques contra sistemas informáticos…», *op. cit.*, pág. 228, que propone que el intrusismo informático sea incluido dentro de los ataques a la intimidad pero en un capítulo propio, para dejar patente esta peculiaridad de vulneración de otros bienes jurídicos.

pliación del bien jurídico intimidad que ya había comenzado por medio de la protección penal del *habeas* informático respecto a los datos contenidos en ficheros. La nueva figura típica conecta con la intimidad en tanto que acceder mediante la red a un ordenador personal puede permitir extraer un retrato de la persona usuaria del mismo (peligro abstracto respecto a la intimidad); pero lo que lo hace especialmente disvaliosa respecto a la intimidad y le dota de relevancia penal es que es la forma en la que se custodian los datos: protegidos por mecanismos de seguridad, por lo que en esa medida son datos «secretos» o excluidos del alcance de los demás (pero no por el contenido de los datos, que ahora pueden ser en sí mismos intranscendentes desde el punto de vista estricto de la vida personal o familiar, ni porque haya que comprobar un específico ánimo en el sujeto que desea acceder a los mismos), de modo que el quebranto de las barreras establecidas para hacerlos inaccesibles a terceros nos sitúa ante la forma espiritualizada de abrupta intromisión en un ámbito particular.

— En caso de que la intromisión sea a un sistema informático que hemos calificado como «impersonal», el acceso a los datos o programas impersonales contenidos en el mismo constituye una conducta ajena a la intimidad personal. Pero la particular forma en que se encuentran los datos, excluidos de alcance a terceros no autorizados, y la forma comisiva, vulnerando medidas de seguridad que expresamente se han establecido para acceder a la información, apunta a la presencia de un bien jurídico consistente en la confianza o seguridad informática del concreto usuario.

— Su concreta lesión viene provocada por el hecho de rebasar las medidas que dejan el dato al descubierto, pero al mismo tiempo, este acceso al dato apunta a la posible afección a otros bienes jurídicos particulares de los que el dato o programa es su objeto, de manera que el tipo lo es, también, de peligro concreto respecto al ulterior bien jurídico afectado. Sin embargo, la determinación de ese bien jurídico, es *a priori* imposible de determinar, ya que el delito no aporta ningún dato para esta clarificación.

— Es más, dependiendo del ánimo perceptible en el intruso, nos encontraríamos ante formas de comisión que ya tienen su encaje típico, normalmente por la vía de la tentativa, en otros tipos penales, de manera que el tipo del art. 197.3 del Proyecto queda limitado a ser una cláusula de cierre para los casos en que no se pudiera probar ánimo alguno en la conducta del sujeto que se entromete en un sistema informático y accede a un dato «excluido».

— Finalmente y como conclusión más relevante, entiendo que no estamos ante un *hacking* tan blanco como se había sospechado doctrinalmente, sino ante una forma de afección a otros bienes jurídicos. En particular, el tipo ofrece vías para considerar que lo que está en juego es la intimidad; *pero no solo*. Y para justificar esta presencia de la intimidad (y la de otros bienes jurídicos) ha sido preciso distinguir según el tipo de sistema informático en el que se verifica el acceso: sistema de uso estrictamente personal o sistema destinado a almacenamiento de datos o programas no personales.

— *Por este motivo, y como propuesta legislativa, ya que aún se trata de un Proyecto me parecería sumamente aconsejable la especificación de este dato. De lo contrario, el tipo bandea desde la protección de la intimidad hasta la de otros bienes jurídicos de imposible predicción a priori, pasando por una tutela de la seguridad y pacífico disfrute del sistema protegido. Todo ello empaña la confesada pretensión legislativa de tutela la intimidad ante nuevos modos de ataque (los que proceden de las acciones de hacking), incluso manifestada a nivel sistemático-formal, dad la ubicación del delito entre los que tutelan la intimidad personal pues propicia una extensión del tipo a situaciones ajenas de todo punto de referentes de intimidad*.

Así que, creo que estamos en un momento idóneo para formular esta crítica y reclamar un replanteamiento de este tipo para que, si sigue adelante, a menos clarifique el objeto de protección, pues es diferente según el ámbito en el que nos movamos. Si el legislador efectivamente continua en su apuesta de tratar de proteger la intimidad frente a las entradas no consentidas en sistemas informáticos, y no el mero intrusismo informático en estado puro, como se había venido especulando, sería conveniente introducir una precisión acerca de cuáles son los sistemas sobre los que se incide o el tipo de datos cuya captación tiene relevancia penal.

9. Valoración de la adaptación del artículo 197.3 a las previsiones de la Decisión-Marco 2005/222/jai del Consejo de la Unión Europea

Finalmente, ¿es realmente un tipo que se adapte a lo prescrito por la Decisión-marco del Consejo de la Unión Europea, de cuyas previsiones encuentra causa esta reforma legislativa?

En la primera parte de este trabajo veíamos que desde la Decisión-marco se posibilita que el alcance que se atribuya en cada Estado al tipo penal de intrusismo informático quede a la libertad de éstos. Según dicha Decisión, cada Estado «*podrá decidir*» (es una facultad) que el delito consista en un acceso no consentido a un sistema informático en el que el único requisito sea la trasgresión de las medidas de seguridad («únicamente cuando la infracción se cometa transgrediendo medidas de seguridad»). *Pero ésta es una posibilidad que se ofrece a los Estados, no están obligados a que éste sea el único contenido asignable al delito de hacking, sino que pueden estructurarlo en base a otros requisitos.* Por eso, en el ámbito europeo subsisten diferentes posibilidades de conformación de los tipos penales estatales**:** cabe como opción básica, la respuesta más amplia de tipificación que pasa por configurar como típico el mero proceso del acceso no consentido a un sistema informático sin ni siquiera exigir penalmente la vulneración de las medidas de seguridad que protegen el sistema; se pueden mantener posiciones más estrictas al

exigir, como acabamos de decir, que se violenten esas medidas, sin necesidad de apreciar ningún otro elemento ni en el autor ninguna orientación subjetiva; se puede requerir que el autor actúe movido por una finalidad específica, que puede ser cualquiera, ya que nada en este punto indica la Decisión; es posible, como solución más restrictiva penalmente, que se exijan ambos ingredientes, un ánimo específico y el dato objetivo de la vulneración de las medidas de seguridad. Y finalmente, el marco dibujado por la Comisión no impide, incluso, que respetando ese mínimo de que se trate de un acceso no autorizado, los legisladores nacionales opten por vincularlo a la protección de ciertos bienes jurídicos concretos, como la intimidad o el patrimonio, lo cual puede lograrse a través de la exigencia del elemento subjetivo mencionado o a través de elementos típicos objetivos, que manifiesten en sí mismos, externamente, un particular desvalor respecto a dichos bienes jurídico particulares. De esta manera, el delito de intrusismo informático dejaría de ser el simple acceso ilegal a un sistema informático ajeno, para pasar a convertirse en una modalidad de ataque referido a bienes particulares: intrusismo informático en la intimidad, intrusismo informático patrimonial[92].

Ante ello, concluía señalando que la Decisión-marco presenta una proscripción penal del intrusismo informático que se puede calificar como «regulación de mínimos», ya que se opta por un diseñar un marco típico extenso; se contiene una decisión penal que refleja el espacio de tipicidad más amplio de cuantos esquemas de punición eran posibles, dejando a los Estados la posibilidad de estrecharlo. Es decir, que aunque bajo los parámetros de la previsión europea se da cabida a la punición del *hacking* puro, queda abierta la posibilidad de que sobre la base de que se trate de una conducta de acceso informático no autorizado las legislaciones nacionales establezcan otros requisitos. Y esto es lo que ha decidido nuestro legislador:

— Regula una conducta de acceso a un sistema informático.

— Adopta el requisito ofrecido por la Unión Europea de que se actúe vulnerando las medidas de seguridad.

— Pero no establece ese requisito como el «único».

— Establece, además, que en acceso al sistema *avance hasta la toma en contacto con los datos o programas que en él se contengan*.

— Dicho acceso a datos y su carácter de datos protegidos por medidas de seguridad que los cierran de penetraciones por parte de terceros, hace de este delito una posible forma de afección relevante para la intimidad desarrollada en un nuevo espacio, el informático. Pero también, si el sistema informático al que se accede no es estrictamente personal, el acceso representa un posible riesgo para otros bienes jurídicos.

En conclusión, respetando el «mínimo» exigido por la Decisión-marco, el legislador español, rebasaría la conducta del *hacking* blanco o del mero paseo por un sistema informático ajeno sin hacer nada más: «Si existe interceptación ya no hay simple acceso inconsentido, sino algo más que el mero intrusismo informático», como se ha sostenido en varias ocasiones. *Por todo ello, considero que justamente lo que quedaría impune en España es el mero paseo informático o hacking blanco, que no ha merecido en nuestro país estimación de desvalor suficiente como para necesitar una respuesta penal*[93]. El problema, ahora, y ya lo apunté en el momento de analizar el alcance armonizador de la citada Decisión-marco, es que este espacio de impunidad plantea el inconveniente de la escasa armonización, pese al anhelo europeo, y de la consiguiente creación de «lagunas» o paraísos delictivos.

92. Que en el caso del Código Penal español requeriría de una labor de interpretación de la aptitud del delito de estafa informática del 248.2, y en concreto del elemento «manipulación informática» para acomodar en él los casos de acceso subrepticio a un sistema informático que ocasione dicha alteración patrimonial.

93. Así, RUIZ MARCO, F.: *Los delitos contra la intimidad…*, *op. cit.*, pág. 27.