# LOS ATAQUES CONTRA LOS SISTEMAS INFORMÁTICOS: CONDUCTAS DE HACKING. CUESTIONES POLÍTICO-CRIMINALES

**María Ángeles Rueda Martín**
**Profesora Titular de Derecho penal en la Universidad de Zaragoza**

**SUMARIO:** I. INTRODUCCIÓN. Delimitación de conceptos. II. CONSIDERACIONES POLÍTICO CRIMINALES EN TORNO A LOS ATAQUES CONTRA LOS SISTEMAS INFORMÁTICOS EN EL ÁMBITO INTERNACIONAL Y DE LA UNIÓN EUROPEA. 1. El Convenio del Consejo de Europa sobre Cibercriminalidad (Budapest, 23 de noviembre de 2001). 2. La Decisión Marco 2005/222/JAI del Consejo de la Unión Europea de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información. 3. La regulación penal de los accesos ilícitos a un sistema informático en Derecho comparado. 4. La regulación penal de los accesos ilícitos a un sistema informático en España. III. EL BIEN JURÍDICO PROTEGIDO EN EL ACCESO ILÍCITO A UN SISTEMA INFORMÁTICO. IV. PROPUESTA POLÍTICO CRIMINAL SOBRE LA CONSIDERACIÓN COMO DELITO DEL ACCESO ILÍCITO A UN SISTEMA INFORMÁTICO. 1. Necesidad de la represión penal autónoma de las conductas de accesos ilícitos a sistemas informáticos. 2. Sistema de criminalización.

## I. INTRODUCCIÓN. Delimitación de conceptos

Las manifestaciones delictivas relacionadas con las tecnologías de la información y comunicación (TIC´s) son muy variadas y también abundantes. Sin embargo, intentar definir dichas manifestaciones es una tarea compleja tanto por su imprecisión como por su carácter polisémico[1].

---

* Este trabajo tiene su origen en la ponencia que la autora presentó en el *Seminario de Derecho penal, Ciencia, Tecnología e Innovación Tecnológica (I)*, dirigido por el Dr. D. Carlos Mª Romeo Casabona, Catedrático de Derecho penal en la UPV, y organizado por la Cátedra Interuniversitaria Fundación BBVA-Diputación Foral de Bizkaia de Derecho y Genoma Humano de la Universidad de Deusto y la Universidad del País Vasco.

Por tanto es necesario exponer, previamente, en qué consisten estas conductas que suponen o pueden suponer un ataque a sistemas informáticos. Por una parte, nos encontramos con las denominadas conductas de hacking que consisten en acceder de forma no autorizada o no consentida a bases de datos o a sistemas informáticos ajenos mediante la vulneración de puertas lógicas o passwords. Estas conductas de acceso no autorizado, englobadas bajo el término hacking o más concretamente hacking blanco, se caracterizan porque están impulsadas por la insaciable curiosidad de los hackers en encontrar en los sistemas informáticos la existencia de agujeros (o puertas falsas) y fallos o a qué se deben, pero una vez conseguido este propósito dentro de la máquina, no borran ni destruyen nada[2]. Conviene indicar que en ocasiones se suele utilizar el término hacking para aludir de forma comprensiva a cualquier ataque a un sistema informático, incluidas conductas de cracking o de

---

Además este trabajo desarrolla uno de los objetivos de estudio planteados en el proyecto de investigación del Ministerio de Educación y Ciencia, titulado "*El Derecho penal de la Unión Europea*" (SEJ 2005-07811), y dirigido por el Dr. D. Luis Gracia Martín.

1 Véanse Morón Lerma, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, 2ª ed., Aranzadi, 2002, p. 50; Gutiérrez Francés, «El intrusismo informático (Hacking): ¿Represión penal autónoma?», *Informática y Derecho, II Congreso Internacional de Informática y Derecho, Actas, Volumen II, números 12-15, 1996,* p. 1165.

2 Véanse Morón Lerma, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, pp. 52 y 53; González Rus, «Los ilícitos en la red (I): hackers, crakers cyberpunks, sniffers, denegación del servicio y otros comportamientos semejantes», *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales,* Romeo Casabona coord., Comares, Granada, 2006, p. 243; Sieber, «Documentación para una aproximación al delito informático», *Delincuencia informática,* Mir Puig (coord.), PPU, 1992, pp. 77 y 78; Gutiérrez Francés, «Delincuencia económica e informática en el nuevo Código penal», *Ámbito jurídico de las tecnologías de la información,* Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, 1996, pp. 299 y ss.; Hilgendorf, Frank, Valerius, *Computer- und Internetstrafrecht. Ein Grundriss,* Springer, Berlin, 2005, p. 184; Maiwald, *Fundamentos de seguridad de redes,* 2ª ed., McGraw-Hill Interamericana Editores, México, 2003, pp. 36 y 37. En el Manual de Naciones Unidas sobre delincuencia informática también se definen así las conductas de hacking; véase «United Nations Manual on the prevention and control of Computer-Related Crime», *International Review of Criminal Policy,* núm. 43 y 44, 1994, parágrafo 74. Un ejemplo de este tipo de conductas de hacking puede verse en Piqueres Castellote, «Conocimientos básicos en internet y utilización para actividades ilícitas», *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?,* Velasco Núñez (Dir.), Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, 2006, pp. 61 y 62; Mansfield, *Defensa contra hackers. Protección de información privada,* Ediciones Anaya Multimedia, Madrid, 2001, pp. 57 y ss.
Aunque en la actualidad se utilice el término hacker con connotaciones negativas, su origen es más bien de signo contrario puesto que el desarrollo de internet y de determinados sistemas operativos, gratuitos y universales, debe mucho a algunas personas que comparten unos valores positivos que conforman la ética hacker; véase al respecto, Himanen, *La ética del hacker y el espíritu de la era de la información,* Prólogo de Linus Torvalds y Epílogo de Manuel Castells, Ediciones Destino, Madrid, 2002.

ciberpunking, impulsadas por una finalidad dañina de diversa índole[3]. Nosotros optamos por distinguir estos comportamientos porque tienen una diferente trascendencia en el ámbito penal.

Por otra parte, destacan las conductas de cracking caracterizadas por eliminar o neutralizar los sistemas de protección de un sistema informático que impide su copia no autorizada o la de una aplicación shareware que impide su uso, pasada una determinada fecha, con vulneración de los derechos de autor[4]. También hay que mencionar las conductas de ciberpunking que propiamente son conductas de daños informáticos o de vandalismo electrónico, concretadas en asaltos sobre máquinas o sistemas informáticos para ocasionar perturbaciones sobre dichos sistemas o para modificar o destruir datos[5]. Finalmente hay que aludir a una serie de comportamientos lesivos de la denominada privacidad informática que consisten en introducir en los discos duros de los ordenadores programas con la finalidad de buscar cierto tipo de información[6]. Este grupo de conductas tiene en común dos notas: en primer lugar, para su realización es necesario que, previamente, se haya producido un acceso ilícito a un sistema informático; en segundo lugar, dichas conductas recaen sobre los sistemas informáticos o sobre la información que se contiene en los mencionados sistemas, con la finalidad de su perturbación, destrucción o modificación.

---

3 Utilizan el término hacking de esta forma, por ejemplo, Rodríguez Mourullo, Alonso Gallo, Lascuraín Sánchez, «Derecho penal e internet», *Régimen jurídico de internet*, Cremades, Fernández-Ordoñez, Illescas coords., Editorial La Ley, Madrid, 2002, p. 266, nota 36.

4 Véanse Morón Lerma, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, p. 40; Gómez Martín, «El delito de fabricación, puesta en circulación y tenencia de medios destinados a la neutralización de dispositivos protectores de programas informáticos (art. 270, párr. 3º CP). A la vez, un estudio sobre los delitos de emprendimiento o preparación en el CP de 1995», *Revista Electrónica de Ciencia Penal y Criminología,* 04-16 (2002), p. 3, nota 3. Sin embargo, González Rus utiliza el término cracking para referirse específicamente a los daños informáticos que se producen accediendo a sistemas informáticos ajenos a través de internet o redes de transmisión de datos, ya que originariamente tenía este sentido dicho término; véase González Rus, «Daños a través de internet y denegación de servicios», *Homenaje al profesor Dr. Gonzalo Rodríguez Mourullo,* Jorge Barreiro y otros coords., Civitas, Madrid, 2005, p. 1470 y nota 3.

5 Véase Morón Lerma, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, p. 41.

6 Véanse Morón Lerma, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, pp. 31 y ss.; González Rus, «Los ilícitos en la red (I): hackers, crakers, cyberpunks, sniffers, denegación del servicio y otros comportamientos semejantes», p. 242.

En el presente trabajo no nos vamos a ocupar de la relevancia penal de las conductas de cracking, ciberpunking o lesivas de la privacidad informática, sino que, por el contrario, nos centraremos en los simples accesos ilícitos, con carácter general, a sistemas informáticos. Desde un punto de vista político criminal en relación con estas conductas de hacking, se plantea la duda sobre la necesidad de criminalizarlas de una forma autónoma, si no van acompañadas de un ulterior fin relevante penalmente añadido al mero deseo de curiosidad y/o de demostración de pericia informática en el hacker. El tratamiento de esta cuestión nos obliga a plantearnos cuál es el bien jurídico protegido en un tipo delictivo que tipifique como delito el acceso ilícito, sin autorización, a un sistema informático, puesto que el debate político criminal en torno al objeto de protección en estas conductas de hacking nos condicionará después la respuesta a cuestiones tales como la exigencia de una finalidad jurídico penalmente añadida al simple deseo de curiosidad y/o de demostración de pericia informática en el hacker. Por otra parte, si concluimos que es necesario tipificar las conductas de hacking como un delito autónomo, deberemos preguntarnos por su sistema de incriminación: o bien mediante tipos específicos que contemplen la incriminación del acceso ilícito a sistemas informáticos en aquellas figuras delictivas que lo requieran; o bien mediante un tipo penal genérico que tipifique como delito el acceso ilícito a sistemas informáticos.

Antes de tratar estas cuestiones, a continuación y con carácter previo, conviene realizar unas consideraciones político criminales en el ámbito internacional y de la Unión Europea. El marco actual en el que ha de abordarse un análisis político criminal de la criminalidad informática es el del Derecho penal de la globalización con un marcado carácter sectorial, básicamente económico-empresarial[7], de modo que su objetivo es eminentemente práctico: se trata de proporcionar una respuesta uniforme o, al menos, armónica de la delincuencia transnacional que evite la conformación de "paraísos jurídico-penales"[8]. Por esta razón debemos

[7] Véanse Silva Sánchez, *La expansión del Derecho penal. Aspectos de la política criminal en las sociedades postindustriales*, 2ª ed., Civitas, Madrid, 2001, p. 99; Gracia Martín, *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. 89 y ss.

[8] Véase Silva Sánchez, *La expansión del Derecho penal. Aspectos de la política criminal en las sociedades postindustriales*, p. 88. No podemos olvidar que los comportamientos englobados bajo la denominación criminalidad informática, son comportamientos que

abordar, brevemente, qué planteamientos político criminales se han realizado en torno a los ataques a los sistemas de información en nuestro entorno más cercano.

## II. CONSIDERACIONES POLÍTICO CRIMINALES EN TORNO A LOS ATAQUES CONTRA LOS SISTEMAS INFORMÁTICOS EN EL ÁMBITO INTERNACIONAL Y DE LA UNIÓN EUROPEA

### 1. El Convenio del Consejo de Europa sobre Cibercriminalidad (Budapest, 23 de noviembre de 2001)

El Convenio del Consejo de Europa sobre Cibercriminalidad (Budapest, 23 de noviembre de 2001)[9] recoge en su Capítulo II un conjunto de medidas que deben ser adoptadas por los Estados Parte para prever como infracción penal una serie de conductas contempladas en dicho Convenio: el acceso ilícito a la totalidad o a una parte de un sistema informático (art. 2), la interceptación ilícita de transmisiones privadas de datos informáticos (art. 3), atentados contra la integridad de datos informáticos (art. 4), atentados contra la integridad del sistema (art. 5), la producción, venta, utilización, importación, distribución o cualquier forma de hacer posible cualquier dispositivo, password electrónico, código de acceso o datos similares con la finalidad de cometer las infracciones de los arts. 2, 3, 4 y 5 (art. 6), falsedades informáticas (art. 7), fraude informático (art. 8), infracciones relacionadas con la pornografía infantil (art. 9) e infracciones relacionadas con la violación de derechos de la propiedad intelectual y derechos afines (art. 10)[10]. En concreto en la Sección I sobre Derecho penal

---

cada vez se dan con mayor frecuencia y lo que añade un especial grado de peligrosidad al fenómeno de dicha criminalidad, es la conexión internacional o transfronteriza de estos comportamientos, de modo que sus actuaciones pueden ir más allá de un ámbito geográfico concreto.

9 Sobre el proceso de gestación de este Convenio, véanse, Morales García, «Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre *Cyber-Crime*», pp. 16-25; Lezertúa, «El proyecto de Convenio sobre el cybercrimen del Consejo de Europa», *Internet y Derecho penal*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, 2002, pp. 17 y ss. Asimismo, véanse, Morón Lerma/Rodríguez Puerta, «Traducción y breve comentario del Convenio sobre Cibercriminalidad», *Revista de Derecho y Proceso Penal,* nº. 7, 2002, pp. 167 y ss.; Sánchez Bravo, «El Convenio del Consejo de Europa sobre cibercrimen: control vs. Libertades públicas», *La Ley*, 2002, D-109, pp. 1851 y ss.

10 Véanse, Morales García, «Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre *Cyber-Crime*», pp. 26 y ss.;

sustantivo del mencionado Capítulo II, en su Título I acerca de los "*Delitos contra la confidencialidad e integridad de los datos informáticos y los sistemas*" se establece en el artículo 2 que: «*Los Estados Parte deberán adoptar las medidas legislativas y otras que resulten necesarias para establecer como infracción criminal, conforme a su derecho interno, el acceso intencional sin autorización a la totalidad o parte de un sistema informático. Los Estados podrán requerir que el hecho sea cometido infringiendo medidas de seguridad o con la finalidad de obtener datos u otra finalidad deshonesta o, en relación con los sistemas informáticos, que se encuentren conectados a otros sistemas informáticos*»[11].

En cuanto a la definición de "sistema informático", el artículo 1 de dicho Convenio dispone que «*hace referencia a todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, al ejecutar un programa, el tratamiento automatizado de datos*». Por otro lado, los "datos informáticos" se definen como «*toda representación de hechos, informaciones o conceptos expresados bajo una forma tratable informáticamente, incluido el programa destinado a hacer que un sistema informático ejecute una función*».

A los efectos que nos interesa en este trabajo el Convenio de 2001 plantea las siguientes propuestas político criminales. En primer lugar, se distingue, por un lado, la protección de los sistemas informáticos (artículos 2, 5 y 6 del Convenio) y, por otro lado, la protección de los

---

Rodríguez Bernal, «Los cibercrímenes en el espacio de libertad, seguridad y justicia», *Revista de Derecho informático*, nº. 103, febrero de 2007, pp. 12 y ss.

[11] Además en el artículo 6 de este Convenio se dispone que «*1. Los Estados Parte deberán adoptar las medidas legislativas o de otro género que fueren necesarias para establecer como infracción criminal la comisión dolosa y antijurídica de:*
*a) la producción, venta, el procurarse para el uso, la importación, distribución o cualquier forma de hacer posible: 1. cualquier dispositivo, incluidos los programas informáticos, diseñados o adaptados principalmente con el propósito de cometer alguno de los delitos descritos en los artículos 2 a 5; 2. un password electrónico, código de acceso o datos similares a través del cual un sistema informático o parte de él consigue ser accesible, con la finalidad de ser usado con el propósito de cometer los delitos descritos en los artículos 2 a 5;*
*b) la posesión de cualquiera de los aparatos descritos en los números 1 y 2 de la letra a) con la finalidad de ser usado para cometer los delitos establecidos en los artículos 2 a 5. Las Partes deberán establecer mediante ley que sea poseído un determinado número de este tipo de dispositivos antes de la atribución de responsabilidad.*
*2. Este artículo no debe ser interpretado como imposición de responsabilidad criminal donde la producción, venta, procurarse para el uso, importación, distribución o la facilitación o posesión referidas en el párrafo primero de este artículo no lo sea con la finalidad de cometer los hechos descritos en los artículos 2 a 5 de esta Convención, como por ejemplo para el chequeo autorizado o la protección de un sistema informático.*
*3. Los Estados podrán reservarse el derecho de no aplicar el párrafo primero de este artículo*».

datos o de la información que se contiene en dichos sistemas[12]. En segúndo lugar, aunque se propone que se tipifique como delito el simple acceso intencional sin autorización a la totalidad o parte de un sistema informático, con carácter facultativo los Estados podrán establecer algunas exigencias a la hora de configurar esta infracción penal: o bien que el acceso sea cometido infringiendo medidas de seguridad, o bien que el acceso se realice con la finalidad de obtener datos u otra finalidad deshonesta, o por último, en relación con los sistemas informáticos vulnerados, que éstos se encuentren conectados a otros sistemas informáticos[13].

### 2. La Decisión Marco 2005/222/JAI del Consejo de la Unión Europea de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información

En el ámbito de la Unión Europea destaca la Decisión Marco 2005/222/JAI del Consejo de la Unión Europea, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, que tiene como objetivo aproximar «la legislación penal en materia de ataques contra los sistemas de información para conseguir la mayor cooperación policial y judicial posible respecto de las infracciones penales vinculadas a ataques contra los sistemas de información y para contribuir a la lucha contra el terrorismo y la delincuencia organizada». Por ello se plantea un enfoque común respecto de los elementos constitutivos de las siguientes infracciones penales:

1) En primer lugar, en relación con el acceso ilegal a los sistemas de información el artículo 2 establece que: «1. *Cada Estado miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad. 2. Cada Estado miembro podrá decidir que las conductas mencionadas en el apartado 1 sean objeto de acciones judiciales únicamente cuando la infracción se cometa transgrediendo medidas de seguridad».*

---

[12] Resalta también esta distinción Quesada Morales, «La protección penal de los sistemas de información: Normativa actual y perspectivas de futuro», *Revista Aranzadi de Derecho y Nuevas Tecnologías,* nº. 4, 2004, p. 106.

[13] Véanse las consideraciones críticas en torno a estas exigencias que expone Morón Lerma, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, pp. 70, 71, 72 y 73.

2) En segundo lugar, respecto de la intromisión ilegal en los sistemas de información el artículo 3 dispone que: «*Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad*».

3) En tercer lugar, en relación con la intromisión ilegal en los datos en el artículo 4 se contempla que: «*Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad*».

Asimismo en el artículo 1 se define como "sistema de información" a «*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*»; y como "datos informáticos" se comprende «*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*».

Finalmente debemos indicar que en el artículo 7 se recogen algunas circunstancias agravantes: «*1. Cada Estado miembro adoptará las medidas necesarias para garantizar que las infracciones mencionadas en los artículos 2, apartado 2, 3 y 4 se castiguen con sanciones penales de dos a cinco años de prisión como mínimo en su grado máximo cuando se cometan en el marco de una organización delictiva tal como la define la Acción Común 98/733/JAI, con independencia del nivel de sanción mencionado en dicha Acción Común. 2. Los Estados miembros podrán adoptar asimismo las medidas contempladas en el apartado 1 cuando la infracción de que se trate haya ocasionado graves daños o afectado a intereses esenciales*».

En este texto normativo también se distingue la protección de los sistemas informáticos (artículos 2 y 3) de la protección de los datos o de la información contenidos en dichos sistemas. Y, además, se propone tipificar el simple acceso ilegal no autorizado, intencionado, al conjunto o a una parte del sistema de información sin que se exija de una forma expresa el acompañamiento de una ulterior finalidad delictiva siquiera facultativamente. No obstante queda abierta la posibilidad de añadir tal elemento subjetivo cuando se refiere a la tipificación como delito del acceso intencionado «al menos en los casos que no sean de menor gravedad». Por otro lado y potestativamente los Estados pueden criminalizar aquellos accesos ilegales que se hayan realizado transgrediendo medidas de seguridad[14].

Como conclusión en estos textos normativos internacionales que acabamos de exponer se distingue claramente:

1) Por una parte, la protección de los sistemas informáticos mediante la propuesta de tipificar como delito conductas de simple acceso no autorizado a sistemas informáticos, y también aquéllas que suponen una obstaculización o interrupción del funcionamiento de los mismos.

2) Por otra parte, la protección de los datos o de la información que albergan los sistemas informáticos con la propuesta de considerar como delito las conductas que suponen un atentado o una intromisión lesiva en los datos o la información contenida en los mencionados sistemas (que implica su modificación, inutilización, destrucción, etc.).

[14] No obstante conviene apuntar que la Propuesta originaria de esta Decisión-Marco consideraba que «el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea tipificado como delito cuando sea cometido: (I) contra una parte cualquiera de un sistema de información que es objeto de medidas de protección especiales; o (II) con la intención de causar un daño a una persona física o jurídica; o (III) con la intención de obtener un beneficio económico». Véase González Rus, «El cracking y otros supuestos de sabotaje informático», *Delincuencia Informática, Drogas de abuso: aspectos científicos y jurídicos, Experiencias aplicativas de la LORPM, Estudios Jurídicos del Ministerio Fiscal*, Madrid, 2003, p. 214.

### 3. La regulación penal de los accesos ilícitos a un sistema informático en Derecho comparado

Tal y como acabamos de exponer tanto en el Convenio como en la Decisión-Marco se recogen dos opciones político criminales en torno a la incriminación de los accesos ilícitos a sistemas informáticos. En primer lugar, tipificar como delito el simple acceso a la totalidad o a una parte de dichos sistemas informáticos. En segundo lugar, tipificar como delito esta conducta pero añadiendo más exigencias ya sean de carácter subjetivo como de carácter objetivo. A continuación repasaremos diversas regulaciones jurídico penales de algunos países de nuestro entorno, en las que encontramos coincidencias y alguna opción político criminal nueva no contemplada en los citados textos internacionales.

La tipificación como delito del simple acceso a la totalidad o a una parte (datos o programas) de un sistema informático la encontramos en algunos países como, por ejemplo, en Gran Bretaña en cuyo *Computer Misuse Act* de 1990 se dispone en la *Section 1 (1)* que «*una persona es culpable de un delito si: a) hace que un ordenador ejecute una función con la intención de asegurarse un acceso a cualquier programa o a los datos almacenados en cualquier ordenador; b) el acceso que pretende asegurarse no está autorizado; y c) conoce en el momento en que ejecuta dicha función en el ordenador que tal acceso no está autorizado*». También en el Código penal francés de 1994 en los artículos 323-1 hasta 323-7 se tipifican los atentados contra los sistemas de tratamiento automatizado de datos. En concreto el artículo 323-1 dispone que «*el hecho de acceder de manera fraudulenta a la totalidad o a parte de un sistema de tratamiento automatizado de datos, o de mantenerse en él fraudulentamente, será castigado con dos años de prisión y 30.000 euros de multa. Si de ello resultare, bien la supresión o la modificación de datos contenidos en el sistema, o una alteración del funcionamiento del mismo, la pena será de tres años de prisión y de 45.000 euros de multa*».

En otros países, sin embargo, se ha optado por la incriminación del acceso ilícito a sistemas informáticos acompañado de ulteriores exigencias, ya sea una determinada finalidad o una vulneración de las medidas de seguridad. Así en Portugal la Ley nº. 109/91 sobre criminalidad informática recoge en el artículo 7 como delito el acceso ilícito a un sistema o a una red informáticos: «*1. Quien acceda de cualquier modo, no estando autorizado y con la intención de obtener, para sí o para otro, un beneficio*

*o ventaja ilegítimos, a un sistema o red informáticos será castigado con la pena de prisión, de hasta un año o con la pena de multa, de hasta 120 días. 2. La pena será de prisión de hasta tres años o multa si el acceso se consigue con la infracción de medidas de seguridad. 3. La pena será de prisión de uno a cinco años cuando: a) a través del acceso, el sujeto haya tenido conocimiento de un secreto comercial o industrial o de datos confidenciales, protegidos por ley; b) el beneficio o ventaja patrimonial obtenidos sean de valor considerablemente elevado. 4. Se castiga la tentativa. 5. En los casos previstos en los números 1, 2 y 4 el procedimiento penal depende de querella*». En Italia el artículo 615 ter del Código penal tipifica como delito «*el acceso abusivo a un sistema informático o telemático*»: «*Quien abusivamente se introduzca en un sistema informático o telemático protegido por medidas de seguridad o se mantenga en él contra la voluntad expresa o tácita de quien tiene el derecho de excluirlo, será castigado con prisión de hasta tres años*». Asimismo en el Título II relativo a las "*Infracciones contra el patrimonio*" del Libro II del Código penal suizo se establece en el artículo 143 bis que «*quien se introduzca ilícitamente, sin la intención de enriquecerse, a través de un dispositivo de transmisión de datos, en un sistema informático ajeno y especialmente protegido contra cualquier acceso, será castigado, según la petición, con una pena privativa de libertad de hasta tres años o pena de multa*».

Mención a parte merece la regulación penal alemana que había tipificado como delito el espionaje de datos en el § 202a del Código penal alemán que establecía lo siguiente: «*Quien se procure para sí o para otro datos no autorizados que no le estén destinados y que estén particularmente asegurados contra accesos ilícitos, será castigado con una pena privativa de libertad de hasta tres años o con pena de multa*». En relación con este precepto se planteaba la polémica de si abarcaba las conductas de hacking al exigir el tipo la adquisición de datos no autorizados[15]. No obstante y como afirmaba Schünemann las conductas de hacking que suponían la apropiación de algunos datos, como un password, sí quedaban abarcadas por el tenor literal del tipo indicado[16]. Las dudas, sin embargo, se han disipado con la nueva redacción otorgada al § 202a, apartado 1, del Código penal alemán donde se aclara que la conducta típica ya no consiste en la

[15] Véanse Schünemann, «§ 202a», *Leipziger Kommentar Großkommentar*, Jähnke, Laufhütte, Odersky, 11ª ed., Walter de Gruyter, Berlin, 2000, núm. marginal 2, pp. 65 y ss.; Schnabl, «Strafbarkeit des Hacking-Begriff und Meinungsstand», *Wistra (Zeitschrift für Wirtschafts- und Steuerstrafrecht*, nº. 6, 2004, pp. 211 y ss.

[16] Véanse Schünemann, «§ 202a», *p. 65.*

adquisición de datos sino en el acceso ilícito a determinados datos: «*Quien se procure para sí o para otro el acceso a datos que no le estén destinados y que estén particularmente asegurados contra un acceso ilícito, que se consiga con la vulneración de un acceso de seguridad, será castigado con una pena privativa de libertad de hasta tres años o con pena de multa*».

### 4. La regulación penal de los accesos ilícitos a un sistema informático en España

En España no se contempla expresamente este comportamiento como un delito autónomo en nuestro Código penal[17]. Estas conductas de acceso ilegal sin autorización en un sistema informático *desprovistas de cualquier intención específica*, no se pueden subsumir en ninguna infracción constitutiva de un ilícito penal en nuestro Código penal actualmente en vigor[18].

Morón Lerma se plantea si en el artículo 256 del Código penal se pueden subsumir ciertos actos de hacking. En dicho precepto se establece que «*el que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a 400 euros, será castigado con la pena de multa de tres a doce meses*». Esta autora concluye, sin embargo, que este precepto es un cauce inapropiado para el castigo de esta clase de conductas de hacking, entre

[17] Véase Morón Lerma, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, pp. 55 y ss.

[18] Véanse Morón Lerma, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, p. 70; González Rus, «Los ilícitos en la red (I): hackers, crakers, cyberpunks, sniffers, denegación del servicio y otros comportamientos semejantes», p. 246; el mismo, «El cracking y otros supuestos de sabotaje informático», pp. 246 y ss.
En España se han llevado ante los tribunales algunos casos de accesos ilícitos sin autorización a sistemas informáticos. Así, por ejemplo, el Juzgado de lo Penal de Madrid, de 29 de julio de 2005 [A. 70162/2006], enjuició un acceso al sistema informático de una entidad pública (Ministerio de Economía y Hacienda) y de un periódico de gran tirada, y absolvió al presunto autor de un delito continuado de daños y de un delito continuado de descubrimiento y revelación de secretos al no resultar acreditado la causación de daños ni la apropiación de datos reservados en perjuicio de tercero. Por otro lado, el Juzgado de Instrucción número 2 de Lorca acordó mediante un Auto de 29 de enero de 2002, el sobreseimiento libre y el archivo de la causa en relación con un hacking al Ministerio del Interior, al no ser esta conducta constitutiva de un delito en nuestro Código penal. Finalmente el denominado caso Hispahack (un acceso no autorizado, a través de internet, a los ordenadores ubicados en las dependencias de la Universidad Politécnica de Cataluña desde un ordenador de la Universidad de Oviedo), terminó con la absolución de los procesados en la sentencia del Juzgado de lo penal número 2 de Barcelona, de 28 de mayo de 1999.

otros motivos, porque su ámbito típico se ciñe a perjuicios que consisten en perturbaciones, molestias o alteraciones en el correcto funcionamiento del sistema que, primero, sean aprehensibles y cuantificables y, segundo, perjudiquen directamente al titular del equipo y no a un tercero. Además, a su juicio, supeditar la perfección comisiva a la producción de un perjuicio patrimonial excluye aquellas conductas de mero acceso al sistema, una vez descubierta la puerta falsa, y abandono del mismo[19].

Ahora bien sí que puede constituir un ilícito penal el acceso no autorizado a un sistema informático realizado para cometer otra conducta delictiva, ya sea en grado de consumación o tentativa, como por ejemplo:

a) el acceso a un sistema informático para descubrir un secreto o vulnerar la intimidad de otro será constitutivo de un delito tipificado en el artículo 197.1 del Código penal[20],[21];

---

[19] Véanse Morón Lerma, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, pp. 55 y ss.

[20] El artículo 197.1 establece que «*el que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses*».

[21] Fernández Palma y Morales García afirman que las conductas de acceso ilícito a sistemas informáticos se pueden subsumir en el artículo 197.1 del Código penal, de modo que «el sujeto que consigue entrar en el sistema central de una Universidad, dejando dolosamente su rastro para que quede constancia de su acceso, no parece que vaya acompañado de un elemento subjetivo enderezado a la vulneración de la intimidad de otro. Ahora bien, puesto que no es necesario que se descubran los datos o se tenga conocimiento de ellos para que el elemento subjetivo se entienda realizado, y los datos de carácter personal serán una constante en dicho sistema, en la práctica no será difícil convenir en que el acceso no autorizado al mismo podrá ser constitutivo de delito independientemente de que la finalidad íntima del intruso sea la de superación de barreras informáticas o la de conocimiento expreso de los datos»; Véanse Fernández Palma/Morales García, «Los delitos de daños informáticos y el caso Hispahack», *La Ley*, 2000, D-2, p. 1525. Sin embargo hay que tener en cuenta que el verbo típico de este precepto, «interceptar comunicaciones» incluidas las comunicaciones a través de redes de información, ya no supone un simple acceso no consentido como las mencionadas conductas de hacking, sino que implica introducirse en dichas comunicaciones con la aludida finalidad de descubrir los secretos o de vulnerar la intimidad de otro. Vulnera el principio *in dubio pro reo* presuponer que en todos los accesos ilícitos a sistemas informáticos existe, además de una finalidad de curiosear la existencia de agujeros (o puertas falsas) y fallos, la de vulnerar la intimidad de las personas.

b) el acceso a un sistema informático que sea un registro o un archivo de datos reservados de carácter personal o familiar de otro y su posterior alteración o utilización en perjuicio del titular de los datos o de un tercero, será constitutivo de un delito tipificado en el artículo 197.2 del Código penal[22];

c) o el acceso a un sistema informático y la posterior destrucción, alteración, inutilización o cualquier otro daño de sus datos, programas o documentos electrónicos, será constitutivo de un delito tipificado en el artículo 264.2 del Código penal[23].

Sin embargo, hay que mencionar el Proyecto de Ley Orgánica por la que se modifica la Ley orgánica 10/1995, de 23 de noviembre, del Código penal, presentado en el Congreso de los Diputados el 15 de enero de 2007, en cuya exposición de motivos se indica que «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 artículo 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. La realidad de que los actos de invasión en la privacidad en todas sus manifestaciones no son siempre llevadas a cabo por individuos aislados han determinado la incorporación de una cualificación punitiva

[22] Véase sobre este delito Rueda Martín, *Protección penal de la intimidad personal e informática. (Los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código penal)*, Atelier, Barcelona, 2004, pp. 67 y ss.

[23] Véase González Rus, «El cracking y otros supuestos de sabotaje informático», pp. 223 y ss.

para todas las acciones descritas en el artículo 197 en el caso de que se cometan en el marco de organizaciones criminales». En el artículo 197 se ha introducido un nuevo apartado 3 con el siguiente tenor: «*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 penas de prisión de seis meses a dos años*»[24]. De manera similar en el reciente Anteproyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código penal, fechado el 14 de noviembre de 2008, se ha introducido otra vez un apartado 3 en el artículo 197 del Código penal con la siguiente redacción[25]: «*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 penas de prisión de seis meses a dos años.*

---

[24] En el mencionado Proyecto de Ley Orgánica por la que se modifica la Ley orgánica 10/1995, de 23 de noviembre, del Código penal se prevé también una reforma del artículo 264: «*1. El que sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciere 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. 2.º Haya ocasionado daños de especial gravedad o afectado a los intereses generales. 4. Cuando los delitos comprendidos en este artículo se hubieren cometido en el marco o con ocasión de las actividades de una persona jurídica y procediere la declaración de su responsabilidad penal de acuerdo con lo establecido en el artículo 31 bis de este Código, se le impondrá la pena de multa del tanto al duplo del perjuicio causado en los supuestos previstos en los apartados 1 y 2, y del tanto al décuplo en el supuesto del apartado 3*».

[25] En la Exposición de Motivos del Anteproyecto de Ley Orgánica por la que se modifica la Ley orgánica 10/1995, de 23 de noviembre, del Código penal, de 14 de noviembre de 2008, se establece que «*Para cumplimentar la Decisión Marco 2005/222/JAI de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información, se ha resuelto incardinar las conductas punibles en dos apartados diferentes, al tratarse de bienes jurídicos diversos. El primero sería el relativo a los daños donde quedarían incluidas las consistentes en borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos ajenos, así como obstaculizar o interrumpir el funcionamiento de un sistema de información ajeno; y el segundo, en el apartado del descubrimiento y revelación de secretos, donde estarían comprendidos el acceder sin autorización vulnerando las medidas de seguridad a datos o programas informáticos contenidos en un sistema informático o en parte del mismo*».

*Cuando el delito se hubiere cometido en el marco o con ocasión de las actividades de una persona jurídica y procediere la declaración de su responsabilidad penal de acuerdo con lo establecido en el artículo 31 bis de este Código, se le impondrá la pena de multa del tanto al duplo del perjuicio causado*»[26].

Nuestro legislador se ha decidido, en los mencionados proyectos de reforma del Código penal, por la opción de incriminar las conductas de acceso ilícito a datos o programas informáticos de un sistema informático o de parte del mismo dentro del Título X del Código penal, sobre los "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio". Esto significa que el legislador ha vinculado esta clase de comportamientos a la protección penal de la intimidad personal y familiar y ha añadido una exigencia objetiva, la vulneración de medidas de seguridad. Conviene destacar asimismo que no se castiga el acceso ilícito a un sistema informático o a una parte del mismo –como se propone tanto en el Convenio del Consejo de Europa sobre Cibercriminalidad de 2001 y en la Decisión Marco 2005/222/JAI del Consejo de la Unión Europea–, sino que se concreta aún más el objeto material en este comportamiento: los datos o programas informáticos contenidos en dichos sistemas informáticos[27].

---

[26] En este Anteproyecto de Ley Orgánica por la que se modifica la Ley orgánica 10/1995, de 23 de noviembre, del Código penal, de 14 de noviembre de 2008, se prevé asimismo una reforma del artículo 264: «*1. El que sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciere 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. 2.º Haya ocasionado daños de especial gravedad o afectado a los intereses generales. 4. Cuando los delitos comprendidos en este artículo se hubieren cometido en el marco o con ocasión de las actividades de una persona jurídica y procediere la declaración de su responsabilidad penal de acuerdo con lo establecido en el artículo 31 bis de este Código, se le impondrá la pena de multa del tanto al duplo del perjuicio causado en los supuestos previstos en los apartados 1 y 2, y del tanto al décuplo en el supuesto del apartado 3*».

[27] Véase también una exposición de los problemas de interpretación entre los apartados 1, 2 y 3 del artículo 197 y las consideraciones críticas en torno a esta propuesta de regulación penal contenida en el Proyecto de Ley Orgánica por la que se modifica la Ley orgánica 10/1995, de 23 de noviembre, del Código penal, de 15 de enero de 2007, efectuadas por Morón Lerma, «Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos», *Delito e informática: algunos aspectos,*

La ubicación sistemática en las propuestas de reforma del Código penal de esta conducta de acceso ilícito a datos o programas informáticos contenidos en un sistema informático o en parte del mismo, obliga a considerar que dichos datos o programas informáticos deben albergar información relevante para la intimidad personal y familiar, de modo que en ellos se manifieste la pretensión de valor de este bien jurídico. Por otra parte, en torno a esta propuesta de regulación Morón Lerma ha estimado que el acceso a los datos castigado en el posible apartado tercero del artículo 197 del Código penal se halla ya previsto en el artículo 197.2, lo que suscitaría, a su juicio, una situación contradictoria: el artículo 197.3 exigirá un plus para su comisión centrado en la vulneración de medidas de seguridad; pero la pena que lleva aparejada (prisión de seis meses a dos años) es notablemente menor que la del artículo 197.2 (prisión de uno a cuatro años y multa de doce a veinticuatro meses)[28]. En mi opinión, sin embargo, no se castigan las mismas conductas porque en el actual artículo 197.2 del Código penal se tipifica el acceso a un sistema informático que sea un registro o un archivo de datos reservados de carácter personal o familiar de otro y su posterior alteración o utilización *en perjuicio del titular de los datos o de un tercero*. Se exige, por tanto, un elemento subjetivo de lo injusto (en perjuicio del titular de los datos o de un tercero) que delimita suficientemente la conducta que se pretende castigar[29], y que no está presente en el posible apartado 197.3 que castiga el simple acceso ilícito a datos o programas informáticos contenidos en un sistema informático o en una parte del mismo. Además, desde un punto de vista valorativo es más grave el acceso a datos y su posterior alteración o utilización realizado en perjuicio del titular de tales datos o de un tercero, que el simple acceso ilícito a datos contenidos en un sistema informático o en una parte del mismo.

La vinculación de esta clase de comportamientos que consisten en un acceso ilícito a los datos o programas informáticos de un sistema informático con la protección penal de la intimidad personal y familiar plantea algunos interrogantes: ¿Se puede castigar por este tipo delictivo al hacker que accede a un sistema informático que almacena datos

Cuadernos penales José María Lidón, número 42007, Bilbao, Universidad de Deusto, pp. 101 y ss; Morales Prats, «Los delitos informáticos: dudas e incertidumbres en el Proyecto de Reforma del Código penal», *Delito e informática: algunos aspectos,* Cuadernos penales José María Lidón, número 42007, Bilbao, Universidad de Deusto, pp. 227 y ss.

28 Véase Morón Lerma, «Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos», pp. 103 y 104.

29 Véase sobre la exigencia de este elemento subjetivo de lo injusto, Rueda Martín, *Protección penal de la intimidad personal e informática,* pp. 81 y ss.

reservados de personas jurídicas, o al hacker que accede al sistema informático de una empresa que almacena secretos de empresa, o al hacker que accede a un sistema informático militar que almacena información relevante de la seguridad interior y exterior del estado, con el simple deseo de cumplir ese reto? Las respuestas tienen que ser negativas si se realiza una interpretación teleológico sistemática del posible apartado 3º del artículo 197 del Código penal. Al mismo tiempo se plantea otro interrogante: ¿es necesario vincular un tipo penal como el indicado a la protección penal de bienes jurídicos como la intimidad personal y familiar, el patrimonio, etc., para legitimar la intervención del Derecho penal? Para tratar estas cuestiones vamos a abordar el estudio del bien jurídico protegido en un tipo penal que castigue el acceso ilícito a un sistema informático.

## III. EL BIEN JURÍDICO PROTEGIDO EN EL ACCESO ILÍCITO A UN SISTEMA INFORMÁTICO

Como se ha apuntado al comienzo desde un punto de vista político criminal se plantea la duda sobre la necesidad de criminalizar las conductas de hacking, si no van acompañadas de un ulterior fin relevante penalmente añadido al mero deseo de curiosidad y/o de demostración de pericia informática en el hacker. Algunos autores, como Morón Lerma, sí exigen la necesidad de añadir un fin ilícito a estas conductas de hacking para que intervenga el Derecho penal, de modo que estas conductas de simple acceso no deberían encontrar una respuesta jurídica en el ámbito del Derecho penal sino en el ámbito del Derecho administrativo sancionador, como, por ejemplo, en la Ley Orgánica 15/1999, de Protección de Datos Personales[30]. El tratamiento de esta cuestión nos obliga a plantearnos cuál es el bien jurídico protegido en la tipificación como delito de estos comportamientos de hacking, que nos condicionará después la respuesta a cuestiones tales como la exigencia de una finalidad jurídico penalmente añadida al simple deseo de curiosidad y/o

[30] Véase Morón Lerma, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, pp. 74 y ss.
Sin embargo, no desconoce esta autora que la tutela ofrecida por la LOPDP y sus Reglamentos de desarrollo se proyecta sólo sobre un sector de la delincuencia informática y, por tanto, y en esa medida, deviene insuficiente. A juicio de dicha autora esta Ley puede ser un cauce idóneo para sancionar buena parte de las conductas de hacking; véase, la misma, ob. cit., pp. 76, 77 y 78.

de demostración de pericia informática en el hacker y si es necesario adelantar la barrera de intervención del Derecho penal para tipificar las conductas de hacking como un delito autónomo.

Antes de comenzar conviene poner de relieve qué propuestas de bien jurídico protegido se han realizado en aquellos países que han adoptado en su legislación penal este comportamiento de accesos ilícitos a sistemas informáticos. Por ejemplo, Fiandanca y Musco en Italia consideran que se protege un interés que se sintetiza en la exigencia de que el uso de un sistema informático se produzca en unas condiciones de libertad y autonomía tales que permitan la integridad y la reserva del sistema mismo y de los datos allí recogidos; el bien jurídico protegido en el artículo 615 ter del Código penal italiano es el denominado "domicilio informático" entendido como la extensión virtual del sujeto titular de un sistema informático[31]. En Alemania el bien jurídico protegido en el § 202a del Código penal es una cuestión discutida. Möhrenschlager apunta que 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 los datos, que pone de manifiesto tal interés mediante el aseguramiento. Sin embargo, a su juicio, no es preciso que los datos protegidos constituyan secretos en sentido material, dejando abierta el legislador la cuestión de si se protegen también los intereses del individuo afectado por el contenido de los datos[32]. Por su parte Schünemann señala que el bien jurídico protegido en este tipo delictivo es el poder de disposición sobre la información contenida en los datos. En opinión de este autor el § 202a no presupone en particular una lesión del ámbito secreto o vital personal, sino que protege también intereses económicos o de otra clase[33].

La cuestión en torno a cuál es el bien jurídico protegido en esta clase de comportamientos no es pacífica ni en la doctrina ni en el legislador. Morón Lerma estima que asistimos a «un nuevo valor social, un interés de nuevo cuño, cifrado en la seguridad de los sistemas informáticos, o en la seguridad informática, o en la seguridad en el funcionamiento de dichos sistemas informáticos». A juicio de esta autora «parece emerger un

---

31 Véanse Fiandanca, Musco, *Diritto penale, Parte speciale, Volume II, tomo primo, I delitti contro la persona*, 1ª ed., Zanichelli editore, Bologna, 2006, pp. 244 y 245; Garofoli, *Manuale di diritto penale, Parte speciale II,* Dott. A. Giufrè Editore, Milano, 2005, p. 209.

32 Véase Möhrenschlager, «El nuevo Derecho penal informático en Alemania», *Delincuencia informática,* Mir Puig (Comp.), PPU, Barcelona, 1992, p. 137.

33 Véase Schünemann, «§ 202a», núm. marginal 2, pp. 65 y 66.

interés difuso, inmaterial, digno de tutela, pero que, en ningún caso, puede ser identificado, apriorísticamente, con un bien jurídico merecedor de protección penal»[34]. Otro sector doctrinal considera que la seguridad en los sistemas informáticos es el bien jurídico protegido en estos comportamientos, merecedor de protección penal, de carácter supraindividual y difuso[35]. Ahora bien, con carácter general, estas definiciones de bienes jurídicos que hacen referencia a la seguridad se caracterizan, de una manera explícita o implícita, por la descripción de una situación de ausencia de riesgos o de lesión para determinados bienes jurídicos como en este caso el patrimonio, la capacidad competitiva de la empresa, la propiedad intelectual, la intimidad personal y familiar, etc. Sin embargo, el valor de la seguridad como bien jurídico no le dota de autonomía, es decir, le impide atribuir a este substrato un valor homogéneo, unitario y autónomo porque no hay una seguridad en sí misma si no es puesta en relación con estos otros bienes jurídicos[36],[37].

Un sector doctrinal va más lejos y ha afirmado la existencia de un nuevo bien jurídico protegido, estrictamente informático, que es objeto de lesión o puesta en peligro en todos los delitos informáticos: la confiden-

---

[34] Véase Morón Lerma, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, p. 85; la misma, «Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos», p. 106.

[35] Véanse Gutiérrez Francés, *Fraude informático y estafa*, Madrid, 1991, pp. 619-620; la misma, «El intrusismo informático (Hacking): ¿Represión penal autónoma?», p. 1183; Mir Puig, «Sobre algunas cuestiones relevantes del derecho penal en internet», *Internet y Derecho penal*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2002, p. 303.

[36] Como apunta González Rus «tal como aparece concebida y formulada, la seguridad informática no tiene aún, a mi juicio, un contenido sustancial lo suficientemente elaborado y preciso como para permitir una construcción certera de la tutela penal. Prueba de ello es que unas veces se la relaciona con el honor, el patrimonio y la intimidad, y otras, además, con la libertad de información, el secreto de las comunicaciones, la libertad de expresión, etcétera, lo que dice bastante de la ambigüedad del concepto»; véase González Rus, «Precisiones conceptuales y político-criminales sobre la intervención penal en Internet», *Delito e informática: algunos aspectos,* Cuadernos penales José María Lidón, número 42007, Bilbao, Universidad de Deusto, p. 21.

[37] Asimismo indica Soto Navarro que las propuestas doctrinales que conceptualizan los bienes jurídicos colectivos en torno a la idea de protección de expectativas de seguridad y confianza, renuncian a la búsqueda de criterios objetivos que permitan fijar el daño social y consideran motivo suficiente para incriminar la aparición de actitudes de preocupación generalizada ante cierto tipo de conductas. A su juicio estas concepciones no garantizan la lesividad verificable en el caso concreto del comportamiento verificado; véase Soto Navarro, *La protección penal de los bienes colectivos en la sociedad moderna,* Comares, Granada, 2003, p. 236.

cialidad, integridad y disponibilidad de los datos y sistemas informáticos, de manera que estaremos ante un delito informático cuando se realice una conducta que lesione o ponga en peligro dicho bien jurídico[38]. Este objeto de protección se encuentra expresado en el preámbulo del Convenio del Consejo de Europa sobre Cibercriminalidad (Budapest, 23 de noviembre de 2001), donde se indica que «*es necesario para prevenir las acciones que suponen un atentado a la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y datos, así como el uso fraudulento de tales sistemas, redes y datos, velando por la incriminación de aquellos comportamientos descritos en el presente convenio*». Asimismo en la comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, titulada "Seguridad de las redes y de la información: propuesta para un enfoque político europeo" se define la seguridad de las redes y de la información como «*la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes ofrecen o hacen accesibles*». Además estudios técnicos sobre seguridad informática recogen la necesidad de proteger la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos[39].

Desde mi punto de vista esta es la línea correcta para definir el bien jurídico protegido en la tipificación de las conductas que consisten en un acceso ilícito a sistemas informáticos, si bien es cierto que es necesario distinguir, por un lado, la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos y, por otro lado, de los datos propiamente dichos. En nuestro Código penal ya se protege la obtención, la utilización o modificación de los datos que se almacenen en un sistema

---

[38] Véanse Rodríguez Mourullo, Alonso Gallo, Lascuraín Sánchez, «Derecho penal e internet», p. 260, 261, 262 y 269; Sieber, «Legal Aspects of Computer-Related Crime in the Information Society —Comcrime-Study—, prepared for the European Commission by Frof. Dr. Ulrich Sieber, versión de enero de 1998, p. 42, se refiere también a la integridad del sistema informático que resulta vulnerada con estas conductas de hacking.

[39] Véanse Ribagorna Garnacho, «Seguridad de las tecnologías de la información», *Ámbito jurídico de las tecnologías de la información,* Consejo General del Poder Judicial, 1996, pp. 307 y ss.; Longstaff, Ellis, Hernan, Lipson, McMillan, Pesante, Simmel, «Security of the Internet», *The Froehlich/Kent Encyclopedia of Telecommunications*, Marcel Dekker, New York, 1997, vol. 15, pp. 231-255.

informático mediante diversos tipos delictivos en función de la naturaleza de tales datos (artículos 197, 200, 248, 256, 263.2, 270, 278 ó 598 del Código penal), lo que parece sistemáticamente más correcto. Nos vamos a centrar, exclusivamente en la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, entendiendo por tales, como se indica en el artículo 1 del Convenio del Consejo de Europa sobre Cibercriminalidad «*a todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, al ejecutar un programa, el tratamiento automatizado de datos*». A continuación indagaremos tanto en la necesidad de la existencia de este bien jurídico protegido como en su autonomía.

El Derecho Penal es un sector del ordenamiento jurídico que tiene encomendada la misión de proteger los bienes vitales fundamentales del individuo y la comunidad, los cuales son elevados por la protección de las normas del Derecho a la categoría de bienes jurídicos[40]. Los bienes jurídicos no tienen una entidad material o física sino que, por el contrario, son valores ideales que se atribuyen por la comunidad social a determinados objetos, cosas, situaciones o relaciones en virtud de su aptitud e idoneidad instrumental para la satisfacción de necesidades individuales y colectivas[41]. Estas necesidades y los intereses que satisfacen ya sean individuales o colectivos son además plurales, variados y, a menudo, también contrapuestos. Sin embargo, el bien jurídico debe ser una entidad libre de conflictos y antagonismos, pues en cuanto instrumento social y políticamente sancionado y dispuesto para la satisfacción de

[40] Véase Cerezo Mir, *Curso de Derecho penal español, Parte General, I. Introducción*, 6ª ed., Tecnos, Madrid, 2004, p. 13.

[41] A los efectos que aquí nos interesan acogemos la noción de necesidad de Terradillos Basoco para quien «las necesidades son expresión de valores y cuanto más universales sean éstos, más radicales serán aquéllas. De otro modo no tendría ningún sentido acudir a este criterio que llevaría a un burdo utilitarismo afectado por las mismas limitaciones que las inherentes a la idea de interés. Pero parece atractivo tomar a la necesidad como punto de referencia, pues ello nos permite, de entrada, eliminar los riesgos de postergación del individuo… o de utilización ético-ideológica del Derecho penal… El concepto de necesidad contiene además elementos de generalidad y contrastabilidad que le hacen especialmente apto para ser la base de un discurso racional». Véase Terradillos Basoco, «La satisfacción de necesidades como criterio de determinación del objeto de tutela jurídico-penal», *Revista de la Facultad de Derecho de la Universidad Complutense*, nº. 63, 1981, p. 137. Más adelante concluye que «una política criminal alternativa que pretenda no ser autoritaria ha de limitarse, hoy, a la defensa, de las posibilidades reales de participación igualitaria y ha de tender, por ello, a la satisfacción del máximo de necesidades del máximo número de ciudadanos»; véase el mismo, ob. cit., p. 140.

necesidades e intereses plurales[42], el bien jurídico, como afirma *Bustos Ramírez*, surge como una síntesis normativa (fijada por el ordenamiento jurídico) de una relación social determinada y dinámica[43]. Lo que interesa salvaguardar, entonces, son las relaciones sociales mismas, la posición concreta que en ella ocupan los individuos, su intermediación con objetos y entes, y sus transformaciones por la interacción social. Los bienes jurídicos, concluye *Bustos Ramírez*, lo que hacen es plasmar de una forma concreta este complejo real social que interesa proteger[44].

Los bienes jurídicos configuran un espacio social que delimita, a su vez, las condiciones necesarias para que otros bienes jurídicos involucrados en dicho espacio, se desenvuelvan correctamente. Cuando estas condiciones necesarias para el desenvolvimiento correcto de los bienes jurídicos se desarrollan con normalidad, posibilitan a los bienes unas mayores posibilidades de rendimiento y aprovechamiento. La normalidad en el desarrollo de estas condiciones necesarias puede, incluso, acarrear la subordinación absoluta de un bien jurídico al cumplimiento de la función social de otro[45]. En este espacio social se puede constatar la existencia de dos clases de bienes jurídicos.

a) Por un lado, existen unos bienes jurídicos de corte clásico cuyas notas más importantes son su fácil determinación, su directa vinculación a la persona en sus relaciones específicas de modo que afectan a las bases mismas de existencia del sistema social, esto es, a las personas y están referidos a las relaciones de una persona con otra, de ahí que sean de tan fácil y elemental delimitación[46]. Estos

---

42 Véase la noción de necesidad en este contexto desarrollada por Terradillos Basoco, «La satisfacción de necesidades como criterio de determinación del objeto de tutela jurídico-penal», pp. 136 y ss., siguiendo a A. Heller.

43 Véanse Bustos Ramírez, «Del estado actual de la teoría del injusto», *Control social y sistema penal*, PPU, Barcelona, 1987, p. 138; Bustos Ramírez/Hormazábal Malarée, *Lecciones de Derecho penal*, Parte General, Editorial Trotta, Madrid, 2006, pp. 71 y ss.

44 Véase Bustos Ramírez, «Política criminal e injusto. (Política criminal, bien jurídico, desvalor de acto y de resultado)», *Control social y sistema penal*, PPU, Barcelona, 1987, p.166.

45 Véase sobre estas tesis, más ampliamente, Gracia Martín, *Fundamentos de dogmática penal. Una introducción a la concepción finalista de la responsabilidad penal*, Atelier, Barcelona, 2006, pp. 215 y ss., 216 y ss, 224 y ss.

46 Véase Bustos Ramírez, «Perspectivas actuales del Derecho Penal Económico», *Política criminal y reforma penal. Homenaje a la memoria del Profesor Dr. D. Juan del Rosal,* Editorial Revista de Derecho privado, Editoriales de Derecho Reunidas, Madrid, 1993, pp. 213 y 214.

bienes jurídicos, con carácter general, no admiten quedar involucrados en el quehacer cotidiano de las relaciones sociales y este es el motivo por el que sus afecciones suelen ser de carácter estrictamente personal y puntual[47]. En efecto, la vida, la intimidad personal y familiar o el patrimonio son bienes jurídicos que responden a tales características y que se denominan bienes jurídicos individuales.

b) No obstante, por el dinamismo que ha adquirido la sociedad moderna se han ido configurando unos bienes jurídicos que presentan múltiples dificultades para su determinación y que han recibido la denominación de "bienes jurídicos colectivos"[48]. Una nota característica de estos bienes jurídicos, entre otras[49], es que éstos están ligados al funcionamiento del sistema ya que no se trata sólo de relaciones sociales básicas dentro del sistema y configuradoras del orden social[50]. Ahora bien, estos bienes jurídicos no constituyen una categoría que está por encima del individuo o que va más allá de él, sino que hay «que definirlos a partir de una relación social basada en la satisfacción de necesidades de cada uno de los miembros de la sociedad o de un colectivo y en conformidad con el funcionamiento del sistema social»[51]. Este grupo de bienes jurídicos aparecen como

---

47 Véase Bustos Ramírez, «Los bienes jurídicos colectivos. (Repercusiones de la labor legislativa de Jiménez de Asúa en el Código Penal de 1932)», *Revista de la Facultad de Derecho de la Universidad Complutense*, nº. 11, p. 158. Naturalmente determinados bienes jurídicos, ya sean estos individuales o colectivos, pueden resultar afectados al encontrarse involucrados de un modo consustancial en una actividad social valorada positivamente por la utilidad general que reporta. Estas afecciones no constituyen un desvalor penal del resultado porque son socialmente adecuadas. Sobre esta tesis, véanse, Rueda Martín, *La teoría de la imputación objetiva del resultado en el delito doloso de acción. (Una investigación, a la vez, sobre los límites ontológicos de las valoraciones jurídico-penales en el ámbito de lo injusto)*, J. Mª. Bosch, Barcelona, 2001, pp. 247 y ss., 251 y ss., 278 y ss.; Gracia Martín, «El finalismo como método sintético real-normativo para la construcción de la teoría del delito», *Revista Electrónica de Ciencia Penal y Criminología 06-07 (2004)*, pp. 17 y ss.

48 Se ha optado por esta denominación bastante utilizada en la doctrina frente a otras denominaciones porque, como indica Soto Navarro, el adjetivo "colectivo" denota la dualidad de "ser perteneciente o relativo a cualquier agrupación de individuos"; véase Soto Navarro, *La protección penal de los bienes colectivos en la sociedad moderna*, pp. 193 y 194.

49 Sobre las características de los bienes jurídicos colectivos, véase el estudio de Soto Navarro, *La protección penal de los bienes colectivos en la sociedad moderna*, pp. 193 y ss.

50 Véase Bustos Ramírez, «Los bienes jurídicos colectivos. (Repercusiones de la labor legislativa de Jiménez de Asúa en el Código Penal de 1932)», p. 158.

51 Véase Bustos Ramírez, «Los bienes jurídicos colectivos. (Repercusiones de la labor legislativa de Jiménez de Asúa en el Código Penal de 1932)», p. 159.

complementarios, desde una perspectiva material, de otros bienes jurídicos que no tienen que ser, exclusivamente, individuales; es decir, tienen que prestar una serie de utilidades a otros bienes jurídicos[52]. La función de los bienes jurídicos colectivos, de prestar utilidades a otros bienes jurídicos, a juicio de *Gracia Martín*, se bifurca en dos direcciones, de modo que podemos hablar de una doble función según que contemplemos los aspectos de ésta que podemos llamar, respectivamente, negativo y positivo[53]. Por un lado, hay que destacar una función negativa de contención de riesgos para determinados bienes jurídicos reconocida, unánimemente de forma implícita o explícita, en la doctrina lo que explica su relación de complementariedad[54]. Por otro lado, existe asimismo una función positiva de creación y configuración de espacios que delimiten las condiciones en las que los bienes jurídicos a los que complementan pueden cumplir realmente una función social para todos los ciudadanos y que les dota de autonomía[55]. Ambas funciones están estrechamente entrelazadas y sólo por razones expositivas se distinguen. Tampoco debe olvidarse que una vez reconocido por el ordenamiento un bien jurídico colectivo, con carácter general, debe

---

52 Véase Bustos Ramírez, «Los bienes jurídicos colectivos. (Repercusiones de la labor legislativa de Jiménez de Asúa en el Código Penal de 1932)», p. 159. Este autor, sin embargo, se refiere a la relación de complementariedad entre los bienes jurídicos individuales y los colectivos. A mi juicio dicha relación de complementariedad se establece con carácter general entre los bienes jurídicos colectivos y otros bienes jurídicos ya sean individuales o colectivos.
Una consecuencia de esta nota de los bienes jurídicos colectivos es la vertiente positiva del carácter indisponible de dichos bienes jurídicos, contemplada como la posibilidad de aprovechamiento por todos, sin que nadie pueda ser excluido y sin que el aprovechamiento individual obstaculice ni impida el aprovechamiento por otros; véase Hefendehl, *Grund un Grenzen des Schutzes kollektiver Rechtsgüter im Strafrecht,* Carl Heymanns Verlag KG, Köln, 2002, pp. 21, 126-128.

53 Véase Gracia Martín, «Nuevas perspectivas del Derecho penal tributario. (Las "funciones del tributo" como bien jurídico)», *Actualidad Penal, nº. 10, 1994,* pp. 210 y 211. En la p. 211, nota 103, pone como ejemplo de bien jurídico colectivo la seguridad e higiene en el trabajo, pues no sólo cumple una función negativa de contención de riesgos para los bienes vida, integridad física y salud, sino la positiva de delimitar un espacio social en que dichos bienes más allá de su existencia material alcancen la calidad adecuada a la dignidad humana.

54 Véase Bustos Ramírez, «Los bienes jurídicos colectivos. (Repercusiones de la labor legislativa de Jiménez de Asúa en el Código Penal de 1932)», pp. 158 y ss.

55 La doctrina mayoritaria se pronuncia a favor de la autonomía de los bienes jurídicos colectivos. Como ha afirmado Soto Navarro la función social de los bienes jurídicos colectivos permite conceptuarlos de forma autónoma; véase Soto Navarro, *La protección penal de los bienes colectivos en la sociedad moderna,* p. 231.

admitirse su independencia y su posibilidad de lesión sin necesidad de exigir un efecto simultáneo sobre bienes jurídicos individuales.

El bien jurídico aludido y que se refiere a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos constituye una barrera de contención de riesgos para otros bienes jurídicos que se puedan encontrar involucrados en la función social que desempeñen tales sistemas y redes informáticos: la intimidad personal y familiar, el patrimonio, etc.[56]. Así, por ejemplo, el bien jurídico intimidad personal y familiar puede encontrarse involucrado en la función social que desempeña el bien jurídico relativo a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos. Con respecto al bien jurídico intimidad personal y familiar, el Código penal organiza un sistema de tipos delictivos recogidos en el artículo 197. En el apartado 2 de este tipo delictivo[57], la protección penal de la intimidad personal y familiar se lleva a cabo a través de unas acciones consistentes, por una parte, en el acceso y la alteración o, por otra parte, en el acceso y la utilización de los datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado por parte de una persona no autorizada, de manera que se realizará la conducta típica del artículo 197.2 del Código penal siempre y cuando se actúe "en perjuicio del titular de los datos o de un tercero". Estas conductas lesionan el bien jurídico intimidad personal y familiar de una típicamente relevante[58], pero también hay que constatar que con tales compor-

[56] En relación con el bien jurídico definido como la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, Mourullo, Alonso y Lascuraín apuntan que éste «tiene un carácter instrumental con respecto a otros intereses jurídicamente relevantes, sean éstos objeto directo de protección por el derecho penal o no»; véanse Rodríguez Mourullo, Alonso Gallo, Lascuraín Sánchez, «Derecho penal e internet», p. 261. Véase también la exposición realizada en la p. 269.

[57] En el artículo 197.2 se establece que: «*2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán, a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero*».

[58] Véase Rueda Martín, *Protección penal de la intimidad personal e informática,* p. 77. En este ejemplo, en la medida que se encuentra involucrado el bien jurídico intimidad personal y familiar en estos comportamientos a través de la alteración de los datos reservados contenidos en ese sistema informático, el simple acceso al sistema informático constituirá

tamientos se produce la lesión de la confidencialidad, integridad y disponibilidad de los sistemas informáticos mediante el simple acceso a los mismos, tanto si se realiza en perjuicio del titular de los datos o de un tercero como si se realiza con la finalidad de descubrir fallos o puertas falsas en dichos sistemas informáticos que albergan archivos de datos reservados. Si se registran unos datos reservados de carácter personal o familiar de una persona en un fichero telemático, la protección del bien jurídico intimidad personal y familiar se reforzará y se asegurará si se protege penalmente la confidencialidad, la integridad y la disponibilidad del sistema que albergue dicho fichero. Lo mismo sucede respecto al bien jurídico relativo a la capacidad competitiva de la empresa, dada la posición ventajosa en las relaciones del tráfico económico que ostenta el titular de la información, entendida como valor económico[59], protegido en el artículo 278.1[60], el patrimonio protegido en el artículo 264.2[61] del Código penal o incluso la seguridad y/o defensa nacional en relación con el artículo 598 del Código penal[62].

---

una tentativa del artículo 197.2 del Código penal, si concurre el elemento subjetivo de lo injusto indicado.

59 Véase Morales Prats/Morón Lerma, *Comentarios al Nuevo Código Penal*, Quintero Olivares (Dir.)/Morales Prats (coord.), Aranzadi, Pamplona, 4ª ed., 2005, p. 1415.

60 El artículo 278.1 del Código penal establece que «*El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses*». El empleo de alguno de los medios descritos en el artículo 197.1 puede suponer el acceso al sistema informático de una empresa que almacene datos o documentos electrónicos que contengan secretos de la misma. Como sucedía con el tipo comentado anteriormente (artículo 197.2) si en esta acción no concurre el elemento subjetivo de descubrir un secreto de empresa, quedará impune dicho acceso.

61 El artículo 264.2 del Código penal establece que «*La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos*». Respecto del bien jurídico protegido en el citado precepto es necesario indicar que hay una discusión doctrinal, ya que entre otras opiniones un sector estima que es el patrimonio [véanse, por ejemplo, González Rus, «Daños a través de internet y denegación de servicios», p. 1471; Mata y Martín, *Delincuencia informática y Derecho penal*, Edisofer, Madrid, 2001, pp. 77 y ss.], mientras que otro sector considera que se protege la integridad o disponibilidad de los datos y sistemas informáticos [véanse, por ejemplo, Rodríguez Mourullo, Alonso Gallo, Lascuraín Sánchez, «Derecho penal e internet», pp. 282 y ss.].

62 En relación con este bien jurídico, véase, Morales García, *Comentarios al Nuevo Código Penal*, Quintero Olivares (Dir.)/Morales Prats (coord.), Aranzadi, Pamplona, 4ª ed., 2005, p. 2558.
El artículo 598 del Código penal establece que «*El que, sin propósito de favorecer a una potencia extranjera, se procurare, revelare, falseare o inutilizare información legalmente calificada*

En estos ejemplos y en otros se pone de relieve que los mencionados bienes jurídicos se verán más protegidos en tanto en cuanto se garantice la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos en los que se involucren. Este bien jurídico actúa como una barrera de contención de riesgos para otros bienes jurídicos como los citados. Ahora bien como se ha indicado antes, para que un objeto, situación o relación adquiera la categoría de bien jurídico colectivo es preciso que, además de esa función negativa de contención de riesgos, cumpla una función positiva de creación y configuración de espacios que delimiten las condiciones en que los bienes jurídicos a los que complementan puedan cumplir realmente su función social[63]. Vamos a analizar a continuación si el bien jurídico que estamos estudiando desarrolla esta función positiva.

Si nos detenemos en el funcionamiento del sistema social en la actualidad es innegable la importancia que han adquirido las nuevas tecnologías de la información y de la comunicación (TIC´s), con la utilización de redes y sistemas de tratamiento de la información, como medio de crecimiento económico y desarrollo social[64]. Las TIC´s se han esténdido y se han enraizado en nuestras modernas sociedades de tal manera que han conformado unas estructuras y unas relaciones comerciales, administrativas, laborales, formativas, etc., que trascienden el ámbito estrictamente económico y que son radicalmente nuevas[65]. La generalización de las TIC´s ha permitido la aparición de nuevos escenarios como, por ejemplo, el comercio electrónico (*e-commerce*), el acercamiento de los

*como reservada o secreta, relacionada con la seguridad nacional o la defensa nacional o relativa a los medios técnicos o sistemas empleados por las Fuerzas Armadas o las industrias de interés militar, será castigado con las penas de prisión de uno a cuatro años*».

63 Véase Gracia Martín, «Nuevas perspectivas del Derecho penal tributario. (Las "funciones del tributo" como bien jurídico)», pp. 210-211.

64 Véanse Romeo Casabona, *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información,* Fundesco, 1987, Madrid, pp. 19 y ss.; Gutiérrez Francés, «Delincuencia económica e informática en el nuevo Código penal», pp. 250 y 274. Al comienzo de la Exposición de Motivos de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (BOE de 23 de junio de 2007), se indica que «las tecnologías de la información y las comunicaciones están afectando también muy profundamente a la forma e incluso al contenido de las relaciones de los seres humanos entre sí y de las sociedades en que se integran».

65 Véase Ribagorna Garnacho, «Seguridad de las tecnologías de la información», p. 310. Estas estructuras y relaciones se pueden mantener mediante el ordenador e internet, pero también mediante SMS o la Televisión Digital. En cualquier caso en un futuro más o menos inmediato pueden aparecer otros canales que aún no están disponibles hoy en día.

bancos a los clientes (*home-banking),* la gestión electrónica de los recursos de las empresas (*e-management*) o la gestión doméstica (*domótica*)[66]. En estos escenarios se involucran bienes jurídicos tales como el patrimonio, la intimidad personal y familiar o la capacidad competitiva de la empresa, de manera que los sistemas de información y comunicación permiten su desarrollo en las modernas sociedades.

Nuestra organización social (la Administración pública, el sistema financiero, el sistema sanitario, las infraestructuras básicas de transporte, las empresas, los particulares, etc.) ha pasado a depender de forma extraordinaria de unos sistemas y redes informáticos, por lo que de los riesgos que se derivan de su vulnerabilidad[67] ha surgido, consecuentemente, un interés en la seguridad de la utilización de las TIC´s, que se encuentra expresado, por ejemplo, en la reciente Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos de la siguiente manera, de modo que con carácter general, el Derecho al proteger las TIC´S reconoce su valor social positivo como necesario y vinculante para un correcto funcionamiento del sistema social. En el artículo 1.2 se establece que «*las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias*». Asimismo en el artículo 3.3 se dispone como fin de la mencionada Ley, «*crear las condiciones de confianza en el uso de medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos*»[68].

---

[66] Véase Salom Clotet, «Delito informático y su investigación», *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?,* Velasco Núñez (Dir.), Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, 2006, pp. 93 y ss.

[67] Rodríguez Mourullo, Alonso Gallo, Lascuraín Sánchez señalan asimismo que «los estudios doctrinales y los informes de agencias internacionales y de organizaciones públicas y privadas han advertido una y otra vez sobre los riesgos derivados de la vulnerabilidad de unos sistemas y redes informáticos de los que toda la organización social (el sistema financiero, las infraestructuras básicas, las empresas, los organismos públicos, los particulares) ha pasado a depender de forma extraordinaria»; véanse los mismos, «Derecho penal e internet», p. 257.

[68] En la reciente Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos se contempla como uno de sus principios generales en el artículo 4, f)

La utilización de las TIC´s en los ámbitos reseñados ha conducido al surgimiento de unos intereses que tienen unas notas comunes. Por una parte, los particulares tienen interés en que se proteja la integridad o la confidencialidad de los sistemas informáticos al margen de los contenidos de naturaleza personal o patrimonial que se almacenen en los mismos[69], como un instrumento que facilita sus relaciones sociales, económicas, etc. También las empresas tienen en los modernos sistemas informáticos un instrumento que facilita y potencia su actividad económica y que supone una notable ventaja competitiva en el mercado[70], y tienen interés en que se proteja no sólo el contenido de la información que almacenan, sino además la confidencialidad y la integridad de dicho sistema. Del mismo modo, los organismos públicos tienen interés en la protección de los sistemas informáticos que almacenan los datos personales de todo tipo o que regulan las relaciones de las distintas administraciones con los administrados, fundamental para el debido funcionamiento de las mismas. Además de este interés generalizado debemos observar que la realización de diversas operaciones económicas, financieras, empresariales, laborales, administrativas, etc. por parte de los usuarios tiene que llevarse a cabo de una forma práctica pero segura, es decir, garantizando tanto la disponibilidad del sistema informático como la identidad o la autenticación de la persona que accede a dicho sistema. Los usuarios (administrados, empresas, etc.) tienen interés en que cumpliendo unos determinados requisitos se pueda acceder a dichos sistemas informáticos para llevar a cabo aquellas operaciones que sean relevantes, sin que se interpongan demasiados obstáculos. En suma nos encontramos con la convergencia de todos estos intereses que explican, por una parte, la función social de los sistemas de información y comunicación como importantes herramientas de crecimiento y desarrollo económico y social; y, por otra parte, explican la demanda de medidas de seguridad de carácter técnico y de organización en su utilización, que incluyen mecanismos y prácticas profesionales que permiten tanto un uso

el «principio de seguridad en la implantación y utilización de los medios electrónicos por las Administraciones Públicas».

69 Véase Gutiérrez Francés, «Delincuencia económica e informática en el nuevo Código penal», p. 301.

70 Véase Gutiérrez Francés, «Delincuencia económica e informática en el nuevo Código penal», p. 274, quien destaca que la informatización para las empresas implica contabilidades, carteras de clientes, balances, informes y proyectos empresariales, estrategias de mercado, procedimientos económicos o tecnológicos de carácter reservado, o datos de investigación y desarrollo de tecnología.

continuado de las tecnologías como el establecimiento de acciones destinadas a interrumpir o sabotear su funcionamiento o la interpretación de datos elaborados y tratados por otros[71].

Esta seguridad en la utilización de los sistemas informáticos de forma más o menos generalizada se manifiesta en la confidencialidad, integridad y la disponibilidad de los sistemas de comunicación e información[72], y que constituye propiamente el bien jurídico a proteger en la tipificación de conductas de acceso ilícito a sistemas informáticos. La integridad de un sistema informático alude a su utilización con las pertinentes modificaciones del contenido de la información almacenada en el sistema por parte de la/s persona/s autorizada/s. La confidencialidad de dicho sistema se basa en que su utilización corresponde exclusivamente a la/s persona/s autorizada/s. La disponibilidad hace referencia al control sobre la utilización de un determinado sistema por parte de la/s persona/s autorizada/s. De esta manera cuando un hacker penetra ilícitamente en un sistema informático ajeno, tanto si se han infringido medidas de carácter técnico como si no ha sido así, se encuentra en un espacio, el propio sistema, en el que su integridad se ha visto afectada porque la sola entrada y el consiguiente uso del sistema da lugar a modificaciones en los datos del mismo, junto con las alteraciones de tales datos para intentar borrar los rastros que pudieran identificarles. Asimismo la confidencialidad del sistema se ve afectada si se utiliza por parte de una persona que no está autorizada. Finalmente la disponibilidad del sistema se afecta cuando penetra una persona no autorizada. Se puede constatar que en estos supuestos de accesos ilícitos a un sistema informático se vulnera el bien jurídico expuesto con independencia de las ulteriores finalidades que haya perseguido el hacker con tales entradas.

Se suele afirmar, con carácter general, que estas conductas de hacking blanco son más beneficiosas que perjudiciales ya que revelan las deficiencias de los sistemas informáticos a los encargados de la seguridad de los mismos, a quienes también se favorece con la posterior comunicación de tales deficiencias con el fin

---

71 Sobre esta demanda de medidas de seguridad de carácter técnico y de organización, véase Morón Lerma, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, p. 48. En cuanto a las medidas de seguridad, desde un punto de vista técnico, véase la exposición realizada por Huidobro Moya/Roldán Martínez, *Seguridad en redes y sistemas informáticos*, Thomson Paraninfo, 2005.

72 Véase Ribagorna Garnacho, «Seguridad de las tecnologías de la información», pp. 312 y 313.

de fortalecer la seguridad de los mencionados sistemas. Al respecto cabe señalar, en primer lugar, que este argumento sólo es atendible si el hacker, una vez descubierta la vulnerabilidad de un sistema y producido el acceso, informa directamente a los administradores o a los encargados de la seguridad de los sistemas. El problema se centra más bien en que cuando se descubre una vulnerabilidad en un sistema aparece el denominado "exploit", que en el entorno hacker se refiere al método concreto de explotar una vulnerabilidad. Normalmente un "exploit" se presenta como un programa, que puede estar creado en cualquier lenguaje, y que aprovecha algún error del sistema operativo, por ejemplo, para obtener los privilegios del administrador y así tener un control total del sistema[73]. Estos "exploits" se publican en webs especializadas por lo que se difunden las vulnerabilidades descubiertas a través de diversas vías como los canales IRC (Internet Relay Chat) que los hackers establecen para dar a conocer sus accesos y sus operaciones, pero antes de publicarse se ofrece un tiempo a los administradores de los sistemas para que solucionen las vulnerabilidades descubiertas. La licitud de esta forma de proceder puede aceptarse porque, por una parte, muchas empresas de productos de seguridad disponen de bases de datos actualizadas con las vulnerabilidades, su descripción técnica y su solución. Por otra parte, los fabricantes de programas deben actualizar sus productos constantemente para evitar las vulnerabilidades que se van descubriendo[74] ya sea por sí mismos o por la comunicación de algún hacker. Lo que no puede aceptarse es que se haya descubierto la vulnerabilidad de un sistema y producido el acceso, no se informe de ningún modo a los administradores o a los encargados de la seguridad de los sistemas.

En segundo lugar, este mismo fin de encontrar fallos en los sistemas informáticos y de fortalecer, así, la seguridad de los sistemas informáticos, se consigue con la disposición de las necesarias medidas de seguridad de carácter técnico y de organización por parte de las empresas competentes, por lo que la función que un hacker ajeno al sistema realice se desempeñaría igualmente por personal adecuado y con garantías. En ocasiones se argumenta también que el hacking suele ser una actividad de estudio o de investigación y que por este motivo resulta exagerado criminalizar a aquellos hackers que persiguen únicamente aprender. Si se realizan estas actividades de estudio y de investigación puede solicitarse una autorización al administrador o encargado del sistema

[73] Véase Piqueres Castellote, «Conocimientos básicos en internet y utilización para actividades ilícitas», p. 62.

[74] Véase Piqueres Castellote, «Conocimientos básicos en internet y utilización para actividades ilícitas», p. 62.

informático, por lo que ya no sería un acceso ilícito siempre y cuando se cumplieran todos los requisitos para los que se otorga dicha autorización.

Del desarrollo de la función positiva del bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas informáticos se derivan algunas consecuencias que exponemos a continuación. En primer lugar, se justifica que no sea necesario añadir ninguna finalidad ilícita adicional a las conductas de hacking para que intervenga el Derecho penal, porque para constatar una perturbación en la función social del bien jurídico indicado no es necesario que concurra una finalidad específica adicional referida a la involucración de otros bienes jurídicos en el contexto en el que aquél desarrolle su función positiva. La existencia de una finalidad adicional nos ayudará sólo a delimitar los comportamientos ilícitos que se centran en la "información" almacenada, tratada y transmitida mediante un sistema informático[75], pero a mi juicio no es necesaria para delimitar las acciones que lesionen o pongan en peligro el bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas informáticos. Este bien merece la protección del ordenamiento jurídico y dada la importante función social que desempeña, se legitima la intervención del Derecho penal en su protección, así como en la represión de aquellos comportamientos que lo lesionen[76]. En segundo lugar, la incorporación de ulteriores exigencias objetivas para incriminar las conductas de hacking, como la vulneración de las medidas de seguridad del sistema, puede ser admitida desde un punto de vista político criminal como manifestación de una mayor gravedad de tales comportamientos.

---

[75] Véase Gutiérrez Francés, «Delincuencia económica e informática en el nuevo Código penal», pp. 274 y 275.

[76] Con la exposición que ha precedido a estas conclusiones se ha intentado responder a una pregunta central que ha planteado claramente González Rus: «si la informática e internet suponen factores de peligro adicional para los derechos e intereses individuales y sociales que no estén cubiertos (y que no puedan ser cubiertos) con la aplicación (y, eventualmente, con la complementación y ampliación) de las figuras delictivas actualmente disponibles dirigidas a la protección de bienes jurídicos personales, colectivos y generales. Sólo a partir de ahí podrá determinarse si es necesaria para la tutela de los bienes e intereses implicados en las redes de transmisión de datos e internet la creación de "nuevos" bienes jurídicos específicos de naturaleza informática»; véase González Rus, «Precisiones conceptuales y político-criminales sobre la intervención penal en Internet», p. 31.

## IV. PROPUESTA POLÍTICO CRIMINAL SOBRE LA CONSIDERACIÓN COMO DELITO DEL ACCESO ILÍCITO A UN SISTEMA INFORMÁTICO

### 1. Necesidad de la represión penal autónoma de las conductas de accesos ilícitos a sistemas informáticos

Una vez fundamentada la existencia y la autonomía del bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas informáticos, debemos apuntar argumentos que justifiquen la necesidad de represión penal autónoma de estas conductas de hacking. En este sentido encontramos los siguientes:

En primer lugar, cabe destacar la importancia de proteger penalmente y no sólo administrativamente la función social que desempeña el bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas informáticos. Ya hemos explicado que nuestra organización social (la Administración pública, el sistema financiero, el sistema sanitario, las infraestructuras básicas de transporte, las empresas, los particulares, etc.) ha pasado a depender de forma extraordinaria de la utilización de unos sistemas y redes informáticos, como medio de crecimiento económico y desarrollo social. En los últimos años el Derecho ha desplegado una regulación y protección de las nuevas tecnologías de la información y comunicación, y ha reconocido su valor social positivo como necesario y vinculante para un correcto funcionamiento del sistema social. Consecuentemente ha surgido también un interés en la seguridad de la utilización de las TIC´s desde diversos ámbitos, que se concreta en la confidencialidad, integridad y disponibilidad de los sistemas informáticos como bien jurídico protegido dotado de autonomía y que, además, sirve de barrera de contención de riesgos para otros bienes jurídicos que puedan verse implicados en la utilización de sistemas y redes informáticos.

En segundo lugar, elevar a la categoría de delito en nuestro Código penal esta clase comportamientos que consisten en acceder de manera ilícita a sistemas informáticos, supone una obligada armonización penal en este ámbito de nuestra legislación con la dispuesto en otros estados de la Unión Europea, en consonancia con lo establecido en la Decisión Marco 2005/222/JAI del Consejo de la Unión Europea de 24 de febrero

de 2005 relativa a los ataques contra los sistemas de información y del Convenio del Consejo de Europa sobre Cibercriminalidad de 23 de noviembre de 2001. Dicha armonización es necesaria además porque en estos comportamientos podemos encontrar una nota que le añade un especial grado de peligrosidad: su conexión internacional o transfronteriza, de modo que sus actuaciones pueden ir más allá de un ámbito geográfico concreto, y resulta sorprendente que en algún territorio un acceso ilegal a sistemas informáticos con independencia de la finalidad que haya tenido quien accede, resulte impune.

En tercer lugar, hay que tener en cuenta que, como afirma Romeo Casabona, el ciberespacio presenta unos perfiles de gran interés para el Derecho penal entre los que destaca la potencialidad multiplicadora de las acciones ilícitas y de sus efectos lesivos para los bienes jurídicos afectados[77]. Esta característica se puede apreciar con especial intensidad en las conductas de hacking, que como ha puesto de relieve un sector doctrinal tienen un efecto criminógeno[78]. Por ello y con carácter general, la informática se presenta en las sociedades modernas como una de las posibles fuentes de riesgos necesitados de control, y dada la gravedad de sus repercusiones sobre diferentes bienes jurídicos se legitima la intervención del Derecho penal.

### 2. Sistema de criminalización

Si nos planteamos el sistema de criminalización de estas conductas de hacking, el Derecho penal puede operar de dos maneras distintas[79]. En

---

[77] Véase Romeo Casabona, «De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal», *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Romeo Casabona coord., Comares, Granada, 2006, p. 4. También destacan, con carácter general, el factor criminógeno del procesamiento electrónico de datos, Sieber, *Computerkriminalität*, 1ª ed., Heymann, Munich, 1977, pp. 158 y ss.; Mata y Martín, *Delincuencia informática y Derecho penal*, p. 17, 24 y ss.; Morón Lerma, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, p. 75.

[78] Véase respecto de las conductas de hacking, Gutiérrez Francés, «El intrusismo informático (Hacking): ¿Represión penal autónoma?», pp. 1179 y ss.; la misma, «Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa», *Estudios de Derecho penal económico*, Tiedemann/Arroyo Zapatero editores, Ediciones de la Universidad de Castilla-La Mancha, 1994, p. 206.

[79] Véase, con carácter general, sobre la tipificación de conductas relacionadas con agresiones en conexión con sistemas informáticos, Romeo Casabona, «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», *Poder Judicial*, 2ª época, número 31, 1993, pp. 180 y 181.

primer lugar, mediante tipos específicos o «tipos de equivalencia» que contemplen la incriminación del mero acceso ilícito a sistemas informáticos en cada figura de delito para suplir las posibles insuficiencias. De esta forma se podría tipificar este comportamiento, por ejemplo, en relación con las conductas de los artículos 197, 200, 248, 256, 263.2, 270, 278 ó 598 del Código penal. Esta opción, sin embargo, plantea inconvenientes como el excesivo casuismo que conllevaría y el no adaptarse a la rapidez de los avances tecnológicos que no se previeran en un determinado momento y que impediría aplicar este delito a determinados ámbitos[80].

En segundo lugar, el sistema de criminalización de estas conductas de hacking se puede llevar a cabo a través del establecimiento de un nuevo tipo penal genérico que tipificara como delito el acceso ilícito a sistemas informáticos. Esta opción es la más idónea al adaptarse a las nuevas formas de criminalidad, si bien es cierto que implica buscar un adecuado lugar sistemático en nuestro Código penal. Desde un punto de vista sistemático decidirse por esta segunda opción supone plantearse la necesidad de formular un nuevo título en el Código penal dedicado a la delincuencia informática. Un capítulo de dicho título puede versar sobre los "Delitos contra los sistemas de información", en el que se contemple la protección penal de los sistemas informáticos y que aglutinaría aquellas conductas que lesionan el bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas informáticos[81]. Los comportamientos que se pueden estimar como delito pueden ser:

---

[80] Véanse Romeo Casabona, «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», p. 181 y sobre la posible intervención del Derecho penal en la red, con carácter general, Álvarez Vizcaya, «Consideraciones político criminales sobre la delincuencia informática: el papel del Derecho penal en la red», *Internet y Derecho penal*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, 2002, pp. 268 y ss.

[81] Véase también en un sentido similar la opinión de Morón Lerma que estima que si se introduce este tipo penal, habría que crear un título autónomo que castigue los atentados a los sistemas informáticos, en el que se ubicara éste y otros incidentes relativos a los mismos, como los daños a los datos y a los sistemas; véase Morón Lerma, «Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos», p. 107. Desde mi punto de vista es discutible que en un Título nuevo del Código penal dedicado a los "Delitos contra los sistemas informáticos" se incorporen conductas como las contempladas en el artículo 264.1 tanto del Proyecto de Ley Orgánica por la que se modifica la Ley orgánica 10/1995, de 23 de noviembre, del Código penal, de 15 de enero de 2007, como del Anteproyecto de reforma del Código penal, de 14 de noviembre de 2008: *«1. El que sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciere inaccesibles datos o programas informáticos ajenos, será castigado, en*

1) Los accesos ilícitos a sistemas informáticos. Por ello proponemos la siguiente tipificación de las conductas de hacking en nuestro Código penal:
«*El que por cualquier medio o procedimiento accediera sin autorización a un sistema de información ajeno o a una parte del mismo, será castigado con penas de prisión de tres meses a un año*».

2) Las conductas que suponen una obstaculización o interrupción del funcionamiento de los sistemas informáticos. En este sentido se puede recoger la propuesta de tipificación de algunas conductas contempladas en el artículo 264.2, 3 y 4 tanto del Proyecto de Ley Orgánica por la que se modifica la Ley orgánica 10/1995, de 23 de noviembre, del Código penal, de 15 de enero de 2007, como del Anteproyecto de reforma del Código penal presentado el 14 de noviembre de 2008:
«*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 impondrá la pena superior en grado a la respectivamente señalada en el apartado anterior 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. 2.º Haya ocasionado daños de especial gravedad o afectado a los intereses generales. 4. Cuando los delitos comprendidos en este artículo se hubieren cometido en el marco o con ocasión de las actividades de una persona jurídica y procediere la declaración de su responsabilidad penal de acuerdo con lo establecido en el artículo 31 bis de este Código, se le impondrá la pena de multa del tanto al duplo del perjuicio causado en los supuestos previstos en el apartados 1 y del tanto al décuplo en el supuesto del apartado 2*».

*consideración a la gravedad del hecho, con la pena de prisión de seis meses a dos años*». Este tema merece una reflexión más profunda al margen de lo estudiado en este trabajo: el bien jurídico protegido en las conductas de acceso ilícito a sistemas informáticos.