Doctrina

Vías para la tipificación del acceso ilegal a los sistemas informáticos (1)

Nuria Matellanes Rodríguez

Profesora de Derecho Penal de la Universidad de Salamanca

Revista Penal, n.º 22.—Julio 2008

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

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

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

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

1. Delimitación conceptual: significado del término «hacking»

La proliferación y diversidad de formas que pueden adoptar los ataques contra los sistemas de información constituye una de las características de la «criminalidad informática»[1]. En general, todas ellas han recibido la denominación genérica de «piratería informática».

De manera particular, el recurso a este término fue inicialmente aplicado a un caso delictivo en particular, es-

1. MORÓN LERMA, E.*: Internet y Derecho penal: hacking y otras conductas ilícitas en la red*, Aranzadi, Pamplona, 2002, pág. 39.

Seguimos la concepción de «delincuencia informática» como categoría criminológica, de carácter funcional, omnicomprensiva de una pluralidad de conductas, que sólo se relacionan entre sí por el hecho de encontrar en ellas un factor de abuso o extralimitación de las funciones propias que los sistemas informáticos. Sobre esta base, el abuso de las mismas bien puede consistir en atentar directamente contra ellas, o bien en utilizarlas como sede de vulneración de algún interés. En esta línea se sitúa de modo mayoritario la doctrina, ROMEO CASABONA, C.M.ª: *Poder informático y seguridad jurídica,* Fundesco, Madrid, 1988, pág. 41;

trictamente denominado «*cracking*», que se vincula a un modo concreto de vulneración de los derechos de propiedad intelectual consistente en romper, eliminando o neutralizando, el sistema informático de protección que impide su copia no autorizada, conducta que hoy se subsume en el art. 270 del Código Penal (incluso en su párrafo 3, que castiga la mera posesión del mecanismo que facilita la supresión o neutralización del dispositivo de protección del programa informático[2]). En la actualidad, el término «*cracking*» se extiende a toda clase de asaltos sobre máquinas o sistemas informáticos para ocasionar perturbaciones sobre dichos sistemas o para modificar o destruir datos. Es lo que se conoce como «vandalismo informático», «sabotaje informático», o de manera más genérica, «daños informáticos». Especifica GONZÁLEZ RUS este concepto destacando que, en todo lo caso, lo indispensable de esta conducta radica en la afección, deterioro o destrucción de los elementos lógicos del sistema informático, para lo cual las vías pueden ser variadas, abarcando desde la actuación sobre el *software* y afectando, por tanto, a archivos y ficheros que componen un sistema informático y que contienen programas, datos utilizados por el programa o documentos electrónicos generados por el programa, como la actuación sobre los elementos físicos o *hardware*, integrado por el conjunto de componentes mecánicos, eléctricos, magnéticos u ópticos que forman un ordenador o equipo informático[3]. Las conductas, en suma, consisten en una generalización del daño, que persigue el objetivo de causar un destrozo en el sistema afectado, inutilizándolo o suprimiéndolo, o destruyendo los datos almacenados en el mismo. En este caso, su encaje jurídico penal se encuentra en el art. 264 del Código Penal, integrador tanto de comportamientos de atentado o daños a sistemas como de daños a programas[4].

GUTIÉRREZ FRANCÉS, Mª.L.: *Fraude Informático y estafa*, Servicio de Publicaciones del ministerio de Justicia, Madrid, 1991, pág. 62, en torno a los fraudes informáticos en el Derecho español», *Actualidad Jurídica Aranzadi*, nº 11, abril de 1994, pág. 7; «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, Madrid, 1996, pág. 250; GALÁN MUÑOZ, A.: El fraude y la estafa mediante sistemas informáticos, Tirant lo Blanch, Valencia, 2005, pág. 35; «Expansión e intensificación del Derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática», *Revista Derecho y Proceso Penal*, nº 15, año 2006-1, pág. 17; en contra, ROVIRA DEL CANTO, E.: Delincuencia informática y fraudes informáticos, Comares, Granada, 2002, pág. 187; REYNA ALFARO, L.M.: «El bien jurídico en el delito informático», *Revista de Derecho Informático*, nº 33, 2001 (http://www.alfa-redi.org) = «La criminalidad informática: cuestiones para una reflexión inicial», *Actualidad Penal*, nº 21, 2002, pp. 539 y ss., que aglutinan a todos estos delitos bajo el paraguas de su afección a un único bien jurídico que definen como la información contenida y tratada informáticamente.

2. Su inclusión en el Derecho interno está plagada de respuestas críticas*;* así, vid. MIRÓ LLINARES, F.: *La protección penal de la propiedad intelectual en la sociedad de la información*, Dykinson, Madrid, 2003; «La protección penal de los derechos de explotación exclusiva sobre el software», *Revista Penal*, nº 13, 2004, pp. 98 y ss.; *Internet y delitos contra la propiedad intelectual,* Fundación Autor, Madrid, 2005, pág. 159.

Su incriminación se conecta a la tutela reclamada por la Directiva 91/250, de 14 de mayo de 1991, sobre la protección jurídica de programas de ordenador, cuyo artículo 7 establece que:

«… los Estados miembros, de conformidad con sus legislaciones nacionales, deberán adoptar medidas adecuadas contra las personas que cometan cualquiera de los actos mencionados en las letras siguientes:

a) la puesta en circulación de una copia de un programa de ordenador conociendo o pudiendo suponer su naturaleza ilegítima;

b) la tenencia con fines comerciales de una copia de un programa de ordenador, conociendo o pudiendo suponer su naturaleza ilegítima; o

c) la puesta en circulación o tenencia con fines comerciales de cualquier medio cuyo único propósito sea facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se hubiere utilizado para proteger un programa de ordenador».

3. GONZÁLEZ RUS, J.J.: «El *cracking* y otros supuestos de sabotaje informático», en *Estudios Jurídicos del Ministerio Fiscal*, II-2003, Ministerio de Justicia, Madrid, 2003, pág. 210.

Con palabras muy precisas lo define MATA Y MARTÍN como los «comportamientos que atacan los elementos lógicos de sistemas informáticos, incluso si su destrucción se produce actuando sobre el soporte físico o el elemento del hardware en el que se encuentran» (MATA Y MARTÍN, R.: *Delincuencia informática y Derecho penal*, Edisofer, Madrid, 2001, pág. 59). Así lo comparte mayoritariamente la doctrina, vid. ANDRÉS DOMÍNGUEZ, A.C.: «Los daños informáticos en la Unión Europea», La Ley, 1999-1, D-31; ROMEO CASABONA, C.: «Los delitos de daños en el ámbito informático», *Cuadernos de Política Criminal*, 1991, pág. 91.

4. Para un análisis detallado al respecto, *vid*. ANDRÉS DOMÍNGUEZ, A.C.: «Los daños informáticos en la Unión Europea», *op. cit.*, D-31; GONZÁLEZ RUS, J.J.: «Protección penal de sistemas, elementos, datos, informaciones, documentos y programas informáticos», *Estudios Jurídicos del Ministerio Fiscal. Responsabilidad Civil en el Nuevo Código Penal. Delincuencia Informática*, Ministerio de Justicia, Madrid, 1997, pp. 526 y ss. (actualizado en *Revista Electrónica de Derecho penal y Criminología*, 1-14, 1999, http://www.recpc); «Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (artículo 264.2 del CP)», *La ciencia del Derecho penal ante el nuevo siglo. Libro Homenaje al Prof. Dr. D. J. CEREZO*, Tecnos, Madrid, 2003, pp. 1285 y ss.; «El *cracking* y otros supuestos de sabotaje informático», *Estudios Jurídicos del Ministerio Fiscal*, II-2003, Ministerio de Justicia, Madrid, pág. 210. «Los ilícitos en la red (I): *hackers*, *crackers, cyberpunks*, *sniffers*, denegación de servicio y otros comportamientos semejantes», *El Cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales*, (ROMEO CASABONA, Coord.), Comares, Granada, 2006, pp. 248 y ss.; ROMEO CASABONA, C.: «Los delitos de daños en el ámbito informático», *op. cit.*, pág. 91.

Al mismo tiempo, de manera más estricta, el término «piratería informática» se ha extendido también a los casos de quienes entran en un sistema informático pero no asistidos de una intención vandálica o destructiva, y ni tan siquiera de hacerse con copias ilícitas de un programa de ordenador, sino que el término pirata ha alcanzado al denominado «*hacker* blanco», quien se cuela en sistemas informáticos ajenos, consiguiendo driblar las medidas de seguridad impuestas, pero sin ninguna otra finalidad añadida a la sola voluntad de acceder a los mencionados sistemas. No se trata, por lo tanto, de una categoría necesariamente excluyente de la anterior, sino acumulativa, pudiendo ser este acceso el camino para efectuar el daño o sabotaje informático.

Y es más, el término «*hacker*» hoy ya resulta absolutamente familiar a casi cualquier persona que esté habituada al empleo de la informática y el ordenador, ya sea como herramienta de trabajo, como medio de distracción, o de obtención de información mediante la Red de Internet, etc. Su percepción como sujeto inofensivo, que realiza una conducta inocua y carente de relevancia jurídico-penal alguna, como sujeto que ayuda al funcionamiento del sistema, propicia esta generalización del término, que casi resulta elogiosa del virtuosismo informático de quien es tildado así[5].

Finalmente, todo este confusionismo conceptual se manifiesta en el empleo de la citada expresión de «pirata informático» para aglutinar todas las conductas enunciadas, es decir, tanto las de mero intrusismo, como las específicamente destructivas, bien por la vía de la vulneración de los derechos de autor, bien por la de los daños informáticos[6].

A efectos metodológicos de este trabajo, y sin negar o desdecir la proyección social y el significado amplio que criminológicamente tiene el término «piratería informática», entiendo necesario circunscribirla a una modalidad específica de comportamientos. Me refiero a los casos denominados de «*hacking* blanco», también denominado «*hacking* puro», consistentes *únicamente en el acceso no autorizado, de forma subrepticia, a un sistema informático o red de comunicación electrónica de datos*. Insisto: únicamente se trata de acceder de manera no tolerada, *sin ocasionar alteración o daño alguno sobre los datos o programas, ni tomar en consideración otras intencionalidades o fines distintos al mero acceso que el intruso pudiera perseguir*. El causar algún daño en el sistema, realizar actos que generen efectos lesivos sobre el patrimonio, o sobre los datos o información contenidos en el sistema, por ejemplo, iría en contra de su prioritaria intención de mezclarse con el usuario normal y atraería la atención sobre su presencia, haciendo que su puerta de ingreso sea cerrada y, por tanto, anulando su deseo de volver a filtrarse en el sistema y dejar al descubierto su vulnerabilidad[7].

El motivo de esta reducción del campo de análisis viene propiciada por las respuestas penales positivas tanto actualmente en vigor, como de inminente introducción en nuestro texto penal. Me explico:

Es evidente, que muchos casos de accesos no consentidos, forman parte del *presupuesto de actuación* de otras conductas que ya tienen su sanción penal. Básicamente, el acceso no autorizado es el paso previo a la conducta de causación de daños o destrucción de sistemas o datos informáticos a los que se refiere el art. 264. 2. Igualmente, una intromisión en el sistema informático es el antecedente necesario para el descubrimiento de datos particulares contenidos en un sistema informático o procesados mediante un programa informático, y que forman parte del secreto, o de la intimidad personal, a cuya atención se refiere el art. 197 o del secreto de empresa del art. 278. De manera unánime, la doctrina concuerda en incorporar estos casos particulares de *hacking* a los delitos antedichos, configurándose, en consecuencia, como un «*modus operandi*» que *técnicamente infiere un caso de tentativa en la que la producción de los daños o el acceso al secreto, como forma consumativa, absorbe el desvalor del acceso intencional precedente*, siempre, por supuesto que en ellos concurran los elementos subjetivos específicos que peculiarizan las citadas figuras delictivas[8]. Se trata sin ningún género de duda de comportamientos que constituyen una modalidad, anticipada ciertamente, de ataque a bienes jurídicos de sólido cuño en nuestro sistema jurídico, como la intimidad personal (art. 197), o el patrimonio[9] o hasta el orden socioeconómico (en los casos de los arts. 264.2 y 278)[10], pero su particular cariz subjetivo, o la exigencia de un resultado dañino concreto, apartan estos casos de accesos ilegítimos de la conducta del «*hacker*» puro[11].

5. Por eso, es denominado también «*hacker* ético», por alusión a la ausencia de intencionalidad lesiva, que deriva en una visión «idealizada» del *hacker*, casi como amigo del sistema o red informáticos, ya que ayuda a descubrir los puntos flacos del mismo y así facilita la adopción de nuevas medidas de seguridad. Es más el término «*hacker*» fue creado para diferenciar justamente esta clase de actuaciones de las de los que utilizaban sus conocimientos sobre las puertas falsas del sistema para apoderarse de datos o secretos o para destruir datos o causar daños a propio sistema y los programas que los hacen funcionar; sobre este particular, *vid.* MOLINST, M.: «*Hackers* éticos», Ciberp@is, nº 15, octubre 2001, pág. 18.

6. MORÓN LERMA, E.: *Internet y Derecho penal*…, *op. cit.*, pp. 40-41.

7. FIGOLI, A.: «El acceso no autorizado a sistemas informáticos», http://www.alfa-redi.org/rdi-articulo.shtml?x=381.

8. Las referencias doctrinales son abundantes, pero, como muestra, *vid.* por todos, MORÓN LERMA, E.: *Internet y Derecho penal*…., *op. cit.*, pp. 51 y 55 y ss.

9. MATA Y MARTÍN, R.M.: *Delincuencia informática y Derecho penal*, *op. cit.*, pág. 80; VALLDECABRES ORTIZ, I.: «Comentarios al Capítulo IX», en *Comentarios al Código Penal de 1995*, vol. II, (VIVES ANTÓN, Coord.), Tirant lo Blanch, Valencia, 1996, pp. 1313-1314.

10. GUTIÉRREZ FRANCÉS, M.: «Delincuencia económica e informática en el nuevo Código Penal», *op. cit.*, pág. 297.

11. Aspecto éste que se desarrollará en la segunda parte de este trabajo.

Junto a ello, y en lo que aún constituye una opción de *lege ferenda*, el *Proyecto de Ley Orgánica de reforma del Código Penal de 15 de enero de 2007*, introduce un nuevo párrafo en el art. 197, que lleva el numeral 3 (consecuentemente desplazando a los demás supuestos insertos en el art. 197), bajo el cual se castiga específicamente el caso específico del intruso que se «cuela» de manera no consentida en el sistema informático, quebrantando las medidas de seguridad que lo preservan de la intromisión de terceros, pero desprovisto de una finalidad saboteadora o lesiva de la intimidad ajena, y que específicamente establece que:

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

Bien, es esta visión del «intrusismo», sin generación de efectos lesivos o destructivos del sistema, datos o programa informático y carente de ulteriores finalidades subjetivas (dañar, espiar, defraudar al patrimonio, etc.) distintos del acceso mismo que lo entronquen directamente con otros bienes jurídicos y, correlativamente, con otros delitos, el que centra nuestro análisis.

2. Objetivos del trabajo

Sobre la base anterior, la cuestión que inmediatamente surge y constituirá el objeto central de este estudio es la de analizar el contenido de esta conducta, valorando si realmente se trata de la incriminación del genuino *hacking* puro en el sentido que se ha delimitado o si, por el contrario, se trata de una conducta diferente. Las exigencias de la proporcionalidad penal, relativas a la evitación del exceso y a la legitimidad de la intervención solo en tanto en cuanto sea necesaria, determinan que la justificación de una nueva respuesta penal solo deba encontrarse bien en la existencia de un nuevo interés jurídico-penal que hasta el momento no haya tenido acomodo en el cuerpo penal, bien en la consideración de que hay una conducta especialmente sin valor que afecta a un bien jurídico ya reconocido penalmente, pero que no está adecuadamente comprendida en los espacios típicos existentes hasta ahora, por lo que en cualquiera de los dos casos se hace preciso un nuevo tipo penal: nuevo bien jurídico o existencia de lagunas de punición respecto a la protección de un bien jurídico y existente.

El objetivo de este trabajo es el de identificar el alcance de la conducta prevista en ese párrafo 3 del art. 197 del Código Penal, que el legislador define como intrusismo informático, a fin de descubrir si se trata del genuino «*hacking* puro» según los términos tradicionales del debate, con lo cual asistiríamos a la inclusión penal de un nuevo interés jurídico, o si supone una extensión de la protección de algún bien jurídico ya preexiste[12]. Para ello, los puntos esenciales de reflexión se estructuran en torno a los siguientes momentos:

— Contextualización normativa internacional del problema, debido a su recepción en normas internacionales en las que toma su causa la reforma legislativa a anunciada.

— Precisión somera de la virtualidad de los tipos penales vigentes hasta el momento para incorporar las conductas de mero intrusismo informático. (En las líneas anteriores ya se apuntó de manera indirecta a que hay «algo», sobre todo de carácter subjetivo que impide su inclusión en algunos tipos.)

— Planteamiento del estado de la cuestión doctrinal hasta este momento acerca de la conveniencia de incriminación del *hacking*.

— Valoración de la posible solución penal española en esta materia.

3. Especial atención al carácter transnacional de la conducta

3.1. La criminalidad informática como manifestación del fenómeno de la globalización

3.1.1. Informática y globalización

El fenómeno de la globalización es un hecho con un detonante claramente económico: aparece vinculado a la necesidad de los medios de producción, tanto de abrir nuevos mercados como de abaratar costes. Por eso, el proceso de globalización no es, por definición, necesariamente positivo o negativo. Depende de quién lo controle. Y aunque no faltan voces que abogan a favor del aprovechamiento o la transformación de este fenómeno en un proyecto humanista («la realización de ese proyecto implica construir un sistema político global que no esté al servicio del mercado global»[13]), el hecho cierto a fecha de hoy es que la globalización es una forma específica de mundialización de la actividad económica desarrollada según unas políticas

12. Otras cuestiones que pudieran estar vinculadas (piénsese, por ejemplo, en los problemas de aplicación de la ley penal en el espacio), no serán abordadas. La omisión es consciente y se justifica en este momento legislativo, en el que el denominado delito de intrusismo informático no es una realidad positiva en nuestro sistema penal, por lo que resulta demasiado adelantado querer abarcar todos los problemas concretos que el tipo plantea. Insisto: el tipo no está aun vigente, pero sí resulta de interés ir desgranando la orientación legislativa en este ámbito.

13. AMÍN, S.: *El capitalismo en la era de la globalización*, Paidós, Barcelona, 1999, pág. 19.

neoliberales que están dañando el bienestar de las clases menos favorecidas[14]. La globalización parece imposible sin establecer relaciones de dominación o sin dictar unas pautas homogeneizadoras impuestas por los más poderosos económicamente (Estados, empresas, *lobbys*…), que disponen de mayor poder. En otras palabras, que existen globalizadores que imponen su criterios, y globalizados que no tienen otra opción más que aceptarlos[15]. De ahí que, efectivamente, el término globalización emerge como un eufemismo bajo el que se esconde la realidad del poder que grandes grupos económicos extienden sobre todo el planeta[16] y con ello se pierde no solo la capacidad de movimiento y de opción en materias tan decisivas como los alimentos, los recursos naturales, la cultura, etc.[17]

Bajo este contexto, la extensión y el uso de las redes informáticas es un fenómeno más de la globalización. Probablemente sea también cierto su contrario: que las comunicaciones telemáticas por medio de sistemas informáticos han contribuido a desplegar este fenómeno[18]. Sea cual sea el origen, el hecho es que en el contexto de ese mundo globalizado, la utilización de las tecnologías informáticas es una pieza configuradora del actual orden social[19] y económico. Las consecuencias de este paradigma tecnológico afectan y modifican la estructura social y económica, dándose lugar a nuevas variables económicas y concepciones del sistema económico. Es el caso de la denominada «Economía informacional»: la capacidad de obtención y direccionamiento de la información es un factor clave en la expansión y solidez económica[20]; o de la «Economía-Red»: que atiende a la descentralización de las grandes empresas y formación de redes o alianzas con pequeñas empresas que funcionan como auxiliares entre sí.

En el año 1962, McLUHAN acuñó el término «aldea global» para referirse a una comunidad cuyos integrantes se relacionaban entre sí a través de los medios de comunicación de masas. En la actualidad, el empleo de los medios de comunicación de masas no es una característica de un sector de la sociedad, sino que es la manera habitual de comunicación, de sociabilidad, de organización, de conocimiento[21]. Nos hallamos inmersos en plena era de la información y la evolución natural de la misma ha derivado en una generalización total del empleo del ordenador y su interconexión en redes y la de éstas en autopistas de la información. Gracias a los ordenadores y a las redes la gente más diversa puede entrar en contacto a lo largo y ancho del planeta. Esta universalidad se experimenta por inmersión: todos estamos sumergidos en el mismo baño, en el mismo diluvio de comunicación.

3.1.2. El «ciberespacio», el «hombre-digital» y la «sociedad de riesgo»

Ello ha dado lugar también a un nuevo medio en el que se desarrollan las relaciones de esos sujetos, el «ciberespacio»[22] que, por tratarse de un medio no físico, no se encuentra demarcado por el eje espacio-temporal clásico,

14. NAVARRO, V.: *Bienestar insuficiente, democracia incompleta: sobre lo que no se habla en nuestro país*, Anagrama, Barcelona, 2003, pág. 149.

15. RECASENS I BRUNET, A.: «Globalización, riesgo y seguridad», *SERTA in memoriam A. Baratta*, (PÉREZ ÁLVAREZ, Ed.), Ediciones Universidad de Salamanca, Salamanca, 2004, pág. 1449.

16. Vid. sobre ello, GARCÍA RIVAS, N.: «Globalización y justicia universal: paralelismo», en *El Derecho penal frente a la inseguridad global*, (GARCÍA RIVAS, Coord.), Bomarzo, Madrid, 2006, pp. 2 y ss.

17. QUINTERO OLIVARES, G.: «El Derecho penal ante la globalización», *El derecho penal ante la globalización*, (ZÚÑIGA/MÉNDEZ /DIEGO DÍAZ-SANTOS, Coords.), Colex, Madrid, 2002, pág. 11; BERGALLI, R.: «Libertad y seguridad: un equilibrio extraviado en la modernidad tardía», *El derecho ante la globalización y el terrorismo*, Actas del Coloquio Internacional Humboldt-Montevideo, abril 2003, Alexander von Humboldt-Tirant lo Blanch, Valencia, 2004, pág. 68 y ss.

18. ROMEO CASABONA, C.M.ª: «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, pág. 1.

19. Como afirma ESCOBAR DE LA SERNA, L.: *Derecho de la información*, Dykinson, Madrid, 2004, pág. 25, el estudio de la influencia de los medios de comunicación ya no sólo se centra en el conocimiento de los efectos que éstos provocan cuanto en los deseos y actitudes de la gente ante los mismo, que ya no sólo los usa como vía de información, sino para conseguir efectos gratificantes de muy diversa índole. A ello, hay que añadir la conformación de un rasgo definidor de la actual sociedad: el anonimato.

20.MATA Y MARTÍN, R.M.: «Perspectivas sobre la protección penal del software», *El Cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales* (ROMEO CASABONA, Coord.), Comares, Granada, 2006, pág. 97.

21. MORALES GARCÍA, O.: «Seguridad en las redes telemáticas de comunicaciones. La tensión libertad versus control en la política criminal internacional», *La seguridad en la sociedad de riesgo. Un debate abierto*, AA.VV. (CÁNDIDO DÂ AGRA, et. al., Eds.), Atelier, Barcelona, 2003, pág. 138.

22. Sobre el origen de este término en la literatura de ciencia-ficción y su evolución hacia su definición como «espacio relacional»; su realidad se construye a través del intercambio de información; el «ciberespacio surge en y por la comunicación y si ésta no existe, el ciberespacio tampoco. De ahí su doble condición de espacio y de medio. Pese a esta consideración «virtual» del ciberespacio, en la medida de que carece de un espacio o lugar físico de referencia, ya que sólo nace y existe como punto de encuentro de comunicaciones, el ciberespacio es verdadero, no una ficción, ya que en él es posible realizar acciones y tomar decisiones; sobre este asunto, vid. AGUIRRE MORENO, J.Mª.: «Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI», en http://www.ucm.es/info/especulo/numero27/cibercom.htlm, 2004.

característica que produce una inadaptabilidad de la generalidad de las normas jurídicas referidas a la actividad humana en el mundo físico o corporal. Esto ha fomentado la aparición de nuevas pautas de conducta para este mundo incorporal; normas que, en principio han sido instaladas por sus propios actores. Sin embargo, no todas las disputas y dificultades que se suscitan en este medio pueden hallar tratamiento apropiado por medio de la regulación nacida de los propios actores en su entorno, ocasión que determinó al legislador a elaborar una normativa encaminada a solucionar los problemas que se puedan constatar en este ámbito, especialmente de seguridad. En suma, es incuestionable que la realidad criminal contemporánea se desenvuelve en un «lugar» indeterminado (casi podríamos hablar de una «nueva dimensión» empleando terminología de la ciencia ficción, al igual que la que ha dado lugar al término «ciberespacio»), en un espacio relacional, que no tiene siquiera un antecedente o presupuesto físico, y cuya realidad se construye a través del intercambio de información. Es decir, es espacio y es un medio. Y es debido a la peculiaridad de este entorno por lo que el impacto derivado de la utilización pervertida de la informática no se detiene en el espacio doméstico de un ordenador, ubicado geográficamente en un lugar y perteneciente a un sujeto concreto, sino que su potencialidad multiplicadora de encuentros y efectos, determina que las fronteras físicas y territoriales no sean conceptos relevante en esta materia; antes al contrario, el ciberespacio es un macrocosmos de conexión digital no ubicable en ningún punto geográfico. Geografía e informática son términos que se repelen. Uno no conoce a otro. Hablan lenguajes diferentes. *La transnacionalidad de los efectos es, posiblemente, el rasgo más sobresaliente de la delincuencia informática*.

Todo ello da lugar a un nuevo tipo de persona, el «sujeto digital»[23]. Un sujeto que es al mismo tiempo emisor y receptor de información en ese espacio virtual, en el que todos comunican con todos. Un sujeto que actúa deslocalizada e innominadamente, generando unas relaciones caracterizadas por el anonimato[24]. Todo lo cual, anonimato e intercomunicación digital global, es factor determinante de uno de los rasgos identificadores de sociedad actual: la «sociedad de riesgo».

A partir de la difusión de la obra de BECK[25] se identifica la nueva sociedad postindustrial, la sociedad de los avances en medicina, la de las economías y la producción a gran escala, la de las telecomunicaciones, la de las utilidades informáticas para todo, etc., como una «sociedad del riesgo»[26]. El extraordinario avance de los medios tecnológicos y técnicos, en particular las tecnologías de la información vinculadas a la informática[27], ha tenido y sigue teniendo repercusiones directas en un incremento del bienestar individual. Pero a su vez, semejante comodidad social tiene un coste de signo negativo: el funcionamiento de esos medios técnicos es el factor desencadenante de la presencia de una elevación en número y entidad de lo factores de riesgo en nuestra sociedad; mayor nivel de riesgo que se mide no solo por la aparición de nuevos focos desencadenantes del mismo, sino también por la mayor capacidad de proyección de los futuros daños, sobre un colectivo humano cada vez más grande (incluso sociedades enteras). La presencia de todos estos riesgos, como coste aparejado indisolublemente a la evolución científica, ha determinado que éstos se constituyan en pieza estructural de la sociedad actual, como elemento que la define y la identifica[28].

La traducción jurídico-penal de esta presencia social del riesgo consiste en la supresión o reducción de los márgenes en los que los ciudadanos permiten o toleran convivir con aquél[29]. Este estrechamiento del nivel de tolerabilidad del riesgo se va haciendo cada vez más férreo a fin de dar satisfacción a las demandas sociales de freno a estos riesgos percibidos socialmente como especialmente peligrosos (percepciones que en muchos casos son más subjetivas que ciertas[30]). Esta restricción de la capacidad social

23. Sobre ello, TÉLLEZ AGUILERA, A.: *Nuevas tecnologías. Intimidad y protección de datos*, Edisofer, Madrid, 2001, pp. 21 y ss.

24. Todas estas precisiones en MORÓN LERMA, E.: *Internet y Derecho penal…, op. cit.*, pág. 88.

25. BECK, U.: *La sociedad del riesgo. Hacia una nueva modernidad*, (NAVARRO/JIMÉNEZ/BORRÁS, trads.), Paidós Ibérica, Barcelona 1998; una versión resumida en BECK, U.: «De la sociedad industrial a la sociedad del riesgo», *Revista de Occidente*, nº 150, 1993, pp. 19 y ss.

26. Y se caracterizan, según BECK, porque: a) no son limitables espacial, temporal y socialmente (en cuanto al ámbito de afectados); b) no son imputables según las vigentes reglas de la causalidad, culpabilidad y responsabilidad; c) no pueden ser compensados ni asegurados; BECK, U.: *La sociedad de riesgo*, *op. cit.*, pág. 19 y ss.

27. En general, sobre esta vinculación de la informática con los problemas propios de la nueva «sociedad de riesgos», ANARTE BORRALLO, E.: «Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho penal de la sociedad de la información», *Derecho y Conocimiento*, nº 1, 2001, pp. 196 y ss.; PÉREZ DEL VALLE, C.: «Sociedad de riesgos y reforma penal», *Poder Judicial*, nº 43-44, 1996, pp. 61 y ss.

28. SILVA SÁNCHEZ, J.Mª.: *La expansión del Derecho penal. Aspectos de la política criminal en las sociedades postindustriales*, BdeF, Montevideo-Buenos Aires, 2006, pág. 14.

29. MENDOZA BUERGO, B.: «El Derecho penal ante la globalización: el papel del principio de precaución», *Derecho penal y política transnacional*, AA.VV. (CANCIO MELIÁ/BACIGALUPO, Coords.), Atelier, Barcelona, 2005, pp. 326 y ss.

30. Sobre este sentimiento de incertidumbre e inseguridad ante el caso particular de las nuevas tecnologías, *vid.* MATA Y MARTÍN, R.M.: «Criminalidad informática: una introducción al Cibercrimen», *Actualidad Penal*, nº 37, 2003, pp. 937-938, «Criminalidad informática: una introducción al Cibercrimen», *Temas de Direito da Informática e da Internet*, Coimbra Editora, 2004, pp. 199-200;

de tolerancia del riesgo deriva en una nueva caracterización de los rasgos definidores de la dogmática penal: ésta se orienta hacia una atribución de un valor decisivo de la acción sobre el resultado (tendencia a la subjetivización del injusto[31]), elevándose el delito de peligro, no el de lesión, como prototipo de injusto penal en el que el resultado efectivamente lesivo se presenta como una mera cualificación; junto a ello, gana terreno la ampliación de las figuras típicas imprudentes y las formas de comisión por omisión en virtud de la figura de la «injerencia» como fundamento de la imputación, al tiempo que se acrecienta la proliferación de los delitos de tentativa[32].

Y es más, el problema es que la fijación normativa de los criterios de cautela y previsibilidad que rigen el funcionamiento y el manejo de esos nuevos espacios de riesgo se realiza en base a hipótesis carentes de una base empírica, porque es que ni siquiera quienes manejan y conocen esa fuente de riesgo son capaces de perfilar con exactitud los parámetros de causación de riesgo de las mismas, ante el desconocimiento de muchas de sus potencialidades[33]; así por ejemplo, ¿cómo saber hoy todos y cada uno de los efectos y, por tanto calcular los riesgos de las conductas relacionadas con la ingeniería genética, que es un campo en el que aún está casi todo por descubrir? En la específica materia de la criminalidad informática este desconocimiento del riesgo es manifestado por los expertos informáticos cuando aseguran que «lo que se manifiesta en los sistemas no es la seguridad, sino la inseguridad o vulnerabilidad. No se puede hablar de que un sistema informático es seguro, sino de que no se conocen los ataques que puedan vulnerarlo»[34]. El «vértigo»[35] de la carrera científica y tecnológica postindustrial corre el peligro de traducir ese sentimiento de inseguridad en respuestas normativas sobre fijación de niveles de riesgo a las cuales los actores difícilmente van a poder atender, pues como señala CORCOY BIDASOLO, «si entendemos que la posibilidad de motivación es lo único que legitima la intervención penal no es lícito prohibir al autor controlar un riesgo, cuando ni tan siquiera la ciencia conocía la existencia de ese riesgo en ese momento»[36].

3.2. Las respuestas normativas en el ámbito europeo

3.2.1. La armonización del Derecho penal europeo en materia de intrusismo informático

Desde este contexto mundial de globalización, en el que la informática ocupa un papel privilegiado, el carácter trasnacional del proceso de intercambio informático de información y la ingente capacidad de hacer llegar datos, noticias, imágenes, etc. en décimas de segundos a millones de personas nos lleva a recalar en la consecuencia normativa naturalmente derivada de esa internacionalidad e interconexión de los riesgos y de sus efectos: la regulación jurídica que se ocupa del control, limitación y sanción de los riesgos globales generados por el manejo abusivo de los sistemas y redes informáticos tiene necesariamente que rebasar el espacio físico de un país, pues solo así es real el control del riesgo en toda su dimensión. Es del todo insuficiente pretender paliar los efectos negativos de esos riesgos con una legislación recluida en las fronteras de cada Estado.

La mayor parte de los hechos delictivos trasnacionales encuentran en las nuevas tecnologías de la información el medio idóneo para, o bien financiar, o bien cometer la infracción penal, extender sus efectos, o bien para encubrir, transformar o mostrar como de origen lícito sus beneficios. El propósito que asiste a estos instrumentos normativos supranacionales es eminentemente práctico en el sentido de que lo que se busca es una uniformidad en las respuestas penales que evite los paraísos jurídico-penales, es decir, se trata de rellenar posibles huecos penales «locales» que provocan un direccionamiento de las acciones ilícitas hacia ese lugar en el que no hay respuesta sancionadora. En to-

---

con carácter general, destaca este sentimiento social de incertidumbre sobre el sí, el cómo y el cuándo del riesgo, SILVA SÁNCHEZ, J.Mª.: *La expansión del Derecho penal*, *op. cit.*, pp. 20 y ss.

31. SÁNCHEZ GARCÍA DE PAZ, I.: *El moderno Derecho penal y la anticipación de la tutela penal*, Universidad de Valladolid, Valladolid, 1999, pág. 84, citando a ESER.

32. Con carácter general sobre estos problemas, las obras de PAREDES CASTAÑÓN, J.M.: *El riesgo permitido en Derecho* penal, Ministerio de Justicia, Madrid, 1995; MENDOZA BUERGO, B.: *El Derecho penal en la sociedad de riesgo*, Civitas, Madrid, 2001.

Críticamente, *vid.* HASSEMER W.: «Derecho penal simbólico y protección de bienes jurídicos», en *Pena y Estado*, P.P.U., Barcelona, 1991, pp. 33 y ss.; HERZOG, F.: «Límites al control general de los riesgos sociales», *Poder Judicial*, nº 32, 1993, pp. 81 y ss.

En particular sobre la materia informática, GALÁN MUÑOZ, A.: «Expansión e intensificación del Derecho penal de las nuevas tecnologías…», *op. cit.*, pp. 22-28.

33. MENDOZA BUERGO, B.: «Gestión del riesgo y política criminal en la sociedad de riesgo», en *La seguridad en la sociedad del riesgo. Un debate abierto* (da AGRA, C./DOMÍNGUEZ, J.L./GARCÍA AMADO, J.A./HEBBERECHT, P./RECASENS, A. Eds.), Atelier, Barcelona, 2003, pp. 77 y ss.

34. MORÁN RAMÓN,J.L./RIBAGORDA GARNACHO, A./SANCHO RODRÍGUEZ, J.: *Seguridad y protección de la información,* Centro de Estudios Ramón Areces, Madrid, 1994.

35. Término empleado por SILVA SÁNCHEZ, J. M.ª: *La expansión del Derecho penal*…, *op. cit.*, pág. 22.

36. CORCOY BIDASOLO, M.: *Delitos de peligro y protección de bienes jurídico-penales supraindividuales*, Tirant lo Blanch, Valencia, 1999, pág. 53.

do caso, esta orientación hacia la unificación del Derecho penal en los espacios propios de los nuevos riesgos, manifiesta una particular visión del papel que le corresponde al Derecho penal. Tiene una lectura en clave político-criminal: es una muestra más de la tendencia a la elevación de la punición y al endurecimiento del Derecho penal. El transnacionalismo de la delincuencia se ha convertido, en palabras de SILVA SÁNCHEZ, en un nuevo factor de «multiplicación de la expansión»[37] del Derecho penal.

De este mismo nodo, la peculiaridad transnacional de las tecnologías de la comunicación, con sus conexiones en todos los lugares del planeta y, por tanto, la internacionalidad de los delitos cometidos bajo su amparo ha generado la necesidad de una aproximación de las diferentes legislaciones nacionales, de modo que pueda llevarse a cabo una represión uniforme de los ataques a los bienes jurídicos afectados mediante el empleo de estas técnicas[38]. En este ámbito del empleo ilícito de los sistemas informáticos, como nuevo factor de vulnerabilidad de bienes jurídicos, la tendencia a fusionar las soluciones normativas, en concreto normativo-penales, ha sido una constante. Y en los últimos tiempos ha sido en el entorno europeo en donde más se han concentrado las respuestas, protagonizados por dos normas de distinto alcance territorial: la primera en el tiempo, *Convenio del Consejo de Europa «sobre criminalidad informática»* (denominado habitualmente Convenio sobre Cibercriminalidad), hecho en Budapest, el 23 de noviembre de 2001[39] que entró en vigor el 1 de julio de 2004 (una vez cumplida la condición establecida en el art. 36.3 en que se obtuvo la ratificación de cinco Estados, tres de los cuales había de ser miembros del Consejo de Europa[40]); más recientemente, en el ámbito de la Unión Europea,, se aprobó la *Decisión-marco 2005/222/JAI del Consejo «relativa a los ataques contra los sistemas de información»,* de 24 de febrero de 2005, con entrada en vigor el 16 de marzo de 2005 (día de su publicación en el Diario Oficial de la Unión Europea, art. 13[41]).

Los objetivos de estas normas europeas son claramente armonizadores[42]: garantizar que los ataques contra los sistemas y redes de información sean castigados en todos los Estados miembros mediante sanciones penales efectivas, proporcionadas, disuasorias y lo más similares posibles para evitar fugas de criminalidad en busca de la impunidad. Y todo ello, buscando al propio tiempo mejorar y fomentar la cooperación judicial y policial, superando las destacadas complicaciones en la persecución y prueba de estos delitos[43]. Objetivos, en fin, que no pueden ser alcanzados de manera suficiente por los Estados miembros

37. SILVA SÁNCHEZ, J. M.ª: *La expansión del Derecho penal*, *op. cit.*, pág. 83.

38. PUENTE ABA, L.: «Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos: ¿debe protegerse de forma autónoma la seguridad informática?, en *Nuevos retos del Derecho penal en la era de la globalización*, AA.VV., (FARALDO CABANA, Dir.,), Tirant lo Blanch, Valencia, 2004, pág. 382.

39. Sobre las vicisitudes de su elaboración, *vid.* MORALES GARCÍA, O.: «Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre el Cibercrimen», *Delincuencia Informática. Problemas de Responsabilidad*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2002, pp. 16 y ss.

40. Artículo 36.- «*Firma y entrada en vigor:*

1. El presente Convenio está abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración.

2. El presente Convenio está sometido a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación deberán ser entregados al Secretario General del Consejo de Europa.

3. El presente Convenio entrará en vigor el primer día del mes transcurridos tres meses desde que cinco Estados, de los cuales al menos tres deberán ser miembros del Consejo de Europa, presten su consentimiento a vincularse al Convenio, conforme a lo dispuesto en los párrafos 1 y 2.

4. Para todos los Estados que hayan prestado su consentimiento a vincularse al Convenio, éste entrará en vigor el primer día del mes transcurridos tres meses desde que hayan expresado su consentimiento, conforme a lo dispuesto en los párrafos 1 y 2».

41. Artículo 13.- «*Entrada en vigor:*

La presente Decisión marco entrará en vigor el día de su publicación en el Diario Oficial de la Unión Europea».

42. Claramente, sobre estos objetivos en el caso del Convenio de Europa, MORÓN LERMA, E./RODRÍGUEZ PUERTA, M.ª J.: «Traducción y breve comentario del Convenio sobre Cibercriminalidad», *Revista de Derecho y Proceso Penal*, nº 7, 2002, pp. 167 y ss.

43. Y determinante de la especialización de la Guardia Civil: Grupo de Delitos Telemáticos, creado en 1996 (inicialmente denominado Departamento de Delitos de Alta Tecnología); más información en https://www.gdt.guardiacivil.es/historia.php. En el caso de la Policía nacional existe una Unidad de Investigación de la Delincuencia en Tecnologías de la Información (Brigada de Investigación Tecnológica); más información en http://www.policia.es/bit/index.htm.

Sobre esta temática, con múltiples datos y referencias bibliográficas, *vid.* SIEBER, U.: «Criminalidad informática: peligro y prevención», en *Delincuencia informática*, (MIR PUIG, compilador), P.P.U., Barcelona, 1992, pp. 13 y ss. Legal aspects of computer-related crime in the information society, *op. cit.*, 32 y ss, 146 y ss., 193 y ss. Computer crime and criminal information law. New trends in the international risk and information society, 1998, http://www.jura.unimuenchen.de/sieber/article/mitis/ComCriCriInf.htm; SARZANA, C.: «Observaciones sobre la victimización informática», *Agora, Oficina Intergubernamental para la informática*, IBI, nº 2, 1986, pág. 77 y que recogen GUTIÉRREZ FRANCÉS, M.ª L.: *Fraude informático y estafa*, *op. cit.*, págs. 80-81 y GONZÁLEZ RUS, J. J.: «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», *Revista de la Facultad de Derecho de la Universidad Complutense*, n.º 12, 1986, pág. 110.

de modo individual y unilateral, de ahí la necesidad de la homogeneización o convergencia de la actuación penal. A este respecto, los «Considerandos» de Decisión-marco hablan por sí solos de esta pretensión unificadora del sistema punitivo en su conjunto tanto en su vertiente normativo-material, como policial. La claridad y concisión de las explicaciones a este respecto, justifican la trascripción y huelgan de cualquier otro comentario:

«(1) El objeto de la presente Decisión marco es reforzar la cooperación entre las autoridades judiciales y otras autoridades competentes, incluida la policía y los demás servicios represivos especializados de los Estados miembros, mediante la aproximación de su legislación penal en materia de ataques contra los sistemas de información.

(2) Se ha comprobado la existencia de ataques contra los sistemas de información, en particular como consecuencia de la amenaza de la delincuencia organizada, y crece la inquietud ante la posibilidad de ataques terroristas contra sistemas de información que forman parte de las infraestructuras vitales de los Estados miembros. Esto pone en peligro la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia, y por tanto exige una respuesta por parte de la Unión Europea.

(...)

(4) En la Resolución del Parlamento Europeo de 5 de septiembre 2001 se destaca la necesidad de sensibilizar más al público sobre los problemas relacionados con la seguridad de la información, así como de proporcionar asistencia práctica.

(5) La distancia y las divergencias significativas que existen entre las legislaciones de los Estados miembros en este ámbito pueden dificultar la lucha contra la delincuencia organizada y el terrorismo y pueden complicar la cooperación eficaz de los servicios de policía y las administraciones de justicia en materia de ataques contra los sistemas de información. La naturaleza transnacional y transfronteriza de los modernos sistemas de información significa que los ataques suelen revestir un carácter transfronterizo, lo que plantea la necesidad urgente de proseguir la aproximación de las legislaciones penales en este ámbito.

(...)

(8) Debe aproximarse 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.

(...)

(11) Es necesario llegar a un enfoque común respecto de los elementos constitutivos de las infracciones penales, estableciendo delitos comunes de acceso ilegal a un sistema de información intromisión ilegal en el sistema e intromisión ilegal en los datos.

(12) Para combatir los delitos cibernéticos, cada Estado miembro debe garantizar una cooperación judicial efectiva respecto de los delitos basados en los tipos de conducta contemplados en los arts. 2, 3, 4 y 5. Es necesario evitar una tipificación penal excesiva, especialmente de los casos de menor gravedad, así como la inculpación de titulares de derechos y personas autorizadas.

(14) Es necesario que los Estados miembros prevean sanciones para reprimir los ataques contra los sistemas de información. Las sanciones previstas deberán ser efectivas, proporcionadas y disuasorias.

(...)

(16) Deben también preverse medidas de cooperación entre los Estados miembros con el fin de combatir eficazmente los ataques contra los sistemas de información. Por consiguiente, los Estados miembros deben hacer uso de la red existente de puntos de contacto operativos para el intercambio de información a los que se hace referencia en la Recomendación del Consejo de 25 de junio de 2001 sobre puntos de contacto accesibles de manera ininterrumpida para la lucha contra la delincuencia de alta tecnología».

A) Convenio del Consejo de Europa «sobre criminalidad informática»

La primera de las respuestas europeas la protagoniza el Consejo de Europa, mediante la aprobación de*: Convenio del Consejo de Europa «sobre criminalidad informática»* (Convenio sobre Cibercriminalidad), hecho en Budapest, el 23 de noviembre de 2001. Su objetivo es doble. Por una parte trata de establecer una red de cooperación internacional para la prevención y persecución de los delitos cometidos mediante o a través de las redes y ordenadores. Por otro lado, y como corolario a esta pretensión de unidad en las respuestas jurídicas, establece un mandato a las partes signatarias para desarrollar una legislación nacional coherente entre todos ellos y represiva de los siguientes delitos: acceso ilegal (*hacking*), interceptación ilegal, interferencia en los datos, interferencia en el sistema informático, mal uso de los aparatos, modificación de datos (falsificación de datos), pérdida de propiedad por modificación o interferencia ilegítima de datos (fraude informático), pornografía infantil y delitos contra la propiedad intelectual.

En lo que se refiere a las conductas que son objeto de nuestra atención, las de *hacking*, el Convenio ocupa su art. 2, situado en su Título I relativo a las infracciones contra la confidencialidad, la integridad y disponibilidad de los datos y sistemas informáticos, Capítulo II relativo a las medidas que deben ser adoptadas a nivel nacional, Sección 1.ª, destinada al Derecho penal material. Dicho art. 2 contempla la criminalización del intrusismo informático o

mero acceso ilegal a un sistema informático, en los siguientes términos:

«Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que estimen necesarias para prever como infracción penal, conforme su derecho interno, el acceso doloso y sin autorización a todo o aparte de un sistema informático. Los Estados podrán exigir que la infracción sea cometida con vulneración de las medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático».

La descripción que se ofrece del delito de intrusismo no consentido es la más objetiva de cuantas cabe imaginar, ya que la conducta se configura como penalmente relevante «desnuda de ingredientes añadidos al acceso mismo»[44], sean de carácter objetivo (la vulneración de las medidas de seguridad), o de carácter subjetivo (la finalidad de descubrir la intimidad, causar un daño patrimonial, etc.), cuya utilización queda a la discrecionalidad de los Estados.

Con ello, el resultado es que el Convenio solo logrará uniformar *mínimamente* la legislación penal en esta materia. Cada Estado dispondrá, sí, de un tipo penal para perseguir el acceso no consentido a un sistema informático, ahora bien, la armonización plena no se busca, puesto que el alcance y contenido de este delito en cada uno de los Estados *dependerá de la decisión de cada uno de optar o no por exigir algún otro elemento típico distinto al mero hecho causal de la entrada consciente a un sistema informático, ya sea aquel de carácter objetivo, como es el caso del requisito de la vulneración de medidas de seguridad, ya subjetivo, como es la concurrencia de un ánimo específico*.

Al dejarse *libertad a cada Estado* para que vincule la tipicidad a la exigencia de que tal acceso no consentido se realice bien infringiendo medidas de seguridad, o bien con la intención de obtener datos informáticos o con cualquier otra finalidad ilícita, desde el Convenio se acepta la posibilidad de diferentes fórmulas de castigo entre los Estados. Éstas irían desde la opción más objetiva, consistente en el mero acceso, aun cuando no se vulnerasen siquiera medidas de seguridad, pasando por la de demandar objetivamente el quebranto de éstas, siguiendo por requerir solo la presencia de elementos subjetivos precisos, de muy difícil prueba, como siempre que estamos ante un elemento intencional, hasta llegar a las fórmulas típicas más exigentes por demandar, tanto unos como otros.

Es interesante subrayar que desde la Convención se daría cabida a la posibilidad de dotar de relevancia penal a los casos de entrada en sistemas informáticos sin vulnerar medidas de seguridad por tratarse de sistemas desprovistos de estas medidas. Es decir, sería típico el aprovechamiento del *hacker* de esta situación de descuido. Este carácter causalista puro del tipo anula toda utilidad valorativo-selectiva del análisis de la imputación objetiva del riesgo permitido, al presumirse la existencia de un riego con relevancia penal, en definitiva objetivizarse su presencia, incluso en los casos en los que éste ha sido creado de manera total por la conducta absolutamente descuidada de la víctima[45], dándose paso, con ello, a la posibilidad de punir conductas carentes de todo dolo o imprudencia del autor, es decir, casos fortuitos de «llegada» a un sistema informático desprotegido. Y a mayor abundamiento, en casos de entrada a sistemas desprotegidos, ¿cómo demostrar el carácter no autorizado del mismo?

B) Decisión-marco 2005/222/JAI del Consejo «relativa a los ataques contra los sistemas de información»

Dentro del ámbito estricto de la Unión Europea y con fecha de 24 de febrero de 2005, se aprobó la *Decisión-marco 2005/222/JAI del Consejo «relativa a los ataques contra los sistemas de información».* Su objetivo armonizador es plasmado de manera expresa en sus «Considerandos» iniciales, en donde justifica la necesidad de armonización de la legislación penal de los Estados en materia de protección de los sistemas informáticos para evitar los espacios de impunidad derivados de un desigual tratamiento punitivo de una materia que no se detiene en las fronteras de cada Estado. «Debe aproximarse —dice el Consejo— 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» (Considerando 8). Por ello, continúa en el Considerando 11, «es necesario llegar a un enfoque común respeto de los elementos constitutivos de las infracciones penales, estableciendo delitos comunes de acceso ilegal a un sistema de información…».

a) Previo a su aprobación definitiva, se dictó una «*Propuesta de Decisión-marco del Consejo sobre ataques a sistemas de información»,* realizada por la Comisión Europea el 19 de abril de 2002. Respecto al acceso no consentido, el art. 3, regulador del «acceso ilegal a los sistemas reinformación» declara que:

«Los Estados miembros dispondrán 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».

La redacción de la Propuesta de Decisión-marco indica una previsión de ceñir el contenido del delito de intrusismo informático a unos *contornos más estrictos que lo que prevé el Convenio* sobre el Cibercrimen, puesto que la vulneración de las medidas de seguridad o la actuación con un ánimo específico constituyen elementos típicos de obliga-

44. MORALES GARCÍA, O.: «Apuntes de política criminal en el contexto tecnológico…», *op. cit.,* pág. 26.

45. Sobre el papel de la víctima en la materialización de los «riegos» o resultados con relevancia penal, *vid.* PAREDES CASTAÑÓN, J.M.: *El riesgo permitido en Derecho pena*l, Ministerio de Justicia, Madrid, 1995, pp. 382 y ss.

toria inserción en los tipos, como así se desprende del empleo de un tiempo verbal imperativo («*dispondrán*») en la definición de la conducta, a diferencia del facultativo «*podrán exigir*» empleado en el Convenio. Es decir, desde el Consejo de Europa se acepta tipificar el solo acceso ilegal en términos objetivo-causalistas estrictos (aunque permite a los Estados reservar la sanción a los casos en que exista una vulneración de las medidas de seguridad), mientras que la Unión Europea, por su parte, eleva el listón del tipo hasta los casos en que hay, al menos, una vulneración esas medidas de seguridad o con un ánimo especial[46], excluyendo la posibilidad de punir el acceso que se produce sin ni siquiera vulnerar los mecanismo de seguridad.

Al mismo tiempo, esta mayor concreción típica planteada por la Propuesta generaría una mayor aproximación entre las legislaciones nacionales que la ofrecida por el Convenio, dada la libertad que éste otorga a cada Estado pueda decidir si para cometer la infracción deben darse o no estas circunstancias[47].

b) Tras la aprobación de esta inicial Propuesta de Decisión-marco, se elaboró por el Parlamento Europeo un Informe sobre dicha Propuesta de Decisión-marco de la Comisión relativa a los ataques a sistemas de información, de fecha 4 de octubre de 2002, en la que se hace una análisis crítico de las incriminación de las conductas de *hacking* en las que solo concurra el elemento objetivo de la vulneración transgresión de las medidas de seguridad del sistema informático pero sin intención de causar daño ni obtener un beneficio económico. El informe aboga por la fórmula de incriminación más exigente del intrusismo, en la que se conceda un peso específico en la tipificación a los elementos subjetivos, prescindiendo de la relevancia penal del acceso mediante la sola vulneración de los sistemas de protección, por considerar estos casos, según sus propios términos, «conductas de bagatela». La base de esta crítica se centraba en el hecho de que esta es una conducta que se hace como «deporte» por muchos jóvenes, comportamiento que, por tanto, según este informe no revela una auténtica conciencia de antijuricidad por parte de los infractores, que solo puede proceder de la exigencia de elementos subjetivos relativos al ánimo de causar algún tipo de perjuicio.

c) Finalmente la Decisión-marco aprobada regula en su art. 2 el acceso ilegal a los sistemas de información estableciendo 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».*

Desde este precepto se desprenden varias consecuencias para la tipificación del intrusismo informático en los Estados de la Unión Europea:

— Primera consecuencia: que el acceso no consentido habrá de ser delito en todos los Estados. La armonización penal requiere este mínimo: ha de haber una incriminación concreta para esta clase de conducta. Se deja a los Estados la adaptación de las medidas necesarias para que ello sea así y, por lo tanto, las posibilidades que aquí se plantean van desde que los Estados ya contengan esta conducta en alguno de los tipos penales de los diferentes Códigos, en cuyo caso, el mandato de armonización está cumplido, hasta que se precise incorporar *ex novo* una fórmula típica particularmente dirigida a ella.

— Segunda consecuencia: que el alcance que se atribuya en cada Estado al tipo penal de intrusismo informático queda a la libertad de éstos. Cada Estado «*podrá decidir*» que, sobre la base de la conducta de acceso no autorizado a un sistema informático, el delito establezca como único requisito específico la trasgresión de las medidas de seguridad («únicamente cuando la infracción se cometa transgrediendo medidas de seguridad*»). Pero ésta es una posibilidad que se ofrece a los Estados, no están obligados a que éste sea el único contenido asignable al delito de hacking, sino que pueden estructurarlo en base a otros requisitos.*

— Tercera consecuencia: subsisten, por lo tanto, las demás posibilidades de conformación de los tipos: cabe como opción básica, la respuesta más amplia de tipificación que pasa por configurar como típico el mero proceso del acceso no consentido a un sistema informático sin ni siquiera exigir penalmente la vulneración de las medidas de seguridad que protegen el sistema; se pueden mantener posiciones más estrictas al exigir, como acabamos de decir, que se violenten esas medidas, sin necesidad de apreciar ningún otro elemento ni en el autor ninguna orientación subjetiva; se puede requerir que el autor actúe movido por una finalidad específica, que puede ser cualquiera, ya que nada en este punto indica la Decisión; y es posible, como solución más restrictiva penalmente, que se exijan ambos ingredientes, un ánimo específico y el dato objetivo de la vulneración de las medidas de seguridad.

— Cuarta consecuencia: el marco dibujado por la Comisión no impide, incluso, que respetando ese mínimo de que se trate de un acceso no autorizado a un sistema informático, los legisladores nacionales opten por vincularlo a la protección de ciertos bienes jurídicos concretos, como la intimidad o el patrimonio, lo cual puede lograrse a través de la exigencia del elemento subjetivo mencionado o a través de elementos típicos objetivos, que manifiesten en sí mismos, externamente, un particular desvalor respecto a dichos bienes jurídico particulares. De esta mane-

46. MORALES GARCÍA, O.: «Apuntes de política criminal en el contexto tecnológico…», *op. cit.,* pág. 27.

47. PUENTE ABA, L.: «Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos…», *op. cit.*, pág. 386.

ra, el delito de intrusismo informático dejaría de ser el simple acceso ilegal a un sistema informático ajeno, para pasar a convertirse en una modalidad (la de intrusismo) referido a bienes particulares: intrusismo informático en la intimidad, intrusismo informático patrimonial[48].

Es decir, que pese a la tendencia punitiva más estricta que se adivinaba en la Propuesta de esta Decisión-marco en comparación a lo pautado por el Consejo de Europa, *el resultado final ha sido el de la concesión de un generoso espacio de decisión a los Estados*.

— Quinta consecuencia: la Decisión-marco presenta una proscripción penal del intrusismo informático que se puede calificar como «regulación de mínimos», ya que se opta por un diseñar un marco típico extenso; se contiene una decisión penal que refleja el espacio de tipicidad más amplio de cuantos esquemas de punición eran posibles, dejando a los Estados la posibilidad de estrecharlo.

— Sexta consecuencia: la opción armonizadora que emerge de esta regulación europea es la más tenue de cuantas cabían. La Unión Europea abre la puerta a una variada gama de regulaciones penales nacionales en la misma materia, solo unidas por el hecho de que en todas el acceder sin consentimiento es delito; ahora bien, en unos países las condiciones penales para su castigo pueden ser más estrechas que en otros y, con ello, el nivel de permisividad puede variar según el sistema elegido.

3.2.2. Breve referencia a la regulación penal de algunos países de nuestro entorno

A) Italia

El art. 615 *ter* del Código Penal dispone:

> *«El que abusivamente se introduce en un sistema informático o telemático protegido por medidas de seguridad o bien se mantiene en él contra la voluntad expresa o tácita de quien tiene derecho a excluirlo, es penado con….».*

Se trata de un precepto que, ubicado en el contexto de los «los delitos contra la libertad individual» del Capítulo III del Título XII (Delitos contra la persona), dentro de la sección 4.ª, sobre «los delitos contra la inviolabilidad del domicilio». Expresamente se atiende en él al intrusismo informático, con la exigencia de que se trate de sistemas protegidos con medidas de seguridad, sin necesidad de ulteriores finalidades en el sujeto activo. La legislación penal italiana desde antes de la entrada en vigor de la Decisión-marco sobre ataques contra los sistemas de información, ya contaba entre sus líneas punitivas con un marco típico para el intrusismo informático, sujeto, únicamente al requisito de que el acceso se diera en sistemas informáticos protegidos por medidas de seguridad. Según esta regulación del intrusismo informático, la legislación italiana no requiere adaptación alguna al proceso de armonización que en esta materia realiza la Decisión-marco, pues sobradamente se respetan las exigencias de la misma al superarse sus requisitos mínimos.

Merece la pena destacar el dato de la ubicación de este delito entre los que tutelan la inviolabilidad del domicilio, lo cual directamente indica que el bien jurídico tutelado es la inviolabilidad ofrece el «domicilio», como espacio de intimidad personal, si bien en este caso, el domicilio no es un espacio físico, sino un espacio informático, cuya intromisión no consentida representa una vulneración semejante a la producido por un allanamiento de morada, aun cuando con esta incursión no se descubra ningún dato de la vida privada[49].

B) Francia

El en Código Penal francés, el art. 323-1, en el ámbito de la regulación de los delitos de atentado contra los bienes, contiene en el Capítulo III, del Título II del Libro III, un precepto que sanciona directamente el intrusismo informático de una manera realmente amplia. Dice así:

> *«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».*

La legislación penal francesa cuenta también con un precepto expresamente destinado a tipificar el intrusismo informático y, además, lo hace en el sentido más amplio en el que es posible la tipificación según las directrices de la Unión Europea: sin ni siquiera necesidad siquiera de que se trate de conductas que se practiquen vulnerando los mecanismos de seguridad que protegen el sistema. Este modelo de objetivización máxima del tipo queda reflejado de modo patente en la fórmula claramente causalista empleada para la descripción: se castiga «*el hecho de acceder*». La opción francesa es extensamente punitiva, dada la no exigencia de otros requisitos típicos distintos al mero acceso, aunque en cualquier caso, encaja con el criterio amplio adoptado por la Decisión europea.

Sin embargo, entiendo que hay una vía para reducir el contenido causalista de la punición y es el que ofrece una posible expresión del acceder «de manera fraudulenta». Si por acceso fraudulento se entiende aquel que se realiza vulnerando las medidas de seguridad, la respuesta penal francesa estará en línea con lo proscrito en Italia. Ahora

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

49. PICA, G.: *Diritto penale delle tecnologie infomatique*, Utet, Turín, 1999, pp. 61 y ss.

bien, si se entiende que es acceso fraudulento es simplemente el acceso no autorizado por el titular, seguirá siendo un precepto meramente perseguidor del «hecho en sí» del acceso sin consentimiento, que se extiende incluso al caso de que sin dicha autorización se haya entrado en un sistema desprotegido.

C) Alemania

En el caso del Derecho alemán la prohibición del intrusismo se incardina en el espacio de los delitos contra la intimidad de la Sección Decimoquinta «Violación al ámbito de la intimidad personal y al ámbito del secreto personal», cuyo art. 202.ª, rubricado «Piratería informática» estipula:

«1.—Quien sin autorización se procure para sí o para otro datos que no estén destinados para él y que estén especialmente asegurados contra su acceso no autorizado, será castigado con pena privativa de la libertad hasta tres años o con multa.

2.— Datos en el sentido del inciso 1, son solo aquellos que se almacenan o trasmiten en forma electrónica, magnética, o de otra manera en forma no inmediatamente perceptible».

La incorporación al Código Penal alemán del intrusismo informático se ha hecho también de manera expresa, por lo que tampoco en este caso, es preciso la introducción de un tipo penal *ex novo*, si bien la estructura de delito es considerablemente distinta a la de los otros dos países: en este caso se trata de acceso a un sistema informático: a) en el que se contienen datos «especialmente asegurados contra su acceso no autorizado», es decir, se contiene el requisito de que ha de ser un sistema informático dotado de medidas de protección para sí y para los propios datos vertidos y almacenados en ese sistema; b) es necesario que el resultado de la conducta de acceso no se detenga solo en la vulneración de los sistemas de seguridad, sino que es preciso que haya un resultado material ulterior, cual es la obtención de datos que forman parte de la intimidad del titular de los mismo en tanto que «no están destinados para él».

El delito de intrusismo informático en el sistema penal alemán sigue, por tanto, una opción más restringida en la configuración del tipo que en los dos casos anteriores. A juicio de la doctrina, en el modelo alemán, el legislador penal ha tenido «ciertos reparos en castigar la mera penetración en un sistema informático ajeno»[50], pues lo que condiciona la tipicidad penal no es la mera llegada del *hacker* al disco duro de un ordenador, sino el contacto y acceso a los datos contenidos en él, lo cual acerca enormemente este tipo a un especial delito contra la intimidad.

Se trata, en todo caso, de una solución que entiendo acomodada a los parámetros de la Decisión-marco, que establece que la posibilidad de que se establezca como único requisito del tipo la vulneración de los sistemas es una facultad que se deja en manos de los Estados, pudiendo éstos optar por utilizarla o no o añadir más elementos típicos o no. Y así ha hecho el legislador alemán: ha incorporado un elemento resultativo que demanda para la consumación del tipo la verificación de un ataque a la intimidad del titular de los datos alcanzados por el *hacker*, quedando en consecuencia en el terreno de la tentativa los supuestos en que el acceso no consentido no llega a producir esa obtención de datos privados.

El modelo alemán encuentra, como veremos en adelante, un notable parecido con el sistema español que finalmente se esboza en la el Proyecto de Ley Orgánica de reforma del Código Penal, que tampoco se detiene en el acceso ilegal los sistemas, sino que reclama un «acceso a datos».

4. La respuesta del sistema español al intrusismo informático

4.1. Los intentos de encaje típico del intrusismo informático hasta la fecha

Hasta el momento, los estudios realizados acerca del intrusismo informático han venido sustentándose sobre la descripción de la conducta en abstracto. O mejor dicho, sobre la base de una caracterización teórica construida sobre lo que jurídicamente se debía entender por intrusismo informático *en estado puro*, a través del deslinde respecto a otros comportamientos que pudieran resultar próximos, tanto por modos de ejecución como por resultados causados. Siendo este el presupuesto del que se ha partido, los argumentos vertidos acerca de la aptitud de un tipo penal para incorporar en la órbita de su prohibición esta clase de comportamiento y la conveniencia o no de realizar una tipificación autónoma de ella no pueden calificarse sino como «especulación teórica» acerca del hipotético contenido, alcance y estructura típica que tendría un eventual tipo de *hacking* concebido bajo ese estereotipo de conducta.

En efecto, el paradigma de la conducta de «*hacking* puro», como he señalado más arriba al referirme a su delimitación y precisión terminológica, siempre ha venido definido por varias notas especiales. Objetivamente se ha caracterizado por ser: a) una conducta consistente en un mero acceso no autorizado a un sistema informático con vulneración de las medidas de seguridad[51] (o incluso sin atender a este dato); y b) una conducta que no ocasiona daños en el sistema, programa o datos informáticos objeto del acceso. Subjetivamente, se la ha restringido a los casos en que el autor no busca otra cosa que el mero acceso, actuando sin voluntad de acceder ni descubrir, datos o secretos, ocasionar algún perjuicio patrimonial, y menos

50. MIR PUIG, C.: «Sobre algunas cuestiones relevantes del Derecho penal en Internet», *Internet y Derecho penal,* Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2001, pág. 300.

51. GONZÁLEZ RUS, J.J.: «Los ilícitos en la red (I)…», *op. cit.*, pág. 244.

aún de producir ningún deterioro o destrucción de los datos o del propio sistema[52].

Así lo han subrayado autores que han analizado el tema con profundidad: MÓRON LERMA, que afirma que cuando hay «interceptación, ya no es por definición un *mero* acceso no consentido»[53]; similares son las palabras de MATA Y MARTÍN, según quien «el mero intrusismo (…) no se trata de acceso a los datos, sino al sistema informático mismo»[54], o de LÓPEZ ORTEGA, que sostiene que «si hay acceso a datos ya no hay un simple acceso inconsentido, sin algo más que el mero intrusismo informático»[55].

Con este presupuesto, se ha llegado, incluso, a esbozar a nivel doctrinal un modelo de tipo penal incriminador del *hacking*, al que se le asignaría un tenor literal semejante al siguiente: «*el que acceda inconsentidamente en un sistema informático o red telemática... será castigado...*»[56].

Pues bien, así perfilados los contornos del debate, cuando se ha trabajado acerca de la capacidad de los tipos penales vigentes en nuestra país para incluir bajo su cobertura el mero acceso no autorizado a un sistema informático, con buen criterio, el *resultado ha sido el de la negación de toda posibilidad de encontrar un encaje propio en cualquiera de ellos*. El análisis que desde mi punto de vista considero más exhaustivo de cuantos se han realizado hasta le fecha, el de E. MORÓN, da sobradas razones de esta inadecuación de los tipos de posible aplicación par abarcar con propiedad una conducta como el *hacking* puro. Todo lo más, llega a advertir la mencionada autora, el intrusismo puede ser la antesala de algunas de estas conductas, por lo que su punición deviene innecesaria al quedar absorbida por la conducta final. En la línea manifestada por esta autora, los argumentos, sintéticamente presentados para sostener esta opinión se pueden reducir a los siguientes:

a) No es posible incorporarlo bajo el espacio típico del art. 256, relativo a la utilización abusiva de terminales de telecomunicación.

El sentido político-criminal del mismo estriba en intentar reprimir el denominado «hurto de tiempo», o de «uso», o de «servicios» de equipos de telecomunicación, ante utilizaciones no autorizadas de los mismos. Inferencia que viene refrendada por la exigencia del citado perjuicio patrimonial, que está cuantificado en 400 euros, lo cual acota el ámbito típico. Además, y por interpretación sistemática con el art. 264.2, sobre sabotaje informático, en caso de que los perjuicios se causen sobre el *hardware* o el *software*, este último precepto sería de aplicación, de manera que el 256 tiene un carácter residual, limitado a los perjuicios consistentes en perturbaciones, alteraciones o molestias derivadas de la utilización del terminal de telecomunicación. Es obvio que la cuantificación de esas molestias en un perjuicio superior a los 400 euros, ocasiona un difícil problema de prueba y que, en todo caso, aun logrando dicha prueba, será absolutamente extraordinario, que una introducción no autorizada en el sistema informático, de manera que el titular de ordenador no pueda utilizarlo, pueda cifrarse en un perjuicio de más de 400 euros[57]. A ello habría que añadir el hecho de que el acceso a un sistema informático no supone necesariamente un uso del «*terminal*», es decir, del ordenador, como sí requiere el 256. El intruso no toma contacto con terminales ajenas, sino son los sistemas ajenos, para lo que se vale de su propio terminal que es el que realmente utiliza[58].

b) Tampoco es posible su encaje típico en los delitos contra la intimidad del 197.1 y 197.2. En el primer caso, porque la presencia de un elemento subjetivo específico, de «*descubrir los secretos o vulnerar la intimidad de otro*», diverge frontalmente con la naturaleza del *hacking* puro, desprovisto, por definición de intencionalidad[59]. Pero es que además «si hay interceptación, ya no es por definición un *mero* acceso inconsentido» y, a mayor abundamiento, desvela una intencionalidad de la que se hayan despojadas las conductas de intrusismo.

En cuanto al párrafo 2.º del 197, de nuevo, el argumento de la carencia de elementos subjetivos en el mero intrusismo determina la inadecuación de este tipo penal, que requiere un comportamiento movido por una actuación «*en perjuicio de...*»[60]. Y de nuevo, también se trata de conduc-

52. También esta conceptualización, en Sentencia del Juzgado de lo Penal nº 2 de Barcelona, de 28 de mayo de 1999, Fundamento Jurídico 1º, caso Hispahack.

53. MORÓN LERMA, E.: *Internet y Derecho Penal*..., *op. cit.*, pág. 60.

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

55. LÓPEZ ORTEGA, J.J.: «Intimidad informática y Derecho penal», *Derecho a la intimidad y nuevas tecnologías*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2004, pág. 119.

56. MORÓN LERMA, E.: *Internet y Derecho penal*…, *op. cit.*, pág. 80, nota 77.

57. MORÓN LERMA, E.: *Internet y Derecho penal*…, *op. cit.*, pp. 55-57.

58. LÓPEZ ORTEGA, J.J.: «Intimidad informática y Derecho penal», *op. cit.*, pág. 120.

59. MORÓN LERMA, E.: *Internet y Derecho penal*…, *op. cit.*, pág. 60; en contra, GONZÁLEZ RUS, J.J.: «Los ilícitos en la red (I)…», *op. cit.*, pág. 247; también en contra DE ALFONSO LASO, D.: «El *hackering* blanco. Una conducta ¿punible o impune?», en *Internet y Derecho Penal*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2001, pág. 521, porque considera que el mero hecho de que la vulneración de las medidas de seguridad (claves de acceso o *passwords*), es en sí misma una conducta de descubrimiento de un secreto, y por lo tanto, incorpora en sí misma el ánimo de vulnerar la intimidad que reclama el artículo 197.1 del Código Penal.

60. En contra, RUIZ MARCO, F.: *Los delitos contra la intimidad. Especial referencia a los ataques cometidos a través de la informática*, Colex, Madrid, 2001, pág. 78.

tas de apoderamiento, captación o acceso a datos[61], es decir, que superan la simple entrada en la red informática, adentrándose el intruso en el ámbito específico de la privacidad, en el sentido de capacidad de control sobre los datos previamente aportados. De nuevo, es algo distinto, *algo más que un mero hacking*.

c) El intrusismo informático tampoco se aviene a las exigencias típicas del delito del descubrimiento de secretos de empresa del art. 278. Este precepto castiga conductas que van desde el apoderamiento de datos que contienen un secreto de empresa, pasando por la difusión o revelación y cesión de los mismos. Dicha secuencia, de nuevo, hace que puedan darse por reproducidas las consideraciones anteriores acerca de las modalidades comisivas que, en el intrusismo, no son más que la entrada y/o permanencia en el sistema, pero sin acceder a dato o información alguna. Y, también aquí, porque la simetría con los delitos contra la intimidad de los arts. 197 y siguientes es evidente, la exigencia de un propósito directamente vulnerador de los secretos empresariales, elimina toda posibilidad de incorporar el mero acceso o *hacking* puro[62].

d) Y finalmente, tampoco es posible recurrir al delito de daños informáticos del art. 264.2, pues requiere una conducta destructiva o menoscabadora de los datos, programas o documentos contenidos en la red o sistema informático[63], conducta destructiva que no define al *hacking*, mucho más «limpio», porque no daña o, mejor dicho, no tiene voluntad de engañar, elemento subjetivo que sí requiere el sabotaje informático.

4.2. El debate doctrinal acerca de la incorporación de un tipo específico de hacking

A la vista de la especificidad de la conducta de *hacking* puro, que impide el recurso a los tipos vigentes hasta el momento, el debate se desplaza hacia la valoración de la conveniencia o no de una incriminación específica para esta conducta. Pues bien, las diferentes respuestas acerca de esta cuestión se han apoyado en razones de diferente contenido, que cabe organizar en torno a dos grandes grupos:

4.2.1. Razones de tipo dogmático

A) ¿Un nuevo bien jurídico? ¿Necesidad de protección penal?

La presencia de un tipo penal específico a las conductas de acceso subrepticio en un sistema informático ajeno sería la respuesta del Derecho penal ante la irrupción de un nuevo bien jurídico de carácter supraindividual o colectivo que podría denominarse, en palabras de GUTIÉRREZ FRANCÉS, «seguridad informática» o seguridad en el funcionamiento de sistemas informáticos, o «confianza en el funcionamiento de éstos»[64]. ROMEO CASABONA lo perfila como «el pacífico uso y disfrute de tales redes (telemáticas), o dicho de otro modo, la comunicación pacífica a través de redes telemáticas»[65]. Por su carácter difuso e inmaterial sería difícil de precisar, si bien su último referente material estaría constituido por la seguridad de la información, o lo que es lo mismo, el quebranto de la confidencialidad del sistema informático[66]. La pregunta es: ¿es realmente necesario atenderle penalmente? ¿El quebranto de esa estabilidad informática, tiene el desvalor suficiente como para ser merecedor de la más dura respuesta sancionadora que puede ofrecer el Derecho? Sobre este punto, las tendencias doctrinales son antagónicas:

Una primera opción es aquélla que rechaza la necesidad de dicha intervención penal porque en el Código es posible encontrar una respuesta a las situaciones en que normalmente se va a presentar el *hacking*: como antesala de otros delitos, de los que sería, consecuentemente una forma de tentativa. Se insiste en el dato aportado desde la criminología de que el *hacker*, por más que se mueva inicialmente por un puro deseo de diversión o de paseo por la red o sistema informático, difícilmente se va a resistir a hacer algo más: curiosear datos (consiguientemente estaríamos en el entorno típico de un delito contra la intimidad) o a utilizar su

61. Acerca de la dificultosa interpretación del artículo 197.2, y tratando de buscar una lógica a la manifiesta repetición de conductas en sus dos incisos, *vid.* CARBONELL MATEU, J.C./GONZÁLEZ CUSAC, J.L.: «Comentarios a los artículos 197 a 204 del Código Penal», *Comentarios al Código Penal de 1995*, Vol. I, (VIVES ANTÓN, Coord.), Tirant lo Blanch, Valencia, 1999, pág. 1001; en contra, MORALES PRATS, F.: «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», *Comentarios a la Parte Especial del Derecho Penal*, (QUINTERO OLIVARES, Dir.), Thomson-Aranzadi, Pamplona, 2005, pp. 426-427.

62. MORÓN LERMA, E.: *Internet y Derecho penal…*, *op. cit.*, pág. 66.

63.GONZÁLEZ RUS, J. J.: «El *cracking* y otros supuestos de sabotaje informático», *op. cit.*, pp. 221 y ss.; «Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (artículo 264.2 del Código Penal)», *op. cit.*, pp. 1295 y ss., entiende que el objeto material del precepto no ha de circunscribirse sólo a los elementos lógicos credos por el sistema (datos o programas), sino también al propio sistema.

64. GUTIÉRREZ FRANCÉS, M.: «Intrusismo informático (*hacking*). *¿Represión penal autónoma?, Informática y Derecho*, nº 12-15, 1994, pág. 1183.

65. ROMEO CASABONA, C. Mª.: «La protección penal de la intimidad y de los datos personales en sistemas informáticos», *Estudios Jurídicos del Ministerio Fiscal*, 2001, pág. 290. «Los datos de carácter personal como bienes jurídicos penalmente protegibles», *El Cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales* (ROMEO CASABONA, Coord.), Comares, Granada, 2006, pág. 189.

66. LÓPEZ ORTEGA, J.J.: «Intimidad informática y Derecho penal», *op. cit.*, pág. 120.

situación de privilegio para conseguir algún beneficio normalmente económico (podríamos aplicar alguna conducta de fraude económico)[67]. Además, es muy posible que a raíz de esa entrada subrepticia en el sistema genere algún destrozo al sistema[68] (y, en consecuencia, cabría acudir al delito de daños). El *hacking* es, más bien, la punta del iceberg de otras conductas de relevancia penal incuestionada y, por lo tanto, la necesidad de su incriminación específica carecería de sustento. En esta línea, señala GONZÁLEZ RUS que «a la postre, por tanto, lo que acaba decidiendo el carácter punible o no del acceso no autorizado a sistemas informáticos ajenos es la finalidad con la que el mismo se hace, resultando típico cuando, siendo un medio comisivo posible, el propósito del sujeto coincida con el del elemento subjetivo del injusto o el dolo propio de algún delito. (…), el simple acceso no autorizado podrá resultar punible si constituye tentativa de los correspondientes delitos»[69]. «Por ello, aunque sí parece emerger un bien difuso, inmaterial, digno de tutela, pero que, en ningún caso puede ser identificado apriorísticamente con un bien jurídico merecedor de protección penal»[70], ya que el principio de intervención mínima, con su componente de utilización racional y necesaria del Derecho penal, aconseja un abandono de respuestas incriminadoras específicas cuando ya existen posibles vías de castigo penal, a través de las figuras específicas en las que el *hacking* es solo su antesala. Así que, una adecuada respuesta penal a esos otros ilícitos, evita la necesidad de una incriminación *ad hoc*. Repetir ilícitos deriva en un saturación penal que genera conflictos concursales de dudosa adecuación a las exigencias de contención legislativa, pues la mera conducta de acceso no consentido daría lugar a un delito consumado que se encontraría con el tipo intentado correspondiente en función de la conducta finalmente manifestada por el intruso o del propósito especifico que se pudiera apreciar en él.

Frente a ella, una segunda opción es propicia a aceptar que estamos ante una conducta que supone en sí misma una agresión directa contra el interés del titular de un determinado sistema de que la información que en él se contiene no sea interceptada y, en esa medida, de necesaria respuesta expresa. Para quienes abonan esta segunda opinión, el sistema informático en sí también es un valor en sí mismo. La dimensión informática se configura como un nuevo espacio social, político, económico, que tiene como característica esencial su incorporeidad. En la red telemática lo esencial es el acceso y la información que suministra. Poder acceder a todos sus puntos facilita la comunicación entre sujetos e instituciones, el comercio, el ocio, la cultura... De ahí que la dificultad o la negación a este acceso pueda suponer una limitación vital: quien no tenga la posibilidad de acceder estará desconectado[71]. En la medida en que el acceso no consentido a sistemas ajenos representa un claro hueco para generar desconfianza en el funcionamiento de sistemas informáticos decisivos para el entramado relacional actual, «no puede en modo alguno considerarse un exceso de reacción penal»[72] la encaminada a su punición autónoma.

Dada esta realidad, el acceso no autorizado a un sistema informático o red de comunicación electrónica de datos supone una agresión contra el interés del titular o «propietario» del sistema o de la información. Interés en mantener su integridad, su reserva, aquello que le pertenece con exclusividad, con independencia del contenido de la información tratada y almacenada en el sistema afectado. Proteger al propietario, en sentido técnico, en el pacífico disfrute de su propiedad frente a inmisiones externas no autorizadas constituye una opción que resulta tan conforme a las exigencias del principio de intervención mínima como el delito de allanamiento de morada[73]. Y es más, en caso de que el sistema al que se accediera resultara de especial valor o fuera particularmente sensible por razón del tipo de información que en él se almacena (léase datos relativos a la defensa nacional, a la economía, etc.). La vulneración del normal desarrollo de las relaciones sociales o económicas resultaría altamente vulnerada pues, ¿quién podría confiar en que dichas relaciones discurren por un camino de seguridad y normalidad? Por ofrecer un ejemplo, si siempre tuviéramos dudad de que el sistema informático de los bancos estuviera en jaque ante la posible presencia de *hacker*s, ¿confiaríamos en el sistema bancario que a día de hoy condensa toda la información y realiza todos sus movimientos a través de sistemas informáticos?[74].

---

67. GUTIÉRREZ FRANCÉS, M.: «Notas sobre la delincuencia informática: atentados contra la «Información» como valor económico de empresa», *Estudios de Derecho penal económico* (ARROYO/TIEDEMANN, Eds.), Cuenca, 1994, pp. 206 y ss.

68. GONZÁLEZ RUS, J.J.: «El *cracking* y otros supuestos de sabotaje informático», *op. cit.*, pág. 246.

69. GONZÁLEZ RUS, J.J.: «Los ilícitos en la red (I)…», *op. cit.*, pp. 246-247 = «El *cracking* y otros supuestos de sabotaje informático», *op. cit.*, pág. 246.

70. MORÓN LERMA, E.: *Internet y Derecho penal*…, *op. cit.*, pág. 85.

71. ÁLVAREZ VIZCAYA, M.: «Consideraciones político-criminales sobre la delincuencia informática. El papel del Derecho penal en la red», en *Internet y Derecho penal*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2002, pág. 270.

72.Sentencia del Juzgado de lo Penal nº 2 de Barcelona, de 28 de mayo de 1999, Fundamento Jurídico 1º, caso Hispahack.

73. LEZERTÚA, M.: «El Proyecto de Convenio sobre el caber crimen del Consejo de Europa», Internet y Derecho penal, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2002, pág. 33, se refiere este bien jurídico como un «allanamiento de morada informática».

74. GUTIÉRREZ FRANCÉS, M.: «Intrusismo informático (*hacking*)…», *op. cit.*, pp. 1182-1183; SÁEZ CAPEL, J.: *Informática y delito*, Proa XXI, Buenos Aires, 2001, pág. 119.

En esta línea, parece posicionarse MIR PUIG, C.: «Sobre algunas cuestiones relevantes del Derecho penal en Internet», *op. cit.*, pág. 303.

B) Estructura típica para dar tutela a ese bien jurídico: el peligro abstracto

Pero además de las dudas que despierta la existencia de un auténtico bien jurídico-penal necesitado y merecedor de tutela penal consistente en el mantenimiento de una confianza en que el sistema informático funciona sin sobresaltos, los recelos se acrecientan en el momento de valorar la solución típica concreta que reaccionara frente a su perturbación por el *hacking* puro.

Un delito que incriminase el mero acceso no consentido a un sistema informático o red telemática ajeno sería un delito que se sumaría a la tendencia penal a la incriminación de la idea de *seguridad*[75], ahondando en una de las características que mejor definen el Derecho penal de la sociedad de riesgo, la tutela del pacífico disfrute de las actividades que rodean los actuales focos de riesgo estabilidad[76]. A través de él se daría respuesta a una opción político-criminal, propia de un Derecho penal férreamente preventivo, que consiste en incriminar estadios previos de perturbación de otros bienes jurídicos concretos que pudieran verse afectados, como pudiera ser la intimidad, el patrimonio, o la propiedad e integridad del sistema informático mismo, respecto a los cuales el delito contra la «seguridad del sistema» tendría un carácter instrumental, en tanto que actuaría de barrera de contención. Castigando la mera intromisión en sistemas se reacciona anticipadamente contra la posible producción de cuantiosos daños económicos o de perjuicios de otra índole, creándose así esta figura delictiva como una especie de «delito obstáculo»[77]. Lo que se trataría es de obstaculizar la comisión de otros hechos delictivos específicos (ataques a la intimidad o infracciones patrimoniales, por ejemplo) en los que los bienes jurídicos objeto de tutela presentan un alto índice de vulnerabilidad ante las utilizaciones abusivas de la informática, de modo que si el Derecho penal solo interviene cuando estos últimos ya se han lesionado, ya se habrían producido daños muy graves, extensos o irreparables; ante esta situación extrema, estaría justificado adelantar las barreras de protección castigando la conducta peligrosa previa, en este caso la intromisión no consentida, sin esperar a la producción de estas consecuencias[78].

De esta manera, en la medida que se da autonomía típica al acceso ilegal para prevenir otras lesiones o riesgos típicos relativos al manejo de sistemas informáticos (almacenamiento de datos, transacciones económicas, utilización misma del sistema, etc.), lo que técnicamente era una tentativa pasaría a convertirse en una figura autónoma que respondería a una estructura de delito de peligro abstracto, que castiga la potencialidad peligrosa de la conducta[79] para afectar gravemente a los bienes jurídicos especialmente vulnerables frente a empleos clandestinos de la tecnología informática e Internet. Ahora bien, el acceso no autorizado a sistemas informáticos no suponen automáticamente la puesta en peligro grave de un número delimitable de patrimonios, o de intimidades, es decir, no tiene por qué originarse un riesgo para un conjunto más o menos amplio de individuos. Las manipulaciones informáticas suponen tan solo una nueva forma, en general más fácil y segura, de cometer el concreto atentado patrimonial o contra la intimidad, pero tal acceso o interferencia no suponen de por sí un riego para una variedad de bienes jurídicos concretos[80].

En definitiva, semejante opción típica, con sus consabidos déficits de ofensividad material[81], en conexión con el castigo de presunciones (estadísticas si se quiere) de peligro, entroncan con un Derecho penal más represor de una voluntad criminal que de actos efectivamente lesivos (o, al menos efectivamente peligroso)[82] y en definitiva, aconsejan, de nuevo en sede de intervención mínima, un repudio de su incorporación al catálogo delictivo. Y todo ello sin olvidar que de estas objeciones se deduce, a su vez, un problema de índole formal, el de la ubicación sistemática, pues, ¿dónde sería más adecuado su encaje en la actual estructura del Código Penal, dado su carácter de delito-contención de otros delitos específicos?[83], ¿en los delitos patrimoniales?; ¿y si con la aplicación del delito se ha evitado una perturbación a la intimidad personal?, entonces, ¿en los delitos contra la intimidad?; ¿y si con él se ha evitado una estafa a los clientes de un banco? ¿Sería entonces su sede idónea, la de los delitos contra la seguridad colectiva?

75. ANARTE BORRALLO, E.: «Incidencia de las nuevas tecnologías en el sistema penal…», *op. cit.*, pp. 191 y ss.

76. SÁNCHEZ GARCÍA DE PAZ, I.: *El moderno Derecho penal y la anticipación de la tutela penal*, *op. cit.*, pp. 38 y ss.

En la línea de lo que apuntaba más arriba al tratar acerca de de esta vinculación con el Derecho penal de la sociedad de riesgo; vid. supra, epígrafe 3, 3.1.2.- El «ciberespacio», el «hombre-digital» y la «sociedad de riesgo».

77. Sobre éste concepto, GARCÍA ALBERO, R.: «LA tutela penal y administrativa de la salud de los consumidores en materia alimentaria. Consideraciones críticas en torno a su articulación jurídica», *Revista Jurídica de Cataluña*, nº 4, 1990, pág. 98.

78. PUENTE ABA, L.M.ª: «Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos», *op. cit.*, pág. 400.

79. LÓPEZ ORTEGA, J.J.: «Intimidad informática y Derecho penal», *op. cit.*, pág. 120.

80. PUENTE ABA, L.M.ª: «Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos…», *op. cit.*, pág. 402.

81. RODRÍGUEZ MONTAÑÉS, T.: *Delitos de peligro. Dolo e imprudencia*, Universidad Complutense de Madrid, Madrid, 1994, pp. 247 y ss.

82. ROMEO CASABONA, C. Mª.: «De los delitos informáticos al Cibercrimen…», *op. cit.*, pág. 16.

83. Duda que se formula, MORÓN LERMA, E.: *Internet y Derecho penal…*, *op. cit.*, pág. 79.

La alternativa consistente en la elaboración del tipo bajo la estructura de delito de peligro concreto de los individuales bienes jurídicos que pudieran verse afectados no elude del todo las críticas anteriores. Es obvio que elimina la idea de presunción de riesgo sobre tales bienes jurídicos particulares, en la medida en que las afecciones a los mismos pasan a convertirse en elementos de obligado presencia y prueba, pero ello no hace sino pasar a primer término la tesis de que la seguridad en los sistemas informáticos no es un auténtico bien jurídico *per se*, sino una pieza intermedia e instrumental[84] para la integridad de otros bienes específicos, hacia las que se orientaría el tipo, que podría quedar formulado como «*El que acceda sin consentimiento a un sistema informático, poniendo en concreto peligro los datos relativos a la privacidad, etc.*». Claro que, de nuevo, lo que esta solución genera es un problema orden sistemático, en tanto que ocasiona la necesidad de ir elaborando tipos de delito concreto en cada uno de los ámbitos penales relativos a los bienes jurídicos de eventual afección. Esta reiteración típica (una vez como delito de peligro y otra como delito de lesión efectiva), con la consiguiente necesidad de dar una respuesta a lo que técnicamente constituye un concurso de normas, hace surgir de nuevo la sombra de la duda de si no estaríamos ante una solución contraria a las exigencias de una intervención penal reducida a lo indispensable[85].

Frente a estas objeciones, quienes defienden la necesidad de la intervención penal y apuestan por el reconocimiento de un auténtico bien jurídico-penal (recuerdo, la seguridad de los sistemas informáticos) consideran que el delito de intrusismo informático puro constituye un auténtico delito de lesión, carente, eso sí, de un resultado material distinto al solo acceso y por lo tanto, estructurado a través de la acción de acceso subrepticio, que en sí misma constituye el resultado lesivo sobre ese bien jurídico de nuevo cuño[86]. Para quienes así opinan, pese a que formalmente el tipo se estructuraría como una figura de peligro abstracto, ello no es un óbice para sostener su efectiva lesividad, pues realmente «el peligro parece abstracto únicamente si es referido a otros intereses individuales, mientras que si se toman en consideración los aspectos supraindividuales (sociales) del bien jurídico (…) estos intereses son lesionados (y no únicamente puestos en peligro) por el delito»[87]. Se trataría, por tanto, de un delito de mera actividad, integrador, en sí mismo, de un elevado componente de lesividad sobre el nuevo bien jurídico que se violenta de manera efectiva desde el momento en que el *hacker* se introduce en el sistema, dejando totalmente de lado otras finalidades u otros resultados lesivos, que de concurrir, en todo caso, darían lugar a tipos independientes y ya consolidados en nuestro sistema. Es decir, el tipo de *hacking* introduce una forma de lesión a un bien jurídico desconocido hasta este momento y, por ello, sirve para colmar una laguna en nuestro ordenamiento jurídico que demanda una protección añadida a los sistemas informáticos que no consiguen ofrecer, dada su especificidad, los tipos vigentes hasta la fecha

4.2.2. Razones de política criminal

A) Relativas a la dificultad de descubrimiento y prueba de los tipos

Sobre la base de la constatación criminológica ya reseñada de que los delitos cometidos mediante el ordenador presentan una alta cifra negra, derivada de las dificultades de detección y prueba de su comisión, la doctrina discrepa sobre la virtualidad de este dato para justificar la conveniencia práctica de un tipo específico para el intrusismo informático.

Para unos, esta dificultad de detección de los ilícitos cometidos por medio de la informática alienta la necesidad de incriminar estadios previos a la lesión efectiva del bien jurídico protegido en los tipos particulares, puesto que evitaría la impunidad de otros atentados de mayor gravedad. Así, no pudiendo castigar por ejemplo el fraude, por falta de pruebas, pues que al menos sea posible castigar el previo intrusismo, el acceso ilícito al sistema[88]. Para otros, sin embargo, una razón de índole tan pragmática resulta en exceso simplista y peligrosa desde la perspectiva de la exigencia de una intervención penal legítima, que lo es en tanto se estructure sobre criterios de idoneidad y necesidad de la intervención por existir un auténtico bien jurídico-penal, y no sobre razones de facilidad o rapidez en la respuesta[89]. Mantener que razones de carácter práctico, relativas a la mayor facilidad para acabar con ilícitos de mayor gravedad de los que el intru-

84. Sobre esta implicación entre los bienes jurídicos intermedios y los delitos de peligro concreto, *vid.* MATA Y MARTÍN, R.M.: *Bienes jurídicos intermedios y delitos de peligro*, Comares, Granada, 1997, pp. 78 y ss.

85. Se destaca cómo además de significar un exceso de intervención punitiva, la repetición de injustos supone una perversión de la legalidad, en la medida en que incorpora directamente casos de non bis in idem, a resolver por las reglas del concurso de normas, que como señala MIR PUIG, S.: *Derecho penal. Parte general*, Reppetor, Barcelona, 2004, pág. 651, que en algunos casos (supuesta de la alternatividad del artículo 8.4º) no hacen sino delatar que el legislador erró al incorporar un precepto que ya existía.

86. GUTIÉRREZ FRANCÉS, M.: «Intrusismo informático (*hacking*)…», *op. cit.*, pág. 1184, donde mantiene que «si lo que estuviera tras el *hacking* fuera algún bien jurídico de nuevo cuño, tampoco exigiría el recurso a la tan denostada estructura de los delitos de peligro».

88. TIEDEMANN, K.: *Poder económico y delito (Introducción al Derecho penal económico y de la empresa)*, Ariel, Barcelona, 1985, pág. 36.

89. GUTIÉRREZ FRANCÉS, M: «*Intrusismo informático (hacking):* ...», *op. cit.*, pág. 1180.

sismo es solo su inicio, constituyen una base en la que justificar el adelantamiento de la intervención penal, supone un inversión «perversa»[90] de los términos del raciocinio penal, en la medida en que implícitamente deja entrever que no es precisamente el Derecho penal lo más adecuado sino la vía más fácil y más rápida, por lo que soterra las soluciones apoyadas en criterios de legitimidad de la intervención vinculados a la necesidad de tutela a las que tupe mediante un vulgar abultamiento del sistema punitivo. Con ello, el resultado es que si existían dificultades para perseguir esos delitos, lo que seguirá sucediendo es que esa misma dificultad seguirá estando, incluso más agravada, pues ahora hay que descubrir la comisión delictiva antes de que salgan a la luz sus efectos lesivos, con lo cual, el efecto habrá sido conservar (e incluso agrandar) los fallos siendo, por lo tanto, una vía de actuación justificado de las carencias del sistema penal. Si lo que hace falta es facilitar el descubrimiento de esos delitos, la solución, lógicamente, ha de venir de la dotación de mecanismos armonizadores a nivel internacional, para evitar «fugas», o, a nivel interno, de la especialización de los operadores jurídicos implicados en esa persecución (mayor inversión para la creación y formación de unidades especializadas)[91], pero no abrir otros frentes delictivos en los que vuelven a plantearse los problemas de descubrimiento y prueba.

Y es más, se aduce que aceptar que incriminando el estadio anterior a los comportamientos graves supone un avance en el deseo de reducir la elevada cifra de delitos que quedan sin respuesta, posiblemente no sea más que un espejismo jurídico, un argumento basado en una mera conjetura, porque, si es muy difícil descubrir el hecho ulterior más grave, ¿cómo se va a descubrir el momento previo, que es más silencioso y carente de resultados lesivos «visibles»?[92] Recuérdese que el *hacker* actúa «borrando» pistas y que, justamente, lo que menos le interesa es dejar cualquier huella en el sistema que le cierre el camino y le impida volver a repetir su conducta.

B) Relativas a la función preventiva del Derecho penal

Se ha alegado cómo las respuestas penales utilizadas en algunos ordenamientos jurídicos, como el norteamericano en el que el recurso a la sanción penal ha servido para generar en la población una conciencia reacia hacia estas conductas que siempre han venido gozando de una complacencia por parte de la ciudadanía[93]. La repulsa social ante lo que se ha considerado una conducta claramente lesiva de un nuevo interés o de otros bines jurídicos respecto a cuya afección el *hacking* es el primer paso se ha ido consiguiendo a base de «educación» penal. En nuestro país, ello supone una legitimación del recurso a la función promocional del Derecho penal que atiende al hecho de que en una sociedad democrática, la fijación de un modelo de convivencia no puede ser una decisión agotada, sino un proyecto en constante evolución, por lo que el Derecho no se puede limitar a la conservación de un determinado orden social preexistente, sino que también va a ser un factor condicionante de su desarrollo y de la búsqueda de nuevas metas, lo cual le confiere una orientación crítica al Derecho penal, superadora de una opción meramente conservadora o estabilizadora del sistema[94].

Frente a esta posición, se arguye que la incapacidad de motivación del intruso informático, que actúa con la consideración de que sus conductas lejos de ser contrarias a derecho representan una exhibición de dominio frente a la máquina a la que son capaces de superar. En esa medida, la necesidad de respuesta penal decae por innecesaria, ya que está de antemano condenada a no generar ninguna utilidad preventiva[95]. La prevención general no puede ser la única justificación de la pena, pues se atenta gravemente contra la dignidad del hombre al que se le hace sufrir un castigo no fundado en la gravedad del acto que ha causado, sino en el deseo de enseñar a otros e intimidarlos para que no le imiten. La justificación de la intervención del Derecho penal solo desde el punto de vista de la prevención general acaba por comprometer el principio de proporcionalidad y otorgar primacía, de nuevo, a la búsqueda de respuestas eficaces y rápidas en defecto de las garantistas[96].

90. TERRADILLOS BASOCO, J.: «Función simbólica y objeto de protección del Derecho penal», *Pena y Estado*, nº 1, PPU, Barcelona, 1991, pág. 10.

91. Es el término que emplea MORÓN, E.: *Internet y Derecho Penal...*, *op. cit.*, pág. 82.

92. Ibidem, pág. 82.

93. NIMMER, R.T.: *The law of computer technology*, New York, 1985, pp. 9 y ss.

94. HOLLINGER, R.C./LANZA-KADUKE, K.: «The process of criminalitation. The case of computer crime laws», *Criminology*, vol. 26-1º, 1988, pp. 114 y ss.

95. Sobre esta función «promocional», vid. BERDUGO GÓMEZ DE LA TORRE, I./ARROYO ZAPATERO, L.: *Manual de Derecho penal. Parte General. I. Instrumentos y principios básicos del Derecho penal* ROMEO CASABONA, C.M.ª: *Poder informático y seguridad jurídica, op. cit.,* pág. 40.

96. MORÓN LERMA, E.: *Internet y Derecho Penal..., op. cit.,* pág. 83.