El intrusismo informático (Hacking): ¿Represión Penal Autónoma?

MARILUZ GUTIÉRREZ FRANCÉS

Departamento de Derecho Público. Area Penal Universidad de Salamanca

I. INTRODUCCION

En unas Jornadas celebradas en Madrid a finales de febrero de 1992 sobre Seguridad Informática, la Organización nos sorprendió en la última de las sesiones con la intervención de un joven *hacker* informático, quien nos desveló con algún detalle -y no sin cierto orgullo-, su principal afición: pasar largas horas delante de su ordenador personal y, con la ayuda de un *modem* y del teléfono, descubrir las vías de entrada secretas a grandes sistemas informáticos de entidades y empresas públicas y privadas de toda índole. Ante el asombro de los allí presentes, el joven *hacker* nos refirió algunas de las técnicas empleadas para alcanzar su objetivo; enumeró, como si de un trofeo se tratara, un listado de redes y sistemas informáticos a los que había logrado acceder subrepticiamente (de distintos Ministerios y organismos públicos, de entidades financieras, de seguros, agencias de viaje, etc.). E hizo referencia a la existencia, ya sólo en España, de varios miles de jóvenes que participaban de su misma afición/pasión, en permanente comunicación a través de los *electronic bulletin boards systems*, que les servían para compartir y transmitir las técnicas y métodos de infiltración descubiertos.

Apenas sin reflejos para reaccionar, finalmente alcanzamos a preguntarle si no tenía la más mínima conciencia de estar actuando de forma ilícita, incorrecta o, cuanto menos, irregular, a lo que respondió, casi ofendido, que no: primero, porque él no era un *cracker*, sino un *hacker*, al moverle únicamente la intención de "acceder", "interceptar" sistemas o comunicaciones electrónicas de datos, sin perseguir causar perjuicios; y, segundo, porque sólo cabía imputar la responsabilidad por estas conductas de intrusismo a las empresas y entidades que mantenían tales deficiencias en materia de seguridad.

Que hayamos seleccionado este caso para abrir la presente exposición -en lugar de acudir a otros, ciertamente más espectaculares, de los que suministra la literatura estadounidense, alemana o japonesa, por ejemplo-,[1] se debe al extraordinario impacto que entonces nos causó:

1º porque suponía una indubitada confirmación de algo que, tras varios años de investigación sobre cuestiones planteadas por la delincuencia informática, sólo habíamos llegado a conocer a través de estudios criminológicos realizados más allá de nuestras fronteras (fundamentalmente, de la mano de autores como PARKER, NYCUM, NIMMER, BEQUAI o SIEBER):[2] el alto grado de vulnerabilidad de los sistemas de procesamiento electrónico de datos, de la información en estos almacenada y de las comunicaciones electrónicas. Esta nota dejaba de ser una simple intuición o un artículo de fe. "La informática se ha instalado entre nosotros; pero también sus riesgos", habíamos admitido hasta entonces sin reservas.[3] Pues bien, al escuchar a nuestro joven *hacker*, -cuyas características, curiosamente, se ajustaban con exactitud al estereotipo de "delincuente informático" que presentaban los primeros estudios criminológicos-, se comprendía que dichos "riesgos" tampoco entre nosotros podían considerarse una mera anécdota. Hablamos de una realidad bastante más seria;

2º porque incrementó notablemente nuestra curiosidad sobre un aspecto de la criminalidad informática que sólo habíamos abordado incidentalmente y de forma marginal en trabajos anteriores: el intrusismo informático o *hacking*. Y como fruto directo de ese renovado interés, nos proponemos, a continuación, esbozar algunas reflexiones que entendemos suscita el tema, más bien orientadas a abrir cauces para un futuro debate en torno a esta parcela de la criminalidad informática: el debate, todavía pendiente, sobre la caracterización y delimitación de las conductas de *hacking*; sobre las posibilidades que ofrecen, para su represión, tanto el Derecho positivo como los textos punitivos en proyecto; y, muy especialmente, sobre el bien o bienes jurídicos en juego, con las consecuencias que de este punto central se deriven en orden a una eventual tipificación autónoma.

- 1 *Vid.*, por todos, SIEBER, U., *The International Handbook on Computer Crime*, John Wiley and Sons, Chichester, 1986, pp. 15-20; BEQUAI, A., *Technocrimes. (The Computerization of Crime and Terrorism)*, Heath Lexington Books, Lexington, 1987, *passim.*
- 2 GUTIERREZ FRANCES, M., *Fraude informático y estafa*, Servicio de Publicaciones del Ministerio de Justicia, Madrid, 1991, pp. 39 y ss.
- 3 ult. cit., p.43.

II. CARACTERIZACION DEL INTRUSISMO INFORMATICO

No hallamos en la doctrina un concepto unívoco sobre lo que aquí venimos invocando con la expresión "intrusismo informático", como tampoco se ha logrado consenso en punto a qué ha de entenderse por "delincuencia informática" (categoría más amplia de la que, en principio, el "intrusismo informático" debiera formar parte.)[4] Este mismo dato, unido a la inexistencia, en el Derecho positivo español, de una figura siquiera asimilable al presente objeto de nuestro estudio, nos confiere una cierta dosis de flexibilidad, que, sin embargo, nunca será absoluta. En efecto, no es posible ignorar experiencias legislativas próximas a la nuestra (donde se conocen, y en muchos casos se tipifican, conductas de intrusismo informático, tal es el caso de Francia, Grecia, Estados Unidos, etc.),[5] ni los trabajos elaborados por expertos en materia de delincuencia informática, bajo el auspicio de diversas organizaciones internacionales (en cuyas resoluciones se reconoce como un grave problema de las sociedades de nuestro tiempo, y se recomienda encarecidamente a los Estados la represión del intrusismo informático. En tal sentido, las recomendaciones de la Organización para la Cooperación y Desarrollo Económico, de 1985, las del Consejo de Europa, de 1990, las de Naciones Unidas, de 1992, o las de la Asociación Internacional de Derecho Penal, del mismo año).[6]

Tomando, pues, tan cualificados puntos de referencia, advertimos, desde ahora, que el objeto de nuestro actual interés se circunscribe al conjunto de comportamientos de acceso o interferencia no autorizados -de forma subrepticia- a un sistema informático o red de comunicación electrónica de datos, y a la utilización de los mismos sin autorización.

Sin embargo, tal delimitación resulta insuficiente, pues, como ya advierte SIEBER,[7] el acceso no autorizado a sistemas informáticos puede llevarse a cabo por motivaciones bien diversas: puede formar parte de un juego, o responder a la simple curiosidad, o a un reto permanente del hombre frente a la máquina (se trata de poner a prueba la seguridad de un sistema informático, descubrir

- 4 Una visión más amplia sobre los problemas para caracterizar y sistematizar las distintas manifestaciones de la criminalidad informática en GUTIERREZ FRANCES, cit., pp. 49-70.
- 5 *Vid.* VASSILAKI, I., "Computer Crimes ans Other Crimes against Information Technology in Greece", *International Review of Penal Law. AIDP.*, vol. 64, érès, 1992, pp. 361 y ss.; DEVEZE, J., "Commentaire de la loi nº88-19 du 5 janvier 1988 relative a la fraude informatique", *Lamy droit de l'informatique*, febrero, 1988, pp. 3 y ss.; sobre la regulación de las conductas de *hacking* en los Estados Unidos, tanto a nivel estatal como a nivel federal, GUTIERREZ FRANCES, ult. cit., pp. 123 y ss.
- 6 Bien es cierto que las conductas de acceso y uso no autorizado de sistemas informáticos se hallan en la llamada "lista opcional", y no en la "lista de *minimum*", al no existir consenso en torno a la necesidad de su criminalización. *Vid.* Council of Europe, *Computer-Related Crime*, Recommendation Nº. R(89) on Computer-Related Crime, Strasbourg, 1990, pp. 60 y ss.
- 7 SIEBER, *The International Handbook...*, cit., p. 19.

sus escapes, como sucede en muchos de los casos de *hacking* de aficionados); mas, junto a tales hipótesis, al tiempo han de citarse otros casos en los que el intrusismo informático obedece a objetivos más graves, como sabotear, espiar, defraudar o falsificar. Es decir, en muchos de los ilícitos informáticos el acceso ilícito forma parte del *modus operandi*, quedando absorbido por el hecho principal; y el examen de su eventual tratamiento jurídico penal corresponderá, en su caso, a la sede del espionaje, o a la del sabotaje, o al marco de las defraudaciones, o de las falsedades... Evidentemente, no son estos los delitos que despiertan aquí nuestro interés, si bien resultará inevitable alguna referencia a los mismos. Por lo demás, hay que reseñar que, cualquiera que sea la concreta solución que los distintos ordenamientos jurídicos prevean para hechos como los anteriores, no resultan particularmente conflictivos: se admite, sin excepción, que son o debieran ser merecedores de una sanción penal. Interesa, en cambio, aquí, otro bloque más problemático de supuestos: los de intrusismo informático propiamente dicho, en expresión de SIEBER,[8] integrado por las conductas de mero acceso y/o permanencia no autorizados en un sistema informático, las interferencias subrepticias en las comunicaciones electrónicas de datos y las conductas de uso no autorizado de computadora, también conocido como "hurto de servicios" del ordenador,[9] pero despojadas de toda intención de dañar, perjudicar, lucrarse o falsificar..., distinta al acceso mismo.

En este punto, correspondería un acercamiento a la caracterización de estos comportamientos, de sus autores y de sus víctimas. Sin embargo, apenas nos detendremos en tal dimensión, pues, si como parece, los hechos conocidos constituyen sólo la punta del iceberg,[10] las investigaciones que se han llevado a cabo desde la perspectiva criminológica han debido tomar como referencia tan parca muestra, lo que nos induce a cuestionar la veracidad y fiabilidad de los resultados obtenidos. Nos limitaremos, por tanto, a hacer sólo algunas observaciones:

*En primer término, debemos recordar que precisamente en el *hacking* se ha encontrado el filón más importante de los estudios criminológicos en la todavía reciente historia de la delincuencia informática. Tan es así, que aun hoy hallamos descripciones del "delincuente" y del "delito informático" que son verdaderas reproducciones miméticas -y casi míticas- de los primeros *hackers* descubiertos en los Estados Unidos y de las conductas de intrusismo informático por ellos realizadas. A nuestro juicio, es tiempo de poner fin a dicha simplificación:

- 8 SIEBER, U., "Documentación para una aproximación al delito informático", Trad. U. Joshi, *Delincuencia informática*, S. Mir Puig (Comp.), PPU, Barcelona, 1992, p.77.
- 9 DURHAM, C., "The Emerging Structures of Criminal Information Law: Tracing the Contours of a New Paradigm", *International Review of Penal Law. AIDP.*, vol. 64, cit., pp. 100-101.
- 10 *Vid.* GUTIERREZ FRANCES, *Fraude informático...*, cit., pp. 80 y ss.

consideramos injustificado -confundir la parte con el todo- el identificar delincuente informático/*hacker* o delito informático/*hacking*. Lo cierto es que, de llegar a merecer la calificación de delictivas en un ordenamiento jurídico concreto, las conductas de los llamados "piratas informáticos", en el mejor de los casos, sólo serán una aspecto de la criminalidad informática y, seguramente, ni siquiera el más representativo.

*En segundo término, quisiéramos contribuir desde estas líneas a la desmitificación del *hacker* informático. Es verdad que, del examen de los hechos conocidos, parece inferirse que el *hacker* suele ser un joven, entre quince y veinte años, por lo general varón, de clase media-alta, de coeficiente intelectual superior a la media (y, en ocasiones, calificado como superdotado), social y familiarmente integrado, y con una absoluta falta de conciencia de estar actuando ilícitamente (con frecuencia, afectado por el "síndrome de Robin Hood"). Mas, aunque todo esto resultara, al fin, ajustado a la realidad, nuevamente la escasez de hechos descubiertos aconseja mantener un margen razonable para la duda. Porque, ¿quién puede asegurar que en lo que ha salido a la luz justo hallamos la expresión del arquetipo de *hacker* o "pirata informático"? ¿No existen, más bien, razones para sospechar que precisamente los hechos más sofisticados y mejor ejecutados técnicamente, así como los autores más hábiles, astutos y capacitados serán los que permanezcan en el anonimato, engrosando esa extraordinaria cifra negra[11] de la delincuencia vinculada a las nuevas tecnologías de la información?

*Desde la perspectiva de los autores, en cualquier caso, sí nos inclinamos a admitir, con BEQUAI, que normalmente responderán a la caracterización criminológica del conocido como "delincuente de cuello blanco", pese a que la popularización creciente del ordenador pueda, en un futuro próximo, alterar dicha comprensión (en la medida en que el ordenador vaya implantándose, como un instrumento más de "trabajo", entre delincuentes habituales, grupos terroristas, organizaciones mafiosas, narcotraficantes, etc., según sugiere el propio autor, apoyándose en ilustrativos ejemplos).[12]

*En cuanto a los hechos, nada más lejos de nuestro ánimo que pretender aquí una descripción de técnicas y modos de infiltración subrepticia (cuestión que dejamos a técnicos y expertos).[13] Sí nos interesan, desde un punto de vista penal y procesal, ciertos rasgos que pueden incidir en la prueba y eventual represión de estas conductas: primero, el desarrollo de las nuevas tecnologías

- 11 *Vid.* SIEBER, U., *The International Emergence of Criminal Information Law*, vol. I, Carl Heymanns Verlag KG, Köln, 1992, pp. 6-8.
- 12 BEQUAI, A., *Computer Crime*, Heath Lexington Books, Lexington, 1978, pp. 1-4.
- 13 Describe algunas de las técnicas y métodos de infiltración de los *hackers* el Manual de Naciones Unidas sobre delincuencia informática, *vid. United Nations Manual on Computer-Related Crime (Draft)*, September, 1992, pp. 17-18.

favorece las actuaciones a distancia, desde una terminal de un sistema, desde el lugar de trabajo o desde el ordenador personal de la mesa o escritorio privado; en la propia ciudad, o en otra distinta, a muchos kilómetros, incluso más allá de las fronteras nacionales. Todo ello, unido a la intercomunicación que parece existir entre los *hackers*, como comentábamos anteriormente, incrementa la peligrosidad de estos hechos (en un breve lapso de tiempo, la vía de infiltración al sistema informático de una empresa o multinacional puede ser conocida -y utilizada- por el gran colectivo internacional de *hackers*)[14] y dificultará considerablemente su descubrimiento y prueba. No olvidamos, sin embargo, que el primer obstáculo en orden a la detección y prueba del *hacking* se halla en la habitual ausencia de todo rastro de la conducta -que suele pasar absolutamente inadvertida para la propia víctima cuando no va acompañada de alguna suerte de alteraciones de datos o no provoca alguna perturbación en el sistema-. Además, cabe reseñar que la dinámica comisiva propicia la continuidad delictiva (descubierta la puerta falsa del sistema, no será infrecuente que se acceda de forma reiterada, incrementándose, de este modo, los riesgos).

III. EL INTRUSISMO INFORMATICO A LA LUZ DEL DERECHO POSITIVO ESPAÑOL.

Sólo conociendo los avateres y sobresaltos políticos que ha vivido nuestro país en los últimos tiempos, se acierta a comprender que aún no haya sido encarada la extraordinaria y necesaria empresa de modernizar el Derecho punitivo. La cuestión resulta particularmente sangrante en materia de criminalidad informática, ni siquiera vislumbrada por el legislador del diecinueve, pero que tampoco se ha visto favorecida por ninguna de las sucesivas reformas de que ha sido objeto el Código Penal español desde la entrada en vigor de la Constitución. Así las cosas, habremos de seguir aferrándonos a las figuras delictivas tradicionales -con todas sus lagunas y limitaciones, como bien se ha denunciado por la doctrina y la jurisprudencia dentro y fuera de nuestras fronteras-[15] como única vía posible para encauzar las nuevas manifestaciones de la criminalidad surgidas al socaire de las altas tecnologías de la información.

- 14 *Ibidem.*
- 15 Por todos, ROMEO CASABONA, C.M., "Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías", *Poder Judicial*, nº 31, Consejo General del Poder Judicial, Septiembre 1993, pp. 163 y ss.; GUTIERREZ FRANCES, M., "Notas sobre la delincuencia informática: atentados contra la información como valor económico de empresa", *Estudios de Derecho Penal Económico*, (Ed. L. Arroyo Zapatero y K. Tiedemann), Colección Estudios, nº 18, Ediciones de la Universidad de Castilla-La Mancha, 1994, pp. 183 y ss.

Pero fijémonos ahora en la suerte que pueden correr, a la luz de nuestro Derecho Penal vigente, las conductas que venimos denominando como intrusismo informático. (Adviértase que no sometemos a debate, de momento, la cuestión preliminar en torno al bien o bienes jurídicos que pudieran estar en juego con estos comportamientos, ni la procedencia o improcedencia de una tipificación autónoma de todas o algunas de sus manifestaciones, aspectos que serán abordados más adelante). Las posibilidades que nos ofrece la regulación actual se reducen, a nuestro juicio, a las siguientes:

*El mero acceso sin autorización y de forma subrepticia a un sistema informático, cualquiera que sea el titular o usuario de dicho sistema y sea cual fuere el contenido de la información en el mismo tratada, en principio resultará impune. Ni contamos con una figura específicamente diseñada al efecto (en la línea del art. 370C, pfo.2 del Código Penal griego, o del art. 462.2 del Código Penal francés, por ejemplo), ni cabe el recurso a alguna de las figuras tradicionales del texto punitivo actual.

Ahora bien, no podemos ignorar que, en la realidad de las cosas, quien accede subrepticiamente a un sistema informático, frecuentemente "hará algo más". Cuesta creer que todos o la mayoría de los *hackers* carecen, incluso, hasta de la más mínima curiosidad y que su conducta se detiene en el momento de vencer el obstáculo que representan los sistemas de seguridad (es decir, descubierto el escape o puerta falsa del sistema, o la clave de acceso secreto, conseguido el objetivo, se salen del sistema). Parece, a todas luces, poco realista. Más nos inclinamos a pensar que lo habitual será justo lo contrario: que, al menos, intentarán conocer o descubrir en todo o en parte la información secreta o reservada a la que se ha logrado acceder. Y decimos que "intentarán conocer", porque el acceso al contenido y el entendimiento de la información interferida no siempre será posible: pensemos, a título de ejemplo, en los supuestos en los que el autor carece de capacitación técnica suficiente para aprehender el contenido de la información interceptada (v.gr.: unos planos sobre estrategias militares que le resultan incomprensibles; procedimientos expresados en fórmulas matemáticas indescifrable para el profano; textos en lengua extranjera...), o bien, habiendo accedido al sistema, sólo capta ciertos datos, carentes de valor desgajados de otros que se presentan como inaccesibles. Pues bien, si nos centramos sólo en los casos en los que el *hacker* se infiltra en el sistema y descubre la información total o parcialmente (aún estamos en "lo mínimo" que probablemente hará el pirata informático: "entrar y mirar"), en este punto ya empezaría a tener trascendencia la titularidad del sistema afectado por la conducta de intrusismo y la naturaleza de la información vulnerada:

a) Si se tratara de datos relativos a la *privacidad* de los individuos (utilizando la expresión que ya ha hecho suya el legislador en la LORTAD, por las razones que indica en la Exposición de Motivos de dicha Ley),[16] las posibilidades que ofrece el Código vigente son prácticamente nulas, como ha puesto de relieve nuestra más cualificada doctrina.[17] La formulación típica de los dos tipos penales con particular vocación para proteger penalmente el bien jurídico intimidad (art. 497 y art. 497 bis) constituyen una barrera infranqueable para su aplicación a las conductas que ahora examinamos: el primero, por circunscribir su ámbito a los secretos contenidos en "papeles y cartas", que han de ser objeto de "apoderamiento material", y el segundo, porque exige que el autor intercepte las telecomunicaciones o utilice instrumentos o artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen (según la nueva redacción incorporada por la Ley Orgánica 18/1994, de 23 de diciembre).[18] En suma, si un sujeto accede desde su microordenador, a distancia, en el sistema informático del Hospital Clínico Universitario, por ejemplo, y descubre los datos médicos reservados relativos a su vecino, contenidos en la historia clínica informátizada del banco de datos del Hospital, realiza un comportamiento impune, aun cuando posteriormente los divulgue. (No se olvide que, en cambio, sí sería punible, por la vía del artículo 497 vigente, la conducta del sujeto que, hallándose en casa de su vecino, se apodera del informe médico que le ha remitido el Hospital; de la lectura de dicho informe, descubre aquellos aspectos reservados relativos al precario estado de salud de su vecino y los divulga entre la comunidad de propietarios).

b) Si el contenido de la información interceptada y descubierta consiste en **secretos empresariales o comerciales** que afectan a la capacidad competitiva de una empresa en el mercado, las perspectivas no son mejores. Desde luego, si

- 16 Justifica el legislador por qué opta por la expresión "privacidad" en la Exposición de Motivos de la LEY ORGANICA 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal: "Nótese que se habla de la privacidad y no de la intimidad: Aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en la que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado."
- 17 Sobre la inadecuación del Derecho Penal vigente para la protección de la *privacy, vid.* MORALES PRATS, F., *La tutela penal de la intimidad: privacy e informática*, Ed. Destino, Barcelona, 1984, *passim.*; ROMEO CASABONA, "Tendencias actuales...", cit., pp. 177-179.
- 18 La reforma de este precepto (como la del art. 192 bis, por idénticas razones), era demandada por la doctrina casi desde su incorporación al Código Penal, en 1985, al dejar impunes todos los atentados contra la intimidad mediante la utilización de artificios de reproducción o grabación de la imagen. No obstante, llama la atención la prisa repentina por cubrir esta laguna, cuando ya hoy se han detectado muchas otras lagunas en la actual regulación, acaso más graves, justamente en materia de atentados contra la intimidad por medios informáticos, que la reciente reforma no resuelve. Quizá hubiera merecido la pena aprovechar la ocasión y hacer el esfuerzo por aprehender de una forma más acabada y completa los atentados contra la intimidad, particularmente ante el futuro incierto del Proyecto, y por si este se retrasara más aún.

el intruso informático consigue la entrada subrepticia al sistema informático de una empresa sin otro ánimo, en principio, que el vencer las medidas de seguridad de que ha sido dotado, y sólo después, al calibrar la importancia de la información descubierta (v.gr.: carteras de clientes, balances y estado de cuentas, archivos, procedimientos tecnológicos y estrategias comerciales, etc.), con ánimo de lucro decide hacer uso, en perjuicio del titular, de aquella información de valor para el tráfico económico de la industria o comercio, entonces carecerá de importancia que el *hacking* pueda ser o no castigado como delito. Nos encontraríamos ante un supuesto de "espionaje informático empresarial" y procedería examinar los cauces para su posible represión en el Derecho actual. Pero no es esta la sede para el estudio del espionaje informático, aun tratándose de una de las parcelas donde el Código vigente presenta mayores lagunas, como reiteradamente viene denuciándose.[19] (Baste recordar que, más allá de las posibilidades que la Ley -extrapenal- de Competencia Desleal, y de la limitada virtualidad que poseen en esta materia la normativa para la protección de la propiedad intelectual y de la propiedad industrial, en el Código Penal hoy el secreto industrial se protege mediante una figura tan anacrónica y limitada como el art. 499, dirigido al "encargado, empleado u obrero de una fábrica u otro establecimiento industrial que en perjuicio del dueño descubriere los secretos de su industria..." Es decir, de partida, no cabe la protección penal del secreto industrial frente a las conductas de terceros ajenos a la empresa o industria afectada). Pues bien: si los hechos susceptibles de ser catalogados como "espionaje informático" sólo muy difícilmente podrían reprimirse a la luz de nuestro Derecho positivo -nuevamente, ante la ausencia de una tipificación específica, frente a la tendencia más extendida en el Derecho comparado-,[20] con menor motivo hallaremos una vía para la represión del mero intrusismo informático que afecte a sistemas de procesamiento electrónico de datos de empresas de cualquier índole.

c) Sólo cuando se trata del acceso no autorizado a sistemas que almacenan y procesan información sobre cuestiones relativas a la **defensa nacional** ("información legalmente clasificada, relacionada con la seguridad nacional o la defensa nacional o relativa a los medios técnicos o sistemas empleados por las Fuerzas Armadas o las industrias de interés militar", dice el Código en su art. 135 bis a), el sólo llegar al conocimiento de tal información podría castigarse a tenor de dicho artículo 135 bis a, referido a quien, "sin propósito de favorecer a una potencia extranjera, se procurare, revelare, falseare o inutilizare" aquella información. (Nótese que la formulación típica es suficientemente amplia como para abarcar los supuestos de *hacking*, especialmente a través del verbo "procu-

- 19 *Vid.* GUTIERREZ FRANCES, "Notas sobre la delincuencia informática...", cit., pp. 186-193.
- 20 Una panorámica global sobre la tipificación del espionaje informático en los ordenamientos jurídicos próximos al nuestro, en DURHAM, "The Emerging Structures...", cit., p.104, nota 88.

rarse", que puede ser aplicado a los casos en los que se llega al conocimiento de la información reservada por la simple lectura de los datos en pantalla).(Nótese, también, que de conformidad con este precepto, un supuesto de mero intrusismo informático sobre los sistemas informáticos del Ministerio de Defensa puede llevar aparejada una sanción de privación de libertad de hasta seis años). Desechamos, sin embargo, la posibilidad de aplicar la figura paralela a la anterior, del artículo 122bis del Código Penal, por exigir al autor la actuación con el propósito de favorecer a una potencia extranjera. Se trataría, más bien, de una conducta de espionaje contra la seguridad exterior del Estado que un problema de intrusismo informático, y deliberadamente hemos excluido tales hechos de nuestro estudio.

Finalmente, -y marginando, como se apuntó, el acceso no autorizado a un sistema de proceso de datos con finalidad defraudatoria, o de sabotaje, o con ánimo de falsear datos-, lo cierto es que el mero acceso por "puro deporte" no siempre resulta tan inocuo como algunos pretenden. Con harta frecuencia ocasiona perjuicios no perseguidos directamente por el *hacker*, aunque pudieran serle imputados al menos a título de imprudencia: modificaciones o supresión total o parcial de datos; perturbaciones o alteraciones en el normal funcionamiento del sistema; obstaculización del acceso al sistema a sus legítimos usuarios; contagio de "virus informáticos" de extraordinarios efectos sobre la información, etc. Ante todo este elenco de posibles consecuencias, tampoco protege el ordenamiento punitivo vigente a los titulares y usuarios de los sistemas informáticos de modo suficiente. Con las notables limitaciones que ha detectado la doctrina,[21] cabría plantear la aplicación de las figuras de daños, siempre que los perjuicios irrogados fueran de carácter patrimonial, y en la medida en que se admita una lectura de los tipos vigentes distinta a la tradicionalmente admitida.[22] Pero, ¿qué solución adoptaríamos ante perjuicios de naturaleza diversa, no patrimoniales o no cuantificables? Más allá de la agravación del artículo 558.5º del Código Penal (si los daños se producen "en un archivo, registro, museo, biblioteca, gabinete científico, institución análoga o en el patrimonio histórico-artístico nacional"), supuesto notablemente limitado, una vez más, por la exigencia de que se ocasione daño en patrimonio ajeno cuyo importe exceda de 250.000 pesetas, sólo se nos ocurre otra posibilidad: si la información afectada por el *hacking* se refiere a los medios o recursos de la defensa nacional, intentaríamos la subsumción de la conducta en el tipo del artículo 135 bis e). Dicho pre-

- 21 Sobre las dificultades para la aplicación de los delitos de daños al sabotaje informático, *vid.*, CORCOY BIDASOLO, M., "Protección penal del sabotaje informático. Especial consideración de los delitos de daños", *Delincuencia informática*, S. Mir Puig (Comp.), PPU, Barceloba, 1992, pp. 145 y ss.; GUTIERREZ FRANCES, "Notas sobre la delincuencia informática...", cit., pp. 199-203.
- 22 GUTIERREZ FRANCES, ult. cit., nota 53, p. 201.

cepto, formulado en términos suficientemente amplios, tendría aquí, a nuestro juicio, alguna virtualidad, ya que castiga al que "destruyere, dañare de modo grave, o inutilizara para el servicio, aun de forma temporal, obras establecimientos o instalaciones militares, buques de guerra, aeronaves militares, medios de transporte o transmisión militar, material de guerra, aprovisionamiento u otros medios o recursos afectados al servicio de las fuerzas armadas..."

Inevitablemente, debemos concluir que los canales para la protección de la integridad de la información suministrados por nuestro texto punitivo, al menos hasta este punto, resultan insatisfactorios.

*Las posibilidades, en cambio, de castigar la interferencia no autorizada en una comunicación electrónica de datos informátizados parecen mayores, a la vista del vigente artículo 497bis. Apreciamos aquí, sin embargo, algún obstáculo relevante a destacar. En primer término, desde la perspectiva del bien jurídico, se trata de un precepto que tiende a la protección del bien jurídico intimidad personal (frente a las posibles agresiones mediante artificios técnicos de escucha o reproducción del sonido y de la imagen), extremo éste en torno al que se respira un consenso prácticamente absoluto entre los autores.[23] Pese a todo, la referencia alternativa a los "secretos o la intimidad" ("El que para descubrir los secretos o la intimidad de otro...") suministra un cauce para orientar la aplicación de tal delito a la protección de secretos no relativos a la intimidad. En cualquier caso, será preciso forzar la interpretación del precepto para aplicarlo a supuestos de interferencia en la transmisión electrónica de datos, aun por vía telefónica, cuando dichos datos no sean concernientes a la intimidad personal.[24] El segundo obstáculo lo hallamos en la misma formulación típica, que impide, en puridad, reconducir por esta vía cualquier interferencia en las comunicaciones electrónicas de datos no preordenadas por ese elemento subjetivo del injusto ("para descubrir los secretos o la intimidad de otro..."), o los casos en los que la información interceptada no concierna a la intimidad personal o no pueda ser calificada de secreta (por no constituir un conocimiento reservado a un círculo determinado de personas, con exclusión de las demás).[25] La virtualidad del artículo 497 bis frente a las conductas de *hacking* reseñadas queda, en suma, bastante mermada.

- 23 Por todos, MUÑOZ CONDE, F., *Derecho Penal. Parte Especial*, 9ª ed., Tirant lo Blanch, Valencia, 1993, pp. 159 y ss.
- 24 Algunos autores, como LEDERMAN y SHAPIRA, en Israel, proponen ampliar el ámbito del delito de escuchas ilegales para dar cabida inequívoca a las interferencias en las transmisiones electrónicas de datos: LEDERMAN, E., SHAPIRA, R., "Computer Crimes and Other Crimes against Information Technology in Israel", *International Review of Penal Law. AIDP.*, vol. 64, cit., pp. 403-405. En sentido similar, en España, CORCOY, M., JOSHI, U., "Delitos contra el patrimonio convertidos por medios informáticos", Separata de la *Revista Jurídica de Cataluña*, nº 3, 1988, p. 147.
- 25 *Vid.* MORALES PRATS, F., "Problemática jurídico-penal de las libertades informáticas en España tras diez años de vigencia de la Constitución de 1978", Separata de *Estudios Penales y Criminológicos*, XII, 1989, pp. 361 y ss.

* En un ordenamiento como el nuestro, en el que el hurto de uso es impune salvo cuando se trata de vehículos de motor ajenos -en la misma línea, la mayoría de las legislaciones próximas-,[26] no cabría esperar que el uso no autorizado de ordenador y programas informáticos fuera considerado delito. Evidentemente, si el legislador español aún no ha procedido a la tipificación de otros comportamientos ilícitos vinculados a las nuevas tecnologías de la información respecto a los que se respira, a nivel nacional e internacional, un cierto consenso en orden a su punición, menos aún habría de hacerlo respecto a una conducta sobre cuya represión existe un total desacuerdo.

IV. A LA ESPERA DE UN NUEVO CODIGO PENAL

Todavía expectantes ante la suerte que haya de correr el último Proyecto de Código Penal, y sin demasiada esperanza -minada ésta por tanto intento previo fracasado-, nos aproximaremos, a continuación, al estado actual de las cosas a nivel de Proyecto. El texto de referencia, presentado a Cortes el pasado septiembre de 1994, incorpora innovaciones en materia de delincuencia informática notables. Con todo, se mantiene aún bastante alejado -acaso con acierto- del nivel de "juridificación" de esta expresión de la realidad criminal propuesto en las distintas sedes internacionales antes apuntadas.

Las conductas de mero intrusismo informático (acceso no autorizado a un sistema informático, interferencia subrepticia en una transmisión electrónica de datos y uso no autorizado de un sistema informático o programa de ordenador) no son objeto de una regulación específica suficiente en el Proyecto de Código Penal de 1994.

Y es que, no puede estimarse como suficiente la previsión del artículo 254 donde se castiga entre las "defraudaciones de fluido eléctrico y análogas", al que "hiciere uso de cualquier equipo terminal de telecomunicación, subrepticiamente, y sin consentimiento de su titular, ocasionando a éste un perjuicio superior a ciencuenta mil pesetas". La incardinación sistemática de tal infracción (entre los delitos patrimoniales), así como su conformación típica (conducta dolosa que ha de provocar un perjuicio cuantificable, identificable, superior a ciencuenta mil pesetas), revelan una percepción bastante simplista de la realidad del intrusismo informático, minimizando injustificadamente. La fórmula, muy poca ambiciosa a nuestro juicio, ignora que el intrusismo informático más rele-

26 *Vid.* DURHAM, "The Emerging Structures...", cit., pp. 100-101.

vante no se halla necesariamente unido a un perjuicio patrimonial cuantificable, según apuntábamos. Por lo demás, no resultará siempre fácil compatibilizar este nuevo tipo con la previsión incorporada al párrafo segundo del artículo 261, donde se contempla, también desde la óptica de la lesión patrimonial, la destrucción, alteración, inutilización o daños causados en programas, datos o documentos electrónicos ajenos, contenidos en soportes o sistemas informáticos. Finalmente, debe resaltarse que, a la luz del mencionado artículo 254, resultarán punibles las conductas de "hurto en tiempo de máquina", pero siempre condicionado a la demostración del perjuicio irrogado que prescribe el precepto. En suma, a la vista de estos datos no cabe afirmar que el Proyecto se ocupe satisfactoriamente del intrusismo informático a través del artículo 254, cuyo futuro, mucho tememos, puede quedar reducido a una función meramente testimonial.

Adicionalmente, habida cuenta de la estrecha relación del *hacking* con otros comportamientos delictivos más graves, la suerte que corra el intrusismo informático -si acaso llegara a convertirse el Proyecto en Derecho positivo- resultará eventualmente afectada por la nueva regulación propuesta frente a estas otras conductas. En un breve repaso, mencionaremos ahora aquellas disposiciones del Proyecto que, a nuestro juicio, incidirán de modo más relevante en la futura represión del *hacking*:

*La nueva regulación de los delitos de "descubrimiento y revelación de secretos" en el texto de 1994, inequívocamente diseñados como atentados "contra la intimidad y el domicilio", solventa algunas de las limitaciones de la normativa vigente. El artículo 188, de especial interés para nosotros, posibilitará el castigo de los "piratas informáticos" que accedan subrepticiamente a archivos y registros informatizados y bancos de datos de carácter personal o familiar, o cuando interfieran la transmisión electrónica de datos de esa misma naturaleza, siempre que alcancen aprehender su contenido (es decir, el simple acceso al sistema, sin acceder al contenido de los datos, no será punible; pero si, una vez infiltrado en el sistema, el *hacker* conoce, descubre el contenido de los datos personales, la conducta merecerá sanción penal). Esta conclusión pasa por una interpretación de la desafortunada fórmula verbal utilizada ("se apoderase de datos...") en un sentido distinto al actual, que permitiera incluir la simple lectura y memorización de los datos en pantalla, sin la exigencia de un desplazamiento material de algún tipo de soporte físico. (Confiamos que la fórmula sea mejorada en la discusión parlamentaria, de modo que el verbo "apoderarse" -históricamente vinculado a la exigencia de "desplazamiento material"- sea sustituido por otro más adecuado a la conducta de captación de datos por cualquier medio, incluida la simple lectura, memorización y reproducción manteniendo intacto el original. Sería también deseable una ampliación del tipo que permi-

tiera reprimir conductas impunes a la luz del artículo reseñado, como el tráfico de datos de carácter personal).

*Dentro de los "delitos contra el patrimonio y contra el orden socioeconómico", hallamos otra figura que sin duda incidirá en la suerte de las conductas de intrusismo informático, el artículo 273, que castiga al que, "para descubrir o revelar un secreto de empresa obtenga, por cualquier medio, datos, documentos escritos o electrónicos, soportes informáticos u otros objetos, o empleare alguno de los medios o instrumentos señalados en el apartado primero del artículo 188..." Concluye estableciendo: "Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieren corresponder por el apoderamiento o destrucción de los soportes informáticos". No es éste, desde luego, el momento de valorar críticamente la protección que dispensa al secreto industrial o comercial el Proyecto.[27] Pero, de la lectura del tipo indicado, parece inferirse que el prelegislador aprehende mejor las conductas de intrusismo en los sistemas informáticos de empresa, aún sin pretenderlo, que el espionaje industrial por medios informáticos, como parece ser su objetivo. (Baste observar que el tipo se conforma con exigir al autor "ánimo de descubrir o revelar un secreto de empresa...", aunque de hecho no se descubra ni revele nada. No se estima relevante la naturaleza de los datos interceptados, ni siquiera el valor o importancia que tengan para la empresa víctima. No se exige que se actúe con ánimo de afectar a la capacidad competitiva de la empresa en el mercado, ni la intención de obtener un lucro. En suma, entendemos que, a este tenor, resultaría punible la conducta del "pirata informático" que se infiltra subrepticiamente en el sistema informático de una multinacional, por ejemplo, y, movido por la curiosidad, lee en pantalla sus listas de clientes, balances y estrategias de mercado, información de la que después no hará uso ilícito. (Entendemos que la expresión "obtenga, por cualquier medio..." debe incluir también la simple lectura de datos en pantalla).

*La última de las versiones del Proyecto de Código Penal incorpora otra novedad en materia de delincuencia informática ya mencionada. Dentro de la regulación de los delitos de daños, y tras la descripción de las formas agravadas, el artículo 261 procede a la tipificación de sabotaje informático, al disponer en su segundo párrafo: "La misma pena se impondrá al que destruyere, alterare, inutilizare o de cualquier modo dañare los datos, programas o documentos electrónicos ajenos contenidos en soportes o sistemas informáticos, por cualquier medio". El juego que puede desplegar este precepto, en relación con los artícu-

■ 27 Algunas de las deficiencias que plantea la regulación propuesta para reprimir el espionaje industrial por medios informáticos, en GUTIERREZ FRANCES, "Notas sobre la delincuencia informática...", cit., pp. 193-198. (Aunque se toma como referencia el Proyecto de 1992, no existen, en este punto, diferencias respecto al Proyecto de 1994.)

los 264 y 265, en la parcela del *hacking* es notable (prescindiendo ahora de la eventual superposición parcial de tal previsión y la contenida en el artículo 254 referido). Pues, si como advertíamos anteriormente, el *hacker* no persigue, en principio, causar daños, (no modifica, destruye o inutiliza datos de propósito, por la propia delimitación que hemos hecho del *hacking*) no cabría la aplicación de un delito doloso de daños; en cambio, aquí cobra un especial interés el concreto diseño de los tipos imprudentes en el Proyecto, a fin de conocer si será posible el castigo cuando se ocasionen perjuicios por imprudencia. Es por ello que conectábamos el párrafo segundo del artículo 261 con el artículo 265, ya que en este último se establece el régimen general del tipo imprudente de daños: "Los daños causados por imprudencia grave en cuantía superior a veinte millones de pesetas, serán castigados con la pena de multa..."

Adicionalmente, el artículo 264 presenta un tipo imprudente de daños especial, para cuando estos se provoquen, también por imprudencia grave, "en un archivo, registro, museo, biblioteca, centros docentes, gabinete científico, institución análoga o en bienes de valor artístico, histórico, cultural, científico o monumental", siempre que la cuantía del perjuicio sea superior a cincuenta mil pesetas. (Entendemos que también son objeto de protección por este cauce los archivos y registros informatizados, públicos o privados).

Del examen de esta regulación en proyecto, y sin apartarnos del objeto prioritario de nuestra investigación, cabe inferir que se amplían las posibilidades de actuar penalmente contra los "piratas informáticos" que, por una falta grave de cuidado, provoquen la modificación o supresión de datos informatizados, inutilicen o perturben el correcto funcionamiento del sistema en que se han infiltrado, obstaculicen el acceso al mismo a los usuarios autorizados, o infecten con "virus informáticos" los ordenadores o programas. Pero esa eventual reacción penal se ve limitada, primero, por la incardinación sistemática de estas figuras, dentro de los atentados contra el patrimonio (¿puede decirse que la introducción de un "virus informático" en el sistema informático de un complejo hospitalario, por ejemplo, que provoca la inutilización parcial del mismo, constituye un atentado contra el patrimonio?) y, segundo, por la exigencia de un perjuicio -patrimonial- cuantificable, identificable, susceptible de ser traducido en una cantidad de pesetas (que, por lo demás, no podrá ser inferior a la cifra que en cada uno de los preceptos señalados indica el Proyecto). (¿Cómo valoramos, en precios de mercado, los perjuicios que ocasiona a los usuarios legítimos de un sistema el que se les entorpezca, dificulte u obstaculice la normal utilización del mismo como consecuencia de las conductas de intrusismo, por ejemplo?).

*Recordamos, en fin, que el Proyecto también regula expresamente, en el artículo 241.2, la estafa por medios informáticos -de la que nos hemos ocupado en otro lugar- y consagra en el artículo 26, con gran transcendencia a los efectos de las falsedades documentales, un concepto amplio de "documento", (en el sentido en que ya se había pronunciado el Tribunal Supremo en Sentencia de 19 de abril de 1991), incorporando el documento producido electrónicamente. No dudamos que dichas previsiones, en caso de convertirse en Derecho positivo, afectarán también a la represión de las conductas de intrusismo informático cuando se integran en hechos más graves, como fraudes informáticos o falsedades por medio de manipulación informática.

Concluimos este rápido repaso indicando que el Proyecto, probablemente de forma no meditada -y aquí está lo grave-, ha seguido la opción de legislaciones como la alemana o japonesa, que mantienen impunes los comportamientos de mero *hacking* con carácter general, al estimarse que, cuando son hechos realmente graves, siempre les será de aplicación alguna otra figura delictiva ya consagrada, ya sea uno de los delitos tradicionales, ya uno de los de nuevo cuño antes mencionados. Ahora bien, aferrarse al criterio del perjuicio patrimonial cuantificable como indicador de la gravedad de un hecho, constituye, particularmente en esta parcela, una criticable reminiscencia decimónica que el Proyecto no logra superar y que limita ostensiblemente su virtualidad.

V. REFLEXIONES SOBRE LA TIPIFICACION AUTONOMA DEL INTRUSISMO INFORMATICO

Sorprende que, a estas alturas, cuando ya muchas legislaciones de nuestro entorno se han decidido por la represión penal de las conductas de mero intrusismo informático, atendiendo a las recomendaciones emitidas reiteradamente desde distintos foros de la comunidad internacional (Consejo de Europa, OCDE, Naciones Unidas, Asociación Internacional de Derecho Penal), en España no haya sido abordado seriamente el tema, ni en nuestra doctrina ni, por lo que conocemos, en los trabajos preparatorios del Proyecto de nuevo Código Penal. Cuando se cita, a título de ejemplo, algún supuesto de *hacking* -siempre extraído de una realidad social distinta a la nuestra-, más bien parece invocado a modo de anécdota curiosa y hasta divertida, pero no como motivo para una reflexión seria. Y, por otra parte, la solución que hallamos en el Proyecto tampoco parece fruto de una decisión meditada, a diferencia de lo que ha ocurrido en otros países como Alemania. El tema, a nuestro juicio, merece mayor atención que la de una anécdota, aunque sólo sea por algunas de las razones que apuntamos:

1º Los estudios criminológicos realizados en otros países demuestran que, comportamientos inicialmente de mero intrusismo informático -detectados pero no reprimidos en su momento-, desprovistos, inicialmente, de toda intención distinta al propio "acceso no autorizado", terminaron convirtiéndose en otros ilícitos mucho más graves, como fraudes, espionaje informático, sabotaje, atentados contra la intimidad, etc. Descubierta la puerta de entrada a un sistema, su punto vulnerable, el *hacker* difícilmente se resiste a agotar las posibilidades que tiene a su alcance, y comete atentados contra el patrimonio, contra la intimidad, contra la seguridad del Estado, etc. Aunque mantengamos intactas nuestras reservas sobre la fiabilidad de los resultados obtenidos en aquel tipo de estudios, según hemos justificado, lo cierto es que conocemos algunos ejemplos paradigmáticos de la criminalidad informática que avalarían el argumento anterior:

*En Nueva Jersey (EE.UU), en 1985, la policía en un suburbio de la ciudad requisó, a varios jóvenes de diecisiete años, los ordenadores personales, impresoras, radios y discos de ordenador llenos de información. Se les acusaba, entre otras, de las siguientes infracciones: conspiración para el uso ilícito de computadoras, sustracción de números de tarjetas electromagnéticas para hacer llamadas de larga distancia y compras de equipos electrónicos. Posteriormente, también se descubrió que habían interceptado los sistemas informáticos del Pentágono, llegando a modificar, mediante manipulaciones a distancia, importantes datos secretos relativos a la construcción de material de defensa y situación de satélites artificiales.[28]

*En Hamburgo (Alemania), a comienzos de la década de los ochenta, salió a la luz el caso del *Chaos Computer Club*, cuyos integrantes habían logrado interceptar diversos sistemas informáticos a nivel nacional e internacional (incluidos, entre ellos, el sistema de videotex de Correos en Alemania Occidental, o los sistemas de procesamiento de datos de la NASA). Minimizada por las autoridades, entonces, la importancia de aquellas infiltraciones informáticas a distancia, unos años después, los mismos sujetos fueron detenidos por diversas infracciones patrimoniales por medio de manipulaciones informáticas y por la venta a la antigua Unión Soviética de información secreta, interceptada de forma subrepticia por medios informáticos.[29]

Se argumenta, en este sentido, que castigando el *hacking* se adelanta la barrera de protección frente a hechos más graves, bien sean provocados de propósito (se accede subrepticiamente sin otra intención que el jugar o el "poner a

- 28 MARBACH, W.D., KASINDORF, m., SANDZA, R., "Was It Really War Games?", *Newsweek*, vol. 106, julio, 1985, p. 23.
- 29 SIEBER, *The International Handbook...*, cit., p. 19.

prueba" a la máquina, y de forma sobrevenida se decide la comisión de un fraude, o se copia información secreta, o se falsifican datos informatizados...), bien de forma no intencional (sin perseguirlo, el *hacker* que accede sin autorización modifica o borra datos, provocando perjuicios de entidad, o se imposibilita el acceso al sistema a otro usuario del mismo con autorización...). Así se explican las palabras de DEVEZE, cuando califica como "delito obstáculo" la figura tipificada en el artículo 462.2 del Código Penal francés, introducida por la Ley nº88-19 de 5 de enero de 1988, y que castiga "al que accede a un sistema informático o se mantiene en el mismo sin autorización". Según comenta el mismo autor, dicha tipificación responde a una vieja demanda de la práctica y de la doctrina, y en la misma se procede a incriminar el intrusismo independientemente del resultado -como primera fase, que suele ser, de un fraude más grave-.[30]

2º También se dice, en la misma línea, que la intervención penal en tales supuestos evitaría la impunidad de otros de mayor entidad, pero de difícil descubrimiento y prueba. (Constando, en ocasiones, la comisión de un fraude, por ejemplo, sin embargo, lo único que puede probarse es la entrada ilícita y subrepticia al sistema. Así, no pudiendo castigar por el fraude, por falta de pruebas, que al menos sea posible castigar el intrusismo, el acceso y utilización ilícita del sistema).

El argumento, por pragmático que resulte, entendemos que no puede considerarse baladí, habida cuenta de que son precisamente los problemas de descubrimiento, prueba y persecución el más grave obstáculo para la represión de la delincuencia informática,[31] en particular, cuando se trata de infracciones a distancia, realizadas por autor desconocido y con conocimientos técnicos suficientes para introducir rutinas o series de rutinas que hagan desaparecer todo rastro del ilícito principal cometido. Si las cuestiones de prueba y persecución pueden llegar a convertir en simple papel mojado incluso la más completa y acabada regulación, posiblemente la represión de todas o algunas de las conductas de acceso no autorizado paliaría dichos riesgos.

3º En ordenamientos jurídicos como el estadounidense, se han invocado, asimismo, razones de "educación a la población", lo que para nosotros sería "prevención general", función de motivación de la norma penal. Como hacen notar HOLLINGER y LAZA-KADUCE,[32] las primeras leyes para reprimir estas conductas han realizado una función simbólica (en el sentido de "educar",

- 30 DEVEZE, "Commentaire de la loi nº 88-19 du 5 janvier 1988...", cit., p. 5.
- 31 SIEBER, "Documentación para una aproximación...", cit., pp. 90 y ss.
- 32 HOLLINGER, R.C., LANZA-KADUCE, J., "The Process of Criminalization: The Case of Computer Crime Laws", *Criminology*, vol. 26, nº 1, 1988, pp. 114 y ss.

"socializar" y "moralizar" a los usuarios del ordenador), transmitiendo a los jóvenes disidentes de las clases privilegiadas un mensaje claro acerca del valor de la propiedad y de la *privacy*; pues, se había llegado a una situación en que la sociedad miraba con simpatía esta clase de hechos, y faltaba toda conciencia social de ilicitud -por no mencionar el conocido "síndrome de Robin Hood"[33] de los propios *hackers*-. Sin embargo, si se observa el desarrollo del proceso de criminalización del *computer abuse*, y el escaso énfasis que se ha puesto en la concreta penalización de los autores, bien puede afirmarse, con los mismos autores, que se ha perseguido "estigmatizar el *hacking*, pero no al *hacker*".[34]

4º Por último, en los distintos foros internacionales donde esta cuestión ha sido planteada, comienza a revelarse una gran preocupación por las conductas de intrusismo informático, particularmente peligrosas y difíciles de detectar y probar cuando poseen una dimensión transfronteriza, recomendándose, por ello, a los Estados una armonización legislativa en torno al tema, a fin de evitar la creación de verdaderos "paraísos informáticos" (*computer heavens*).[35] Este argumento, evidentemente, no tiene tanta fuerza en materia de *hacking* (en torno a cuya tipificación autónoma no existe consenso) como en otras manifestaciones de la criminalidad informática (atentados contra la intimidad, fraudes, falsedades por medios informáticos, espionaje informático, etc., respecto a las que encontramos una casi absoluta unanimidad en el orden internacional).

Consideramos que, como punto de partida, España no puede mantenerse de espaldas al proceso de armonización legislativa -y de cooperación policial y judicial- que se está siguiendo más allá de nuestras fronteras. Ello exige, como mínimo: 1ºun estudio serio y contrastado de la situación real del intrusismo informático en nuestro país; 2ºun debate a fondo, con una cuidada ponderación de los argumentos a favor y en contra de la tipificación de estas conductas o de algunas de ellas, valorando su coherencia o incompatibilidad con los principios en que se asienta nuestro Derecho Penal y, 3º una opción meditada final que, entonces sí, podrá coincidir, o no, con la solución comparada más extendida. Es decir, que ninguno de los anteriores argumentos sería suficiente para proceder a tipificar el *hacking* si esta solución no resulta compatible con nuestro sistema punitivo. Pero lo que consideramos inaceptable es la falta absoluta de planteamiento.

Con el ánimo de contribuir al debate, apuntamos las principales razones invocadas en contra de la represión autónoma de las referidas conductas: en pri-

- 33 PARKER, D.B., *Crime by Computer*, Charles Scribner's Sons, N.Y., pp. 12 y ss.
- 34 HOLLINGER, LANZA-KADUCE, ult. cit., p. 118.
- 35 SIEBER, *The International Handbook...*, cit, pp. 147 y ss.

mera instancia, se rechaza la tipificación del mero intrusismo informático porque supone la creación de un delito de peligro abstracto -en relación con bienes jurídicos como la intimidad, el patrimonio, la fe pública, la seguridad del Estado, etc.-, y nada menos que por razones utilitarias y procesales, como las ya indicadas. Además, estaríamos infringiendo el principio de intervención mínima del Derecho Penal, cuando parecería suficiente el recurso a sanciones extrapenales para conductas tan insignificantes y de tan escasa entidad. Por lo demás, una adecuada represión de las demás manifestaciones de la criminalidad informática conducirá, inevitablemente, a que las formas más graves y peligrosas de *hacking* resulten ya castigadas por otros delitos.

A nuestro modo de ver, es tiempo de abordar el tema en términos distintos. Es momento de empezar a preguntarse qué interés o intereses sociales valiosos están -o pudieran estar- en juego cuando se produce una infiltración subrepticia en un sistema informático o en una comunicación electrónica de datos, y si merecen o no la reacción del Derecho Penal. Pues bien, con las cautelas y el respeto que nos merece el tema del bien jurídico, particularmente cuando se trata de la posible emergencia de alguno de nuevo cuño, defendemos la tesis que ya sugerimos hace algún tiempo: estamos asistiendo al nacimiento de algún nuevo bien jurídico en este ámbito (mejor hablaríamos, todavía, de "interés social valioso" cuya protección penal es demandada de forma creciente). Distingamos dos niveles:

*Primero, cualquier 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 individual 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 (por eso, en algunos ámbitos los tipos de acceso y uso no autorizados se analizan bajo la rúbrica: "protección al titular de la información").[36] Proteger al "propietario" (en sentido atécnico) en el pacífico disfrute de su "propiedad" frente a agresiones y perturbaciones externas no autorizadas, constituye una opción legislativa, desde luego. Pero puede ser tan contrario -o tan conforme- al principio de intervención mínima como el delito de allanamiento de morada, por ejemplo, o como la figura de reciente factura que introduce el Proyecto de Código Penal en el artículo 195, cuando castiga al que "entrare o se mantuviere contra la voluntad de su titular en el domicilio de una persona jurídica pública o privada, despacho profesional u oficina, o en establecimiento mercantil o local abierto al público fuera de las horas de apertura".

■ 36 *Vid.* VASSILAKI, "Computer Crimes and Other Crimes...", cit, pp.362 y ss.

*En este segundo plano, analizamos el intrusismo en sistemas o equipos informáticos particularmente relevantes, por razón del contenido de la información que procesan y almacenan (información catalogada como "sensible") y por las funciones que tienen asignadas (y que le son reconocidas jurídicamente), en el seno de las relaciones jurídicas, económicas y sociales. A nuestro entender, el *hacking* sobre estos "sistemas sensibles" está afectando a un interés supraindividual o colectivo, que pudiéramos denominar "seguridad informática" o "seguridad en el funcionamiento de los sistemas informáticos", o "confianza en el funcionamiento de estos", etc. Por su carácter difuso e inmaterial, resulta difícil de aprehender y definir. Y, sin embargo, todos tenemos constancia de que existe, de que hoy constituye un ingrediente indispensable para el normal desarrollo de las relaciones del tráfico, y que se tambalea peligrosamente cuando se desvelan y salen a la luz determinados supuestos de intrusismo informático. Pensemos en el siguiente ejemplo: el Banco de España descubre que un grupo de adolescentes, jóvenes "piratas informáticos", se han infiltrado en el Sistema Nacional de Compensación Electrónica -si ello fuera posible- y utilizan el mismo para jugar, enviarse mensajes e intercambiarse información. Si el hecho saliera a la luz pública, ¿no se vería afectado ese interés colectivo a que nos referimos, seguridad en el funcionamiento de los sistemas informáticos, o similar, aunque constara que no se había provocado ningún perjuicio, alteración de datos, etc.? ¿Quién podría confiar en que las transacciones y operaciones de transferencias electrónicas de fondos efectuadas se ajustaban a la realidad y no habían sido manipuladas?

Así las cosas, no creemos que dispensar una adecuada protección penal al correcto funcionamiento de determinados sistemas "sensibles" frente a perturbaciones, conductas de acceso ilícito, uso no autorizado, modificación de información valiosa, etc., pueda considerarse un exceso en la reacción penal y contrario al principio de intervención mínima. La experiencia estadounidense, que tantas veces nos ilustra con llamativos sucesos, en esta materia bien podría aportarnos alguna luz. Resulta significativo que, en aquel contexto, sólo hayan sido cuestionadas por la doctrina, como un "exceso de reacción penal", las normas estatutarias que a nivel local castigan el mero *hacking* indiscriminadamente, pero nadie cuestione la tipificación, a nivel federal, de las conductas de intrusismo, modificación o descubrimiento de información o utilización sin autorización de los sistemas informáticos del Gobierno, o usados en su interés.[37] Subyace a este planteamiento, a nuestro juicio, la intuición de que "no está en juego lo mismo" en unos y otros casos, es decir, lo que entre nosotros se resolvería en sede del bien jurídico.

■ 37 Sobre la regulación a nivel estatal y federal del intrusismo informático en los Estados Unidos y su valoración, *vid.* GUTIERREZ FRANCES, *Fraude informático y estafa*, cit, pp.123 y ss.

En suma, consideramos equivocada la simplificación del problema del *hacking*. No se puede descartar, de partida, y como solución contraria al principio de intervención mínima, una posible tipificación de algunas de sus formas por implicar el castigo de conductas insignificantes. Por lo demás, 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. Cerramos aquí estas reflexiones, pero abriendo cauces para un futuro debate, con la mirada fija en el esperado "nuevo Código Penal" que, por hallarse en fase de Proyecto, aún podría admitir nuevas sugerencias y mejoras. Esperamos que, tras un proceso de reforma tan largo, para el debate que proponemos no sea ya demasiado tarde.