ALGUNAS RAZONES PARA LA REPRESIÓN PENAL AUTÓNOMA DEL INTRUSISMO INFORMÁTICO

*Nuria Matellanes Rodríguez**

Hace ya varios lustros que venimos asistiendo, en el marco de la ordenación jurídica de las sociedades postindustriales, al debate acerca de la cuestión de si el derecho penal debe, y en su caso cómo y hasta dónde, ocuparse de aquellos comportamientos en los que la informática, herramienta que ha condicionado la orientación de las relaciones sociales y económicas en esta nueva sociedad, aparece como el medio para vulnerar bienes jurídicos tradicionales o incluso como un nuevo objeto de ataque en sí misma[1]. Pues bien, estas páginas se van a dedicar a la reflexión sobre un tipo de conducta, el intrusismo o *hacking*, en la que el normal funcionamiento de los sistemas informáticos constituye el objeto del ataque.

En general, el *hacking* alude a aquellos comportamientos en los que un sujeto utiliza determinadas técnicas para acceder sin la debida autorización a un sistema informático o red de comunicación electrónica de datos, si bien en esta intervención nos vamos a ceñir al *hacking* en estado puro, es decir, al intrusismo despojado de cualquier elemento de tendencia subjetiva ulterior y distinto del mero acceso mismo. O más exactamente, la intención que mueve al *hacker* a infiltrarse en el sistema puede ser el puro paseo por placer (*joyring*), la curiosidad, el juego o, en general, la superación del

* Profesora Asociada de Derecho Penal. Universidad de Salamanca.

1 En general, sobre esta vinculación de la criminalidad informática con los problemas propios de la nueva "sociedad de riesgos, el trabajo de C. Pérez Del Valle. "Sociedad de riesgos y reforma penal", en *Poder Judicial*, n.º 43-44, 1996.

desafío que representa la máquina; en todo caso, desprovisto de un ánimo de agredir intereses individuales o colectivos ulteriores, como la intimidad, la propiedad, el patrimonio, la seguridad nacional, etc.

Curiosamente, pese a que el *hacker* constituye el modelo de "delincuente informático" por excelencia, en tanto que es el que mejor se adapta al perfil diseñado con suma atención y profusión de datos por los estudios criminológicos (joven, normalmente varón, de clase media-alta, de coeficiente intelectual superior a la media, social y familiarmente integrado, con una absoluta falta de conciencia de estar actuando ilícitamente...), no existe apenas en los códigos penales de los países de nuestro entorno una atención directa para esta clase de conducta, sino que, más bien, la tónica habitual es la consideración de que, en la realidad de las cosas, quien accede subrepticiamente a un sistema informático "hará algo más", siendo ese "algo más", lo que cualificará al inicial intrusismo, convirtiéndolo en un medio para la vulneración de un interés jurídico diferente y, en consecuencia, procediéndose a su absorción técnica por el delito que proceda según el bien jurídico agredido.

Tal es el espíritu del Código Penal español, en el que el puro acceso sin autorización a un sistema informático, cualquiera que sea el titular o usuario de dicho sistema y sea cual fuere el contenido de la información alcanzada resulta, en principio, impune, mientras que tales accesos no autorizados con fines que van más allá que el solo intrusismo pueden encontrar acomodo en figuras delictivas como el sabotaje, los daños, los ataques a la intimidad, etc., quedando integrado el acceso no consentido por el desvalor que supone la afección a alguno de esos intereses. Es decir, el legislador ha optado por un sistema de tipos de equivalencia, consistente en la introducción en la descripción típica de previsiones que contemplan a la informática como un particular *modus operandi* de ofensa del bien jurídico "tradicional" del que se ocupen en cada caso. De esta manera, se logra una mayor seguridad jurídica al permitir una mejor delimitación del ámbito de la tipicidad, aunque ello tiene, a su vez, el coste de poder generar lagunas jurídicas, ya que se corre el riesgo de una falta de previsión de nuevas formas comisivas que en este ámbito es fácil que se produzcan dada la rapidez de los avances tecnológicos[2].

Siendo esta la opción mantenida por nuestro derecho penal, el resultado ha sido la ausencia de tipos que se ocupen de la descripción de conductas normalmente peligrosas para el regular y correcto funcionamiento de los sistemas informáticos en sí. Es decir, de tipos en los que precisamente la red informática y lo que ella representa es el objeto mismo del ataque y el interés lesionado. Justamente es en este ámbito donde se residencia la conducta de *hacking* que nos ocupa y que hemos definido más arriba:

2 M. Álvarez Vizcaya. "Consideraciones político-criminales sobre la delincuencia informática: el papel del derecho penal en la red", en *Internet y derecho penal*, Madrid, Consejo General del Poder Judicial, 2001, p. 271.

no hay intención tendente a vulnerar otro bien jurídico, en cuyo caso serían de aplicación los tipos generales, con sus cláusulas o previsiones informáticas.

Ahora bien, la implantación de esta opción de un tipo particular que se ocupe de los actos de intromisión ilícita en los sistemas informáticos con la única intención del acceso requiere una reflexión, que en este caso ha de ser necesariamente breve, acerca de si el *hacking* implica la agresión de un auténtico interés jurídico-penal digno de protección y merecedor de una atención autónoma y separada de la que ya llevan implícita los tipos particulares. ¿Cuál es exactamente el interés al que protegería un hipotético tipo autónomo del *hacking*? ¿El desvalor que representan las conductas de intromisión en los sistemas informáticos tiene entidad suficiente para ser considerado un interés con relevancia penal? Entendemos que son dos, básicamente, las notas que componen la esencia de este interés y que justifican su rango penal:

A. Por una parte, todo acceso no autorizado a un sistema informático o red de comunicación electrónica de datos supone una agresión contra el interés del propietario o titular del sistema o de la información, de manera que la entrada o permanencia en el sistema supone un ataque a un ámbito que le pertenece en exclusiva porque, de hecho, tiene vetado el acceso al sistema a terceros, veto que es justamente el que quebranta el *hacker* con su conducta. Sería, en definitiva, la entrada a un reducto de la vida de una o varias personas restringido al alcance de otros, comparable a la entrada en una morada o domicilio físico ajeno. Según esto, la respuesta penal ante el hacking resulta tan conforme al principio de intervención mínima como el delito de allanamiento de morada[3].

B. De otro lado, mantenemos que 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[4]. Dada esta magnitud de la trascendencia del sistema informático, podemos afirmar que el *hacking* sobre los sistemas o equipos informáticos puede estar afectando a un interés supraindividual, que podemos denominar "seguridad informática" o "seguridad en el funcionamiento de los sistemas informáticos", o "confianza en el funcionamiento de éstos", etc.[5]. Por su carácter inmaterial resulta difícil de aprehen-

---

3 María L. Gutiérrez Francés."Intrusismo informático (*hacking*): ¿Represión penal autónoma?", en *Informática y Derecho*, n.º 12-15, p. 1182.

4 M, Álvarez Vizcaya. "Consideraciones político-criminales", cit., p. 270.

5 María L. Gutiérrez Francés. *Fraude informático y estafa*, Madrid, Ministerio de Justicia, 1991, pp. 619 y 620.

der 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.

Pero la caracterización de este interés como bien jurídico digno de tutela penal específica y su consecuencia de una tipificación penal autónoma ha generado críticas entre la doctrina:

A. Se subraya la dificultad de prueba y de detección del *hacking* en estado puro: normalmente lo que se descubren son otros comportamientos delictivos de los que el *hacking* constituye el medio para su perpetración. Ante esta situación, los tipos específicos dan oportuna respuesta y la punición del *hacking* deviene inútil.

Nuestra respuesta ante esta objeción consiste en subrayar que las dificultades de detección de un comportamiento no pueden convertirlo en impune, sino que reclamarán la intensificación de los esfuerzos por lograr medios adecuados de persecución e investigación. Pero es más, la enorme complejidad que presenta la averiguación de las actuaciones ilícitas en los sistemas informáticos nos muestra que en no pocas ocasiones lo que se constata no es la ejecución de un hecho delictivo posterior cometido mediante un acceso no autorizado, sino que éste es lo único que se puede probar cuando se detecta un perjuicio ulterior, por ejemplo un fraude, del que no hay medios para probar cómo se cometió[6]. De manera que la punición autónoma del *hacking*, lejos de convertirse en inútil, justamente lo que evita es la impunidad.

B. Se invoca una violación a las exigencias del principio de intervención mínima y un exceso de respuesta penal, ya que el *hacking* se encuentra en relación medial para conseguir un fin último que es el ataque al bien jurídico intimidad, patrimonio...

Sin embargo, la vulneración de un ámbito reservado para el titular del sistema o de los datos que el intrusismo representa puede resultar paralela a la inmisión en un espacio físico que es la morada, por lo que resultará tan conforme o tan en contra a la intervención mínima como se entienda la punición del allanamiento de morada. Del mismo modo, la violación de la confianza en el funcionamiento del sistema informático puede ser comparable con el interés en la seguridad en el tráfico rodado, o con la confianza en la transparencia de los mercados, cuya mayor tangibilidad excluye las dudas acerca de la conveniencia de tipificar las conductas que perturban esa confianza o seguridad, tan esenciales para el desenvolvimiento de nuestras relaciones diarias como puede ser la seguridad en el sistema virtual de comunicaciones.

---

6 Gutiérrez Francés. "Intrusismo informático (*hacking*)", cit., p. 1180; en contra, E. Morón Lerma. *Internet y derecho penal: hacking y otras conductas ilícitas en la red*, Aranzadi, 1999, pp. 70 y 71.

Dada esta relevancia de los intereses en juego, se justifica el que no consideremos una respuesta penal excesiva para los casos en los que el intrusismo es el camino para lesionar otro interés y, por lo tanto, van a recibir la solución agravatoria del concurso de delitos.

C. Se objeta a una tipificación autónoma del *hacking* por entenderla perturbadora de las exigencias básicas de la prevención general, puesto que, dada la escasa o nula capacidad de motivación del *hacker*[7], se incurriría en un derecho penal puramente simbólico y promocional que genera una instrumentalización del individuo y una primacía, sin opción de equilibrio, de la eficacia sobre las garantías. Ahora bien, el derecho penal, funcionando en el seno de un sistema integral de control social, constituye también un medio para dirigir la evolución del modelo social hacia metas no alcanzadas y no puede, por tanto, limitarse a ir detrás del orden social sino que, en especial a través de la introducción de nuevos bienes jurídicos, puede y debe encauzar la evolución del modelo social. En esta línea, es oportuno recordar que el empleo del derecho penal como instrumento motor en la ordenación de las conductas antes de que la sociedad las considere merecedoras de respuesta punitiva ha dado frutos muy positivos en otros ámbitos. Es el caso de la Hacienda Pública, cuyo correcto funcionamiento hoy es considerado un interés vital para el mantenimiento del sistema socioeconómico constitucionalmente diseñado, pero que en los años ochenta no tenía calado entre la ciudadanía, que no consideraba al fraude un ilícito de relevancia, sino simple picaresca y, paralelamente, "admiraba" al que tenía la capacidad y los conocimientos para defraudar a las arcas del Estado, llegándose incluso a incorporar al organigrama financiero de grandes empresas a alguno de estos "ingenieros de las finanzas". Exactamente lo mismo que sucede con los *hackers*[8].

Ahora bien, por supuesto que este móvil preventivo-penal ha de venir reforzado por otros medios si se quieren conseguir resultados eficaces: la compatibilidad de las medidas penales de represión y de otras medidas preventivas y de seguridad previas no debe ser puesto en duda.

En suma, consideramos que la represión penal autónoma del *hacking* cuenta con argumentos sólidos sobre los que construirse. Sin embargo la vacilación y la timidez de las respuestas siguen siendo una constante en nuestros ordenamientos jurídicos. Como muestra, la previsión que sobre esta materia realiza el Convenio del Consejo de Europa sobre el Cibercrimen, del 23 de noviembre de 2001, permitiendo a las partes escoger entre castigar el mero acceso o interceptación de los datos informáticos de otro sistema informático o el acceso con ulteriores intenciones delictivas, sin que obligue a las Partes contratantes a castigar necesariamente el mero intrusismo

7 C. Romeo Casabona. *Poder informático y seguridad jurídica*, Madrid, 1987, p. 40.

8 D. De Alfonso Laso. "El hacking blanco. Una conducta ¿punible o no punible?", en *Internet y derecho penal*, cit., p. 513.

informático. Aunque al menos hay una atención específica para el intrusismo informático, la respuesta unívoca y decidida no existe y la disyuntiva sigue estando ahí. Ya que la unificación de las respuestas de los ordenamientos jurídicos es esencial para conseguir resultados eficaces en la lucha contra la delincuencia informática, sirvan estas palabras de sencilla reflexión a favor de la tesis de la tipificación autónoma.