El intrusismo informático. Reflexiones sobre su inclusión al código penal.

Por Eduardo E. Rosende.

I.- Introducción.

Sin duda alguna, la informática es hoy por hoy la técnica más importante que tiene a su alcance el hombre a los efectos de hacerse con el éxito en cualquier actividad que se proponga. Competir utilizando medios tradicionales contra una persona que se sirva de un sistema informático, es una empresa condenada al fracaso desde su misma ideación.

Vista la actual comunidad internacional, que correctamente ha sido catalogada como sociedad de la información[1], el procesamiento automático de datos por distintos dispositivos en reemplazo del cerebro humano, produce innumerables consecuencias que deben ser analizadas y de hecho lo son, por distintas ciencias como un factor social, cultura, educativo, económico, etc., de enorme trascendencia.

El término informática se deja descubrir por primera vez en el idioma francés (*informatique*), y según la Real Academia Española[2] significa: "Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores". Esta definición coincide con aquella dada por gran cantidad de autores del mundo jurídico, entre ellos Marcelo Alfredo Riquert[3], Pierre Gratton[4], Esther Morón Lerma[5], y a prácticamente todos los restantes autores del derecho informático, que se vuelcan a analizar en su ciencia las consecuencias de la informática.

El sistema penal por supuesto no ha permanecido pasivo en este sentido. No hablaremos aquí de cuestiones filosóficas del orden de la justificación y problemática de este sistema en si mismo, aceptándolo simplemente como una realidad, dentro de la cual se han creado ya varias figuras penales motivadas en el abuso de los sistemas informáticos, ya sea como medio u objetivo final.

Así pues, antes podíamos utilizar la frase “delitos informáticos” a efectos meramente pedagógicos o para delimitar ciertas actividades abusivas que en el orden internacional eran consideradas conductas penalmente reprimidas. Más hoy, la posibilidad de hablar de delitos informáticos a nivel nacional es perfectamente posible.

En este tema también se exponen gran cantidad de opiniones para delimitar el alcance de lo que debe considerarse delito informático, haciéndolo desde varias ópticas como ser:

a.- por como son usadas las computadoras, esto es, como medio u objeto (Sloan[6], Pierre Gratton[7] y Orjales[8]);

b.- enumeración de actividades abusivas por medio del procesamiento automático de la información (Correa-Palazzi[9], OCDE, etc.), haciendo luego una clasificación por afectación de bienes jurídicos;

c.- por las características funcionales de los datos manipulados -de entrada, salida, primarios, y secundarios- (José Sáenz Capel[10]).

Partiendo de la base que sin un derecho afectado no puede haber un imputación penal válida, conforme así lo manda el artículo 19 de nuestra Constitución Nacional, entendemos que podríamos definir al abuso o delito informático como toda aquella actividad realizada a través del procesamiento automático de la información, por medio de la cual se produzca la afectación de un bien jurídico.

Preciso es aclarar también que podemos efectuar una sub-clasificación del delito informático para distinguir dos segmentos: los abusos o delitos informáticos propios y impropios. Los primeros serán aquellos que no puedan ser realizadas o imaginados sin la utilización de un sistema informático, entendiendo este como el conjunto e interrelación del hardware, software, operador e información. Las actividades por excelencia de este tipo, que han generado incluso la discusión acerca de la existencia de un nuevo bien jurídico (la informática como cuestión en si misma), son:

A.- Las amenazas lógico informáticas (es decir su creación, manipulación, almacenamiento, distribución, ejecución y sus consecuencias);

B.- La utilización de programas de rastreo (sniffer);

C.- *Cracking* o piratería informática (violación y ruptura de sistemas de seguridad de los programas y creación de los denominados "cracks" y *"keygenerators"*; y

G.- Intrusismo o acceso informático (*hacking*).

Sobre el análisis de esta última actividad estarán girando las páginas que continúan, con el objetivo de reflexionar acerca de su inclusión como conducta típica dentro de nuestro ordenamiento punitivo. En síntesis, la duda final que nos propones evacuar es: ¿la actividad de *hacking* debe ser reprimida?

II.- Problemática conceptual.

Responder esa pregunta sin explicar que es un *hacker*, como son, cual es su finalidad y en que consiste la actividad de *hacking*, sería incorrecto desde el punto de vista metódico, pues estaríamos tratando de afirmar una hipótesis sobre nuestro objeto de estudio sin delimitarlo. Pero tampoco podemos analizar debidamente todas estas cuestiones. Deberemos entonces simplemente conformarnos con dar un concepto de *hacker* y de la actividad de *hacking* que mínimamente pueda ser aceptado por todos. Dejaremos al imaginario positivista efectuar una clasificación en base a descripciones físicas y psíquicas de estos personajes y su distinción con los *lamers* (entre otros), o a los partidarios del alarmismo extremo que incorporan al *hacker* como miembros de actividades terroristas.

Para delimitar nuestra área de estudio en forma correcta también habremos de dejar fuera todas aquellas cuestiones relativas a la ideología que movería la actividad del *hacking*, toda vez que ello nos arrojaría nuevamente a la arena de la discusión filosófica, más debemos efectuar un punto de inflexión en el sentido de no dejarnos llevar por las publicaciones efectuadas por distintos medios de comunicación que solo llevan a resaltar la criminalidad o un sentido netamente negativo de la actividad de *hacking* y a confundirnos para poder entender de lo que estamos hablando.

Prueba de esto último, es el claro proceso penal mediático que llevo a condenar a distintos integrantes del grupo de *hackers LOD* (Legión of Doom) en Estados Unidos, a principios de la década de 1990 por realizar actividades extremadamente peligrosas como ser la de haber ingresado a un servidor privado y apoderarse de un documento cuyo nombre era "E911" que contenía información respecto del sistema de emergencias de la empresa AT&T en ese país. Dicha información era simplemente los mecanismos que se debían seguir en casos de emergencia y su conocimiento era público. Para evitar esto, solo veremos y utilizaremos la realidad, previo a evaluar

algunas consideraciones en torno al origen del término y su evolución etimológica, pues ha variado mucho.

Hoy día el uso de sistemas informáticos se extiende a todos los ámbitos de la vida y por ello el usuario o titular de una computadora (entre otras cosas) guarda gran cantidad de información en los dispositivos de almacenamiento (sean estos de acceso directo o remoto), y para resguardar la misma deberá tomar medias de seguridad desde dos puntos de vista: uno físico y otro lógico. Ambos son abarcados por la Seguridad Informática.

El ámbito físico será todo aquel necesario a los efectos de resguardar el acceso a esa información en forma directa, esto es, o bien cualquier circunstancia de la naturaleza que pueda afectar al sistema (temperatura, humedad, incendios, problemas eléctricos, etc.), o la aproximación corpórea de una persona no autorizadas al lugar donde se encuentra la computadora o de las fichas de conexión o la visualización de una pantalla.

El ámbito lógico en cambio estará destinado a proteger esa información pero ya desde el punto de vista digital o electrónico, como ser inclusión de políticas de seguridad en cuanto a contraseñas y cifrado, la existencia de firewalls, la actualización de aplicaciones y sistemas operativos, la corrección de vulnerabilidades, etc.

Teniendo en cuenta estos parámetros, comencemos a delimitar conceptos. Mas allá que se relacione a los primeros hackers con el *MIT*[11], lo cierto es que las palabras *hacker* y *hacking* están íntimamente relacionadas con las computadoras, los dispositivos de almacenamiento automático de la información (informática) y toda tecnología, siendo dicho instituto por su calidad e especificidad el lugar idóneo para el origen de estos términos.

Hoy día, en su página puede verse una definición del *hacking*, como el despliegue de una broma original y deslumbrante, que genera el agrado y diversión de toda la comunidad en dicho lugar, diferenciando así su aplicación en ese ámbito del utilizado para el mundo de las computadoras y también del *cracking* y el *ciberpunking.*

La confusión de la terminología del mundo informático en los medios ajenos a este es importante. Así, en primer lugar debemos aclarar que quienes fueron *hackers* en un primer momento buscaron diferenciarse de otros personajes que utilizaban el concomiendo del medio informático con fines indeseados, con lo cual, la diferencia radicaba así en la subjetividad. El *hacker* era el bueno, solo buscaba superar cualquier barrera, logrando siempre un mayor grado de

conocimiento de los sistemas, sus desafíos y posibilidades, existiendo en el segundo la intención de dañar a terceros, o por lo menos manipular datos o violar la intimidad.

Con el término hacking, que hace alusión a la acción de hachar[12], se pretende describir la conducta de ingresar a sistemas informáticos sin estar autorizado, eludiendo los sistemas de seguridad, pero sin afectar la información contenida, con excepción de aquella donde se registre la entrada del extraño y posibilite su rastreo. El hacking es algo diferente al cracking y a la piratería informática. El *cracking* es una actividad necesaria para permitir la violación de los sistemas de seguridad de los programas de computación protegidos por la ley de Propiedad Intelectual (11.723) mientras que el *ciberpunking* sería la actividad de destrucción de datos e información digital, cuestión hoy no abarcada por el derecho penal (Art. 183 del Código Penal).

En este sentido, coincidimos parcialmente con la definición que expone Sáez Capel[13], en la cual expresa: “Con la expresión hacking, se hace referencia a un conjunto de comportamientos de acceso o interferencia subrepticios, a un sistema informático o red de comunicación de los mismos, sin autorización o más allá de lo debido”.

Si bien no es necesario efectuar una defensa del *hacker*, en el sentido más estricto del término a los efectos de este trabajo, lo cierto es que esta práctica sería un potencial riesgo para el derecho a la intimidad del titular de un sistema informático, lo cierto es que nada tiene que ver con este otro tipo de actividades. El *hacking* responde a una cuestión de entretenimiento y desafió ante la manipulación de los dispositivos informáticos, basado en una ideología de libre acceso y total a la información pública. Es preciso reconocer que el actual estado de evolución de la informática se debe en gran parte a los hackers, desde los apasionados grupos de programadores del Instituto Tecnológico de Massachusetts (MIT), los creadores del juego *CORE-WAR*, hasta la existencia del sistema operativo *LINUX*.

Para obtener una mayor ilustración del término *hacker*, resulta mas que abundante la información y el análisis social de este fenómeno contenido en la obra de Himanen[14], en cuyo prefacio en la página 7 se da un dato muy importante a los efectos de distinguir al *hacker* de los “piratas informáticos”: “Con posterioridad, a mediados de la década de 1980, los medios de comunicación empezaron a aplicar el término a los criminales informáticos. A fin de evitar la confusión con aquellos que dedican su tiempo a escribir virus informáticos y a colarse en los sistemas de información, los hackers empezaron a denominar crackers a estos usuarios destructivos o piratas informáticos. En este libro utilizamos esta distinción entre *hackers y crackers*.”

Hechas estas primeras diferencias, debemos mencionar también una forma de obtener información pero sin acceder a un sistema informático donde se almacena la información que necesitamos. Hablamos del *sinfín,* que son mas que programas, sistemas que permiten el monitoreo de la información que circular por las redes. Claros ejemplos son los sistemas *Carnívore* y *Echelon*[15], por medio del cual Estados Unidos, Gran Bretaña, Canadá, Australia y Nueva Zelanda interceptan en la actualidad mensajes de correo electrónico, comunicaciones de voz, envíos de fax y cualquier envío de datos por los nodos de Internet.

Habiendo explicado brevemente todas las cuestiones relativas al *hacker* y a la actividad del *hacking* que aquí interesan, y diferenciado esto del *cracking* y del *sinfíng*, es preciso decir que en la actualidad los términos *hacker* o *hacking* encuentran dos vertientes, el *hacking* ético o blanco, y el *hacking* no ético o negro. El primero responde al sentido de la palabra *hacker* en su primer momento. Esto es, el *hacker* blanco es aquel que tiene un interés en los sistemas informáticos, dedicándose a su estudio, a la programación, a la búsqueda de vulnerabilidades y al mejoramiento de todo el sistema. Un *hacker* blanco pudo haber ingresado a un sitio web, una base de datos, o una computadora personal, encontrando para ello una vulnerabilidad en el sistema operativo o aplicaciones, y su siguiente paso será advertir de ello al responsable de la seguridad del sistema informático accedido. Además, muchas actualizaciones de seguridad de Microsoft y otras empresas, se deben a la actividad de este tipo de personas, que son luego publicadas en sitios web para que los programadores y usuarios puedan estar protegidos.

En consecuencia habrá una línea gris dentro del cumulo de actividades que desarrolla el *hacker* que podrá verse relacionado con la legislación penal. Obviamente el desarrollo de un programa de licencia libre no lo es, pero el acceso a un sistema informático ajeno si. Por esto, podemos definir a esa zona gris como la realización de distintos métodos y técnicas a los efectos de acceder a sistemas informáticas sin autorización de sus titulares, eludiendo todas las medidas de seguridad lógicas implementadas para evitar ese objetivo. El *hacking* no es otra cosa entonces que el mero acceso, con todos los pasos previos que ello requiere y el *hacker* es quien tiene los conocimientos informáticos necesarios para evaluar vulnerabilidades y poder penetrar a través de ellas. Debemos aclarar que quien accede a un sitio no debe ser catalogado como *hacker*, pues muchas veces simplemente quien accede utiliza programas o guías para llegar a esos objetivos.

III.- Hacking y derecho penal. La situación en el orden nacional e internacional.

En nuestro país, la actividad de desplegar distintas pruebas o métodos de penetración contra sistemas informáticos, el acceder a ellos aprovechándose de las vulnerabilidades detectadas, el obtener, modificar y/o destruir la información contenida en dispositivos ajenos y el utilizar esos datos con beneficios propios o en perjuicio de otro, no constituyen delitos conforme nuestro código penal respecto del 99% de los equipos informáticos.

Las excepciones son los sistemas donde se reservan "secretos de estado", teniendo en cuenta las aplicaciones del término "revelare"[16] conforme el artículo 222 del Código Penal, las leyes 24766 en cuanto a la información digital que puedan constituir secretos comerciales, el Régimen Penal Tributario establecido por la ley 24769 para las modificaciones de las bases de datos del fisco y la Ley de Inteligencia Nacional N° 25.520 para cuestiones particulares de esta actividad. Así vistas las cosas, el *hacking* como mero acceso e incluso con la intención de obtener información, carece hasta el momento de cualquier relevancia penal hasta el momento, respecto de los particulares, las provincias, los municipios y todo otro sistema informático que no pueda ser ubicado en esas figuras.

En el orden internacional por otra parte, la situación cambia, y bastante. En 1990 el Consejo de Europa[17] sugería a los distintos estados la creación de legislación penal informática, dentro de la cual y como punto prioritario se incluía la represión del *hacking*, describiéndola como "acceso no autorizado" (Unauthorised Access).

El Convenio sobre la Ciberdelincuencia del Consejo de Europa[18], en su artículo dos expone la necesidad de tipificar como delito en el derecho interno de los estados parte el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático, pudiéndose exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva.

Así pues, el mero acceso informático o hacking, a nivel objetivo esta previsto como delito en Estados Unidos a través de la sanción de diferentes actas, en Chile[19], Francia[20], Italia (Art. 615 del Código Penal) y Venezuela[21], entre otros.

En cuanto a España, Portugal y Alemania, se, exige que el mero acceso este destinado a obtener datos o información contenida en el sistema. La descripción de la ley alemana del *hacking* es una de las mas correctas, sencillas y por ello de fácil acceso y aplicación práctica. Es lógico tal

cuestión dado que este país fue uno de los primeros en enfrentar hace larga data hechos y abusos de este tipo.

Todo lo contrario sucede en países como Argentina, Brasil y Austria[22] que no sancionan de ningún modo el mero acceso informático. Debemos aquí llamar la atención en un sentido a los efectos de afirmar la atipicidad en todo lo relativo a acceso a sistemas informáticos, apoderamiento de casillas de correo electrónicas o daño informático. Más allá de que la intención sería la de sancionar estas conductas, como ya veremos, en Argentina se han trazado tipos penales que sancionar conductas que rodean lo que es el acceso y daño informático pero no a dichas conductas específicamente, ante lo cual nos podríamos encontrarnos ante una clara posición de dejarlas atípicas, más allá de que nuestros tribunales se esfuercen en forzar la ley.

IV.- La intención en Argentina. Proyectos de reforma del Código Penal.

En la última década se han generado infinidad de tentativas de modificar el código penal para que abarquen conductas informáticas o crear de por si leyes integrales que abarquen la totalidad de actividades abusivas relacionadas con la informática. En algunos se incluía el *hacking* o mero acceso informático y en otro no. Transcribiremos aquí los más importantes:

a.- Proyecto de ley número 0117-S-2000:

Artículo 1°.- Incorporase al artículo 153 del Código Penal el siguiente como segundo párrafo:

"Será reprimido con la misma pena a quien con el objeto de descubrir secretos de un tercero o vulnerar su intimidad y sin consentimiento de este:

(1) se apoderare mensajes de correo electrónico o cualquier otro documento o efecto producido en soporte digital.

(2) Interceptare comunicaciones cuando por las mismas circularen mensajes de correo electrónico o cualquier otro documento en soporte digital.

(3) Utilizare artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen de una persona o cualquier otra comunicación cuando fueran obtenidas invadiendo su vida privada".

Art. 2°.- Incorporase al artículo 153 del Código Penal el siguiente como tercer párrafo:

"La pena aumentará en un tercio a quien ilegítimamente se apoderare, utilizare, modificare, revelare, difundiera o cediera datos reservados de carácter personal que se hallen registrado en ficheros o soportes informáticos, electrónicos o telemáticos; y en la mitad cuando dichos actos afecten datos de carácter sensible que revelen la ideología, creencia, religión, salud, vida sexual u origen de su titular".

Art. 3°.- El actual segundo párrafo del artículo quedará incorporado como cuarto párrafo.

b.- Proyecto de ley 0064/CD/2002:

Art. 2°- Acceso no autorizado: Será reprimido con pena de prisión de quince días a seis meses, si el hecho no constituye un delito más severamente penado, el que ilegítimamente y a sabiendas accediera por cualquier medio, a un sistema o dato informático, sin que medie autorización del propietario o excediéndose de los límites de la autorización conferida.

La pena será de un mes a un año de prisión si el autor revelare, divulgare o comercializare la información accedida ilegítimamente.

Art. 3°- Espionaje informático. Será reprimido con prisión de un mes a un año, si el hecho no constituye un delito mas severamente penado, el que interceptare, interfiriere o accediere a un sistema informático para obtener datos de forma no autorizada, violando la reserva o secreto de la información de dicho sistema.

La pena será de un año a cuatro años de prisión si los datos o la información obtenida constituyeren secreto político o militar concerniente a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación.

c.- Proyecto de ley 3873-CD-2006:

Art. 3: Agregase como art. 153 bis del Código Penal el siguiente texto: "Será reprimido con prisión de uno a seis meses, el que a sabiendas accediere sin la debida autorización o excediendo la que posea, a un sistema informático ajeno de acceso restringido, siempre que no se cometiere un delito más severamente penado. La pena será de un mes a un año de prisión cuando

el acceso fuese en perjuicio del sistema informático de un organismo público nacional, provincial, o municipal, o de un proveedor de servicios públicos, bancarios o financieros".

d.- Proyecto de ley 5084-CD-2006:

15) Hacker: Es el individuo que con la finalidad de causar daños, o bien obtener ilegalmente información de uso reservado, procura ingresar a las computadoras ajenas, para violar e investigar sus recursos de control.

CAPITULO II - DE LOS DELITOS Y LAS PENAS - DEL ACCESO NO AUTORIZADO

Art. 3 .- Será reprimido con pena de multa de dos mil a cien mil pesos, si no resultare un delito mas severamente penado, el que accediere, por cualquier medio, a una computadora, sistema de computación, medios de almacenamiento de datos, o a datos de computación, que no le pertenezcan sin que lo haya autorizado el propietario, o habiendo excediendo los limites de la autorización que le hubieran conferido.

Exceptuase de lo dispuesto en el caso en que la computadora o sistema de computación, medios de almacenamiento de datos, o datos de computación, estén librados al acceso público, sin restricciones de ningún tipo; o que el acceso del autor no se encuentre comprendido entre las restricciones establecidas.

e.- Proyecto de ley 5.864-D.-2006:

"Art. 5º – Incorpórase como artículo 153 bis del Código Penal de la Nación, el siguiente: Artículo 153 bis: Será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, el que ilegítimamente y a sabiendas accediere por cualquier medio sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un mes a un año de prisión cuando el acceso fuere en perjuicio del sistema informático de un organismo público estatal o de un proveedor de servicios públicos."

f.- Proyecto de reforma integral del Código Penal:

Por resolución del Ministerio de Justicia y Derechos Humanos N° 303 (14/12/2004) se creo la Comisión para la elaboración del proyecto de ley de reforma y actualización integral del código penal, cuyo trabajo fue abierto a consulta pública hasta el 15 de agosto de 2006 (resolución 736/06) y publicada en el sitio de dicha cartera.

Dentro del Libro II, Título IV, Capitulo III se encuentran los artículos 138 al 147, que buscan resguardar la privacidad a través de la prohibición de distintas actividades, entre las cuales se encuentran varias realizadas a través de medios tecnológicos. Entre ellas la apertura de correos electrónicos, la intercepción de comunicaciones, etc.

El acceso o intrusismo informático esta contenido en el artículo 146 que reprime con pena de prisión de seis meses a dos años al que ilegítimamente accediere, de cualquier forma, a un banco de datos personales. Luego el artículo sigue, pero haciendo referencia a las acciones de insertar en este banco datos falsos, entre otras cuestiones.

g.- Análisis global:

Los proyectos anteriormente expuestos son un claro muestreo de las distintas posibilidades que pueden darse con respecto a la toma de posición de la ley penal en cuanto al *hacking*, mas allá de pretender hacer algo innecesario y peligroso como definir a nivel jurídico un concepto que en el lenguaje llano presenta una innumerable cantidad de sentidos y definiciones, haciendo del Código Penal o de las leyes diccionarios.

Las opciones en definitiva son las siguientes:

- No prohibir de ninguna forma el acceso o intrusismo informático (*hacking*). Esta sería la iniciativa tomada en el proyecto 0117-S-2000, que parecería solo reprimir el apoderamiento de información electrónica sin hacer referencia al medio que utilice el agente para llegar a esos datos, dejando al mero intrusismo informático posiblemente como acto preparatorios no punible.

- La situación contraria ocurre en los proyectos 0064/CD/2002 y 3873-CD-2006, donde se reprime el mero acceso a un sistema o dato informático, sin requerir que se ingrese a sectores del sistema donde se almacenen datos específicos de su titular. Ante esto debemos decir, como crítica, que en toda computadora conectada a internet y que puede ser accedida por un hacker habrá información, mas su visualización no afecta de por si la intimidad de una persona en forma

- El proyecto 5084-CD-2006 va mucho mas allá pues no solo reprime le mero acceso a un sistema informático, sino a cualquier dispositivo de almacenamiento, no requiriendo para logar dicho acceso la violación de algún sistema de seguridad. La pregunta es, si muevo el ratón de una computadora y veo un correo electrónico en la pantalla, o me siento en una computadora y visualizo su disco rígido, sin efectuar ninguna actividad que elude medidas de seguridad, estoy realizando lo que sería el tipo penal de mero intrusismo informático. Este proyecto parece saltar por alto la cualidad intrínseca de curiosidad que tiene el hombre. Peor aún podría ser la respuesta a la pegunta: ¿Cuáles serían los actos de ejecución de este tipo penal? El proyecto 5.864-D.-2006 tiene la misma consecuencia para el mero intrusismo informático a sistemas o datos informáticos (que pueden estar almacenados en distintos soportes), con el aliciente de incluir la frase “acceso restringido”.

- Finalmente, el proyecto de reforma integral citado solo reprime el mero intrusismo a un banco de datos personales, pero no a sistemas informáticos que no lleguen a poder ser clasificados de esa forma.

V.- <u>Conclusiones y nuestra opinión:</u>

Hemos empezado estas páginas haciéndonos una pregunta. Luego hemos tratado de explicar o al menos aclarar la gran confusión en cuanto a los términos *hacker* y *hacking*. Dimos una visión rápida de lo que suceden actualmente a nivel internacional en la legislación penal con el *hacking* y finalmente efectuamos un repaso de algunos proyectos de reforma que como muestreo daban una perspectiva de la situación de esta problemática en nuestro país. Es hora de dar nuestra opinión y dar fin a este análisis.

Empezaremos recordando que el término *hacker* en el ámbito del que hablamos y en su sentido original, hace referencia a personas que poseen un alto grado de interés en el desarrollo de la informática, de programas de uso libre, y del mejoramiento del sistema en su totalidad. Para trazar un paralelo y utilizando palabras de Linus Torvalds, los que participan en este encuentro, lo hacen no porque lo necesitan, sino para analizar y discutir sobre algo que los entretiene: la ciencia penal. De la misma forma el hacker se sienta ante una computadora o ante otro sistema automático de procesamiento de la información justamente por eso, para entretenerse, y en ese entretenimiento surgen acontecimientos extremadamente positivos, entre los que podemos nombrar el cambio de

una red de defensa (ARPANET) a una red de comunicaciones sin fronteras, censuras o discriminaciones donde la información circula libremente y el acceso al conocimiento esta al alcance de la mano (Internet); o la creación de sistemas operativos y su posterior desarrollo que de tal forma que le permita a países pobres poder contar con sistemas operativos para competir con aquellos cuyo desarrollo es superior.

Definir al *hacker* como una persona peligrosa o improductiva, es un insulto liso y llano, y un total desconocimiento de las implicancias del término *hacker* y de la actividad del *hacking* en la actualidad.

Dentro de las innumerables actividades que se encuentran dentro del termino *hacking*, se encuentran aquellas que buscan establecer las vulnerabilidades de un determinado sistema informático, y en caso de encontrarlas poder establecer si pueden acceder. Escribir códigos de programación en la línea del explorador para tomar conocimiento de los errores de una base de datos, o efectuar pruebas de distintos códigos y contraseñas contra un sitio son ejercicios que sea realizan a diario.

Esto nos debe servir a todos los que participaron en el saber científico penal que los *hackers*, mediante su actividad, participan en forma constante en el mejoramiento y desarrollo de la seguridad informática, y reprimirla, en muchos casos nos convertiría de hecho en una amenaza para ese objetivo. Dando vuelta la cuestión, aquel que no quiera conscientemente que exista seguridad informática, buscaría sancionar de cualquier forma la mínima actividad destinada a comprobar los errores que permitan el acceso a un determinado sistema informático.

En consecuencia, el *hacker* y el *hacking* son tenidos en el marco de este trabajo como términos saludables y necesarios para el desarrollo de la informática y su seguridad. Pero debemos ir más allá. Nadie puede pretender que cuando una persona ingrese a un sitio no trate de borrar sus rastros para evitar cualquier tipo de responsabilidad, justamente por que existimos nosotros que pretendemos sancionar a aquellos que ingresen en forma subrepticia a un sistema informático.

Hay un supuesto que es claro en este sentido. Una persona comprueba la existencia de una vulnerabilidad en el cliente de correos Outlook de Microsoft, o en una base de datos de un organismo público, empresa o sitio particular. Su siguiente paso será tratar de ingresar. Lo logra. Así pues, ya tenemos dos actividades:

a.- Comprobar la existencia de una vulnerabilidad; y

b.- Utilizar esa vulnerabilidad e ingresar al lugar.

Luego, el sujeto puede hacer lo siguiente:

c.- borrar sus huellas mediante la modificación de los *logs* del servidor para evitar ser rastreado (téngase en cuenta que existen legislación que prevén esta actividad como delito);

d.- hacerse de algún dato sin importancia para probar su ingreso y alardear (todos hacemos esto en nuestras vidas);

e.- dar aviso al responsable de la seguridad de ese sitio;

f.- descargar la totalidad de la base de datos del sistema con distintos fines; y

g.- destruir o modificar todo el contenido del sitio o del sistema.

En los casos “f” y “g” nadie discutirá que nos encontramos ante una conducta que debe tener consecuencias dentro del derecho, incluso el penal, pero, a alguien se le ocurre que debería ser sancionado los supuestos de los puntos “a”, “b” o incluso el “e”.

Pues bien, imaginemos que los proyectos 0064/CD/2002, 3873-CD-2006, 5084-CD-2006 o el de reforma integral del código del Ministerio de Justicia y Derechos Humanos cobren vigencia, y el responsable del sitio al recibir la comunicación efectúa la denuncia penal: ¿Condenaríamos a sujeto activo por este hecho? Cuando su conducta solo puede tener beneficios positivos para la comunidad y para el propio denunciante. Con esto haríamos simplemente afectar la seguridad de la información y tendríamos noticias del acceso informático cuando sea tarde y ya el bien jurídico haya sido afectado. Si debe haber una ley, esta debe dejar claro que el denominado intrusismo informático y la actividad de muchas personas que realizan pruebas de seguridad y acceso (seguridad ofensiva) con fines “éticos”, no resultan abarcados por el código penal.

Dictar este tipo de leyes sería adoptar la postura inocente de esperar que nadie trate de ingresar a sitios o lugares que no le pertenecen. Debemos preguntarnos: ¿es que nunca nos tentamos con hacer esto?

Distintos son los casos donde el ingreso se produce con otros fines como ser el hacerse bases de datos para defraudar, extorsionar, obtener ventajas económicas y otro sin fin de circunstancias, y donde el denominado mero intrusismo informático deviene un acto preparatorio de

esas actividades. Sancionar el segundo por no poder acreditar el primero también es una política criminal incorrecta.

Incluso se ha dicho, y con razón, que el *hacking* presenta una problemática compleja que dificulta su sanción por la legislación penal, pues se ha dicho más de una vez que esta conducta, por su insignificancia, se encuentra fuera de los límites de intervención del poder punitivo[23].

Tampoco podemos, en casos como estos, establecer tipos penales donde la diferencia entre el ámbito de libertad y prohibición que queremos asignar quede en la mera esfera subjetiva de la persona que realiza el delito, descansando el sistema en la capacidad probatoria de la rama procesal, donde además el delito de violación de secretos aplicable a este caso resulta ser de acción privada (Arts. 73 y 153 del Código Penal), y justamente la capacidad de denunciar recae en personas que no tendrán conocimiento de que sus computadoras han sido accedidas, salvo cuando vean publicadas su información privada.

Si nos planteamos proteger seriamente la privacidad de las personas, debemos tener en cuenta estos factores, pues justamente los usuarios son los mas desprotegidos ante actividades informáticas destinadas a ilícitos, ya que los sistemas informáticos públicos se encuentran a resguardo en algunos casos por leyes especiales y las informaciones confidenciales de las empresas encuentran también protección desde la ley 24.766. Debemos aclarar que a estos fines, a un *hacker* le resultará mucho mas entretenido ingresar a un sistema llamativo que a una computadora personal, salvo que tenga noción en este último de la existencia de datos llamativos, con lo cual ingresará para hacerse de esa información y de esa forma caerá fuera de los límites del mero intrusismo informático.

Finalmente y como para todos los delitos, la inclusión de un tipo penal de mero intrusismo aún con penas extremadamente graves, tiene dudosa consecuencias de prevención de este tipo de hechos.

Debemos entonces decir que la prohibición legal para estos casos debe partir desde la mera descripción sistemática del tipo penal, y por ello solo nos queda, respetando todos los principios y realidades esbozadas en estas hojas, no prever en nuestro código penal el delito de mero intrusismo informático o mero acceso no autorizado o *hacking*.

En síntesis, y ante la pregunta que nos hicimos, la respuesta es un claro no, por las siguientes cuestiones:

1.- Por política criminal servirá mas a los efectos de garantizar la seguridad jurídica no sancionar el mero acceso o intrusismo informático.

2.- La privacidad comercial en la empresa ya esta debidamente resguardada por la ley 24.766, como así también lo están los secretos de índole militar y de defensa, o las bases de datos de ciertos organismos públicos.

3.- Un sistema informático no es un domicilio, y en consecuencia la intimidad de una persona no se encuentra afectada de la misma forma por el mero ingreso a su computadora que a su lugar de habitación, ante lo cual, desde el punto de vista informático, su ámbito de intimidad comienza a ser afectado cuando el intruso empieza a obtener datos y objetos determinados del titular del sistema.

4.- Resulta difícil establecer aquellos casos donde el mero intrusismo informático pueda constituir actos previos de otras actividades penales mas graves, pero ello es posible. Resulta inaceptable suplantar las deficiencias procesales del sistema mediante la inclusión de un tipo penal que prevé esta conducta como delito autónomo justamente por no poder acreditar ultra finalidad o como adelantamiento de la berra punitiva y por ende disminuyendo el ámbito de libertad de las personas.

5.- Rigen los principios de insignificancia y proporcionalidad del Derecho Penal.

En caso de que pretenda tipificarse la violación de la intimidad desde el medio informático, lo cual nos parecería lógico y penalmente viable, será preciso establecer dos puntos fundamentales para no caer en la irracionalidad:

- el hecho debe ser realizado violando parámetros, aún mínimos, de seguridad. Con esto evitaremos que el mero acceso o lectura de la pantalla de una computadora nos convierta en un delincuente.
- el bien jurídico intimidad o privacidad sea realmente afectado.
- el mero acceso o comprobación de vulnerabilidades de un sistema informático, debe ser una conducta no punible.

Por ello, entendemos que sería coherente con estos postulados la creación de un tipo penal con una redacción similar a la siguiente: el que mediante la violación de medidas de seguridad y sin

estar autorizado, acceda, obtenga, transfiera o copie datos o información privada o de acceso restringido de personas físicas, contenidas en un sistema informático u otro dispositivo semejante.

Dicha legislación debería entrar a jugar hermenéuticamente con las leyes y artículos penales relacionados con la privacidad informática referida en las páginas anteriores, o bien producirse una reforma integral de estos temas.

Eduardo E. Rosende

Citas:

[1] http://www.itu.int/wsis/index-es.html
[2] http://buscon.rae.es/diccionario/drae.htm
[3] Riquert, Marcelo Alfredo: "Informática y Derecho Penal Argentina", Editorial Ad-Hoc, 1° Edición, Buenos Aires, 1999, pág. 21.
[4] Gratton, Pierre: "Protección informática", Editorial Trillas, 1° Edición, México, 1998, pág. 23.
[5] Morón Lerma, Esther: "Internet y Derecho Penal: Hacking y otras conductas ilícitas en la red", Editorial Aranzandi, Segunda Edición, Navarra, 2002, Pág. 25.
[6] Sloan, Irving J.: "The Computer & The Law", Legal Almanac Series, N° 38, 1984, Oceana Publications Inc., pág. 2.
[7] Gratton, Pierre: "Protección informática", Editorial Trillas, 1° Edición, México, 1998, Pág. 34.
[8] Presentación efectuada en el I° Seminario Internacional sobre delitos relacionados con la tecnología, realizada el día 13 de julio de 2004, organizado por la Asociación de Magistrados y Funcionarios de la Justicia Nacional, el Ministerio Público Fiscal, Policía Federal Argentina, Ministerio de Relaciones Exteriores, Comercio Internacional y Culto, Ciudad Internet y América On Line.
[9] Palazzi, ob. Cit. Páginas 39 y 43.
[10] Sáez Capel, José: "Informática y Delito", Editorial PROA XXI, Segunda Edición, Lanús, Provincia de Buenos Aires, 2001, Página 109.
[11] http://web.mit.edu/
[12] Hernández, Claudio: "Hackers. Los piratas del chip y de Internet", Edición Electrónica en Español, 2001, Página 19 –http://person.wanadoo.es/snickers-.
[13] Sáez Capel, José: "Informática y Delito", Editorial PROA XXI, Segunda Edición, Lanús, Provincia de Buenos Aires, 2001, Página 109.
[14] Himanen, Pekka: "La ética del hacker y el espíritu de la era de la información", Editorial Destino, 1° reimpresión en Argentina, Valentín Lasina, Provincia de Buenos Aires, 2002.
[15] Sobre las implicancias para la privacidad de la comunidad del sistema Echelon, ver http://www.el-mundo.es/ariadna/2002/100/1025768636.html.
[16] El Diccionario de la Lengua Española, en su 23° edición define a este término así: "**1.** tr. Descubrir o manifestar lo ignorado o secreto. U. t. c. prnl." Ver www.rae.es.
[17] Council of Europe –European Committee on Crime Problems-: "Computer-Related Crimes. Recommendation No. R (89) 9 on computer-related crime and final report" (Prefacio por August Bequai), Edición Electrónica, Strasbourg, 1990, páginas 33 a 68.
[18] http://www.guardiacivil.org/telematicos/formatos/ciberdelincuencia.pdf
[19] http://www.adi.cl/admin/articlefiles/181-19223.pdf
[20] Gorini, Jorge Luciano: "Límites a la tutela penal de la integridad de la información. La actualidad del daño informático", Publicado en la Revista La Ley, Suplemento de Derecho Penal, Buenos Aires, 23 de Agosto de 2004, página 30, y en www.laleyonline.com.ar.
[21] Ley especial contra delitos informáticos (Gaceta Oficial Nº 37.313 de fecha 30 de octubre de 2001).
[22] http://www.sbg.ac.at/ssk/docs/stgb/stgb_index.htm
[23] Gutiérrez Francés, M.: "El intrusismo informático: ¿represión penal autónoma?", en Informática y Derecho, Universidad Nacional de Educación a distancia, Mérida, 1995.

Bibliografía:

- A.A.V.V.: "El Derecho y las nuevas tecnologías", Editorial Depalma, Buenos Aires, 1990.
- Bravo, Rodolfo Herrera; Zabale, Ezequiel y Guillermo Beltramone: "Delitos informáticos", publicado en eldial.com.
- Brond, Leonardo - Brignani, Sebastián: "Delitos informáticos: panorama deslindante y criterio de demarcación", publicado en laleyonline.com.ar 06/04/2004.
- Brown, John A.: "Computadoras y Automatización", Editorial GLEM, 1965.
- Buompadre, Jorge Eduardo: "La tutela penal del sistema informático", LL, 1988-A-985.
- Buompadre, Jorge E.: "Delitos contra la libertad", Editorial Mave. 1° Edición, Avellaneda, 1999.
- Castells, Manuel: "La Era de la Información. La Sociedad Red", Volúmen 1, 1996. Alianza.
- Castells, Manuel: "Hackers, crackers, seguridad y libertad", Lección inaugural del curso académico 2001-2002 de la Universidad Abierta de Cataluña, España (UOC), publicado en
- Charney, Scot: "Crímenes en la Red", publicado en la Revista Derecho de Alta Tecnología (DAT), Año IX, número 99, Noviembre de 1996.
- Chiaravalloti, Alicia - Levene (n.), Ricardo: "Delitos informáticos", LA LEY 1998-E, 1228.
- Chiariglione, Leonardo: "Contenido electrónico", publicado en la Revista Derecho de Alta Tecnología (DAT), Año XI, número 100, junio de 1999, página 19.
- Creus, Carlos: "El miedo a la analogía y la creación de vacios de punibilidad en la legislación penal (Intercepción de comunicaciones telefónicas y aproximaciones de e-mail", publicado en J.A., N° 6165 del 27/10/99.
- García, Fabián y Palazzi, Pablo: "Consideraciones para una reforma penal en materia de Seguridad y Virus Informáticos", publicado en la Revista Derecho Penal de Alta Tecnología, Año IX, número 99, noviembre de 1996, página.
- Garfinkel, Simon y Spafford, Gene: "Seguridad práctica en Unix e Internet", Editorial O´Reilly, 2° Edición, México, 1999.
- Gorini, Luciano Jorge: "La necesaria Protección jurídico-penal de la información", publicado en El Derecho, Jurisprudencia General, Universidad Católica Argentina, Tomo 198, Buenos Aires, 2002.
- Gratton, Pierre: "Protección informática", Editorial Trillas, 1° Edición, México, 1998.
- Gutiérrez Frances, M.: "El intrusismo informático: ¿represión penal autónoma?", en Informática y Derecho, Universidad Nacional de Educación a distancia, Mérida, 1995.
- Hernández, Claudio: "Hackers. Los piratas del chip y de internet", Edición Electrónica en Español, 2001, http://person.wanadoo.es/snickers.
- Himanen, Pekka: "La ética del hacker y el espíritu de la era de la información", Editorial Destino, 1° reimpresión en Argentina, Valentín Lasina, Provincia de Buenos Aires, 2002.
- Palazzi, Pablo A.: "Delitos informáticos", Editorial Ad-Hoc, Primera Edición, Buenos Aires, 2000.
- Rifkin, Jeremy: "La era del Acceso. La revolución de la nueva economía", Editorial Paidós, 1° Edición en castellano, Avellaneda, 2000.
- Riquert, Marcelo Alfredo: "Informática y Derecho Penal Argentina", Editorial Ad-Hoc, 1° Edición, Buenos Aires, 1999.
- Saéz Capel, José: "Informática y Delito", Editorial PROA XXI, Segunda Edición, Lanús, Provincia de Buenos Aires, 2001.
- Salt, Marcos: "Delitos Informáticos", publicado en Justicia Penal y Sociedad – Revista Guatemalteca de Ciencias Sociales, Año IV, número 6, Guatemala.
- Sieber, Ulrich: "Legal Aspects of Computer-Related Crime in the Information Society – Comcrime-Study-". Informe preparado para la Comisión Europea. Versión electrónica 1.0 del 1 de enero de 1998, contenida en la base de datos de www.sage.com.
- Sloan, Irving J.: "The Computer & The Law", Legal Almanac Series, N° 38, 1984, Oceana Publications Inc.
- Sterling, Bruce: "La caza de los hackers", Edición electrónica en de Libros en Red (www.librosenred.com), 1994.
- Vianna, Tulio: "Brasil: Do Delito de Dano e de sua Aplicação ao Direito Penal Informático", Alfa - Redi: Revista de Derecho Informático, Viernes, 12 Noviembre del 2004, http://www.alfa-redi.org/revista/data/64-8.asp
- Zaffaroni, Eugenio Raúl: "Derecho Penal Parte General", Editorial Ediar, 2° Edición, Capital Federal, 2002.

o Otras fuentes, recursos y enlaces utilizados:

- 2º Encuentro Internacional de seguridad informática, Presentaciones publicadas en CRYPTEX - Seguridad de la Información - http://seguridad-informacion.blogspot.com/.
- II Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de Las Américas Sobre Delito Cibernético (Lima, Perú - 1 al 3 De Marzo De 1999).
- III Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de Las Américas Sobre Delito Cibernético (1 al 3 De Marzo De 2000 San José, Costa Rica).
- IV Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de Las Américas sobre Delito Cibernético (Puerto España, Trinidad y Tobago 10 al 13 De Marzo de 2002).
- V Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de Las Américas sobre Delito Cibernético (Washington, Dc, 28 Al 20 De Abril De 2004).
- VIII Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública, Panamá, 28-31 Oct. 2003
- VIII Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública, Panamá, 28-31 Oct. 2003
- Convención sobre criminalidad del Consejo de Europa, también llamado Convenio sobre Cyber Crimen, o Cyber criminalidad, o Convenio sobre Criminalidad del Consejo de Europa.
- Council of Europe –European Committee on Crime Problems-: “Computer-Related Crimes. Recommendation No. R (89) 9 on computer-related crime and final report” (Prefacio por August Bequai), Edición Electrónica, Strasbourg, 1990.
- Cyber Security Enhancement Act of 2002
- http://www.france.diplomatie.fr/actual/evenements/cybercrim/jospin.gb.html.
- http://conventions.coe.int/treaty/en/projets/delincuencia cibernética.htm.
- http://www.delitosinformaticos.com/
- http://laws.justice.gc.ca
- OECD (Organization for Economic Cooperation and Development), "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", 23/9/1980.
- Regulations of Investigatory power acts
- Regulation of investigatory Powers Bill
- Revista Z.net en Español Defensa de derechos civiles en Internet
- The Electronic Communications Act 2000
- The Freedom of Information Act 2000
- The Terrorism Act 2000
- USA PATRIOT ACT
- www.congreso.gov.ar
- www.usdoj.gov
- www.cybercrime.gov
- www.oea.org
- www.rae.es