Delitos Informáticos: La punibilidad del Hacking y sus consecuencias.

Marcelo G. I. Temperini

Director de la Red Iberoamericana de Derecho Informático – elderechoinformatico.com, Estudiante de Derecho de FCJS de UNL. Cientibecario UNL Convocatoria 2010 e integrante de CAID "Gobierno Corporativo y Responsabilidad Social Empresaria". Director de AsegurarTe – Consultora en Seguridad de la Información. temperinimarcelo@gmail.com

Abstract Español. Dentro de la gama de los delitos informáticos, la actividad del hacking o acceso indebido sin daño ha sido fuente de discusiones y debates. Su actividad, como filosofía de vida con fines intelectuales lleva más de 50 años de desarrollo, existiendo en la actualidad, grupos sociales que realizan estas prácticas en total ausencia de animosidad de causar daños. Argentina, a través de la Ley 26.388 lo ha incorporado como delito de peligro abstracto, haciendo innecesaria la comprobación de daño efectivo para la configuración del mismo, y creando de manera indirecta, riesgos propios e inherentes a esta clase de delitos penales. Como argumento, se afirma la protección de la información como interés colectivo o macro-social, siendo los bienes jurídicos tutelados, los secretos y la privacidad. En un primer nivel de debate, se discute sobre si es adecuada su tipificación penal, o si podría considerarse alternativas para su sanción. Considerando su tipificación penal, existe una discusión de segundo grado: ¿es adecuada su sanción a través de pena privativa de la libertad?

Abstract en Inglés: Within the range of computer crime, hacking activity or improper access without damage has been a source of discussion and debate. His activities as a way of life to intellectual pursuits has over 50 years of development, there are at present, social groups that carry out these practices in the total absence of animosity to cause damage. Argentina, through 26 388 of the Act has incorporated as a crime of abstract danger, making it unnecessary to check actual damage to its configuration, and creating an indirect way, inherent risks to this kind of criminal offenses. As an argument, affirming the protection of information as a general interest or macro-social, being legally protected, secrets and privacy. In a first level of debate, we discuss whether the criminal offense is adequate, or whether alternatives could be considered for endorsement. Considering their criminalization, there is a discussion of second degree: ¿is it right through his sanction of deprivation of liberty?.

Keywords: delitos informáticos, hacking, hacker, privacidad, confidencialidad, información.

Introducción.

Dentro del campo de los delitos informáticos, la intromisión ilegal a los sistemas de información (junto a los ataques de denegación de servicios) han sido desde los comienzos, los delitos clásicos a combatir.

Es común escuchar o leer el concepto de *hacking* o *hacker*, asociado a la intrusión en sistemas informáticos, seguidos de robo de información, modificación de datos, hasta incluso, cuando existe supresión de la información.

En la generalidad de las veces, esta mala utilización del vocablo, es empujado y alimentado por los medios masivos de comunicación que, por lo general, responden a dos factores de desconocimiento: interno y externo. Interno, porque el propio redactor de la noticia, desconoce el tema, y por lo tanto, ante un hecho que acontece, decide encabezar el título utilizando ese vocablo: "Hackearon la página de un diario kelper en Malvinas"[1]; "Acusan a un hacker de robar los datos de 130 millones de tarjetas de crédito"[2].

Externo, es por el propio desconocimiento social sobre el concepto *hacker*. Es decir, el común de las personas, sin conocimientos avanzados ni profundos en materia de informática, en su mente, al darle significado a tal vocablo, su representación es precisamente aquella que aprendieron de los propios medios de comunicación, ya sea a través de las propias noticias, películas o internet, haciendo que el aspecto interno y externo se retroalimenten, generando cada vez más degeneración del concepto.

Raíces del hacking.

Al momento de buscar la raiz, la fuente de más confianza es sin dudas acudir al Jargon File, un diccionario informático, construído por informáticos. En él se han recolectado los significados más utilizados dentro de la cultura técnica de los centros de desarrollo más grandes de informática (MIT, SAIL, CMU, WPI, entre otras)[3].

En una pequeña digresión, pero de importancia para comprender la fuente y la entidad del contenido en tal diccionario, diré que el Jargon File fue iniciado por Raphael Finkel en 1975, aunque incluso algunos términos datan de años anteriores. Al comienzo, el archivo estaba muy orientado a conceptos relativos a la Inteligencia Artificial, pero con el tiempo, se fue ampliando. Años después, Richard Stallman[4] realizó grandes aportes, en lo relativo a términos de MIT e ITS.

Dentro del Jargon File[5], repasaremos el concepto de hacker y cracker, con las diferentes acepciones consideradas. El diccionario original, del cuál se extrae lo siguiente, está en idioma inglés, el cuál traduzco para este trabajo.

***hacker**: n.[6]. Originalmente, alguien que hace muebles con un hacha.*

[1] http://www.clarin.com/diario/2010/02/21/um/m-02144818.htm
[2] http://www.clarin.com/diario/2009/08/17/um/m-01980137.htm
[3] Instituto Tecnológico de Massachusetts (MIT); Laboratorio de IA de Stanford (SAIL), Universidad de Carnegie-Mellon (CMU), Instituto Politécnico de Worcester (WPI).
[4] Richard M. Stallman, Programador Estadounidense, Fundador del Movimiento de Software Libre, la FSF y el Proyecto GNU.
[5] Versión 4.4.7, modificada por última vez el 29 de Diciembre . www.catb.org/jargon
[6] http://catb.org/jargon/html/H/hacker.html

1) Una persona que disfruta explorando los detalles de los sistemas programables y en cómo extender sus capacidades, a diferencia de la mayoría de los usuarios, que prefieren aprender sólo el mínimo necesario. En RFC1392, un glosario de los usuarios de Internet, ayuda ampliándolo como: Una persona que se complace en tener un conocimiento íntimo del funcionamiento interno de un sistema, las computadoras y redes informáticas, en particular.

2) Alguien que programa con entusiasmo (incluso obsesivamente) o que disfruta de la programación y no sólo teorizar acerca de la programación.

3) Una persona capaz de apreciar el "valor hacker".

4) Una persona que es buena programando rápido.

5) Un experto en un programa en particular, o uno que con frecuencia no funciona, como en "un hacker de UNIX". (Definiciones de 1 a 5 están correlacionadas, y las personas que se ajustan a ellas se congregan.)

6) Un experto o entusiasta de cualquier tipo. Uno puede ser un hacker de la astronomía, por ejemplo.

7) Uno que disfruta el reto intelectual de superar o sortear creativamente las limitaciones.

8) (obsoleto) Un entrometido malicioso que intenta descubrir información sensible por curiosidad. Por ejemplo: hacker de contraseñas, hacker de la red. El término correcto para este sentido es cracker.

El término hacker 'también tiende a connotar pertenencia a la comunidad global definida por la red (consulte la red. Para la discusión de algunos de los fundamentos de esta cultura, consulte el Cómo hacer en el FAQ Hacker). También implica que la persona descrita se considera suscripta a alguna versión de la ética hacker (véase la ética hacker).

Es mejor ser descrito como un hacker por otros que para describir a sí mismo de esa manera. Los hackers se consideran algo de una élite (una meritocracia basada en la capacidad), aunque se reciben a los nuevos miembros de buen grado. Así pues, es la satisfacción del ego que se había determinado en la identificación de sí mismo como un hacker (pero si una persona se jactase de ser un hacker y no lo es, rápidamente se los etiquetará como un fraude). Véase también geek, wannabee.

Este término parece haber sido adoptado por primera vez como una insignia en la década de 1960 por la cultura hacker que rodean TMRC y el Laboratorio de Inteligencia Artificial del MIT. Tenemos un informe que se utilizó al concepto en un sentido restringido por radioaficionados adolescentes y experimentadores electrónicos, a mediados de la década de 1950.

Como vemos, dentro del mismo concepto, se han ido plasmando las diferentes acepciones que podemos llegar a conocer de este vocablo, algunas de ellas, más que interesante para profundizar.

Tal como se señala en final del punto 5, las primeras cinco acepciones, giran alrededor de un marco de características comunes, resumiéndolas como "una persona experta en programación, que conoce íntimamente los sistemas y la red, que disfruta explorando sus límites, descubriendo desafíos y comprendiéndolos, cuyo fin es experimentar diferentes alternativas para vencer el sistema, sin tener intereses en la información que exista dentro del mismo (valor hacker). Este primer concepto de hacker, al cuál en este trabajo me referiré como de carácter restringido, dado que si

bien conserva los caracteres comunes de la actividad, la misma es siempre circunscripta al contexto de la informática, los ordenadores, sus sistemas y las redes. Con este sentido, utilizaré el concepto de hacker a lo largo de este trabajo.

A partir del sexto inciso, se observa que el vocablo adquiere un significado más amplio, como de aquellas personas que son expertas o entusiastas en cualquier materia, dando el ejemplo de un "hacker en astronomía". Estas personas, están marcadas por algunas características que ya hemos visto en el aspecto restringido, en el sentido que son aquellas personas que disfrutan de vencer desafíos, de explotar sus capacidades y conocimientos inventando y creando nuevas formas de relacionarse con el sistema (en su acepción general). Este concepto será de carácter amplio.

Si bien considero que metodológicamente, era más correcto precisar primero el significado amplio del concepto, para luego dar lugar al restringido, lo he desarrollado así por una razón histórica, ya que en los comienzos, el vocablo nació en su sentido original (ver nota al pie Nº 20), que era restringido, y luego con el tiempo su acepción se fue tomando en algunos entornos en su sentido amplio. El nacimiento de este vocablo, es en los años 50, expresando la manera (dando un golpe brusco) en que algunos sujetos reparaban los equipos telefónicos del momento (hack - hachar).

El valor hacker.

En el punto 3 del concepto de hacker del Jargon File, introduce este elemento del "valor hacker", dando un vínculo hacia la concepción del mismo glosario informático[7]. El mismo, trae esta descripción:

Generalmente presentado como la razón o motivación para el esfuerzo con un objetivo aparentemente inútil, donde el punto es que la meta lograda es una de poca entidad. *Por ejemplo, MacLISP tenía características para leer e imprimir los números romanos, que fueron instalados exclusivamente para lograr este valor hacker. Mirar una pantalla de hack es un método de cálculo del valor hack, pero esta realidad no se puede explicar, sólo a través de la experiencia. Como Louis Armstrong dijo en una ocasión cuando se le pide que explique de jazz: "Hombre, si tienes que pedir que te lo expliquen, es que nunca lo has conocido."*[8]

Considero de importancia la significación del valor hacker, ya que expresa el real aspecto subjetivo, que luego deberemos tener en cuenta al analizar el tipo penal. Rápidamente observamos lo dicho anteriormente con respecto a la finalidad, resumiendo la idea en que el hacker no se interesa en el final (meta lograda u objetivo, que sería la información que guarda el sistema) sino en el camino (el proceso para sortear los límites del sistema). Queda claro que la marca distintiva del valor hacker es el reto intelectual, necesitando en consecuencia dos factores. Primero una persona con verdadero y profundo conocimiento sobre alguna materia. Luego desafíos, en el sentido de aquellos planteos que supongan alguna dificultad para la persona, que incentive a resolver el enigma, a utilizar su conocimiento como base y su mente creativa como herramienta para inventar posibles soluciones.

[7] http://www.catb.org/jargon/html/H/hack-value.html
[8] La negrita pertenece al autor.

Sobre este contexto es que se sacan las escenas conocidas de las películas, de aquellos "chicos en sus computadoras del garage", trabajando hasta largas horas de la noche. En aquellos que duermen pensando en las alternativas a sus teorías para resolver el desafío, que piensan una y otra vez las líneas de código, y vuelven a leer hasta el cansancio el error que devuelve la pantalla, repasando en un instante las cientos de líneas que han hecho para probar su teoría. Se puede aquí observar porque en la acepción de significado restringido, se vincula la figura del hacker a los programadores, ya que son aquellos los que generalmente están acostumbrados a este tipo de prácticas.

Pekka Himanen, en su obra más difundida desarrolla los fundamentos y consecuencias de la ética hacker. En el prólogo de este libro [9], Linus Torvalds[10], desarrolla de manera impecable una explicación sobre el tema del valor hacker, al hablar sobre el tema de las motivaciones. A través su "ley de Linus", categorizando las motivaciones en 3 escalones: supervivencia, vida social y entretenimiento (en mayúscula).

Sostiene Linus que entretenimiento es aquello que está más allá de la supervivencia y la vida social. Es cualquier ejercicio mental del individuo, que tenga como fin explicar para sí el universo. Da un ejemplo nombrando a Einstein, afirmando que él no estaba motivado por la supervivencia cuando pensaba en la física, ni por cuestiones sociales, sino por algo que excedía todo aquello, que era su pasión, su motivo, su ENTRETENIMIENTO (con mayúsculas). Termina definiéndolo como algo intrínsecamente interesante y capaz de plantear desafíos.

Analizaremos por último, la conceptualización dada en el Jargon File sobre **cracker**.

"Aquel que rompe la seguridad en un sistema. Acuñado en 1985 por hackers en defensa contra el mal uso periodístico del hacker (ver el sentido 8). Si bien se espera que cualquier verdadero hacker habrá hecho algún juego de grietas y conoce muchas de las técnicas básicas, cualquiera que haya pasado esa etapa de larva, se espera que ya no caigan en el deseo de hacerlo, a excepción que se necesite inmediatamente, de manera benigna y por razones prácticas (por ejemplo, si se trata de resolver algunos de seguridad con el fin de trabajar un poco). Por lo tanto, hay mucho menos de solapamiento entre los hackers y crackers que el lector mundano cree, engañado por el periodismo sensacionalista. Los crackers tienden a reunirse en pequeños, muy unidos. A menudo les gusta describirse a sí mismos como hackers, piratas informáticos, cuando estos los consideran una forma separada e inferior de vida."[11]

La diferencia clara que existe entre una actividad y otra, que tiene tanta relevancia a nivel objetivo como subjetivo.

A nivel objetivo, podemos observar que los hackers, al testear y comprobar vulnerabilidades de seguridad, por sus propios principios, no dañan (sentido general de no copia, no modificación, no supresión, etc.) la información contenida, siendo que en muchos casos, ni siquiera acceden a la misma [12]. El hacker, al retirarse del sistema

[9] HIMMANEN, Pekka. "La ética hacker y el espíritu en la era de la información". Edición Digital de Licencia GPL. [http://www.educacionenvalores.org/IMG/pdf/pekka.pdf]

[10] LINUS, Torvalds. Creador del Sistema Operativo Linux y uno de los hackers más respetados de la comunidad.

[11] http://www.catb.org/jargon/html/C/cracker.html

[12] Ver clasificación de información en este trabajo.

(si es que accedió), en la mayoría de los casos se contacta con quien tiene el sistema a cargo (administrador), para informar sobre la situación y aconsejar sobre la solución a esa grieta de seguridad.

El cracker, al comprobar la vulnerabilidad existente, buscará la manera de explotarla para acceder al sistema, navegar por dicha información, normalmente copiando, modificando o suprimiendo la misma. En la mayoría de los casos, modifican o agregan información, con leyendas que hagan referencia a su paso por el sistema, con la finalidad de alimentar su ego y poder mostrarlo a sus pares (meritocracia degenerada), tal como aquel ladrón que antes de irse pinta la pared con algún mensaje alusivo.

Estas diferencias son también claras a nivel subjetivo, donde el hacker tiene intenciones de mejorar sus habilidades en la programación y la comprensión de los sistemas, donde el incentivo es un desafío intelectual y no la violación de secretos ni privacidad alguna. **Por ello es que el foco es puesto en los sistemas en sí, y no en la información que contienen.**

En el cracker, la finalidad perseguida sí es la información resguardada detrás de alguna barrera, la vulneración de secretos. Muestra clara de ello, es la irrelevancia sobre el "cómo se accede" a la misma, que puede ser con técnicas básicas o incluso utilizando algún rootkit[13] automatizado, denotando es lo inverso al hacker. El foco no es el sistema, sino en lo que se esconde detrás, la información.

Clasificación del hacking.

Tomando la clasificación realizada por Claudio Manzur, se señala que el hacking puede clasificarse en directo o indirecto. Será directo (también conocido como mero intrusismo) el hacking propiamente dicho, explica este autor, que consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o passwords, no causando daños inmediatos y tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor. La voluntad de divertirse generalmente se traduce en paseos por el sistema haciendo alarde de la intromisión. Es por ello que esta delincuencia se ha nominado "short pants crimes", es decir, crímenes en pantalones cortos; su motivación no es la de causar un daño, sino que se trata de obtener personales satisfacciones y orgullos, basados principalmente en la burla de los sistemas de seguridad dispuestos. Esta clase de hacking no representa un importante nivel de riesgo, toda vez que el hacker no busca causar un daño.[14]

En lo que atañe al hacking indirecto, este autor considera que es el medio para la comisión de otros delitos como fraude, sabotaje, piratería, y espionaje. Señala que en

[13] Un rootkit es una herramienta, o un grupo de ellas que tiene como finalidad esconderse a sí misma y esconder otros programas, procesos, archivos, directorios, claves de registro, y puertos que permiten al intruso mantener el acceso a un sistema para remotamente comandar acciones o extraer información sensible.

[14] MANZUR, Claudio Líbano. "Chile: Los Delitos de Hacking en sus Diversas Manifestaciones", (Revista Electrónica de Derecho Informático). Abogado Profesor. Director Secretario Ejecutivo de la Asociación de Derecho e Informática de Chile (ADI-CHILE)

el caso del hacking indirecto, el ánimo del delincuente está determinado por su intención de dañar, de defraudar, de espiar, etc., entendiendo que no desaparece el delito de acceso indebido, dándose la hipótesis del concurso ideal o formal de los delitos.

El Dr. Hugo Carrión, realiza algunas consideraciones muy interesantes sobre la clasificación del Dr. Manzur. Sostiene que si el acceso ilegítimo al sistema informático es el medio para alterar, modificar o suprimir la información, no habrá hacking sino cracking que supone una acción concreta de daño sobre la información y el elemento subjetivo en el autor –dolo- constitutivo del conocimiento y la voluntad de provocarlo. En lo que atañe a las figuras de hacking y cracking, discrepa en que se verifique el supuesto de concurso ideal de delitos. Como señala, el hacking es el presupuesto necesario del cracking (todo crack supone un hack previo), pero cuando se consuma este ilícito, el anterior queda subsumido en él por reunir las exigencias del tipo, dándose un concurso aparente de delitos por razones de especialidad. Lo contrario importa una doble persecución penal (non bis in idem), situación que se encuentra proscripta por el principio constitucional de legalidad.[15]

Párrafo aparte para una especie diferente del hacking, como lo es el hacking ético, siendo este una actividad desarrollada por profesionales de la seguridad como servicio para empresas u organizaciones que quieran informarse acerca del estado de seguridad de sus sistemas. De esta manera, previo permiso y consentimiento del titular de los sistemas, el profesional habilitado utiliza diferentes técnicas de ataque, tal como utilizaría algún sujeto extraño que quisiera colarse por esos sistemas vulnerando la seguridad, a fin de confeccionar un informe. Este tipo de actividad, es plenamente lícita, ya que queda fuera del tipo penal al considerarse que en estos casos, no se da el requisito de "indebido" (dada la expresión de consentimiento del titular) que exige el tipo penal argentino.

Distintas Posturas

Desde hace tiempo existe la discusión sobre la intervención del derecho penal sobre el hacking, no sólo en nuestro país (que no es uno de los más rápidos en reaccionar frente a los nuevos hechos tecnológicos) sino en los demás países.

En una primera etapa, la discusión giró alrededor de si debía o no punirse el hacking. Una primera posición encuentra a aquellos que no consideran que el hacking sea una conducta disvaliosa de tal entidad que justifique la participación del derecho penal (pero que sí podría traer consecuencias de responsabilidad civil). No habría dudas en el caso del cracking, donde existe un daño real y concreto sobre la información, justificando sí la sanción penal. En el otro extremo, se encuentra la posición que elige considerar al hacking como conducta delictuosa, como delito de peligro, teniendo en consideración las supuestas implicancias negativas que existirían socialmente si el legislador penal no tomara intervención en el asunto.

Dentro de esta última posición, que es sin duda la receptada por la mayoría de los países, podemos distinguir una nueva dicotomía, presentando por un lado a aquellos

15 CARRION, Hugo Daniel. "Presupuestos para la punibilidad del hacking", *1º Jornadas Latinoamericanas de Derecho Informático, Organizacón Mundial de Derecho e Informática,* Mar del Plata, 2001. [http://www.delitosinformaticos.com/trabajos/hacking.pdf]

que adhieren a una posición de castigar la actividad del hacking directo (o mero intrusismo) con pena privativa de la libertad, frente a aquellos que consideran que es suficiente con una sanción de multa y/o inhabilitación, dejando la pena de prisión para el caso de la producción real de un daño o apropiación de datos en un sistema informático (crack).

Ya en las conclusiones de la comisión de delitos informáticos de la *"1º Jornadas Latinoamericanas de Derecho Informático"*[16], se incluyó la recomendación expresa de profundizar el debate sobre la eventual incriminación del mero intrusismo.

Aquellos que consideran al hacking como delito penal con pena de privativa de la liberad, argumentan que la experiencia es demostrativa que, en la mayoría de los casos, quien accede a un sistema informático intentará copiar información, destruirla, borrarla o apropiarse de algún dato valioso[17]. Fundados en estudios criminológicos realizados en otros países que han demostrado que (en términos generales) los comportamientos que inicialmente se configuraron como de mero intrusismo informático, detectados pero no reprimidos por la legislación de ese momento, culminaron por pasar o dar paso a otros ilícitos más graves, como los diversos atentados a la intimidad, además del sabotaje, espionaje o defraudaciones informáticos. En función de ello, legislaciones como la de Estados Unidos optó por penalizar el mero intrusismo como un tipo residual, en la inteligencia de que ello actuaría como una suerte de *"delito barrera"* o *"delito obstáculo"*.[18]

Esta solución es la adoptada por la legislación argentina a partir de la Ley 26.388, en el art. 153 bis. En su redacción final, el tipo penal queda configurado con el mero acceso (indebido) a un dato o sistema de acceso restringido (sin exigencia de comprobación de daño real), y la pena que corresponde es de prisión (de 15 días a 6 meses).

Dentro de esta postura de sanción penal, otros autores consideran que caer en la pena privativa de la libertad para el hacking es excesivo, pensando en la posibilidad de los otros tipos de sanciones que incluye nuestro Código Penal en el art. 5, como la multa e inhabilitación (más allá de la responsabilidad civil que pudiere corresponder en el caso concreto). Siguiendo en esta línea al Dr. Marcelo Riquert, al cuál adhiero en su opinión, que al comentar la redacción del art. 153 bis incorporado al Código Penal Argentino, expresa su diferencia en el tema: "Entendemos que habiéndose optado por la criminalización de esta conducta disvaliosa resignando la vía contravencional, al menos podría haberse evitado la utilización de la pena privativa de libertad en la figura básica. Es claro que no sólo en el imaginario colectivo, sino en la mente del legislador, sigue instalada férreamente la idea de que "penar" significa "privar de libertad". No albergo dudas de que estamos frente a una conducta que

[16] Mar del Plata, 6 al 8 de setiembre de 2001, organizadas por la OMDI, Organización Mundial de Derecho e Informática

[17] PALAZZI, Pablo Andrés. "El acceso ilegítimo a sistemas informáticos: la urgente necesidad de actualizar el código penal", JA 1999-III-321.

[18] RIQUERT, Marcelo Alfredo. "'Hacking, Cracking, Email y dos fallos judiciales que denuncian lagunas en la legislación penal argentina".

tendría una respuesta punitiva más racional si se la hubiese conminado con multa o alguna inhabilitación especial o alternativa reparatoria."[19]

Posición similar fue considerada y fundamentada en el anteproyecto del 2001, coordinado por la Dra. Mercedez Vazquez, que si bien considerada la actividad como ilícito penal, afirma: "Consideramos apropiada aquí, la fijación de una pena de multa, atento que se trata de una figura básica que generalmente opera como antesala de conductas más graves, por lo que no amerita pena privativa de la libertad, la que por la naturaleza del injusto habría de ser de muy corta duración. Este criterio resulta acorde con el de las legislaciones penales más modernas (Alemana, Austríaca, Italiana, Francesa y Española), que ven en la pena de multa el gran sustituto de las penas corporales de corta duración, puesto que no menoscaban bienes personalísimos como la libertad, ni arrancan al individuo de su entorno familiar y social o lo excluyen de su trabajo."[20]

Legislación Argentina

En Argentina, en Junio del 2008, a través de la Ley Nº 26.388 se ha modificado nuestro Código Penal, en general incorporándose algunos artículos, pero también modificando y derogando otros. Dada la especificad de este trabajo, solamente destacaré el tipo penal referidos a la actividad aquí analizada. Es relevante destacar que a través del art. 3 de la citada norma, se ha modificado el título del Capítulo III, Título V, del Libro II del Código Penal, por el siguiente: "Violación de Secretos y de la Privacidad" (antes solamente decía Violación de Secretos). El art. 153 bis tipifica el acceso indebido, mientras que el agregado al art. 183, regula el daño informático.

"Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que 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 (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros."

En el primer elemento, "**el que a sabiendas accediere por cualquier medio**" podemos ver la exigencia del dolo en el sujeto, de manera que quedarían excluídas aquellas situaciones donde por culpa o ignorancia se accediera a un sistema. Aquí encontramos el verbo del tipo, de manera que el delito quedaría consumado al "acceder" (cumpliendo con los demás elementos requeridos). No está claro aún cuál es la correcta interpretación de este concepto, que es de importancia ya que en determinados supuestos prácticos, existirá la duda acerca de su existe o no el acceso. Basta mencionar el ejemplo de aquella persona que realiza escaneo de puertos en una red, consiguiendo variada información de los sistemas interconectados. ¿Existe acceso

19 RIQUERT, Marcelo Alfredo. "Algo más sobre la Legislación contra la Delincuencia Informática en MERCOSUR a propósito de la Modificación al Código Penal Argentino por Ley 26388", publicado en AR-DI, Nº 121, Agosto 2008.

20 Informe preliminar de la Comisión de Delitos Informáticos convocada por la Secretaría de Comunicaciones del Ministerio de Infraestructura y Vivienda de la República Argentina, coordinada por Mercedes Velázquez, presentado el 24 de septiembre de 2001

allí? Opino que no. Que para que exista acceso a los fines de este tipo penal, el sujeto debería tener la posibilidad real de poder disponer de la información accedida indebidamente.

Es feliz la adopción de un criterio amplio al momento de definir los medios a través de los cuáles se podría cometer el delito. Con la dinámica evolución de la actualidad, sería de mala técnica legislativa el indicar una u otra tecnología determinada para la comisión del tipo.

En el segundo elemento: "**Sin la debida autorización o excediendo la que posea**", encontramos uno de los puntos más importantes del tipo, haciendo referencia a la "debida autorización", tema y concepto ya desarrollado de manera impecable por el Dr. Pablo Palazzi en su obra de Delitos Informáticos[21].

La debida autorización deja una puerta abierta para aquellos casos donde se pueda obtener el consentimiento para el acceso, quedando así excluída del tipo penal. Es claro ejemplo las organizaciones que contratan servicios de *penetration test*, servicio prestado en general por las empresas relacionadas con la Seguridad de la Información.

La segunda parte, al mencionar "o excediendo la que posea", deja también un interesante espectro de posibilidades abierto. En el ejemplo mencionado, de un servicio de detección de vulnerabilidades desde el exterior o interior de la empresa, podría configurar el delito si el profesional realizará actividades traspasando los límites impuestos en su contrato de servicios. Otro ejemplo podría suceder en una organización X, donde siguiendo prácticas normales de Seguridad de la Información, se clasificara la misma en tres niveles: bajo, medio y alto. A su vez, al realizar los perfiles de usuario, y atribuyendo los privilegios que correspondan según cada uno, quedará también un entramado de limitaciones definido. Así, la secretaria podrá entrar a información clasificada en la importancia baja; los gerentes a la clasificada media y los miembros de la dirección, al nivel alto de información. ¿Que pasaría entonces si la secretaria accediera a información de nivel medio o alto? Estaría excediendo la autorización que posee, quedando configurado el delito de acceso indebido.

Tercer y último elemento de este tipo penal, es la mención de "**a un sistema o dato de acceso restringido**". Creo fuera de discusión el significado de sistema o dato, ya que la formula es lo suficientemente amplia como para limitar su alcance. Es destacable el significado de "acceso restringido", concepto del cuál he intentado en reiteradas ocasiones obtener (con no mucho éxito) algún consenso técnico-jurídico sobre el mismo. Con razón se me ha respondido (desde las ciencias duras) en que si el sistema fuera público o no restringido, el hecho quedaría excluído del tipo penal Existe actualmente cierto consenso sobre que si el sistema posee algún tipo de verificación de identidad para el sistema (logueo), ello sería suficiente para ser considerado restringido. Concepto que creo acertado pero insuficiente para dar respuesta a la gran cantidad de variables existentes en la realidad, y por ello insisto en lo importante de llegar a un espacio de mínimo acuerdo sobre el nivel de seguridad necesario para poder calificar como restringido.

Opino que debería profundizarse en el tema, estableciendo desde la Seguridad de la Información, algunos parámetros objetivos para poder demostrar lo "restringido" de un sistema, máxime si se trata de sistemas estatales, donde la información (en su

[21] PALAZZI, Pablo. "Los Delitos Informáticos en el Código Penal. Análisis de la Ley 26.388". Edit. Abeledo Perrot. 2009.

mayoría) es de alto valor, y donde debería extremarse las precauciones de Seguridad. Requisitos que se podrían atenuar tratándose de sistemas hogareños de cualquier particular, que bien podría carecer de todo conocimiento informático de seguridad.

Legislación Comparada.

En Chile, se incorporaron los delitos informáticos a partir del 2002, con la Ley 19.223, en cuyo art. 2, dice: *"El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio."*. En esta misma norma, en el art. 3 se tipifica por separado el daño informático.

En Colombia, desde el 5 de Enero del 2009, con la Ley 1273, se agrego al Código Penal el Título VII BIS, denominado *"De la protección de la información y los datos"*, en cuyo primer artículo incorporado, tipifica al acceso indebido: *"El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes."*.

Dentro del Derecho Comparado, existe la Decisión 2005/222/JAI de la Unión Europea, cuyo objeto es reforzar la cooperación entre las autoridades judiciales y otras autoridades competentes, incluida la policía y los demás servicios represivos especializados de los Estados miembros, mediante la aproximación de su legislación penal en materia de ataques contra los sistemas de información. En sus artículos, la Decisión brinda el marco al cuál los Estados Miembros debieron legislar en materia de delitos informáticos.

Artículo 2: *Acceso ilegal a los sistemas de información.*

1. Cada Estado miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

2. Cada Estado miembro podrá decidir que las conductas mencionadas en el apartado 1 sean objeto de acciones judiciales únicamente cuando la infracción se cometa transgrediendo medidas de seguridad.

Artículo 3: *Intromisión ilegal en los sistemas de información*

Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

Podemos observar a simple vista que el art. 2 hace referencia al hacking, y el art. 3 al cracking. De ambos artículos, destaco que si bien obliga a su consideración como infracción penal, no obliga a que ella sea de prisión, dejando margen para su decisión en los Estados Miembros. Además, en ambos, destaco que el acto sea "intencionado",

y que en la última frase, deja un marco de libertad para su regulación, al considerar que se debe sancionar su acceso "**al menos en los casos que no sean de menor gravedad**". De esta manera, podría considerarse dentro del marco jurídico de la Directiva, la existencia de determinadas circunstancias para que la acción sea considerada como de la entidad suficiente para configurar el delito.

Es un ejemplo de este caso, la tipificación en Bolivia, donde a través de la Ley Nº 1768, introduce en el art. 363 ter la siguiente fórmula: "*El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático,* ***ocasionando perjuicio al titular de la información****, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos día."*[22]

Bien Jurídico Protegido.

A partir del art. 3 de la Ley Nº 26.388, se sustituyó el epígrafe, agregándose la privacidad a los secretos, quedando ambos como bienes jurídicos protegidos.

Para definir cuál es la afectación en el hacking, debemos tener en consideración el tipo de información a la cuál se tendría acceso, ya que del contenido de la misma, surgirá la vulneración de uno u otro bien jurídico protegido, o ninguno de los dos.

Cuando la información a la cuál se acceda mediante el hacking, sea sin contenido personal (por ejemplo comercial, industrial, científica, etc), el bien jurídico vulnerado será la confidencialidad y exclusividad de la misma, derivadas de que el sistema se considera como restringido, y por lo tanto, secreto.

Dentro de este grupo de información, planteo el interrogante sobre si la información de sistema (archivos de datos necesarios para el funcionamiento del sistema operativo del equipo) quedaría incluida en este primer grupo. A prima facie, parecería que dicha información no es secreta (incluso estando dentro de un sistema restringido) dado que su contenido es de similares características en millones de equipos informáticos. Similar consideración puede hacerse sobre información pública (por ejemplo que el sistema albergue sólo información de boletines oficiales). Incluso, podríamos plantear en su extremo, el caso que el sistema sólo tenga cargado el sistema operativo, y carezca de todo tipo de información cargada, lo cuál es perfectamente posible. En todos estos casos, aparentemente no habría bien jurídico secreto o privacidad a proteger, quedando la acción en el caso concreto, sin ese requisito de probabilidad exigente en los delitos de peligro: ¿Quedaría en estos casos la acción excluida del tipo penal?.

En un segundo grupo, consideramos que el acceso se realiza sobre información de naturaleza personal (todo tipo de datos personales), quedando clara sí una vulneración a la intimidad y privacidad de las personas.[23]

Prueba de que ello está fuera de discusión, es la creación del tipo penal especial por la Ley Nº 25.326, que incorporó al Código Penal el art. 157 bis.

[22] La negrita pertenece al autor.
[23] CARRION, Hugo Daniel. "Presupuestos para la punibilidad del hacking", op. cit.

El riesgo de los delitos de peligro.

Como se ha trabajado anteriormente, la postura más aceptada en la actualidad, es la punición del hacking a través del derecho penal, quedando el debate sobre la conveniencia o no de considerar a la pena privativa de la libertad como la más adecuada para el mismo. En sus bases se observa que al afectar la confidencialidad (en todos los casos, siempre que el sistema sea restringido) y privacidad (en algunos casos), supone un riesgo para la información como interés colectivo. Dentro de este razonamiento, es entonces que se dan los fundamentos para su tipificación como delito de peligro abstracto, ya que para su configuración, es suficiente la comprobación de la acción (acceder).[24]

Según Hassemer, los delitos de peligro abstracto facilitan la utilización del derecho penal, ya que no es necesario probar la lesión efectiva al bien jurídico, sino que solo basta con demostrar lo peligroso de la acción. Con ello reduce los requisitos para castigar y las posibilidades de defensa. Afirma que la criminalización de estas acciones, disminuyen el significado de derecho penal mínimo, y que es utilizado por el legislador para sus ganancias políticas. En derecho Penal, según el autor citado, ya no se trata de una respuesta adecuada a un hecho pasado, sino del dominio del futuro.[25]

Jiménez de Asúa, trabaja la idea que es una herramienta que debe ser manejada con cuidado y precisión, ya que la simple posibilidad no puede servir de índice para calificar como peligrosa una conducta humana. "Al derecho penal solo le debe interesar un sector de la realidad, el que ofrece el riesgo más alto, pues si fuese a preocuparse de las mínimas posibilidades de amenaza a un interés o bien jurídico, la libertad humana recibiría un rudo golpe". Por lo tanto, ha de exigirse la posibilidad inmediata o sea la probabilidad de lesión, que entendemos puede garantizarse a través de la inclusión de elementos subjetivos especiales del tipo penal.[26]

Afirma el Dr. Carrión, que la tipificación del hacking necesariamente implicará la creación de un delito de peligro, que a los fines de zanjar las posibilidades de ataques constitucionales, propone dotarlo de elementos subjetivos en el ánimo del autor (dolo específico), que deben ser probados para formular el correspondiente reproche penal.[27]

Un caso práctico

Entre los meses de Agosto y Noviembre de 2007, en Chile, salió a la luz un caso que reviste interés para el tema analizado en este trabajo. Relacionado con el portal de licitaciones públicas ChileCompras (www.chilecompras.cl), sitio ganador del premio a mejor web del gobierno en el 2005, premiado por Naciones Unidas por contribuir a la transparencia en el servicio público y destacado por el Banco Mundial. Fue utilizado durante 4 años, y en los cuáles realizó transacciones por más de u$s 4.500

[24] BACIGALUPO, Enrique. "Manual de Derecho Penal". Editorial Temis. 1996, pág. 101
[25] HASSEMER, W. Rasgos y Crisis del Derecho Penal Moderno, Anuario de Derecho Penal y ciencias penales, 1992, págs.235-249
[26] JIMÉNEZ DE AZÚA *"Tratado de Derecho Penal"*, T. III, 1965, p. 472 ss.
[27] CARRION, Hugo Daniel. "Presupuestos para la punibilidad del hacking", op. cit.

millones entre las cerca de 900 mil entidades públicas y sus 80 mil proveedores. El hecho fue que Gino Rojas Tilleman, experto en seguridad informática y usuario del sistema, descubrió que el módulo de cuadro comparativo del portal, poseía una vulnerabilidad de validación de entrada que permitía a cualquier usuario registrado ver información crítica, la cual incluía las propuestas técnicas y económicas de otros competidores antes de que el proceso de licitación terminara.[28] Al hacerlo, grabo un video mostrando la falla y contacto con el organismo chileno varias veces para informar sobre la brecha (y ofrecer sus servicios para solucionarlo), llegando a reunirse personalmente con representantes del mismo.

En el fallo, los Magistrados sostuvieron: "...la conducta desplegada por el acusado Rojas Tilleman, **fue más allá de un simple acceso indebido o hacking directo**, por cuanto la reiteración de éstos, desde su IP y respecto de licitaciones que no dicen relación con el rubro farmacéutico, permitió concluir que tuvo conocimiento de la información contenida en la plataforma comercial virtual de Chilecompras." "...por unanimidad el tribunal ha resuelto condenar a Gino Igor Rojas Tilleman, como autor del delito contemplado en el artículo 2° de la Ley 19.223."[29]-[30]

Rodrigo Gutiérrez (www.secure.cl), experto en seguridad informática con más de 9 años de experiencia internacional, consultado para el caso dijo: "Parece claro que de no ser por la denuncia de Rojas, ChileCompras nunca se hubiera enterado y quizás estaría vulnerable hasta el día de hoy, permitiendo a usuarios maliciosos tener importantes ventajas competitivas frente a los mas honestos".
realizada al abogado de Rojas, el Sr. Karim Abdo dijo "Lograr una absolución era casi imposible, simplemente por el tenor de la ley, y no por la acción que haya realizado Gino, pues deja a los magistrados muy atados de manos. Lo que debiese cambiar aquí es la ley que es de 1993, que claramente está obsoleta". "Con esta ley y actitud, es mejor quedarse callado y que los sistemas sigan fallando", explicó el abogado.[31]

Salidas alternativas

Dentro de la naturaleza del delito de hacking, es importante señalar que según el art. 73 inc. 3 de
violación de secretos (que ahora con la modificación del epígrafe ya visto, son de violación de secretos y la privacidad), con excepción de los arts. 154 y 157 (que hace referencia a empleados de correos o funcionarios públicos).

La importancia de ello radica en las posibilidades que existen para este tipo de delitos, y que en los casos de hacking, podrían significar una salida alternativa.

[28] Terra. "Hackeo a ChileCompras pone en duda a miles de licitaciones públicas del gobierno." [http://www.terra.cl/tecnologia/index.cfm?id_cat=415&id_reg=1055070]

[29] Acta de deliberación RIT 135-2009, RUC: 0700879841-3. Santiago, 28 de Agosto de 2009. Magistrados: C. Bugueño Juárez, M. Olave Astorga y C. Catalán Romero.

[30] La negrita pertenece al autor.

[31] Terra. "Las personas que encuentren fallas no las pueden denunciar". [http://www.terra.cl/tecnologia/index.cfm?id_cat=415&accion=internet&id_reg=1253768]

Dentro de ellas se cuenta con la potestad de extinción de la acción penal, regulado en el art. 59 del Código Penal, expresado con la renuncia del agraviado y que sólo es posible en delitos de acción privada.

Para el caso que el juicio ya se hubiese llevado a cabo con su correlativa sanción, existe la posibilidad del perdón por parte del agraviado (art. 69), extinguiendo la pena impuesta por los delitos enumerados en el art. 73.

En ambos casos, si bien se necesita obviamente de la voluntad del agraviado, es una posibilidad que puede a llegar a ser útil en determinados casos prácticos de verdadero hacking, donde el agraviado comprenda la naturaleza de la actividad y decida renunciar o perdonar el ilícito penal.

Reflexiones finales.

A) Que, reconozco que la tasa de delitos informáticos viene en aumento junto con los avances de la tecnología, y que muchos de ellos encuentran en el acceso indebido en su fase preliminar.

B) Que, no obstante se debe tener en cuenta la existencia de un sector de la sociedad que practica el hacking como desafío intelectual, como filosofía de vida y donde existe total ausencia de animosidad de dañar o lesionar la confidencialidad o privacidad ajena.

C) Que, dada la complejidad y dificultad para reprimir los delitos informáticos, se recurre a un adelantamiento de la barrera penal, creando un tipo de peligro abstracto.

D) Que, ese adelantamiento en la barrera penal, trae consigo una disminución de los requisitos necesarios (daño), generando un espectro más amplio y simple para su sanción, pero así también más riesgoso.

E) Que, dentro de esa gama de riesgos del delito de peligro, se reprime incluso quedando demostrado la posibilidad técnica de que quien acceda indebidamente a un sistema restringido, sólo acceda a información de sistema (que no sería confidencial ni privada), o a información de carácter público, y que en ambos casos no se estaría lesionando los bienes jurídicos tutelados.

F) Que, el tipo penal de delito abstracto utilizado en Argentina para la represión el acceso indebido, no contiene en su estructura requisitos (subjetivos ni objetivos) que aseguren la probabilidad del daño.

G) Que, siguiendo la Directiva Europea, considero adecuado la exigencia de requisitos que demuestren cierta gravedad o peligrosidad en la acción, como presupuestos necesarios para la configuración del tipo penal.

H) Que, dentro de las diferentes posturas planteadas, considero que la actividad del hacking no debería ser perseguida penalmente, dado que la probabilidad de riesgo necesaria para la configuración de un delito de peligro no es suficiente.

I) Que, no obstante, y atento a la realidad argentina (donde ya existe como delito de peligro abstracto), opino que su sanción a través de pena privativa de la libertad no es la adecuada, y que debería ser de multa o inhabilitación temporal para ejercer la profesión.