El Hacking No Es (Ni Puede Ser) Delito

Análisis crítico del Proyecto de Ley que modifica la Ley N° 19.223, que tipifica figuras penales relativas a la informática (Boletín N° 2.974-19), en relación con el Proyecto de Ley que modifica el Código Penal con el objeto de recepcionar, en los tipos penales tradicionales, nuevas formas delictivas surgidas a partir del desarrollo de la informática (Boletín N° 3.083-07)

Eduardo Escalona Vásquez
Abogado – Pontificia Universidad Católica de Chile
Diplomado en Derecho Informático – Universidad de Chile

1. Introducción

En el contexto de la era post industrial, la Dogmática Penal liberal está contribuyendo, quizás forzosa y resignadamente, a crear un nuevo Sistema Penal, en el cual destaca una nueva causa final -la eficiencia- ajena a los ideales antropocéntricos característicos de ella. Este *leit motiv*, morigerado con la referencia al combate de la gran criminalidad, especialmente organizada y económica es, ante todo, utilitarista, y por ello puede dar lugar a la creación de tipos penales en que la conducta sancionada sea, sin embargo, irrelevante jurídico-penalmente, atendida la inexistencia de una lesión e, incluso, de una puesta en peligro a un bien jurídico.

Estimamos, a título de hipótesis de trabajo, que tal es el caso de la conducta de *hacking*, entendiendo por tal, en términos amplios y meramente informáticos, sin connotación aún jurídico-penal, "*acceder de forma ilegal* (ilícita, según nuestra opinión) *a un sistema a fin de obtener información, sin la destrucción de datos ni la instalación de virus*".[1]

[1] Gómez Martín, Víctor. *El Delito de Fabricación, Puesta en Circulación y Tenencia de Medios Destinados a la Neutralización de Dispositivos Protectores de Programas Informáticos (Art. 270, Párr. 3° CP)*, artículo inserto en Revista Electrónica de Ciencia Penal y Criminología, http://criminet.ugr.es/recepc, 04-16/2002, p. 3.

Trazaremos, en consecuencia, el siguiente *iter* para demostrar nuestra hipótesis: un breve marco conceptual de las categorías jurídico-penales que deben considerarse involucradas, el cual nos permitirá introducirnos en el análisis de la ley vigente y del proyecto de ley en tramitación en el Congreso Nacional, para luego reflexionar sobre los argumentos que justifican, por un lado, y que excluyen, por otro, la existencia de un tipo penal para el *hacking*. A continuación, confrontaremos las consecuencias que emanarían de una u otra opción con los derechos fundamentales involucrados, reconocidos en la Constitución Política de la República o en los Tratados Internacionales sobre derechos humanos ratificados por Chile y que se encuentran vigentes, a efectos de demostrar la integración adecuada de éstos con el fenómeno informático y el Derecho Penal. Finalmente, expondremos sintéticamente nuestras conclusiones.

2. Marco conceptual

Para efectos metodológicos, adoptaremos funcionalmente algunos conceptos que nos permitirán cimentar las bases de los juicios axiológicos que, por su carácter político criminal, son indispensables en este trabajo.

La reflexión en torno a un proyecto de ley nos sitúa en el ejercicio de una función esencial del Estado en el contexto del Derecho Penal: el *Ius Puniendi*, esto es, "*...la potestad penal del Estado, por virtud de la cual puede declarar punibles determinados hechos a los que impone penas o medidas de seguridad*".[2]

Igualmente, nos limitaremos a recoger de Jakobs el concepto de pena: "*es una muestra de la vigencia de la norma a costa del responsable*"[3]; éste nos permite recalcar el fin preventivo general de la pena, funcional a la teoría de la imputación objetiva que, mayoritariamente, recogen los autores contemporáneos de la Dogmática Penal, aclarando, en todo caso, que el fin preventivo general es, ante todo, aceptado más bien por resignación que por convicción, como el fin de la pena menos doblegado por las críticas de sus detractores.[4]

Consideramos oportuno, además, tener a la vista concepciones liberales sobre el bien jurídico, dado que éste será el fundamento para tipificar penalmente o no la conducta de *hacking*, haciéndonos parte de la crítica casi unánime a la criminalización fenomenológica. Al respecto, recogemos el concepto de Hormazábal, para quien los bienes jurídicos "*...son relaciones sociales concretas de carácter sintético protegidas por la norma penal que nacen de la propia relación social democrática como una superación del proceso dialéctico que tiene lugar en su seno*".[5] Dicho concepto coincide con la fórmula más escueta de Kindhäuser, para quien "*...bienes jurídicos son las condiciones, jurídicamente garantizadas, de libre desarrollo del individuo en una sociedad concretamente configurada*".[6]

También estimamos pertinente referirnos someramente a los conceptos de lesión y peligro (concreto y abstracto), en virtud que la doctrina nacional y extranjera que considera legítima la criminalización del *hacking*, suele fundamentarla en el segundo tipo de ellos. Al efecto, "*lesiones son menoscabos de la integridad del bien; su lesividad reside en la depreciación del bien en sí mismo (...) peligros concretos son situaciones en las que, desde la perspectiva del bien, es probable una lesión que no puede ser evitada de forma planificada*"[7] y peligro abstracto "*...cuando se ven afectadas condiciones de seguridad que son imprescindibles para un disfrute despreocupado de los bienes. El peligro es abstracto, ya que no se trata de la desprotección actual del bien, sino del menoscabo de patrones de seguridad tipificados cuya eficiencia es medida esencial del aprovechamiento racional de los bienes*".[8]

En torno a tales conceptos, demostraremos que la política criminal estatal no puede, ni debe, tipificar penalmente conductas que sólo se identifican con intereses políticos, militares o económicos (los que normalmente serán, por ende, sectoriales y minoritarios), irreconducibles auténticamente a intereses individuales que la sociedad democrática deba proteger, sea por su impacto microsocial, sea por su relevancia macrosocial, ya que éstos no se ven afectados siquiera a nivel de peligro abstracto, deviniendo por consiguiente las penas que eventualmente se establezcan para tales conductas, en auténticos abusos del Ius Puniendi estatal por parte del Legislador, obviando el principio de mínima intervención y el carácter fragmentario del Derecho Penal que, según nos recuerda Romeo Casabona, le imponen abstenerse de

> "*...intervenir si es suficiente la protección requerida en relación con la informática que puedan otorgar otros sectores del ordenamiento jurídico (civil, administrativo, mercantil, etc.), aunque en ellos sea necesaria la actuación del legislador, partiendo de la evidente necesidad de la ordenación jurídica de la actividad informática; y si, con todo, no resultara bastante, la intervención del Derecho Penal deberá limitarse a castigar como delito únicamente las conductas más intolerables para la convivencia social que supongan una agresión a los bienes, valores o intereses tutelados por el Derecho*".[9]

3. Análisis de la Ley N° 19.223, que tipifica figuras penales relativas a la Informática

Una simple lectura del artículo 2° de la Ley N° 19.223, publicada en el Diario Oficial con fecha 7 de junio de 1993, permite aseverar que la hipótesis de acceso no autorizado a información contenida en sistemas computacionales se encuentra prevista en ella, pero con un texto insuficiente o, a lo menos, con serios problemas de interpretación para quienes consideran *per se*

2 Muñoz Conde, Francisco. *Derecho Penal y Control Social*, Fundación Universitaria de Jerez, Jerez, 1985, p. 14.

3 Jakobs, Günter. *Derecho Penal. Parte General. Fundamentos y Teoría de la Imputación*, 2a. ed., ampliada y corregida, Marcial Pons, Madrid, 1997, p. 9.

4 En el mismo sentido, Politoff, Sergio; Matus, Jean Pierre, y Ramírez, María Cecilia. *Lecciones de Derecho Penal Chileno. Parte General*, Ed. Jurídica de Chile, Santiago, 2004, p. 58.

5 Hormazábal Malaree, Hernán. *Bien Jurídico y Estado Social y Democrático de Derecho. El Objeto Protegido por la Norma Penal*, 2a. edic., Ed. Jurídica Conosur, Santiago, 1992, p. 152. El destacado está en el original.

6 Kindhäuser, Urs Konrad. *Acerca de la Legitimidad de los Delitos de Peligro Abstracto en el Ámbito del Derecho Penal Económico*, artículo inserto en *Hacia un Derecho Penal Económico Europeo. Jornadas en Honor al Profesor Klaus Tiedemann*, Estudios Jurídicos, Boletín Oficial del Estado, Madrid, 1995, p. 445.

7 Kindhäuser, Urs Konrad. Ob. cit., p. 448.

8 Ídem, p. 449.

9 Romeo Casabona, Carlos. *Poder Informático y Seguridad Jurídica*, Fundesco, Madrid, 1987, p. 23.

delictiva tal conducta, pues debe satisfacerse la exigencia de un elemento subjetivo adicional (ánimo de apropiación, uso o conocimiento), que envuelve conceptos polémicos no zanjados por la doctrina en relación con el dolo,[10] lo que sería contradictorio *"...en el contexto del derecho chileno, por razones de simetría,* (pues) *parece decisivo el hecho que la violación de correspondencia y el registro de papeles no exigen que el agente se imponga del contenido de una y otros"*.[11]

El artículo en comento, señala textualmente: *"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 sus grados mínimo a medio"*.

Partidario de la criminalización del *hacking* se declara Magliona quien, además, justifica la inclusión de esta conducta en el Código Penal por su contenido de puesta en peligro de bienes jurídicos, sin distinción entre *hacking* directo o indirecto.[12] Al efecto, señala:

> *"Esta acción de acceder a un sistema, mediante la violación de las medidas de seguridad, por más mínimas que sean, evidentemente significa una puesta en peligro del bien jurídico protegido, ya sea esta la calidad, pureza e idoneidad de la información, la propiedad o la privacidad. Nadie tiene que estar tratando de superar las medidas de seguridad de un sistema de tratamiento de la información o sitio web. Para que el tipo se perfeccione, no se debe exigir ningún ánimo del agente, bastando el acceso al sistema al cual el sujeto activo no tiene derecho a acceder"*.[13]

El comentario citado, se efectúa a modo de crítica por la conducta que se considera inexistente en el tipo penal de acceso no autorizado a datos contenidos en sistemas de información y que, siguiendo a otras legislaciones, considera que debiera tipificarse. Indica, además, que así estaba contemplado en el proyecto de ley original de la moción presentada por Viera-Gallo, pero que el debate legislativo fue desnaturalizando el delito hasta hacerlo desaparecer, lo que sería contradictorio con el artículo 146 del Código Penal, en cuanto *"...sanciona, como primera acción "el abrir", no exigiendo ningún elemento subjetivo, sin perjuicio de sancionar con una mayor penalidad a quien divulgare o se aprovechare de los secretos que la correspondencia o los papeles de otro contienen"*.[14]

Lo expuesto, no ha sido puesto en duda por la doctrina penal nacional, siendo incluso ratificado por una de sus voces más autorizadas en la actualidad[15]; de allí que, para paliar esta

[10] De distinta opinión pareciera ser Etcheberry, pues sostiene, en un primer instante, que *"...la conducta consistirá en "interceptar", "interferir" o simplemente "acceder" a él, requiriéndose en todos los casos obrar con ánimo de apoderarse, usar o conocer"*, pero luego relativiza dicho propósito, quizás sin tener en mente los modos de comisión que permite la Internet, al señalar que *"...en el artículo 2° bastará el simple conocimiento, en su caso"* (Etcheberry, Alfredo. *Derecho Penal. Parte Especial*, 3a. edic., Ed. Jurídica de Chile, Santiago, 1998, Tomo III, p. 271).

[11] Hernández Basualto, Héctor. *Tratamiento de la Criminalidad Informática en el Derecho Penal Chileno. Diagnóstico y Propuestas*, Informe en Derecho para el Ministerio de Justicia, sin publicar, Santiago, 2002.

[12] Vid. *Infra*, nota 17.

[13] Magliona Markovicth, Claudio. *Análisis de la Normativa sobre Delincuencia Informática en Chile*, artículo inserto en *Derecho y Tecnologías de la Información*, Ediciones Universidad Diego Portales, Santiago, 2002, p. 389.

[14] Magliona Markovicth, Claudio. Ob. cit., p. 389.

[15] Hernández Basualto, Héctor. Ob. Cit., p. 4.

pretendida falencia, se haya presentado una moción parlamentaria destinada a tipificar el mero acceso a un sistema de información y que se analizará en el párrafo siguiente.

4. Análisis de Proyectos de Ley [16]

Como se ha anticipado, el pretendido problema aludido en el número anterior, ha servido de fundamento para los proyectos de ley que se han presentado a la Cámara de Diputados para tipificar, entre otros, la conducta de *hacking*.

La moción parlamentaria que contiene el proyecto de ley original (Boletín N° 2.974-19), modificaba exclusivamente la Ley N° 19.223, sin hacerse cargo de la crítica consistente en legislar fenomenológicamente y en una ley especial; en efecto, el *hacking* se contemplaba en la sustitución del artículo 1° de dicha ley, con la siguiente descripción típica: *«el que sin autorización acceda a un sistema electrónico de almacenamiento o procesamiento de datos, o a través del cual se provee un servicio electrónico de comunicaciones, sufrirá...»*. Posteriormente y producto de las exposiciones realizadas por especialistas en el tema ante la Comisión de Ciencias y Tecnología de la Cámara de Diputados, así como por lo expuesto en el Proyecto de Ley del Ejecutivo para la modificación del Código Penal respecto del tratamiento de la criminalidad informática, de 11 de julio de 2002, y el Proyecto de Ley también del Gobierno por el cual se modifica el Código Penal con el objeto de recepcionar, en los tipos penales tradicionales, nuevas formas delictivas surgidas a partir del desarrollo de la informática (Boletín N° 3.083-07), la conducta a sancionar devino, de acuerdo al Informe de la referida Comisión, en una modificación al artículo 146 del Código Penal, del siguiente tenor en lo que respecta al inciso primero:

> *«El que por cualquier medio abriere o registrare la correspondencia o los papeles de otro sin su voluntad o accediere a la información de otro contenida en redes, soportes lógicos o sistemas de tratamiento automatizado de información sin su voluntad sufrirá la pena de presidio menor en sus grados medio a máximo si divulgare o se aprovechare de los secretos que ellos contienen, y en el caso contrario la de reclusión menor en sus grados mínimo a medio».*

En los incisos siguientes, se establecen dos causales de justificación, una que se encuentra recogida en el vigente artículo 146 del Código Penal, referida a ciertos parientes, y la otra que se orienta a *«...aquellas personas a quienes por ley, reglamento o contrato les es lícito instruirse de comunicaciones o informaciones ajenas»*, ampliando por consiguiente la que existe actualmente en el inciso tercero de la norma referida, en cuanto se limita a las autorizaciones legales y reglamentarias para instruirse de correspondencia ajena.

De acuerdo a esta modificación, aprobada en el primer trámite legislativo ante la Cámara de Diputados, la conducta de *hacking* pasa a ser punible desde el instante mismo en que se accede a la información de otro contenida en redes, soportes lógicos o sistemas de trata-

[16] Análisis de Proyecto de Ley que modifica la Ley N° 19.223, que tipifica figuras penales relativas a la informática (Boletín N° 2.974-19), en relación con el Proyecto de Ley que modifica el Código Penal con el objeto de recepcionar, en los tipos penales tradicionales, nuevas formas delictivas surgidas a partir del desarrollo de la informática (Boletín N° 3.083-07).

miento automatizado de información, **sin su voluntad**. Luego, la clave interpretativa está en el verbo rector «acceder» y en la inexistencia de una causal de atipicidad que se representaría por la «voluntad» del titular a que se acceda a la información. Hacemos presente, en todo caso, que la existencia de tal voluntad conforme a las categorías jurídico-penales de la llamada Parte General del Derecho Penal es, mayoritariamente concebida como causal de justificación y, por ende, de inexistencia de antijuricidad (el denominado «consentimiento de la víctima»).[17]

En virtud que el objeto de nuestro trabajo está orientado a la justificación de la (in)existencia del delito de *hacking*, siendo secundaria la tipificación concreta que se adopte en uno u otro Ordenamiento Jurídico, sólo diremos, por ahora, que la conducta de «acceder» se verifica desde el instante mismo en que se llega a o se alcanza la información, mientras que la ausencia de voluntad del titular se refiere a cualquier exteriorización de consentimiento o aquiescencia en que se llegue o se alcance la información de otro contenida en redes, soportes lógicos o sistemas de tratamiento automatizado de información, **sin distinción sobre su relevancia, nivel de seguridad para su acceso, perjuicio causado a la víctima o beneficio del autor**. En suma, mero acceso, sin referencia a peligro alguno para información digna de ser considerada secreta respecto de terceros, no obstante encontrarse albergada en un sitio web de libre acceso al público, respecto del cual, actualmente, sólo se protege el nombre de dominio, siendo responsabilidad de la misma potencial víctima el tipo de información que coloca en la red, exponiéndola al "peligro" de ser objeto de *hacking*. Prescindimos, por ende, de las barreras de seguridad predispuestas por el titular del sitio de dominio electrónico, ya que éstas en sí mismas no son objeto de protección, sino que han sido utilizadas, justamente, para impedir la vulneración del bien jurídico que se vislumbra objeto de la protección penal, esto es, la privacidad de los datos que, por decisión del mismo titular, se sustraen del conocimiento público indiscriminado, situación que importaría dotar a tal titular de la potestad de determinar qué es susceptible de protección penal o no, dotando, por consiguiente, de contenido al tipo penal, en circunstancias que esa función es privativa del Legislador.

5. Argumentos a favor y en contra de la criminalización del *hacking*

Para un sector de la doctrina nacional, pareciera ser que toda intromisión en soportes lógicos no autorizada es ilegítima, en cuanto supone violación de las barreras de seguridad para acceder al sistema, predispuestas por su titular para proteger la información contenida en él. Conforme a ello, no sería posible identificar circunstancias justificantes o eximentes de responsabilidad penal, como el caso de aquellos sujetos que desarrollan seguridad de redes,

[17] La distinción, evidentemente, no es menor. Así lo expresan Eser y Burkhardt al responderse la pregunta "*...¿Cómo debería estructurarse el consentimiento?. Ello dependerá de si el consentimiento tiene el efecto de excluir la tipicidad o sólo tiene un efecto de justificación. La relevancia práctica de esta cuestión se relaciona especialmente con el error sobre el consentimiento en relación con la "teoría estricta de la culpabilidad"*, explicando a continuación y sobre la base de un caso de consentimiento presunto (¿tienen presente tal hipótesis los legisladores en el proyecto de ley en discusión?) que "*el consentimiento tiene para algunos autores un efecto excluyente de la tipicidad*" (refiriéndose a Kientzy, Roxin, Schmidhäuser y Maurach-Zipf), pero que "*frente a esta posición la doctrina dominante establece una diferencia entre la "conformidad" que excluye la tipicidad y el "consentimiento" con efecto justificante*" (citando al efecto a Lenckner, Geerds, Geppert y Jakobs). Vid. Eser, Albin y Burkhardt, Björn. *Derecho Penal. Cuestiones Fundamentales de la Teoría del Delito Sobre la Base de Casos de Sentencias*, trad. de Silvia Bacigalupo y Manuel Cancio Meliá, Ed. Colex, Madrid, 1995, p. 273.

aun sin consentimiento del titular de la información (piénsese en el caso del experto informático que, para estar al día en sus conocimientos, "practica" acceso a soportes lógicos para detectar vulnerabilidades y fortalezas de sistemas de seguridad ejecutados por otros).

En abono de la posición referida, podemos compartir que el intrusismo informático, por definición, es penetración por la fuerza a un sistema informático, incluyendo por consiguiente el denominado "*hacker blanco*", esto es, "*el sujeto que practica hacking directo* (con la finalidad) *de franquear la puerta de entrada, acceder al sistema y salir del mismo, demostrando, de este modo, el defecto de seguridad del que adolece*"[18].

Como contrapunto y a partir del mismo ejemplo expuesto, es lógico pensar que en ambientes determinados, con controles y reglas básicas, el intrusismo informático constituya una actividad lícita, exenta de toda clase de sanción penal. Esta situación, de mantenerse en los proyectos de ley referidos en el número anterior, sólo cabría respecto de quien está autorizado por ley o reglamento a acceder a informaciones contenidas en redes, soportes lógicos o sistemas de tratamiento automatizado de información como, asimismo, respecto del sujeto que ha sido autorizado por contrato para tal efecto. Sin embargo, se encuentra excluida, como enunciáramos, una causal de justificación fundada en el consentimiento presunto de la potencial víctima, ya que es insuficiente la mera ausencia de la exigencia típica "sin voluntad", puesto que ella se refiere a la tipicidad, la que desaparece sólo en caso de manifestación expresa o, a lo menos, exteriorizada de tal voluntad por la víctima, la que tendrá en sí misma, por consiguiente y la mayoría de las veces, el poder de la prueba para incriminar o no una conducta.

En el otro extremo, se encuentran aquellos que sostienen la absoluta inidoneidad de la conducta de *hacking* para ser criminalizada, atendiendo principalmente a la distinción con la conducta de *cracking* y los efectos benignos que la primera tiene, justamente, para evitar los efectos nocivos de la segunda.

Pues bien, veremos a continuación que, tanto para criminalizar como para mantener el estado actual de las cosas, existen argumentos razonables, aunque sólo aquellos que se oponen a la criminalización pueden considerarse compatibles con los principios que informan el Derecho Penal liberal en un Estado Social y Democrático de Derecho.

5.1. Argumentos a favor

Los partidarios de la criminalización del *hacking* sostienen que, desde el punto de vista técnico, el ingreso ilegítimo implica la utilización de los recursos del sistema y un concreto riesgo de dañar accidentalmente la información con la simple intrusión, aunque tenga propósitos aventureros, por lo que debe descartarse de plano la hipótesis que el mero acceso sin finalidad alguna no genera ninguna consecuencia sobre el sistema informático.

[18] Por su parte, *Hacking* indirecto es la práctica de *hacking* como "*...un medio necesario para cometer un delito*" (Gómez Martín, Víctor. Ob. cit., p. 3).

Sostienen igualmente este grupo de autores, que se mantiene la percepción sobre la existencia de una alta "cifra negra", en virtud de que muchos incidentes no son denunciados debido a la falta de detección o al miedo de mayores pérdidas debido a la afección de la imagen y la credibilidad de las empresas o entidades[19], todo lo cual se mantendrá en la medida en que el *hacking* no sea penalizado, propósito que, a *contrario sensu*, devela confianzas desmesuradas en el rendimiento que se puede esperar de los escasos instrumentos jurídico-penales con que cuenta nuestro Ordenamiento Penal.

Afirman también, desde un punto de vista criminológico, que la creencia de años atrás sobre las motivaciones de los autores, principalmente jóvenes, identificadas con la búsqueda de conocimientos y el deseo de «mostrar» las habilidades personales, ha variado actualmente, pues tales aparentes inocuos móviles han cedido su espacio a los que tradicionalmente se identifican en la comisión de los delitos comunes, como la obtención de dinero o poder, ejecutándose estos delitos, la mayoría de las veces, por empleados o personas relacionadas con la empresa u organización víctima del atentado.

A partir del argumento anterior, se impone la idea consistente en que el *hacking* es el presupuesto del *craking* y, por ello, se justifica materialmente su punibilidad a título de delito de peligro[20]. En este sentido, es posible observar el artículo 197 del Código Penal español, que sanciona con hasta cuatro años de cárcel el mero apoderamiento de mensajes de e-mail ajenos o la interceptación de los que circulan por la Internet (*sniffing*). La misma pena se aplica al que roba o altera datos de una base de datos informática, o al que simplemente accede a esta base de datos. Como se ve, no es necesario que haya ánimo de lucro, de manera que se puede producir el delito si se accede por simple curiosidad.

Si bien, de acuerdo con nuestro criterio, la técnica legislativa no resulta adecuada por la falta de definición de las conductas involucradas en forma sistemática, podemos decir que la ley española reprime prácticamente todas las modalidades conocidas de *hacking*, *craking*, espionaje y sabotaje informático, estableciendo figuras agravadas en razón de la importancia de los sistemas de información[21].

19 Según señala Morón, "*...la actitud poco favorable a la denuncia se debe al temor de que la trascendencia del hecho se traduzca en una suerte de descrédito de la fiabilidad de la gestión de la propia empresa (que, en este ámbito, se ciñe a una pérdida de confianza en los sistemas de seguridad de las redes de información) y de su prestigio. Así pues, a fin de evitar mayores pérdidas, prefieren resolver el problema internamente*". Morón Lerma, Esther. *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red*, 2a. edic., Ed. Aranzadi S.A., Navarra, 1992, p. 47.

20 "*En este sentido y en la misma línea doctrinal, se sugiere el adelantamiento de la barrera de protección penal, incriminando conductas que sin provocar un resultado lesivo de algún bien jurídico, no obstante se presumen peligrosas, como primera fase de un ilícito más grave, frente al que, en realidad, se adopta la tutela*" (Morón Lerma, Esther. Ob. cit., p. 75).

21 De opinión contraria es Morón, quien exige la concurrencia de un elemento subjetivo del injusto, excluyendo por tanto el mero intrusismo de la sanción penal, avalando su postura en una cita jurisprudencial del Juzgado de Instrucción N° 2 de Lorca (Ponente: Alcázar Fajardo), de 29 de enero de 2002, que señala: "*...las conductas de mero hacking o acceso a los sistemas informáticos perpetrados con la única finalidad de acceder al password o puerta lógica no son actualmente constitutivos de delito pues carecen del elemento subjetivo del injusto*" (Morón Lerma, Esther. Ob. cit., p. 53). Los elementos subjetivos del injusto que adiciona al intrusismo informático son, curiosamente, los mismos que están en el artículo 197 del Código Penal español referidos a otras hipótesis (apoderamiento y alteración o utilización de datos), conclusión a la que llega para "*coherencia del precepto*", produciendo un "*solapamiento de modalidades comisivas*" (Ídem, p. 63).

Por otra parte, se sostiene que, según el tipo de información de la que se trate (que en todos los casos resulta de acceso restringido), se deben establecer sanciones diferentes pero igualmente significativas, dado que por su naturaleza le es indiferente al titular que ésta haya sido solamente conocida, aunque no utilizada. A partir de ello, se distinguen dos grupos: a) la información sensible de naturaleza eminentemente personal y privada, como extensión de las condiciones, atributos y derechos de la persona humana; y b) toda otra clase de información que no se encuentra incluida en el grupo anterior (v. gr.: cultural, financiera, industrial, empresarial, militar, científica, tecnológica, jurídica, etc.). En ambos casos, sin embargo, se encuentra en juego la confidencialidad de la información, bien jurídico que debe protegerse ampliamente, sin exigencias típicas que diluyan su protección.

Ahora bien, podemos decir que con la puesta en peligro de la información descrita en la letra a) del párrafo anterior, se verá afectada la intimidad de la persona, mientras que, en el segundo grupo, la puesta en peligro se identificaría con una afección de la exclusividad de la información.

Finalmente, refutando uno de los argumentos a favor de la inexistencia del delito de *hacking*, en orden a las supuestas virtudes de quienes cometen estos ilícitos, se sostiene que la figura de los *hackers* ha sido sobredimensionada, retratándolos como guardianes o salvadores de la humanidad, como barreras a los abusos de poder de las grandes corporaciones y organismos gubernamentales, lo que pese a ser motivación de unos pocos, es desmitificado por estudios que dan cuenta de propósitos criminales en la mayoría de las intromisiones.

Como corolario, se comparte que "*...estamos asistiendo al nacimiento de un nuevo valor social, un interés de nuevo cuño, cifrado en la seguridad de los sistemas informáticos, o en la seguridad informática, o en la seguridad en el funcionamiento de dichos sistemas informáticos* (...) *pero que, en ningún caso puede ser identificado, apriorísticamente, con un bien jurídico merecedor de protección penal*".[22] Conforme a ello, desarrollamos a continuación los argumentos en contra de la criminalización del *hacking*.

5.2. Argumentos en contra

Frecuentemente se ha tratado de equiparar el espacio informático o virtual al hogar o morada (protegido constitucional y penalmente), para efectos de extender las implicancias doctrinales de la tutela jurídica de este último al anterior. Sin embargo, entendemos que la definición de hogar es normativamente diferente a la información privada contenida en un espacio informático. En efecto, señala la Constitución Política de la República en su artículo 19, que se asegura a todas las personas: "*5.° La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley*", refiriéndose por tanto al "*...recinto en que una persona o grupo de personas viven o desarrollan habitualmente determinadas actividades, con exclusión de la presencia de otros*"[23]. Luego, se trata de un "*edificio o lugar cerrado, esto es, que exista una clara demarcación de sus límites, y que éstos no sean meramente simbólicos, sino que representen un obstáculo más o menos efectivo para el acceso de terceros al interior*"[24].

22 Morón Lerma, Esther. Ob. cit., p. 84.

23 Etcheberry, Alfredo. Ob. cit., Tomo III, p. 255.

24 Ídem, p. 255.

A *contrario sensu*, es imposible concebir el desenvolvimiento de las acciones privadas o la vida de familia dentro del espacio virtual de un sistema informático como puede desarrollarse en el hogar o morada. Sin embargo, estos sistemas pueden albergar, entre otras clases de información, aquella que es elaborada o procurada por una persona, como extensión de sus atributos, en ejercicio de su autonomía y libertad de conciencia, pensamiento y expresión, que encuentran especial protección constitucional en el derecho fundamental de "*respeto y protección de la vida privada*", contenido en el artículo 19 número 4 de la Constitución. Sin embargo, estimamos que tal respeto y protección, conforme a una interpretación progresista y liberal de la Carta Magna nacional, no puede dar lugar a tipificar delitos sin infringir el carácter de *extrema ratio* del Derecho Penal. En efecto, el mandato criminalizador de la Constitución, conforme al inciso segundo de dicha garantía, se restringe **exclusivamente** a las infracciones que hayan sido cometidas a través de un medio de comunicación social, y que consistiere en la imputación de un hecho o acto falso, o que cause injustificadamente daño o descrédito a una persona o a su familia[25]. Toda criminalización en exceso de dicho mandato es, de acuerdo a lo dispuesto en el artículo 19 número 26 de la Constitución, inconstitucional[26], en cuanto afectaría la esencia de otros derechos fundamentales que deben armonizarse: la libertad personal, el derecho a emitir opinión, a informar, a la libre expresión que "*...comprende la **libertad de buscar, recibir y difundir informaciones e ideas de toda índole**, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, **o por cualquier otro procedimiento de su elección***" (Artículo 19 número 2 del Pacto Internacional de Derechos Civiles y Políticos adoptado por la Asamblea General de las Naciones Unidas,[27] garantizados por el Estado en virtud de lo dispuesto en el artículo 5° inciso segundo de la Constitución).

Asimismo, consideramos errónea la equiparación por analogía *in malam partem* del *hacking* al delito de violación de correspondencia, toda vez que la protección constitucional (de la cual deriva la protección penal contenida en el artículo 146 del Código Penal, independientemente que dicha figura sea anterior a la Constitución actual, pues tal disposición está subordinada, según indica el Título III del Libro II del Código Penal, a la tipificación "*de los*

[25] Señala expresamente el artículo 19: "*La Constitución asegura a todas las personas: (...) 4.° El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia. La infracción de este precepto, cometida a través de un medio de comunicación social, y que consistiere en la imputación de un hecho o acto falso, o que cause injustificadamente daño o descrédito a una persona o a su familia, será constitutiva de delito y tendrá la sanción que determine la ley...*".

[26] Compartimos, en este punto, el criterio esbozado por Cury para efectos de su aplicación directa por los Tribunales de Justicia: "*En un Estado Democrático de Derecho, la Constitución determina la actividad concreta de todos los Poderes del Estado y, ciertamente, también la del Judicial. De esta manera, las garantías constitucionales se integran directamente a la normativa penal, configurando su sistema y decidiendo específicamente sobre la aplicación del mismo a los particulares. La importancia política y jurídica de este desarrollo, que desformaliza los conductos a través de los cuales las normas constitucionales imponen sus directivas a la jurisprudencia, es de una trascendencia capital para la instauración de la democracia en el futuro. En efecto, por su intermedio las declaraciones abstractas de derechos contenidas en una Carta Fundamental se transforman en un instrumento puesto al servicio inmediato de los ciudadanos para la defensa de sus derechos personales, y en un recurso de control de constitucionalidad de los actos ejecutados por el legislador y por los órganos de la administración estatal*" (Cury Urzúa, Enrique. *Derecho Penal. Parte General*, reimpresión de la 2a. edic., Ed. Jurídica de Chile, Santiago, 1994, Tomo I, p. 66).

[27] Por su parte, el artículo 13 número 1 de la Convención Americana Sobre Derechos Humanos denominada "Pacto de San José de Costa Rica", señala que "*toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección*".

crímenes y simples delitos que afectan los derechos garantidos por la Constitución") se refiere a la inviolabilidad de la privacidad de comunicaciones y documentos privados que, en el contexto tecnológico existente en el año 1980, se limitaba exclusivamente a comunicaciones entre dos o más personas por medios materiales, o a documentos privados de carácter material. A este argumento debe adicionarse la constatación de la Internet como una "infraestructura de comunicación"[28] de libre acceso, dentro de la cual se introduce y conserva información por diversos titulares que, sin control físico directo, sustraen algunos contenidos informativos para el conocimiento exclusivo de quienes poseen *passwords* (lo que supone voluntad previa para acceder a la información reservada), recayendo por tanto la ilicitud sólo en quienes verifican la conducta *sine qua non* de la navegación en la red, esto es, acceder, sin contar con tales *passwords*, hecho que repugna con el sentido y alcance de la garantía constitucional y de la redacción vigente del artículo 146 del Código Penal, en cuanto la acción de "abrir" supone un sello o resguardo físico controlable por las personas concretas que participan de una comunicación privada y la acción de "registrar" supone examinar un documento igualmente físico cuyo titular reserva para sí. En suma, la diferencia cualitativa está en la exposición de la información que se quiere reservar para ciertos titulares en la infraestructura de comunicación, contrasentido que, a lo menos, denota "exposición imprudente al riesgo" y, por consiguiente, relativiza la dañosidad del acceso por quien ejerce, correlativamente, el derecho fundamental a informarse, en este caso, bajo la modalidad del anonimato que le asegura la Internet (con excepción de las limitaciones legales, las que proliferaron a partir del 11 de septiembre de 2001).

Las insuficiencias de los textos constitucional y legal, motivó los proyectos de ley en análisis, sin reparar que el artículo 146 del Código Penal no puede extenderse más allá del contenido de la garantía constitucional a la inviolabilidad del hogar y de toda forma de comunicación privada, ya que el Legislador nacional no puede considerarse mandatado para criminalizar por el simple hecho de existir el artículo 60 número 3 de la Constitución, que señala dentro de las materias de ley "*las que son objeto de codificación, sea civil, comercial, procesal, penal u otra*", pues el "objeto" se refiere a la codificación y no a la naturaleza penal de la ley, la que debe colegirse de una garantía o derecho constitucional con entidad de ser protegida penalmente y no del mero arbitrio del Legislador de turno que desconoce el limitado rol que le compete al Derecho Penal en el Control Social, recurriendo a él sin consideración a los principios de lesividad y proporcionalidad, así como los caracteres de subsidiariedad y fragmentariedad. Tal pretendido mandato, se reduce al máximo en virtud del acotado imperativo constitucional de criminalización contenido en el artículo 19 número 5 de la Carta Fundamental, referido exclusivamente a las acciones de abrir, registrar o interceptar, según se deduce de la sanción que el Constituyente pretende que se imponga a tales conductas si no se justifican en los casos y formas determinados por la ley.

Consideramos oportuno, igualmente, traer a colación un discutible pero sugerente principio derivado del de legalidad que comenta Zaffaroni, el de "*respeto histórico al ámbito legal de lo prohibido*":

> "*...se debe tomar en cuenta el contexto cultural del texto legal, y cuando se comprueba un fenómeno de inusitada extensión punitiva, se impone una reducción histórica. La legalidad*

[28] Llaneza González, Paloma. *Internet y Comunicaciones Digitales*, Ed. Bosch S.A., Barcelona, 2000, p. 35.

es un principio que sirve para garantizar la limitación del ámbito de programación criminalizante legislativa, y no se puede revertir su sentido convirtiéndolo en un argumento de extensión inusitada y nunca prevista en el contexto originario del texto, cuyo efecto es conceder un espacio selectivo de criminalización que alcanza los límites máximos de arbitrariedad. Un tipo penal no puede erigirse en instrumento para la criminalización indiscriminada. El respeto histórico al ámbito real de lo prohibido se impone en la legalidad porque, de lo contrario, la simple omisión de las agencias políticas extendería de modo inaudito las prohibiciones punitivas: lo punitivo es un ámbito que deben planificar y aumentar las agencias políticas mediante la ley, y la omisión de éstas frente a cambios significativos de contexto cultural o tecnológico constituye una renuncia a su función que no es constitucionalmente admisible. La criminalización primaria se establece por acción de las agencias políticas y no por sus omisiones".[29]

Conforme a dicho principio, no puede ni debe criminalizarse conductas que carecen de la entidad suficiente para ser normativamente consideradas delictuales, situación que se aprecia especialmente en la represión del mero acceso sin ninguna motivación especial.

Presenta, por consiguiente, serios reparos desde el principio de legalidad, en orden a la constitucionalidad de la figura aludida, dado que, como indica Frisch, "*...casi toda acción puede comportar la presencia o producción de condiciones capaces de lesionar un bien. Que ello no **debe bastar para desaprobar una conducta se explica por sí solo**. Una concepción así conduciría a una limitación de la libertad que a nadie le interesa (en especial, tampoco a las potenciales víctimas si se imaginan como afectadas por esas limitaciones de la libertad)*".[30] Consideramos, por tanto, que los derechos a la libertad personal, a emitir opinión, a informar y a la libre expresión con todos sus contenidos, se ven seriamente limitadas o afectadas en su esencia para su ejercicio en el ámbito de la Internet, excediendo por consiguiente la reserva legal contenida en el artículo 19 número 26 de la Constitución Política de la República.

En otro orden de ideas, se considera por los autores que estiman necesaria la criminalización del *hacking*, sin mayor detención, que nos encontraríamos frente a un delito de peligro abstracto, en cuanto la conducta de *hacking* es el primer paso para conductas de *cracker*. Tal atribución de riesgo a la conducta es inadmisible en un Estado Social y Democrático de Derecho, por cuanto importa una auténtica presunción de derecho de responsabilidad criminal sobre una conducta ulterior que, sólo en caso de consumarse, importaría lesión a un bien jurídico. Lo anterior resulta evidente si se analiza la hipótesis más grave que contempla el tipo penal proyectado, esto es, el auténtico *cracker*, en el caso que éste fuere detectado cuando se hubiere dado comienzo a la ejecución por hechos directos, pero falten uno o más actos para su complemento (delito tentado). En tal caso, se da el absurdo jurídico de sancionarse con mayor penalidad al sujeto que realiza una conducta auténtica de *hacking*, pero sin dañar el sistema de información, mientras que el sujeto que tenía por plan delictivo tal propósito, al ser descubierto en una fase anterior de ejecución del delito, resulta "premiado" en la pena abstracta que le corresponde, por un acto

[29] Zaffaroni, Ernesto Raúl. *Derecho Penal. Parte General*, 2a. edic., Ediar, Buenos Aires, 2002, p. 119.

[30] Frisch, Wolfgang. *La Imputación Objetiva. Estado de la Cuestión*, ponencia inserta en *Sobre el Estado de la Teoría del Delito. Seminario en la Universitat Pompeu Fabra*, trad. de Ricardo Robles Planas, Cuadernos Civitas, Madrid, 2000, p. 45. El destacado es nuestro.

ajeno a su voluntad (se rebajaría, de acuerdo al artículo 52 del Código Penal, en dos grados la pena asignada a la conducta de *cracking* tentado, el cual pudo llegar a producir el mismo riesgo que la conducta de *hacking* de cara al bien jurídico protegido).

Por otra parte, es inadmisible penalmente que se sancione a un sujeto por el actuar ilícito de otro, situación que se produce en la relación entre *hacking* y *cracker*, dado que el primero, con el propósito de evitar los daños que produce el segundo, es sancionado en su conducta inocua para el bien jurídico, incluso más, potencialmente garantizadora del mismo. Tal criterio desatiende la prevención de Frisch y, parodiado mediante un ejemplo del ámbito de relación tráfico vial, equivale a prohibir conducir vehículos de noche, para evitar el aumento de choques nocturnos con conductores que desarrollan carreras clandestinas con automovilistas normales.

Luego, estimamos que la solución político-criminal razonable y que reduce el absurdo, es fomentar la comunicación a los titulares de la vulnerabilidad de la información contenida en las redes, soportes lógicos o sistemas de tratamiento automatizado de información, a efectos de evitar que un auténtico *cracker* pueda causar enormes daños a su titular y a terceros que, en virtud de la confianza en su invulnerabilidad, contratan con él. La manera para que este objetivo pueda realizarse es absteniéndose de criminalizar el mero acceso al sistema informático, además de otorgar un "puente de oro" al desistimiento oportuno (previo a la causación de daños) del *cracker* arrepentido, siempre que ponga en conocimiento del titular la vulnerabilidad del soporte lógico.

En consecuencia, el estímulo al desistimiento criminal debe orientarse a prescindir de distinguir (una vez comunicada la vulnerabilidad de la información contenida en redes, soportes lógicos o sistemas de tratamiento automatizado de información), si quien pone en conocimiento del titular tal falencia es un *hacker* o un *cracker*, dirigiéndose sólo la investigación consecuente (motivada por el desistimiento del autor, la mayoría de las veces, dada la difícil prueba de participación de esta clase de ilícitos) a constatar si tal acción produjo o no daños al sistema informático. De la mano de dos ejemplos, uno a propósito de la intimidad y otro a propósito de la morada y la privacidad de los papeles y correspondencia, se demuestra claramente la conveniencia político-criminal de esta solución: a) Si una persona observa, desde su casa, a través de una ventana de la propiedad de su vecina, que ella se encuentra completamente desnuda y, aprovechando la ocasión, la fotografía, verificaría el tipo penal previsto en el artículo 161 A del Código Penal (hoy cuestionado a tal punto, que se demanda socialmente su derogación), pero no debería sancionársele si le avisa a su vecina que por tal o cual ventana se le ve desnuda, permitiendo incluso que se le fotografíe, con tal que no haga uso en forma alguna de tal fotografía y no comunique a terceros los detalles íntimos del cuerpo de su vecina. Con ello, la persona cuya intimidad ha sido violada, podrá evitar que en el futuro tal situación se repita, obteniendo una ventaja respecto de la situación sin estímulo a la comunicación, en que el sujeto, para no ser castigado, no le avisa sobre la vulnerabilidad de su ventana e, igualmente, conserva en su retina y películas fotográficas, la imagen íntima de su vecina. b) Si un sujeto camina por la vía pública y, en ella, encuentra un "hogar" de un mendigo, formado por unas cuantas cajas en las que se interna, deteniéndose ante una de ellas al ver la leyenda "privada", gatillando inmediatamente su curiosidad, decidiéndose por ver hacia su interior para observar, dentro de ella, un certificado de nacimiento y un certificado de antecedentes del pordiosero, no dudamos en que el menesteroso se sentirá vulnerado en su morada y afectado en la intimidad de sus papeles privados, pero no se verifica ninguno de los delitos referidos, el primero porque se requiere que el lugar destinado a la morada esté cerrado, ya

que de otro modo no se podría verificar la conducta de "entrar" en ellas[31], y el segundo, porque no existe un resguardo de los papeles registrados, que impida que su contenido se exhiba a cualquiera que fije sus sentidos sin examen especial.[32]

6. Confrontación de los argumentos a favor y en contra de la criminalización del *hacking* más relevantes con los derechos fundamentales involucrados a la luz del fenómeno informático y el Derecho Penal

En el presente acápite, intentaremos confrontar las conclusiones provisionales que se desprenden de los argumentos a favor y en contra de la criminalización del *hacking* más relevantes, con los derechos fundamentales a la intimidad y a la libertad de información, junto con el posible nuevo derecho a la libertad informática, propósito que pretende cimentar conclusiones definitivas que armonicen íntegramente las consecuencias jurídicas que se extraen de los derechos fundamentales, el fenómeno informático y el Derecho Penal.

6.1. Derecho a la intimidad

Según expone la doctrina nacional, el derecho a la intimidad[33] o derecho a la privacidad[34], se encuentra consagrado en el artículo 19 número 4 de la Constitución, bajo la denominación de "vida privada", junto con dos conceptos adicionales (la vida pública y la honra de la persona y de su familia).[35]

Para García San Miguel, la intimidad es "*...el derecho a no ser conocidos, en ciertos aspectos, por los demás. Es un derecho al secreto, a que los demás no sepan lo que somos o lo que hacemos*",[36] concepto que compartimos en el entendido que, como todo derecho fundamental, no es absoluto, por lo que debe armonizarse con los demás derechos del mismo rango, dentro de los cuales se encuentra el derecho a la información.

De cara a la referida armonización, estimamos que el límite para distinguir lo íntimo, viene dado por lo que García San Miguel denomina el criterio espacial, el cual revitalizamos atendida la exposición hasta aquí desarrollada, en contradicción con la pretendida obsolescencia del mismo, sugerida, entre otros, por el indicado autor:

31 Etcheberry, Alfredo. Ob. cit., Tomo III, p. 259.

32 Ídem, p. 268.

33 Verdugo, Mario, Pfeffer, Emilio y Nogueira, Humberto. *Manual de Derecho Constitucional*, 2a. edic., Ed. Jurídica de Chile, Santiago, 1999, Tomo I, p. 250.

34 Evans de la Cuadra, Enrique. *Los Derechos Constitucionales*, 2a. edic., Ed. Jurídica de Chile, Santiago, 1999, Tomo I, p. 211.

35 En el mismo sentido, Castro Frías, Maritza. *Privacidad, Vida Pública y Honra Frente a la Libertad de Expresión. Soluciones a un Conflicto*, artículo inserto en *Revista de Derecho Público*, Volumen 64, Universidad de Chile, Santiago, 2002, p. 256.

36 García San Miguel, Luis. *Reflexiones Sobre la Intimidad como Límite a la Libertad de Expresión*, artículo inserto en *Estudios Sobre el Derecho a la Intimidad*, Ed. Tecnos S.A., Madrid, 1992, p. 18.

> *"Según este criterio, las conductas, los objetos y situaciones íntimos, serían aquellos que se realizan o sitúan en el interior de la vivienda y de otros espacios cuyo uso se atribuye en exclusiva (aunque sea por tiempo limitado) al individuo, como pudieran ser el reservado de un restaurante o una cabina telefónica. A ellos se equipararían objetos como el teléfono y la carta, igualmente delimitados físicamente".*[37]

Este criterio es coincidente con la garantía prevista en el artículo 19 número 5 de la Constitución, en cuanto protege la "*inviolabilidad del hogar y de toda forma de comunicación privada*", objetos que se remiten necesariamente a un espacio físico, de lo que podemos desprender una protección constitucional reducida a la esencia del derecho y que reconoce la posibilidad de limitaciones establecidas por ley.

Conforme al criterio aludido, consideramos que la intimidad no es compatible con la Internet, tanto desde el punto de vista del titular de datos personales que directamente los expone en la red, como respecto de la empresa que trata datos personales de terceros. Explicamos el criterio expuesto a la luz de una analogía entre la Internet, frecuentemente llamada "supercarretera de la información" con, precisamente, una carretera: Los conductores (usuarios de la red) que ingresan a la carretera (Internet), hacen uso de un bien público o, en su caso, recurso común,[38] dentro del cual otros sujetos también hacen uso. Si un conductor, por cualquier razón, decide detenerse y, al costado de la carretera, cierra su vehículo, abandonándolo momentáneamente, pero dejando en su interior una carpeta con antecedentes comerciales personales, puede pretender que ninguna persona se interiorice del interior de su vehículo, pero no puede evitar que cualquier sujeto, por el móvil que sea, observe, toque y, aun, abra su vehículo, si lo puede hacer sin dañarlo y sin apropiarse de algún objeto (verificados estos supuestos, no se verifica ningún delito contra la propiedad ni contra la intimidad). Por otra parte, el conductor de un vehículo de servicio courier, puede realizar la misma conducta del conductor antes referido, dejando junto a la carretera información comercial de terceros. Si un intruso, con habilidades especiales para vulnerar los mecanismos de resguardo sin siquiera dañarlos, accede a la información a distribuir por la empresa de courier, ¿es subsumible su conducta en algún tipo penal? Creemos que, evidentemente, no hay delito alguno susceptible de imputar a la conducta descrita; no obstante ello, tanto al sujeto que deja su vehículo como al representante de la empresa de courier, les interesa llegar a conocer las debilidades de los mecanismos de protección cuando éstos se exponen a funciones triviales como la simple detención en la carretera (en el caso de la Internet, el examen de la información depositada en el sitio web), a efectos de evitar, en el futuro, la verificación de lesiones efectivas de los bienes jurídicos que transitan o se encuentran depositados en la carretera (o la red).

Por consiguiente, en resguardo del derecho a la intimidad, pero considerando los principios y caracteres esenciales del Derecho Penal,

37 García San Miguel, Luis. Ob. cit., p. 24.

38 En el presente ejemplo, nos referimos a los conceptos económicos de bienes públicos y recursos comunes, siguiendo al respecto la conceptualización de Mankiw, quien se refiere en los siguientes términos a las "*carreteras congestionadas*": "*Las carreteras pueden ser bienes públicos o recursos comunes. Si no están congestionadas, su uso por parte de una persona no afecta a nadie más. En este caso, el uso no es rival y las carreteras son un bien público. Sin embargo, si están congestionadas, su uso genera una externalidad negativa*" (Mankiw, Gregory. *Principios de Economía*, 2a. edic. en español, Ed. Mc Graw Hill, Madrid, 2002, p. 146).

"*la pregunta que surge inmediatamente es si conviene endurecer hasta ese punto* (penas privativas de libertad) *las sanciones. La respuesta dependerá, en último término, de razones de oportunidad, es decir, de la aceptación o rechazo social de las medidas sancionadoras y de su mayor o menor eficacia. No es descartable, por ejemplo, que los tribunales sean remisos a la hora de imponer sanciones penales (y enviar a un periodista a la cárcel) o que la opinión pública reaccionara negativamente cuando esto ocurriera, lo que puede conducir, a la larga, no a la mayor protección de la intimidad, sino a su mayor desprotección)*".[39]

El dilema, en consecuencia, es dilucidar, político-criminalmente, el alcance que le otorgaremos a esta exposición, más o menos imprudente, al daño, considerando especialmente que la tipificación del proyecto de ley y, en general, las recomendaciones de los juristas más connotados en la materia,[40] se refieren exclusivamente a comportamientos dolosos y no imprudentes, siendo en esta última categoría donde los efectos civiles de la exposición imprudente al daño cobra relevancia, a lo menos civilmente,[41] para efectos de rebajar las indemnizaciones a título de perjuicios que se impongan. A partir de lo expuesto, algunos autores consideran que la protección penal de la intimidad no obsta a la civil o administrativa, "*...por la importancia que hoy cabe atribuir a ese bien jurídico para el libre y pacífico desenvolvimiento de la personalidad, por la creciente indefensión de tal bien jurídico frente a los medios técnicos de intromisión en el mismo, y por la necesidad que por ello hay de recurrir al valor simbólico de esa importancia que supone la sanción penal*".[42]

6.2. Derecho a la información

El derecho a la información, amén de la protección en tratados internacionales sobre derechos humanos ratificados por Chile y que se encuentran vigentes,[43] está consagrado en el artículo 19 número 12 de la Carta Fundamental, en cuyo primer inciso se lee que la Constitución asegura a todas las personas: "*La libertad de emitir opinión y la de informar, sin censura previa, en cualquier forma y por cualquier medio, sin perjuicio de responder de los delitos y abusos que se cometan en el ejercicio de estas libertades, en conformidad a la ley, la que deberá ser de quórum calificado*".

Destacamos la expresión "sin censura previa", ya que, enfrentado a la posible comisión de un delito, nuestra Constitución contiene una contradicción aparente que debe resolverse en beneficio del derecho en ejercicio actual (la libertad de información) y, por consiguiente, en perjuicio del derecho en riesgo potencial (la intimidad): un delito, por definición, debe ser, por los mecanismos de Control Social, evitado, situación incompatible con la proscripción de la censura previa, dado que, en caso de evitarse un potencial delito que afectaría la intimidad, necesariamente se está violando una garantía constitucional en su esencia. Retomaremos, a continuación de los recaudos siguientes, esta colisión, precisamente, enfrentados a la conducta del *hacking*.

39 García San Miguel, Luis. Ob. cit., p. 33.

40 Vid., por todos, Sieber, quien señala: "*En principio, las infracciones de la privacy relacionadas con el ordenador, deberían sólo ser punibles si el autor actúa dolosamente. La incriminación de los comportamientos negligentes requiere una justificación especial (Principio de dolo)*" (Sieber, Ulrich. *Documentación para una Aproximación al Delito Informático, artículo inserto en Delincuencia Informática*, Editorial PPU, Barcelona, 1992, p. 94).

41 Lo expuesto, al tenor del artículo 2.330 del Código Civil.

42 Luzón Peña, Diego. *Protección Penal de la Intimidad y Derecho a la Información*, artículo inserto en *Estudios Sobre el Derecho a la Intimidad*, ob. cit., p. 89.

43 Vid. *supra*, p. 18.

Al tenor de la conceptualización adoptada en este artículo, la conducta de *hacking* tiene lugar en la Internet, infraestructura o canal de comunicaciones con una amplia gama de recursos que permite obtener información sin más límites que los regulados o autorregulados. En ambas situaciones de excepción, en todo caso, se explican y tienen valor jurídico las restricciones al libre acceso a cierta clase de información, en el siempre difuso interés de seguridad nacional y en la confianza necesaria para que los usuarios utilicen la red.

Debe tenerse igualmente presente que el derecho a la información, en cuanto libertad para obtenerla, aunque no se encuentra en la letra del precepto constitucional, "*...forma parte integrante de ella, porque de nada sirven las libertades de opinión y de comunicación garantizadas si ellas no tienen destinatarios reales con derecho a exigir su recepción y conocimiento*"[44].

Premunidos de las ideas sucintamente expuestas, nos situamos nuevamente en la escurridiza frontera de la licitud de la obtención de información por un "*cibernauta*", recordando que, según afirmamos, por mandato constitucional, no puede consagrarse, ni aun por ley, censura previa, la que se extiende tanto a la emisión de información como a su recepción. Pues bien, con estricto apego al artículo 19 número 12 de la Constitución, la proscripción de la censura previa implica asunción de los riesgos que contiene la libertad de información, hecho que conlleva la restricción al legislador de criminalizar tal peligro, puesto que, de lo contrario, se afecta la libertad de información. Dicho de otro modo y para destruir la posibilidad de tipificar la peligrosidad inherente a la libertad de información irrestricta: el Constituyente proscribe la creación de tipos penales de peligro abstracto y, aun más, de peligro concreto, ya que establece un sistema de responsabilidad ulterior, sobre la base de los daños causados por los delitos cometidos o los abusos de la libertad de información.

Hemos extraído, por consiguiente, un nuevo fundamento para prohibir al Legislador que tipifique penalmente conductas que se ejercen en el ejercicio del derecho a la información, so pena de inconstitucionalidad: la censura previa impide creación de delitos de peligro, por cuanto las justificaciones de criminalización que contienen, importan necesariamente la anticipación del reproche a la acción causante de una puesta en peligro de los derechos fundamentales que se deben armonizar con el derecho a la información y no un reproche al resultado de lesión del bien jurídico protegido.

6.3. ¿Derecho a la libertad informática?

A partir del análisis de los derechos fundamentales expuestos, surge la pregunta ya aclarada en algunas legislaciones como la española, sobre si es necesario el reconocimiento constitucional de un nuevo derecho, el de la libertad informática, el cual

"*...se concibe como el nuevo derecho de autotutela de la propia identidad informática. Su función se cifra en garantizar a los ciudadanos unas facultades de información, acceso y control de los datos que les conciernen. Dicha libertad informática ha sido concebida por la doctrina y jurisprudencia germanas como un derecho a la autodeterminación informativa,*

44 Evans de la Cuadra, Enrique. Ob. cit., Tomo II, p. 18.

que se refiere a la libertad para determinar quién, qué y con qué ocasión pueden conocer informaciones que conciernen a cada sujeto".[45]

Creemos que, a partir de los problemas de interpretación, armonización e integración de los derechos fundamentales, la consagración expresa de este derecho fundamental de nuevo cuño podría aliviar la miopía del constitucionalismo positivista, atendiendo el reclamo normativo automático frente a un nuevo fenómeno. Sin embargo, acoger tal demanda no sana de tal miopía, entronizada en la ausencia de consideración de la libertad como un solo derecho fundamental que se manifiesta en diversos ámbitos. Por ello afirmamos que la libertad informática es una constatación en los nuevos tiempos de la misma libertad, que no requiere esperar una norma expresa para su reconocimiento universal, situación que, frente a nuevos fenómenos tecnológicos, puede repetirse en nuevas manifestaciones de la libertad o de otra base de la institucionalidad.

Lo expuesto, sin embargo, no obsta a que, por aplicación de los principios del Derecho Penal, el Legislador deba analizar si un nuevo fenómeno contiene un bien jurídico digno de protección penal y, en caso afirmativo, discernir si es susceptible de subsumir en los tipos penales existentes o si, por el contrario, requiere la creación de uno nuevo, el que, en el ámbito de la libertad de información, requiere ser aprobado por una ley de quórum calificado y resguardar que tal derecho no sea limitado en su esencia, de acuerdo al artículo 19 número 26 de la Constitución, incluso cuando tal tipificación sea invocada en resguardo de otro derecho fundamental, como la intimidad.

Por otra parte, la libertad informática, en los términos propuestos, debe contener necesariamente una segunda faz: la libertad informática para acceder a la información contenida en la infraestructura de comunicación. Esto conlleva el derecho a circular libremente por la red, en forma anónima o no según desee el navegante, permitiéndosele incluso que ponga a prueba la vulnerabilidad de los accesos restringidos, ya que pensamos, a *contrario sensu* de lo expuesto por Magliona,[46] que "*nadie puede ni debe evitar que se trate de superar las medidas de seguridad de un sistema de tratamiento de la información o sitio web*", por abyecto que sea el móvil, pues tal comportamiento no es censurable penalmente, no obstante que, en caso de lesión del bien jurídico intimidad, se sancione por tal conducta al sujeto que, por ende, devino en *cracker*.

7. Conclusiones

La relectura de los argumentos expuestos en este trabajo, nos permiten afirmar con mayor convicción que el *hacking* blanco o mero acceso a información contenida en redes, soportes lógicos o sistemas de tratamiento automatizado de información, no se encuentra penalmente tipificado en la legislación nacional vigente.

Concluimos, además, que la conducta habitualmente conocida como *hacking* blanco, desde un punto de vista político-criminal, no puede ni debe ser tipificada penalmente, dado

[45] Peréz Luño, Antonio. *Derechos Humanos, Estado de Derecho y Constitución*, 5a. edic., Ed. Tecnos S.A., Madrid, 1995, p. 378.

[46] Vid. *supra*, p. 7.

que se desarrolla en el ámbito de un bien de libre acceso al público (Internet), en que no existen derechos a la intimidad absolutos sobre la información que se contiene en los sitios de dominio electrónico, puesto que éstos se exponen al riesgo en forma conciente, con pleno conocimiento de la potencial vulnerabilidad de las restricciones al acceso.

Asimismo, consideramos que no existe un mandato constitucional que legitime la afección en la esencia de los derechos constitucionales de libertad personal, a emitir opinión, a informar y a la libre expresión con todos sus contenidos, de manera que la eventual tipificación del mero acceso a la información contenida en la red, soportes lógicos o sistemas de tratamiento automatizado de información, devendría en inconstitucional, por vulneración del artículo 19 número 26 de la Constitución, especialmente si la criminalización abroga la restricción de censurar previamente impuesta por el Constituyente.

Igualmente, estimamos que no existe un peligro abstracto en la conducta de *hacking*, sino que ésta ha sido utilizada para sancionar actos posteriores que participan de una acción base que se puede realizar sin poner en riesgo bien jurídico alguno. Además, conforme con la restricción apuntada en el párrafo precedente, la peligrosidad de la conducta de *hacking*, en cuanto el mero acceso es ejercicio de la libertad de información, no puede ser justificación de tipificación a título de delito de peligro, sin que ello importe violar flagrantemente la proscripción de censura previa.

En definitiva, el tratamiento adecuado del *hacking* pasa, necesariamente, por reconocer la distinción entre *hacker* blanco y *cracker*, otorgando un "puente de oro" o exención de responsabilidad criminal especial para el que, accediendo a la información contenida en redes, soportes lógicos o sistemas de tratamiento automatizado de información, ponga en conocimiento del titular la vulnerabilidad del sistema, a efectos de evitar que el "peligro" que se ha pretendido fundamento de la sanción de dicha conducta, se consume, ya no por dicho *hacker*, sino que próximamente por un auténtico *cracker*; de esta forma, la correcta solución político-criminal para proteger el sistema de información, pasa por fomentar la inhibición o, en su caso, desistimiento de la conducta de vulneración de las barreras para acceder a información que el titular pretende privada, no obstante su exposición en un bien de libre acceso al público, poniendo en conocimiento de ese titular la debilidad del sistema de seguridad de la información y de la forma en que se vulneró, a efectos de propiciar su oportuna corrección, anticipándose al acceso por un auténtico *cracker*. De esa forma, se evita que, por temor a la sanción, se inhiba al *hacker* comunicar la constatación de vulnerabilidad del sistema y, por consiguiente, mantener tal situación de vulnerabilidad.