PRESUPUESTOS PARA LA INCRIMINACION DEL HACKING[1]

Por Hugo Daniel CARRION

SUMARIO:

I- INTRODUCCIÓN. La Sociedad de la Información como producto de la Tecno-era. La informática como nueva forma de poder

I-a) Tecno-era. La encarnación de las historias de ciencia-ficción

I-b) Cambios socio-económicos estructurales

I-c) Informática. El nuevo Poder

II- El derecho frente a las nuevas tecnologías

II-a) Los problemas jurídicos derivados de las nuevas tecnologías

II-b) Autonomía del derecho informático

III- Informática y derecho penal. Aproximación a los delitos informáticos. Bien jurídico tutelado

III-a) Delincuencia informática y Derecho Penal

III-b) Magnitud social de los delitos informáticos. Garantías constitucionales del Derecho Penal

III-c) Bien jurídico tutelado en los delitos informáticos

IV- Delitos informáticos

V- El Intrusismo Informático no autorizado o acceso ilegítimo a los sistemas de información (hacking)

V-a) Hackers. Orígenes. Definición. Diferencias con los Crackers

V-b) Hacking desde la óptica de los “hackers blancos”

V-c) Intrusismo informático en el marco de seguridad de redes (hacking ético)

V-d) Mitos en torno a los hackers

V-e) Algunas experiencias en el derecho comparado. Clasificaciones del Hacking

V-f) Bien jurídico vulnerado por el hacking

V-g) La improcedente analogía de esta conducta con la violación de domicilio

VI- La incriminación del hacking. Marco constitucional

VI-a) El hacking como delito de peligro

VI-b) Propuesta de definición del tipo penal de intrusismo ilegítimo o acceso no autorizado a sistemas informáticos

VII- CONCLUSIONES

- Reflexión final

I- INTRODUCCIÓN. La Sociedad de la Información como producto de la Tecno-era. La informática como nueva forma de poder

I-a) Tecno-era. La encarnación de las historias de ciencia-ficción

Cuando nos asomamos al fenómeno de la denominada "Era Digital" es inevitable llegar a la conclusión que todas aquellas historias de ciencia-ficción creadas por las mentes brillantes de Bradbury, Asimov y Verne, entre muchos otros, no sólo han sido confirmadas, sino que resultan, a poco que se efectúe el contraste respectivo, anacrónicas e ingenuas. Las posibilidades que ofrecen la biotecnología, la nanotecnología y la ingeniera genética son ilimitadas y plantean numerosos dilemas éticos, porque, por un lado, arrastran al hombre a un futuro donde se dispondrá de tiempo para hacer solamente las cosas placenteras, descartando las faenas laborales que tanto tiempo nos insumen y, en no pocas ocasiones, nos molestan, pero, por otro, se rompen límites morales: clonación de seres humanos, patentamiento de la codificación de las cadenas de ADN de determinadas partes del cuerpo humano con fines comerciales (a partir de la decodificación del genoma humano), desarrollo de sistemas de agentes inteligentes (IA -inteligencia artificial-) que potencialmente tienen capacidad de reemplazar a los expertos humanos en las más diversas áreas profesionales y, en el caso del derecho, podrían -por definición- analizar un caso determinado y emitir una decisión como lo haría un Juez[2].

Sin embargo se trata de una incipiente Tecno-era, porque el punto culminante de esta Tercera Revolución Industrial tendrá lugar (y en muy poco tiempo) con la definitiva expansión de la Inteligencia Artificial, la bio-tecnología, la genética y la robótica influyendo en todas las áreas humanas.

I-b) Cambios socio-económicos estructurales

Siguiendo a Manuel Castells[3], debemos señalar que las consecuencias de este paradigma tecnológico también afectan y modifican la estructura social y económica, donde se observan las llamadas Economía informacional (la capacidad de generación y manipulación de infraestructuras informacionales son decisivas para el desarrollo y expansión de las empresas), la Economía Red (descentralización de las grandes empresas y formación de redes o alianzas con pequeñas y medianas empresas que funcionan como auxiliares de aquéllas) y la Economía global o Globalización a secas (donde, en realidad, todos las áreas se encuentran subordinadas a este fenómeno: trabajo, comunicaciones, mercados financieros, cultura, etc.).

Los frutos de estos cambios son naturalmente ambiguos: se crea un proceso donde la información está al alcance de todos (en Internet no sólo fluye la información, sino la sociedad misma), verificándose terribles impactos en lo que atañe a la difusión de la producción cultural y un rediseño de la arquitectura de los negocios y la industria[4]. Sin embargo, el modelo económico neoliberal o post-capitalista globalizado, ha generado situaciones de exclusión e injusticia social a nivel mundial, cuya tendencia pareciera no ceder, destacándose el nuevo escollo, frente a la realidad de los países emergentes, que presentan las nuevas tecnologías de la información, las que, a diferencias de otros inventos (radio, televisión), requieren, como presupuesto mínimo indispensable, la alfabetización de los usuarios.

I-c) Informática. El nuevo Poder

La informática nos rodea y es una realidad incuestionable y parece que también irreversible[5]. Está en casi todos los aspectos de la vida del hombre. Desde los más triviales hasta los más sofisticados. Sin la informática las sociedades actuales colapsarían[6], generándose lo que se conoce como “computer dependency”.

La informática se presenta como una nueva forma de poder[7], que puede estar concentrado o difuminado en una sociedad, confiado a la iniciativa privada o reservado al monopolio estatal. Es instrumento de expansión ilimitada e inimaginable del hombre y es, a la vez, una nueva forma de energía, si se quiere intelectual[8], de valor inconmensurable, que potencia y multiplica de manera insospechada las posibilidades de desarrollo científico y social, erigiéndose en patrimonio universal de la humanidad. FROSINI efectúa, a los efectos de entender el grado de poder de la informática, una comparación entre la civilización con escritura y la civilización sin ella.

II- El derecho frente a las nuevas tecnologías

II-a) Los problemas jurídicos derivados de las nuevas tecnologías

Huelga señalar que este panorama afecta al Derecho, como instrumento regulador de las relaciones humanas en procura del orden social, pudiendo formularnos, entonces, algunos interrogantes: Podemos ajustar las instituciones jurídicas vigentes a estos fenómenos o, por el contrario, es necesario impulsar la creación de nuevas normas? Cuáles son los nuevos intereses colectivos que deben ser objeto de tutela jurídica? Es necesario el desarrollo de una nueva rama autónoma del derecho[9], atendiendo muy especialmente, al valor que posee la información en la sociedad actual?

Más allá de las discusiones teóricas que inevitablemente conllevan las preguntas supra referidas y que, en su mayoría, exceden el marco del presente trabajo, es necesario buscar fórmulas o mecanismos efectivos para solucionar los problemas que acarrean el uso y la proliferación de las nuevas tecnologías, sin

perjuicio de estudiar, paralelamente, el nuevo paradigma del conocimiento y la sociedad toda que impone la realidad actual.

Y los problemas surgen del nuevo espectro de fenómenos de cierta complejidad tecnológica que no parecen encontrar adecuada solución ni en el ordenamiento jurídico vigente ni en las viejas elaboraciones doctrinales: el teletrabajo (esta curiosa modalidad de traspolar la oficina al hogar para el desempeño laboral) puede identificarse con la jornada laboral? Cómo establecer si existe un abuso por parte del empleador? El software, incluído actualmente en la Ley 11.723 de propiedad intelectual, puede identificarse ontológicamente con la obra artística? El mail, en su esencia, reúne las notas típicas del objeto de los delitos previstos en los arts. 153 y ss. del Código Penal? Cuál es el régimen de responsabilidad que corresponde aplicar a los proveedores de Internet (ISP) según el tipo de servicio que prestan? Es correcto que se le imponga el deber de controlar lo que publica o difunde el usuario? Podemos hablar de un dolo general en la conducta del programador que diseña un virus o bomba lógica para enviarlo a un conocido o con fines experimentales, pero finalmente se disemina infectando la computadora de otras personas? De aceptarse la tentativa, es acabada o inacabada? La información, como entidad lógica, es cosa mueble en los términos del artículo 162 del Código Penal? Es susceptible de ser apropiada en los términos del delito de hurto, cuando la víctima sigue conservando la disposición sobre la información y no media afectación a su patrimonio? Cuál es el acto voluntario expresado en la celebración de un contrato cuándo el mismo constituye simplemente un doble click?

Continuar exponiendo estos problemas resulta abrumador y por cierto, interminable.

II-b) Autonomía del derecho informático

Debe apuntarse, en lo que atañe al desarrollo y evolución del derecho informático, que en aquellos países donde el fenómeno de la informática se encuentra masificado, es decir, donde la mayoría de la población tiene acceso real a los sistemas de información, se habla del comienzo de una verdadera autonomía en esta área. No es posible desconocer, por otra parte, que, tal vez no con tanta trayectoria y evolución como la legislación que comprenden otras ramas del derecho, pero sí existe en el ámbito del derecho informático, en el orden mundial, legislación basada en leyes, tratados y convenios internacionales, además de los distintos proyectos y leyes especiales que promueven los entes legislativos con la finalidad de proveer al contralor y encuadre legal de los instrumentos o medios informáticos. Sin embargo, aceptando la necesidad del desarrollo del derecho informático como rama autónoma, la Argentina se encuentra en la actualidad bastante lejos de lograr tal autonomía, habida cuenta que, en concordancia con la doctrina mayoritaria, es necesario que concurran cuatro aspectos: autonomía legislativa, autonomía jurisprudencial, autonomía académica y autonomía científica.

III- Informática y derecho penal. Aproximación a los delitos informáticos. Bien jurídico tutelado

III-a) Delincuencia informática y Derecho Penal

Si bien hemos aludido a las tremendas posibilidades de la informática como instrumento de desarrollo económico-social y cultural y advertido acerca de algunas de sus consecuencias negativas, no nos detuvimos aún en el objeto del presente trabajo: la utilización pervertida de las nuevas tecnologías de la información o, si se quiere, en aquellas nuevas conductas disociales que ameritan la intervención del Derecho penal. Naturalmente que, frente a un fenómeno de tal magnitud como el que se describe, es imposible que la criminalidad quedara exenta del impacto de la tecnología informática. GARCIA PABLOS señala que la informática abre nuevos horizontes al delincuente, incita su imaginación, favorece su impunidad y potencia los efectos del delito convencional[10]. Y a ello contribuye la facilidad para la comisión y encubrimiento de estas conductas disvaliosas y la dificultad para su descubrimiento, prueba y persecución.

III-b) Magnitud social de los delitos informáticos. Garantías constitucionales del Derecho Penal

El abuso de los sistemas de información puede generar consecuencias nefastas. La perversa utilización de la información sensible de los ciudadanos colisiona con las garantías constitucionales propias de un Estado de Derecho, porque información implica poder y éste aumenta la capacidad de control sobre los individuos, los que, cada vez más, se encuentran restringidos en su libertad y autonomía. La denominada "Red Echelon" es un ejemplo palmario de vulneración de derechos republicanos[11], como la intimidad y la libre determinación de las Naciones.

La información, en consecuencia, ha adquirido un valor altísimo desde el punto de vista económico (por los intereses en juego), constituyéndose en un bien sustrato del tráfico jurídico, adquiriendo eminente relevancia jurídico-penal por ser posible objeto de conductas disvaliosas (hacking, craking, fraude informático, espionaje y sabotaje informático, etc.), que integran la delincuencia denominada de "cuello blanco" (pero no estrictamente económica) y por ser instrumento de facilitación, aseguramiento y calificación de los ilícitos tradicionales[12] (casi todos los delitos, salvo aquellos que requieren una intervención físicamente directa y personal del autor como el abuso sexual con acceso carnal, son susceptibles de ser cometidos mediante el uso de sistemas de tratamiento, almacenamiento y flujo de la información, lo cual no implica que se traten de delitos informáticos).

Consecuentemente, adelantando la respectiva toma de postura, consideramos que el bien jurídico tutelado en los delitos informáticos, es la información en sí misma, en toda su amplitud (titularidad, autoría, integridad, disponibilidad, seguridad, transmisión, confidencialidad), sin perjuicio de que con su ataque, subsidiariamente y tratándose de un interés colectivo, afecte otros bienes jurídicos como la intimidad o la propiedad.

Sin embargo y a los efectos de no violentar los principios constitucionales de legalidad y reserva (artículos 18 y 19 de la Constitución Nacional Argentina) tipificando como delitos conductas que no implican una real afectación o un concreto peligro sobre un interés social –cuyo contenido será materia de análisis a continuación-, deberá tenerse presente que el derecho penal es la última ratio del orden normativo, el último instrumento de control social, a disposición del Estado para la prevención de la criminalidad, por lo que su utilización debe limitarse a la intervención necesaria, mínima, para preservar la convivencia humana en la comunidad. El sistema de reacciones penales, por su poder represivo, debe estar necesariamente precedido por medidas de política económica y sociales que, en lo posible, operen

preventivamente sobre las causas de la criminalidad. En su caso, debe intentarse la protección del bien jurídico con remedios jurídicos no penales. Consecuentemente, se desprende que no todos los bienes jurídicos deben ser protegidos penalmente y que sólo se incriminan las lesiones más graves al bien jurídico (el derecho penal es fragmentario).

III-c) Bien jurídico tutelado en los delitos informáticos

Sentado lo expuesto, debemos dejar en claro cuál es el bien jurídico protegido en los delitos informáticos.

Asumimos con MUÑOZ CONDE[13] que la norma penal tiene una función protectora de bienes jurídicos y que para cumplir dicha función, eleva a la categoría de delito, por medio de la tipificación legal, aquellos comportamientos que más gravemente los lesionan o ponen en peligro. En cuanto al bien jurídico en sí, compartimos los alcances de las concepciones trascendentes, en cuanto a que la realidad social es la que le otorga su contenido. Los bienes jurídicos son intereses vitales del individuo o la comunidad, el orden no puede crearlo, lo crea la vida, pero la protección del Derecho eleva el interés vital a bien jurídico[14].

No obstante es imposible soslayar algunas de las conclusiones que emanan de los estudios de algunas escuelas criminológicas, como la del “labelling approach”, o la definición o etiquetamiento de determinados comportamientos desviados, que diera paso a las modernas doctrinas criminológicas críticas, cuyas búsquedas se centran en dos direcciones: el estudio de la formación de la identidad desviada y de lo que se define como “desviación secundaria”, es decir el efecto de la aplicación de la etiqueta de “criminal” y, por otro lado, el problema de la constitución de la desviación como cualidad atribuída a comportamientos y a individuos en el curso de la interacción, lo que conduce al problema de la distribución del poder de definición (quienes detentan en mayor medida dicho poder: las agencias de control social)[15].

En definitiva, si bien es cierto que el legislador recepta los intereses vitales colectivos como bien jurídico al otorgarles especial protección jurídico penal y que, en ese contexto, verdaderamente son compartidos por la mayoría de los integrantes de la comunidad, no lo es menos que, determinadas conductas meramente desviadas, respondiendo a diversos intereses, pueden etiquetarse también como delitos, sin que, esencialmente, ostenten dicho carácter. Ello no significa, en modo alguno, que no deban ser protegidos los intereses involucrados, sino que la respuesta debe ser hallada mediante algún otro mecanismo de control social y no en el que representa el poder punitivo del Estado[16].

En definitiva y tal como lo adelantáramos, atendiendo a las características de esta nueva era y sus implicancias ya descriptas, entendemos que el bien jurídico en los delitos informáticos es la información en sí misma, en todos sus aspectos, como interés macro-social o colectivo, porque su ataque supone una agresión a todo el complejo entramado de relaciones socio-económico-culturales, esto es, a las actividades que se producen en el curso de la interacción humana en todos sus ámbitos y que dependen de los sistemas informáticos (transporte, comercio, sistema financiero, gestión gubernamental, arte, ciencia, relaciones laborales, tecnología, etc.).

IV- Delitos informáticos

Disentimos, acorde con la postura sustentada en torno al bien jurídico tutelado en los delitos informáticos, con las tradicionales distinciones doctrinales de estas conductas ilícitas en delitos informáticos de carácter económico y aquellos que atentan contra la privacidad[17]. En primer lugar, porque toda la información –aún la privada- posee un valor apreciable económicamente y en segundo, porque los intereses vulnerados superan el marco meramente patrimonial, verificándose un verdadero carácter pluriofensivo de las conductas disvaliosas, por implicar afectación de cuestiones que atañen a la seguridad y a la confianza en el correcto funcionamiento de los sistemas informáticos que repercuten en la vida social colectiva. Por otra parte, tal reduccionismo haría innecesaria la creación de la categoría de los delitos informáticos, puesto que no serían más que delitos contra la propiedad, o bien, contra la intimidad o privacidad.

Con el mismo criterio equívoco, Klaus TIEDEMANN[18] señala que, con la expresión criminalidad mediante computadoras (adviértase que en el ámbito tecnológico actual las computadoras u ordenadores tal como los conocemos se encuentran casi obsoletos), se alude a todos los actos, antijurídicos según la ley penal vigente (lo cual no significa más que decir que los delitos informáticos no son otros que los que la ley define como tal), realizados con el empleo de un equipo automático de procesamiento de datos. Esta definición lleva al absurdo de calificar como delito informático o "criminalidad mediante computadoras" (término por demás deficiente para abarcar el fenómeno en estudio) a la acción de matar a una persona aplicándole un golpe con un equipo de computación.

Los delitos informáticos se realizan necesariamente con la ayuda de sistemas informáticos o tecnologías similares, pero tienen como objeto del injusto la información en sí misma, la cual, como expresamos, posee múltiples características que trascienden lo meramente económico.

So riesgo de resultar anacrónicos en muy poco tiempo, debido a los avances tecnológicos y, por ende, a las nuevas formas que asuma la criminalidad informática, señalamos cuáles son las conductas lesivas a la información, según el Consejo de Europa y el XV Congreso Internacional de Derecho, entre otras :

1. Fraude en el campo de la informática.

2. Falsificación en materia informática.

3. Sabotaje informático y daños a datos computarizados o programas informáticos.

4. Acceso no autorizado.

5. Intercepción sin autorización.

6. Reproducción no autorizada de un programa informático protegido.

7. Espionaje informático.

8. Uso no autorizado de una computadora.

9. Tráfico de claves informáticas obtenidas por medio ilícito.

10. Distribución de virus o programas delictivos.

Consecuentemente, entendemos por delitos informáticos aquellas acciones típicas, antijurídicas y culpables, que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, como bien jurídico de naturaleza colectiva o macro-social (abarcativo de otros intereses, vgr.: propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos, etc.), en cualquiera de las fases que tienen vinculación con su flujo o intercambio (ingreso, almacenamiento, proceso, transmisión y/o egreso), contenida en sistemas informáticos de cualquier índole, sobre los que operan las maniobras dolosas.

V- El Intrusismo Informático no autorizado o acceso ilegítimo a los sistemas de información (hacking)

V-a) Hackers. Orígenes. Definición. Diferencias con los Crackers

La palabra hacker proviene de los reparadores de cajas telefónicas (E.E.U.U. en la década del 50), cuya principal herramienta de reparación era un golpe seco al artefecto con fallas (un "hack"), de ahí que se los llamó "hackers". Preliminarmente podemos definirlo como un informático que utiliza técnicas de penetración no programadas para acceder a un sistema informático con los más diversos fines: satisfacer su curiosidad, superar los controles, probar la vulnerabilidad del sistema para mejorar su seguridad, sustraer, modificar, dañar o eliminar información; y cuyas motivaciones también responden a los más variados intereses: ánimo de lucro, posturas ideológicas anarquistas, avidez de conocimientos, orgullo, propaganda política, etc.

Con el tiempo y frente a las actitudes dañosas de alguno de estos individuos, la misma cultura hacker gestó el término "crackers" para aludir a estos sujetos, diferenciándose de los mismos por tener fines más altruistas. Posteriormente, la doctrina receptó tal diferenciación entre intrusismo informático ilegítimo (hacking) y sabotaje informático (cracking), basándose en el elemento subjetivo que delimita la frontera de cada comportamiento; mientras en el último supuesto, la intencionalidad del agente es obstaculizar, dejar inoperante o dañar el funcionamiento de un sistema informático, en el primer caso la acción realizada busca únicamente el ingreso a tales sistemas sin dirigir sus actos a la afectación de la integridad o disponibilidad de la información, pero sí, como se verá, a la confidencialidad y exclusividad de la misma y también, en algunos casos, a vulnerar la intimidad del titular de aquélla.

V-b) Hacking desde la óptica de los "hackers blancos"

"Hacking. La palabra evoca una conjura diabólica de genios de la informática planificando el hundimiento de la civilización mientras hacen desaparecer billones en fondos robados electrónicamente a un banco de Antigua.

Pero yo prefiero definir el hacking como una manera, divertida y aventurera, de aprender acerca de los ordenadores. Los hackers no seguimos el libro al pie de la letra. Nos comemos el coco y probamos cosas raras, y cuando damos con algo divertido se lo contamos a nuestros amigos. Algunos de nosotros puede que sean unos mangantes, pero lo más normal es encontrar buena gente, o al menos gente que no provoca daños."[19]

"Existe una comunidad, una cultura compartida, de programadores expertos y brujos de redes, que cuya historia se puede rastrear décadas atrás, hasta las primeras mini-computadoras de tiempo compartido y los primigenios experimentos de ARPAnet. Los miembros de esta cultura acuñaron el término 'hacker'. Los hackers construyeron la Internet. Los hackers hicieron del sistema operativo UNIX lo que es en la actualidad. Los hackers hacen andar Usenet. Los hackers hacen que funcione la WWW. Si Ud. es parte de esta cultura, si Ud. ha contribuído a ella y otra gente lo llama a Ud. hacker, entonces Ud. es un hacker. La mentalidad de hacker no está confinada a esta cultura de hackers en software. Hay personas que aplican la actitud de hacker a otras cosas, como electrónica o música -de hecho, puede Ud. encontrarla en los más altos niveles de cualquier ciencia o arte-. Los hackers en software reconocen estos espíritus emparentados y los denominan `hackers' también -y algunos sostienen que la naturaleza de hacker es en realidad independiente del medio particular en el cual el hacker trabaja-…Existe otro grupo de personas que a los gritos se autodenominan hackers, pero no lo son. Éstas son personas (principalmente varones adolescentes) que se divierten ingresando ilegalmente en computadoras y estafando al sistema de telefonía. Los hackers de verdad tienen un nombre para esas personas: `crackers', y no quieren saber nada con ellos. Los hackers de verdad opinan que la mayoría de los crackers son perezosos, irresponsables y no muy brillantes, y fundamentan su crítica en que ser capaz de romper la seguridad no lo hace a uno un hacker, de la misma manera que ser capaz de encender un auto con un puente en la llave no lo puede transformar en ingeniero en automotores. Desafortunadamente, muchos periodistas y editores utilizan erróneamente la palabra `hacker' para describir a los crackers; esto es causa de enorme irritación para los verdaderos hackers. La diferencia básica es esta: los hackers construyen cosas, los crackers las rompen…"[20]

Para mayores precisiones sobre conceptos en torno a la cultura hacker puede acudirse al Jargon File de Eric S. Raymon, la gran Biblia para hackers.[21]

Estas definiciones de los propios hackers, que se denominan "blancos", aluden a su accionar como una forma o filosofía de vida, de experimentar y crear, con espíritu aventurero, sin límites ni restricciones, pero sin dañar. La cultura hacker sostiene que son el motor de la infraestructura informacional, puesto que pregonan la absoluta libertad de la información y desarrollan la ingeniería necesaria para el mejoramiento de los sistemas informáticos (free software, seguridad de redes).

V-c) Intrusismo informático en el marco de seguridad de redes (hacking ético)

Si bien todo intrusionismo informático no autorizado resulta ilegítimo por suponer el acto de violentar las barreras de seguridad predispuestas por su titular para proteger la información para acceder al sistema, o lo que es lo mismo, el ingreso contra la voluntad presunta de aquél, no es posible identificar, de acuerdo a circunstancias especiales como es el caso de aquellos informáticos que desarrollan seguridad de redes, que todas estas conductas, en forma indiscriminada, deben ser objeto de sanción penal. En efecto, el

intrusismo informático, por definición, es penetración por la fuerza a un sistema informático, pero el denominado “hacker ético” es aquel que posee autorización o consentimiento expreso del titular del sistema para verificar su seguridad[22].

Es lógico pensar, entonces, que en ambientes determinados (empresariales por ejemplo), con controles y reglas básicas y bajo los pertinentes acuerdos contractuales, el intrusismo informático constituya una actividad lícita, obviamente, exenta de sanción penal alguna, por ausencia de antijuridicidad.

V-d) Mitos en torno a los hackers

No obstante las buenas intenciones que anima a los hackers blancos, resulta meridianamente claro que asumen que casi siempre se encuentran en la frontera con la ilegalidad, por lo que adoptan muchas precauciones para evitar ser descubiertos (aún cuando sostienen que su conducta no es dañosa).

Debe destacarse, desde el punto de vista técnico, que el ingreso ilegítimo implica, sin perjuicio de las ulteriores consideraciones dogmáticas a formular, la utilización de los recursos del sistema y un concreto riesgo de dañar accidentalmente la información con la simple intrusión con fines 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.

Hace algunos unos años atrás, las motivaciones originales eran la búsqueda de conocimientos y el deseo de "mostrar" las habilidades personales. Ahora, existen nuevos deseos de dinero y poder. Sin embargo las estadísticas pueden estar equivocadas, en virtud de que muchos de los incidentes no son reportados debido a la falta de detección o al miedo de mayores pérdidas debido a la mancha de la imagen y la credibilidad de las empresas o entidades (las personas jurídicas en general son el blanco de las conductas bajo examen).

Puede ser que una buena parte de los hacks (la acción de hackear) sean todavía motivados por la curiosidad y el deseo de puntualizar las debilidades de los sistemas, pero como las organizaciones lo han verificado, la mayoría de las amenazas provienen desde adentro de las organizaciones mismas. De acuerdo a un estudio del META Group, los actuales números indican que las recientes brechas de seguridad dentro de las organizaciones de Tecnología de la Información, ocurren internamente el 58% del tiempo, sin perjuicio de destacar que las amenazas desde el exterior aumentan a ritmo constante.

Debe señalarse 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 cual, si bien es una de las motivaciones de algunos (hackers que colaboran para Green Pace, consultando las bases de datos de las grandes petroleras para establecer por dónde pasaran los embarques), los estudios dan cuenta, en realidad, de fines mezquinos y espúreos en la gran proporción de los ataques.

La imagen del adolescente de posición social media, inofensivo, ausente de toda conciencia de estar obrando mal, a menudo influenciado por el “síndrome de Robin Hood” y con un coeficiente intelectual acto resulta el estereotipo que se encuentra en la mente de muchos. Sin embargo y tal como lo apunta la Dra. GUTIERREZ FRANCES[23], esto no es más que un mito, tal como ha sido reconocido Jay Bloom

BACKER, Director del “National Center for Computer Crime”. Estudios efectuados por dicho instituto ponen de manifiesto que los casos más serios y con más graves consecuencias, se llevan a cabo por sujetos que trabajan en el mundo de la informática, de edad superior a aquéllos y ni la mitad de inteligentes.

V-e) Algunas experiencias en el derecho comparado. Clasificaciones del Hacking

El jurista chileno MANZUR[24] señala que el hacking puede clasificarse en directo o indirecto. El hacking propiamente dicho, explica este autor, es un delito informático 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 lo que se ha llamado JOY RIDING, o paseos de diversión. Características de esta clase de hacking:. El hacker es una persona experta en materias informáticas y generalmente sus edades fluctuarán entre los 15 y los 25 años. 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.

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

Es menester formular algunas aclaraciones, en orden a la clasificación antes expuesta. 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.

El hacking es el presupuesto del craking y es por ello, fundamento de su punibilidad como delito de peligro. Sin embargo, como expusiéramos, el mero ingreso ilegítimo posee consecuencias sobre el sistema, amén de que priva a su titular de la confidencialidad y exclusividad de la información y vulnera el ámbito de su intimidad (como extensión de los atributos de la persona), motivo por el cual no compartimos la afirmación de que no representa un importante nivel de riesgo.

En lo que atañe a las figuras de hacking y craking, discrepamos en que se verifique el supuesto de concurso ideal de delitos. Como señalamos, el hacking es el presupuesto necesario del craking (todo crak 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.

Para el legislador chileno, como consta en los antecedentes de la ley 19.223, el delito sub examine consiste en la violación de la reserva o secreto de información de un sistema de tratamiento de la misma. Este delito se encuentra en sus diversas modalidades contemplado en los artículos 2º y 4º de la ley 19.223, los que reproducimos a continuación:

Artículo 2º.- "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".

Artículo 4º.- "El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

Como señalamos, para la ley chilena, el acceso a los sistemas de información, requiere un especial elemento subjetivo que recae sobre el bien jurídico penalmente protegido (la intención de apoderarse, usar, conocer, revelar o difundir la información), lo cual nos parece atinado a los fines de evitar los cuestionamientos constitucionales que puedan formularse en torno a este tipo penal como delito de peligro abstracto.

En España, la situación legal es la siguiente (Código Penal):

Hacking maligno: Apoderarse de mensajes de e-mail ajenos o interceptar los que circulan por la Red (sniffing) está penado con hasta cuatro años de cárcel (artículo 197). La misma pena recae en el que roba o altera datos de una base de datos informática, o al que simplemente accede a esta base de datos. Si estos datos se difunden, la pena puede alcanzar los cinco años de cárcel. Se castiga más al que accede ilegítimamente y sustrae los datos que al que simplemente los sustrae mediante un acceso ilegal creado por otra persona. No es necesario que haya ánimo de lucro, es decir, se puede producir el delito si se accede por simple curiosidad.

Se establecen agravantes para el caso que el acceso lo haya hecho un funcionario encargado de guardar la base de datos, que los datos afecten a la ideología, religión, salud, raza o vida sexual de personas y cuando media ánimo de lucro. Es imprescindible la denuncia del afectado.

La pena puede alcanzar también los cuatro años si se trata de espionaje "industrial" de documentos en soporte electrónico (artículo 278).

Daños mediante hacking maligno o introducción de virus: Causar daños superiores a 50.000 pesetas mediante virus o acciones de hacking está penado con multa. Si el daño se produce en un programa o documento electrónico, la pena puede alcanzar los tres años de cárcel (artículo 264). Si un virus o una acción de hacking afecta a un establecimiento militar, la pena puede alcanzar los cuatro años de prisión (artículo 265).

Hacking catastrófico: Hackear una instalación nuclear se encuentra penado con hasta veinte años de cárcel e inhabilitación (artículo 342 y ss.).

Hackear un aeropuerto, edificio público o vía de comunicación se encuentra penado con hasta veinte años de cárcel si se pone en peligro alguna vida humana (artículo 346).

Hacking militar: El que destruya, falsee o revele información reservada relacionada con la seguridad nacional puede ser castigado con hasta cuatro años de cárcel.

Si bien la técnica legislativa no resulta, a nuestro criterio, adecuada, por la falta de definición de las conductas involucradas en forma sistemática, podemos decir que la ley española reprime casi todas las modalidades conocidas de hacking, craking, espionaje y sabotaje informático, estableciendo figuras agravadas en razón de la importancia de los sistemas de información. Por último manifestamos nuestros reparos, frente al principio de legalidad, en orden a la constitucionalidad de la figura que reprime el acceso ilegítimo sin ninguna motivación especial, lo que será motivo de análisis en los párrafos subsiguientes.

V-*f) Bien jurídico vulnerado por el hacking*

Hemos señalado, en párrafos anteriores, que entendemos por hacking la conducta desplegada por un sujeto, particularmente idóneo en informática, que utiliza técnicas de penetración no programadas para acceder ilegítimamente a un sistema informático, esto es, vulnerando su seguridad, con los más diversos fines y respondiendo a distintas motivaciones. Hemos hecho también la diferenciación de este accionar con el "hacker ético" y con el del cracker (cuya conducta va dirigida esencialmente a menoscabar la integridad y disponibilidad de la información), entendiendo que el hacking supone vulnerar la confidencialidad y exclusividad de la información y atentar, en algunos casos, contra la intimidad del titular de la misma, como aspectos o modalidades de afectación del bien jurídico tutelado en los delitos informáticos.

Para efectuar la distinción antes apuntada, es necesario establecer el tipo de información de la que se trate (que en todos los casos resulta de acceso restringido), para lo cual se proyectan dos grandes 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 incluída en el grupo anterior (vgr.: cultural, financiera, industrial, empresarial, militar, científica, tecnológica, jurídica, etc.).

En definitiva, en ambos casos se encuentra en juego la confidencialidad de la información.

Con rigor académico y pretensiones de encasillamientos dogmáticos, podemos decir que cuando nos situemos frente a un ataque a la información descripta en el punto a), se verá afectada la intimidad de la persona, mientras que, en el otro caso, existirá, predominantemente, una violación a la exclusividad de la información.

Sin embargo, la clasificación antes expuesta no puede resultar tajante, habida cuenta que determinada clase de información (por ejemplo la financiera), ostenta las características de ambos grupos, puesto que, si bien puede incluirse en el b), contiene elementos relativos a las condiciones o circunstancias personales de los individuos.

V-g) La improcedente analogía de esta conducta con la violación de domicilio

Frecuentemente se ha tratado de equiparar el espacio informático o virtual al domicilio privado

(protegido constitucional y penalmente) a los efectos de extender las implicancias doctrinales de la tutela jurídica de éste último al anterior. Sin embargo, entendemos que la definición de domicilio privado es ontológicamente diferente al espacio o morada de la información privada, o cuanto menos, mucho más amplia. Así, Joaquín V. GONZALEZ expresa en su manual de la Constitución: "Si la persona es inviolable y está protegida tan ampliamente por la Constitución, es porque ha sido considerada en toda la extensión de sus atributos, así comprende la conciencia, el cuerpo, la propiedad y la residencia u hogar de cada hombre. La palabra domicilio abraza estos dos últimos sentidos. Hogar es la vivienda y por excelencia el centro de las acciones privadas que la Constitución declara reservadas a Dios y exenta de la autoridad de los Magistrados (artículo 19), allí donde se realizan la soberanía y los actos sagrados misterios de la vida de la familia…" En el mismo sentido, destaca BIDART CAMPOS[25], que el domicilio protegido constitucionalmente es mucho más amplio que los alcances del domicilio civil: es donde el individuo desenvuelve su libertad personal en lo atinente a su vida privada.

Resulta imposible concebir, por lo menos a esta altura de los avances tecnológicos, el desenvolvimiento de las acciones privadas o los misterios de la vida de familia dentro del espacio virtual de un sistema informático como puede desarrollarse en el domicilio físico. Sin embargo, estos sistemas, como señaláramos, pueden albergar, entre otras clases de información, aquella que es elaborada o procurada por una persona, como extensión de sus atributos y en el marco del ejercicio de su autonomía y libertad de conciencia, pensamiento y expresión, que encuentran especial protección constitucional en el principio de reserva ya citado. En consecuencia, su vulneración amerita especial protección penal.

VI- La incriminación del hacking. Marco constitucional

Coincidimos con Pablo PALAZZI[26] en cuanto a que, sin perjuicio de no existir una mención expresa, efectuando una interpretación teleológica del artículo 18 de nuestra Constitución Nacional, que ampara el domicilio y los papeles privados de los abusos o intromisiones del Gobierno y los particulares, podemos concluir que los constituyentes de 1853 buscaron dotar de protección al concepto de privacidad, lo que nos habilita a extender la tutela del derecho a toda la información incluída en los sistemas tecnológicos actuales.

A esta postura de especial receptación y basamento constitucional, adunamos que la reforma de nuestra Carta Magna de 1984, ha introducido en su artículo 43 el derecho a cualquier individuo de acceder y rectificar los datos sobre su persona, contenidos en cualquier clase de banco de datos o registros públicos o en aquellos privados destinados a proveer informes, derecho que fuera expresamente reglamentado con la sanción de la Ley 25.326 de habeas data.

Esta ley, en su artículo 32, ha fijado sanciones penales en relación a la información contenida en sistemas de registros o bancos de datos personales (que sólo representa una porción del universo informacional a proteger):

1. Incorpórase como artículo 117 bis del Código Penal, el siguiente:

"1°. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.

2°. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.

3°. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.

4°. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena".

2. Incorpórase como artículo 157 bis del Código Penal el siguiente:

"Será reprimido con la pena de prisión de un mes a dos años el que:

1°. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2°. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años".

En el Derecho Público Provincial, encontramos que ya se han extendido las garantías constitucionales referidas al uso de la informática. La Constitución de Chaco establece la necesidad de "..orden escrita de juez competente que exprese el motivo para *intervenir los sistemas de almacenamiento de datos y los medios de comunicación de cualquier especie*". En el mismo sentido, la Constitución de La Rioja establece: "Son inviolables... la correspondencia epistolar y las *comunicaciones de cualquier índole*".

La normativa examinada es un elemento más que nos lleva a proponer la incriminación del acceso ilegítimo a los sistemas informáticos, por suponer un riesgo para la información como interés colectivo o macro-social, en lo que atañe a su confidencialidad, que implica a su vez, el ataque contra su exclusividad y contra la intimidad de su titular.

La tipificación de esta conducta, necesariamente implicará la creación de un delito de peligro, que, a los fines de zanjar las posibilidades de ataques constitucionales, proponemos dotarlo de elementos subjetivos en el ánimo del autor (dolo específico), que deben ser probados para formular el correspondiente reproche penal.

VI-a) El hacking como delito de peligro

Según la forma de afectar al bien jurídico los delitos pueden clasificarse en delitos de lesión o de peligro. Estos últimos son aquellos en que existe la probabilidad de una lesión concreta para el bien jurídico, constituyendo un difícil problema dónde poner el límite de esa probabilidad. El delito de peligro no puede desentenderse de que se dé o no efectivamente una situación de peligro, lo contrario convertiría a estos ilícitos en meros actos de indisciplina social, esto es, en delitos de desobediencia[27]. Así en los casos de tipos de peligro abstracto, donde el legislador presume el riesgo que corre el bien jurídico

protegido por la norma, en los que se carece de condiciones objetivas de punibilidad o de elementos subjetivos que permitan afirmar de manera más garantista el principio de legalidad, corresponde indagar en el plano objetivo el peligro corrido por el bien jurídico, siendo insuficiente su presunción, como también lo es en el plano subjetivo la sola desobediencia, "dolus in re ipsa". Si el fundamento de la punibilidad en los delitos de peligro es el peligro, no se puede castigar delitos de peligro sin peligro. Es una exigencia del Estado de Derecho Democrático, la verificación del peligro efectivamente corrido por el bien jurídico tutelado por la norma penal, porque el delito es, ante todo, un hecho dañoso y socialmente peligroso, solo secundariamente implica un disvalor ético[28].

A juicio de Jiménez de Asúa, la simple posibilidad no puede servir de índice para calificar como peligrosa una conducta humana. Al derecho penal solo interesa un sector de la realidad, el que ofrece 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.

VI-b) Propuesta de definición del tipo penal de intrusismo ilegítimo o acceso no autorizado a sistemas informáticos

Proponemos la creación de un tipo penal que reprima esta conducta disvaliosa, que no obstante encontrarnos enrolados en la postura de propiciar la sanción de una legislación especial en materia de delitos informáticos, consideramos que podría ubicarse, no obstante los reparos formales en materia de correcta técnica legislativa, en el Código Penal Argentino, como artículo 157 bis (dentro del Capítulo III –Violación de secretos- del Título V, Libro II), con la siguiente redacción:

"Será reprimido con prisión de un mes a dos años de prisión, el que ilegítimamente acceda, penetre o interfiera, por cualquier medio, en un sistema informático de cualquier índole, de carácter público o privado y de acceso restringido, con la intención de conocer, apoderarse, usar, revelar, divulgar, alterar, modificar, suprimir o comercializar la información contenida en el mismo.

La pena se elevará de un tercio a la mitad si el autor se tratare del responsable de la custodia, operación, mantenimento o seguridad del sistema de información.

Si el acceso se comete en sistemas informáticos que se vinculan a cuestiones de seguridad, orden o interés público, la pena podrá elevarse hasta ocho años de prisión."

VII- CONCLUSIONES

A) La Tecno-era (también denominada Era Digital), de carácter incipiente en la actualidad, ha provoca un cambio de paradigma social y científico, modificando e influyendo definitivamente en las relaciones socio-económicas y culturales, creando la Sociedad de la Información y erigiendo a la Informática en una nueva forma de poder, con consecuencias notables para la expansión, desarrollo y evolución del hombre y su cultura y otras nefastas para su realización en lo que atañe a su esencia.

B) Las implicancias de esta nueva Era también han repercutido en el Derecho, creando todo un nuevo espectro de fenómenos de cierta complejidad tecnológica que no parecen encontrar adecuada solución ni en el ordenamiento jurídico vigente ni en las viejas elaboraciones doctrinales.

C) La criminalidad no queda exenta del impacto de la tecnología informática. Esta ha abierto nuevos horizontes al delincuente, incitando su imaginación, favoreciendo su impunidad y potenciando los efectos del delito convencional.

D) La información, en consecuencia, ha adquirido un valor altísimo desde el punto de vista económico, constituyéndose en un bien sustrato del tráfico jurídico, adquiriendo eminente relevancia jurídico-penal por ser posible objeto de conductas disvaliosas (hacking, craking, fraude informático, espionaje y sabotaje informático, etc.) y por ser instrumento de facilitación, aseguramiento y calificación de los ilícitos tradicionales.

E) Atendiendo a las características de esta nueva Era y sus implicancias ya descriptas, entendemos que el bien jurídico en los delitos informáticos es la información en sí misma, en todos sus aspectos, como interés macro-social o colectivo, porque su ataque supone una agresión a todo el complejo entramado de relaciones socio-económico-culturales, esto es, a las actividades que se producen en el curso de la interacción humana en todos sus ámbitos y que dependen de los sistemas informáticos (transporte, comercio, sistema financiero, gestión gubernamental, arte, ciencia, relaciones laborales, tecnología, etc.).

F) Entendemos por delitos informáticos aquellas acciones típicas, antijurídicas y culpables, que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, como bien jurídico de naturaleza colectiva o macro-social (abarcativo de otros intereses, vgr.: propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos, etc.), en cualquiera de las fases que tienen vinculación con su flujo o intercambio (ingreso, almacenamiento, proceso, transmisión y/o egreso), contenida en sistemas informáticos de cualquier índole, sobre los que operan las maniobras dolosas.

G) Hacking es la conducta desplegada por un sujeto, particularmente idóneo en informática, que utiliza técnicas de penetración no programadas para acceder ilegítimamente a un sistema informático, esto es, vulnerando su seguridad, con los más diversos fines y respondiendo a distintas motivaciones. Debe

diferenciarse este accionar respecto del "hacker ético" y con el del cracker (cuya conducta va dirigida esencialmente a menoscabar la integridad y disponibilidad de la información), entendiendo que el hacking supone vulnerar la confidencialidad y exclusividad de la información y atentar, en algunos casos, contra la intimidad del titular de la misma, como aspectos o modalidades de afectación del bien jurídico tutelado en los delitos informáticos.

H) La interpretación teleológica del marco normativo vigente en el país (artículos 18 y actual 43 de la Constitución Nacional, ley 25.326 de Habeas Data –que introduce modificaciones al Código Penal- y normas de Derecho Público Provincial) es un elemento más que nos habilita a proponer la incriminación del acceso ilegítimo a los sistemas informáticos, por suponer un riesgo para la información como interés colectivo o macro-social, en lo que atañe a su confidencialidad, que implica a su vez, el ataque contra su exclusividad y contra la intimidad de su titular.

I) La tipificación de esta conducta, necesariamente implicará la creación de un delito de peligro, que, a los fines de zanjar las posibilidades de ataques constitucionales, proponemos dotarlo de elementos subjetivos en el ánimo del autor (dolo específico), que deben ser probados para formular el correspondiente reproche penal, acorde a la propuesta legislativa ya expuesta de definición como tipo penal de la conducta objeto del presente trabajo.

Reflexión final

Los hombres del Derecho no pueden quedarse ajenos a este desafío que nos impone la nueva Era Tecnológica, la sociedad entera lo va a pedir a gritos.

Tenemos que empezar a desarrollar respuestas coherentes, generar modelos de conocimiento, métodos de análisis. No importa cuáles sean ni desde qué postura partamos. Pero debemos comenzar a analizar un nuevo mundo, que para algunos es estupendo y lo reciben eufóricamente y para otros, se presenta oscuro y deshumanizado.

Sin embargo, el abogado debe estar en este lugar, aquí y ahora, afrontando el reto y cumpliendo el rol de garante y moderador en los conflictos sociales y, como fin último, protegiendo los intereses individuales y colectivos y salvaguardando la esencia humana.

1 Tesis presentada por el Dr. Hugo Daniel CARRION (Abogado especialista en Derecho Penal. Secretario de la Sala Tercera de la Cámara de Apelación y Garantías en lo Penal del Departamento Judicial de Lomas de Zamora, Provincia de Buenos Aires, República Argentina) en el marco de la Maestría en Derecho, Ciencia y Tecnologías de la Información dictada por la Universidad del Museo Social Argentino y la Universidad de Burgos (España). Materia: Delitos informáticos.

2 Clara SMITH, "Una metodología para la concepción de los sistemas legales inteligentes", Universitas Rerum. Publicación de la Escuela de Filosofía Práctica (Año II – Nº 14); Antonio Enrique PEREZ LUÑO, "Sistemas expertos jurídicos: Premisas para un balance"; MARTINO, A. (1987-88), "Sistemas expertos legales", en Martino, A. (ed.), 1989, 215-241.

3 Manuel CASTELLS, "Globalización, sociedad y política en la era de la información", Ponencia presentada por el autor en el Auditorio León de Greiff de la Universidad Nacional de Colombia el 7 de mayo de 1999.

4 Alvin y Heidi TOFFLER, "La nueva economía apenas comienza", La Nación, 9 de mayo de 2001.

5 GUTIERREZ FRANCES, M. Luz, "Fraude informático y estafa", Ministerio de Justicia, Secretaría General Técnica, Centro de Publicaciones, Madrid, 1991, pág. 41.

6 PEREZ LUÑO, A. E. (1987 b): "Nuevas tecnologías, sociedad y derecho. El impacto socio-jurídico de las N.T. de la información", Fundesco, Madrid.

7 GARCIA-PABLOS MOLINA, A., "Informática y Derecho Penal", en Implicaciones socio-jurídicas de las tecnologías de la información, Citema, Madrid, 1984, pp. 39-40.

8 FROSINI, V., Cibernética, Derecho y Sociedad, Tecnos, Madrid, 1982, pp. 173-175.

9 Ezequiel Zabale y Guillermo Beltramone, "Acerca de la autonomía del derecho informático".

10 GARCIA-PABLOS MOLINA, "Informática y Derecho Penal", cit., pp. 43-44.

11 (N. del A.) Se trata de una red de 120 satélites y radares estratégicamente distribuidos en todo el planeta, y que cuenta con la más sofisticada tecnología hasta hoy conocida. Se originó a comienzos de la década de los '70, pero tuvo la mayor expansión entre 1978 y 1995; para llegar a constituir la mayor red de escucha internacional. Los dueños de la red son Estados Unidos y Gran Bretaña; el funcionamiento y control de la misma se realiza por los servicios secretos de ambos países, respectivamente la N.S.A. (National Security Agency, Agencia Nacional de Seguridad) y la GCHQ (Agencia de Comunicaciones Gubernamentales). Cuenta con la participación de países en cuyos territorios se encuentran ubicados los principales centros de intercepción y rastreo de comunicaciones satelitales: Leitrim (Canadá), Sabana Seca (Puerto Rico), Shoal Bay (Australia), Waihopai (Nueva Zelanda), etc. Para tener una idea cabal de la importancia de la red, cada hora más de dos millones de mensajes son interceptados y clasificados por Echelon, con lo cual llamadas telefónicas fijas o celulares, fax, e-mail, información de Internet, etc., no escapan a dicho control.

Es evidente que tal espionaje pone en riesgo la seguridad de las naciones. La carencia de adecuada regulación normativa que impida tal intromisión, constituye un problema de orden institucional y político internacional.

12 GUTIERREZ FRANCES, M. Luz, ob. Cit., pp. 44-45.

13 MUÑOZ CONDE, F., Teoría General del delito, 2ª. Ed., Tirant lo Blanch, Valencia, 1989, p. 55.

14 LIZT, F. v., Tratado de Derecho Penal, t. II, pp. 6 y ss.

15 BARATTA, Alessandro, "Criminología Crítica y Crítica del Derecho Penal", Siglo XXI Editores, pp. 83 y ss.

16 (N. del A.) Es harto conocido el debate en torno a la legalización de conductas como la tenencia de estupefacientes para consumo personal, el aborto, la eutanasia o el libramiento de cheques sin fondos

17 SIEBER, Ulrich, "The International Handbook on Computer Crime"º, Ed. John Wiley & sons Ltd., 1986, Great Britain, 1986.

18 TIEDEMANN, Klaus, "Poder Económico y Delito", Edit. Ariel, Barcelona, 1985, pág. 122.

19 MEINEL, Carolyn – http://www.happyhacker.org, "Cómo hacer finger a un usuario vía Telnet". (N. del A.) La autora del artículo nos dice que el mismo nos enseñará cómo practicar hacking inofensivo auténtico, pero legal, destacando que no se brindarán explicaciones de cómo hacer daño en las máquinas de otros, ni cómo ingresar en sitios a los que no se pertenece. Asimismo, transcribe un aviso intimidatorio: "Aviso de cárcel: Incluso cuando no provocas ningún daño, si entras en una parte de un ordenador que no está abierta al público, has cometido un delito. Si en Estados Unidos cruzas una frontera estatal al hacer un telnet para introducirte en un sistema, has cometido un delito federal."

20 Archivo de la jerga, "Cómo transformarse en un hacker", Versión original en inglés actualizada en http://www.ccil.org/~esr/faqs/hacker-howto.html, y la traducción al castellano en http://usuarios.santafe.com.ar/~cballard/pf/hacker-howto.es.html.

21 Jargon File Resources (La Biblia de los hackers), http://www.tuxedo.org/%7Eesr/jargon/.

22 (N. del A.) Charles PALMER (informático estadounidense que trabaja en el marco de seguridad de redes y sistemas informáticos para IBM Consultig), en un Reportaje en "Hacking por hackers", señala que el hacking es delito en los Estados Unidos y en la mayoría de los otros países (industrializados), pero cuando se hace a pedido y bajo contrato entre un hacker ético y una organización, está bien. Explica que la diferencia clave está en que un hacker ético tiene autorización para testear (atacar) su objetivo. Manifiesta que "Dependiendo del tipo de evaluación

requerida (desde pruebas a servidores Web a ataques externos de todo tipo), reunimos toda la información posible del objetivo de todas las fuentes públicas disponibles. A medida que vamos aprendiendo más sobre el objetivo y sus subsidiarias y el tipo de conectividad utilizada en sus redes, comenzamos a probarlas en busca de debilidades. Ejemplos de debilidades incluyen pobre configuración de servidores Web, software viejo o "parchado", controladores de seguridad desactivados, y passwords por defecto sin cambiar, o mal elegidas. Mientras vamos encontrando vunerabilidades a explotar, vamos documentando si ganamos acceso, cómo lo hicimos y si alguien de la empresa sabía de ello. (En la mayoría de los casos los Departamento de Sistemas de Información no son notificados de los ataques planeados.) Después trabajamos junto al cliente para solucionar los problemas encontrados".

23 GUTIERREZ FRANCES, M. Luz, ob. Cit., pp. 74.

24 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)

25 BIDART CAMPOS, Germán, "Tratado Elemental del Derecho Constitucional Argentino", Ediar, 1988, T. I, pág. 256).

26 PALAZZI, Pablo Andrés, "El acceso ilegítimo a sistemas informáticos. La urgente necesidad de actualizar el Código Penal".

27 BINDING, Karl, "Die Normen und ihre Vebertretungen", T. I, pág. 370, citado por BUSTOS RAMIREZ en "Control Social y Sistema Penal", Barcelona 1987, pág. 324 y ss.).

28 (N. del A.) La Corte Suprema de Justicia de la Nación tiene dicho que "no es exigencia constitucional que toda figura delictiva deba producir un daño para ser punible, pues tal razonamiento prescinde de la existencia de tipos delictivos constitucionalmente válidos y en los que el resultado de la acción consiste en la creación de un peligro" (FALLOS 317:2561).