UNIVERSIDAD DE CHILE
FACULTAD DE DERECHO

Departamento de Ciencias Penales

Hacking, Cracking y Otras Conductas Ilícitas Cometidas a Través de Internet

Memoria para optar al grado de
Licenciado en Ciencias Jurídicas y Sociales

Autor: Alejandro Acosta Patroni

Profesor Guía: Eduardo Sepúlveda Credar

Santiago, Chile

Marzo, 2003

Índice

ÍNDICE **1**

GLOSARIO DE TÉRMINOS INFORMÁTICOS **4**

I. INTRODUCCIÓN **8**

II. LOS DELITOS INFORMÁTICOS. **13**

1.- GENERALIDADES: 13

2.- EL BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS 27

3.- CARACTERÍSTICAS GENERALES DE LOS DELITOS INFORMÁTICOS 31

3.1.- Permanencia del hecho: *31*

3.2.- Es un delito altamente técnico: *32*

3.3.- Son pluriofensivos: *33*

3.4.- Son delitos masivos, colectivos o difundidos: *33*

3.5.- Son delitos de mera actividad *34*

3.6.- Son delitos de muy difícil averiguación y comprobación: *35*

3.7.- Alto volumen de cifra oscura: *37*

3.8.- Son delitos de creciente frecuencia, diversidad y peligrosidad: *38*

3.9.- Ellos son habitualmente transfronterizos: *40*

4.- CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS 40

4.1.- Clasificación de TÉLLEZ VALDÉS *41*

4.2.- Clasificación de HUERTA Y LÍBANO *42*

4.3.- Clasificación de RAINER RAPP *46*

4.4.- Clasificación de ENRIQUE ROVIRA *48*

5.- SUJETOS ACTIVO Y PASIVO EN LOS DELITOS INFORMÁTICOS 53

5.1.- El Sujeto Activo: *53*

5.2.- El Sujeto Pasivo *59*

III. DELITOS INFORMÁTICOS E INTERNET **61**

1.- INTERNET 62

2.- INTERNET Y EL DERECHO 72

3.- LA DIFICULTAD DE SANCIONAR LOS ACTOS ILÍCITOS COMETIDOS A TRAVÉS DE INTERNET .. 79

IV. HACKING, CRACKING Y OTROS ILÍCITOS COMETIDOS EN INTERNET **97**

1.- HACKERS, CRACKERS Y EL RESTO DE LA FAMILIA UNDERGROUND 100

2.- LOS HACKERS 121

2.1.- Los principios y la ética hacker *129*

2.2.- Requisitos para ser considerado un hacker *150*

3.- LOS CRACKERS 162

V. HACKERS Y CRACKERS ANTE EL DERECHO **177**

1.- HACKERS Y CRACKERS EN EL DERECHO INTERNACIONAL. LA CONVENCIÓN INTERNACIONAL CONTRA EL CIBERCRIMEN 178

1.1.- Antecedentes *181*

1.2.- Objetivos y estructura de la Convención *187*

1.3.- La Convención sobre el Cibercrimen y las conductas de hacking y cracking *189*

2.- HACKING Y CRACKING ANTE LA LEY CHILENA 208

2.1.- La ley 19.233 ..... *208*

2.2.- Críticas a la ley 19.233 ..... *212*

2.3.- El cracking y la ley chilena *218*

2.4.- El hacking en la ley chilena *223*

VI. A MODO DE CONCLUSIÓN **236**

VII. BIBLIOGRAFÍA 247

1.- BIBLIOGRAFÍA Y DOCUMENTOS ELECTRÓNICOS CITADOS EN EL TRABAJO 247

2.- DOCUMENTOS CONSULTADOS EN LA INVESTIGACIÓN, PERO NO CITADOS. 252

Glosario de términos informáticos

- **ADSL:** Abreviación de Asymmetric Digital Subscriber Line, el ADSL es un método de transmisión de datos a través de las líneas telefónicas de cobre tradicionales a velocidad alta. Los datos pueden ser descargados a velocidades de hasta 1.544 Megabits por segundo y cargados a velocidades de hasta 128 Kilobits por segundo. Esa es la razón por la cual se le denomina asimétrico. Esta tecnología es adecuada para el web, ya que es mucho mayor la cantidad de datos que se envían del servidor a un ordenador personal que lo contrario.

- **AOL (American On Line):** El proveedor más grande de servicio de internet. Proporciona muchos servicios de valor agregado, además del acceso a internet. http://www.aol.com

- **Cracker:** 1) Un hacker con intenciones destructivas o delictivas. (2) Intruso. Un "cracker" es una persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas intenciones, en contraste con los "hackers", y suelen disponer de muchos medios para introducirse en un sistema. Ver también: "hacker", "CERT", "Trojan Horse", "virus", "worm". (3) Persona que ingresa ilegalmente en un sistema informático para robar o destruir información, o simplemente para causar desorden. También se llama cracker a quien descifra los esquemas de protección anti-copia de los programas comerciales, para poder utilizar o vender copias ilegales.

- **Hacker:** 1) Experto informático especialista en entrar en sistemas ajenos sin permiso, generalmente para mostrar la baja seguridad de los mismos o simplemente para demostrar que es capaz de hacerlo. (2) Persona que disfruta investigando de los detalles de los sistemas operativos y los programas, buscando nuevas formas de aumentar sus

capacidades. Aquellos que programan, a veces hasta con obsesión, que disfrutan de esto. Experto o entusiasta de cualquier disciplina, no solo de computación. Quien goza con el desafío intelectual que representa el superar las limitaciones impuestas. (3) Una persona que goza alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de un ordenador o de una red de ordenadores. Este término se suele utilizar indebidamente como peyorativo, cuando en este último sentido sería más correcto utilizar el término "cracker".

- **Hardware:** La parte física del ordenador (placa, micro, tarjetas, monitor...).

- **Internet:** Sistema que aglutina las redes de datos de todo mundo, uniendo miles de ellas mediante el protocolo TCP/IP. El mayor conjunto que existe de información, personas, ordenadores y software funcionando de forma cooperativa. La i mayúscula la diferencia de una internet convencional, que simplemente une varias redes. Al ser única se la conoce también simplemente por "la red".

- **IP:** (1) Internet Protocol. Parte del conjunto de protocolos TCP/IP encargada de la interconexión de redes. Es el fundamento básico y de más bajo nivel de Internet. (2) Siglas para Internet Protocol (Protocolo de Internet). Es el protocolo responsable del envío de paquetes de información entre dos sistemas que utilizan la familia de protocolos TCP/IP**,** desarrollada y usada en Internet. El envío de paquetes permite dividir la información en bloques que pueden ser remitidos por separado y después reagrupados en su destino.

- **IRC:** Siglas para Internet Relay Chat. Sistema de conversación por computadora (chat) en el que varias personas pueden participar al mismo tiempo en "canales" dedicados a asuntos específicos. Las

charlas ocurren en tiempo real. Las frases tecleadas por el usuario aparecen en la pantalla de los demás participantes del canal.

- **Motor de búsqueda**: Un motor de búsqueda es una pieza de software, accesible a todos los usuarios de la web, que les permite localizar los sitios relacionados con una palabra clave -ó keyword-. Un usuario, por ejemplo, puede pedir conocer los sitios que en su descripción contengan las palabras tango y baile: el motor de búsqueda
  devolverá entonces una lista de todos los sitios que presenten referencias a esos vocablos.

- **Pagina Web:** Resultado en hipertexto o hipermedia que proporciona un navegador del WWW después de obtener la información solicitada. Su contenido puede ir desde un texto corto a un voluminoso conjunto de textos, gráficos estáticos o en movimiento, sonido, etc. Algunas veces el citado término es utilizado incorrectamente en orden de designar el contenido global de un sitio web, cuando en ese caso debería decirse "sitio web".
- Servidor: Un servidor es un ordenador que trata las peticiones de datos, el correo electrónico, la transferencia de ficheros, y otros servicios de red realizados por otros ordenadores (clientes).

- **Shareware:** Traducido del inglés: programa compartido. Es un software que puede ser utilizado de manera gratuita durante un periodo de prueba, al final del cual se puede comprar el programa a un precio bajo.

- **Software:** Los programas de ordenador, la lógica que permite realizar tareas al hardware (la parte física).

- **Undernet:** sistema que conecta distintos servidores de IRC de modo que los distintos canales y foros son accesibles independientemente del servidor a que se conecte el usuario.

- **Unix:** Sistema operativo utilizado originariamente en grandes sistemas informáticos a los que tienen acceso simultaneo gran cantidad de usuarios. Hoy en día existen multitud de variantes que se adaptan a todo tipo de equipos informáticos. Linux es su variante gratuita y de código abierto. Debido a que fue diseñado para funcionar en Red, es el sistema operativo más difundido en Servidores conectados a Internet.

I. Introducción

Uno de los mayores inconvenientes a que se enfrentan los operadores jurídicos a la hora de analizar y actuar respecto del mundo de la informática, es el poco conocimiento que en esta área se posee, principalmente debido a que, en general, se considera a éste un entorno más propio de las ingenierías y las matemáticas que de las humanidades que es el ámbito natural donde el hombre de derecho está acostumbrado a desenvolverse. Expresión de lo anterior la encontramos en el hecho de que, en la mayoría de la bibliografía especializada consultada en el curso de esta investigación, en general se le dediquen líneas muy breves y escuetas al tratamiento de los diferentes aspectos y caracterizaciones de los delitos informáticos, centrándose la mayoría de las veces el análisis en los aspectos netamente jurídicos de los mismos, y en particular en su consagración legal, sin adentrarse más a fondo en lo que este nuevo ámbito del conocimiento significa, en sus particularidades, en sus antecedentes y explicaciones no sólo jurídicas, sino que también sociales, culturales e incluso filosóficas, puesto que de lo que hablamos no sólo es de la regulación de un sector más del acontecer social, sino que hablamos de todo un mundo nuevo,

esencialmente dinámico, revolucionario, con sus propios rasgos distintivos de interacción y comportamiento; un espacio esencialmente globalizado, en el cual se han demostrado insuficientes los intentos meramente nacionales por regularlo, y en el que se hace imprescindible una acción conjunta de los diferentes países para darle un estatuto jurídico verdaderamente aplicable, real, eficiente y eficaz, que responda a sus propias particularidades, puesto que ya desde antaño se ha constatado que no es el derecho el capaz de transformar, por si solo, las realidades sociales, sino que éste debe adecuarse a ellas, cuestión que tratándose de Internet es aún un desafío a cumplir.

En las páginas que siguen, intentaremos adentrarnos en este misterioso y desconocido mundo de los hackers y los crackers. En primer lugar realizaremos una aproximación a la caracterización de lo que en doctrina son los delitos informáticos, para luego, una vez despejados los conceptos básicos sobre la materia, entrar de lleno al estudio del fenómeno del hacking y el cracking, exponiendo algo de su historia, sus principales características y en particular el pensamiento que se encuentra detrás de estos comportamientos. Por su parte, en el último apartado de esta memoria expondremos cuál es el tratamiento que jurídicamente se ha dado a esta

materia en nuestro país, y el intento por crear una normativa internacional que armonice las diferentes legislaciones en la lucha en contra de estos ilícitos, lo que se ha materializado a través de la llamada Convención del Cibercrimen, de reciente data aunque aún no entra plenamente en vigencia.

Debemos advertir al lector de estas líneas, que tal vez en muchos puntos no encontrará planteamientos realmente novedosos sobre la materia, puesto que hemos preferido guiarnos, fundamentalmente en el tratamiento jurídico de los temas, por la literatura existente, la que es escasa en nuestro país y que muchas veces recurre a lugares comunes en los que los autores no profundizan mayormente.

Sin embargo, un aspecto que estimamos novedoso de esta memoria se encuentra en el hecho de que en ella intentamos profundizar en el conocimiento de lo que realmente significan los fenómenos hacker y cracker, recurriendo para ello, más que a la bibliografía jurídica, a lo que los mismos hackers, crackers y especialistas sobre la materia han escrito sobre el tema. Ello, porque un hecho que en cierta medida lamentamos es que la mayoría de los trabajos que hemos conocido provenientes desde la órbita del derecho sólo se limita a describir conductas o a señalar lo que las leyes

dicen al respecto, sin ahondar mayormente en lo que existe detrás de estas conductas.

Como dijimos, es escasa la bibliografía que existe en nuestro país que se aboque a tratar este tema, y de hecho no logramos encontrar nada que se introduzca especialmente en los fenómenos del hacking y el cracking, es por eso que hemos debido en el curso de la investigación recurrir al uso principalmente de trabajos provenientes desde la doctrina extranjera y en particular documentos electrónicos encontrados en Internet, los que en este espacio si son abundantes, aunque no siempre todo lo profundos que uno desearía.

También hemos usado bastante bibliografía proveniente desde el entorno hacker y cracker, en la cual se describe su pensamiento y accionar, la cual creemos que nos ha permitido develar algunos mitos que existen sobre la materia. En cada caso que hemos recurrido a este tipo de fuentes también hemos colocado la correspondiente referencia al lugar de Internet en el cual es posible encontrarla.

Esperamos que las páginas que siguen logren cumplir con su cometido de servir como puerta de entrada a quien desee introducirse mayormente en los fenómenos aquí tratados. No cabe duda de que hay

muchos aspectos que tal vez no han sido lo eficientemente desarrollados o sobre los que nos hubiese gustado ahondar más, sin embargo las pretensiones y características propias de un trabajo del tipo que presentamos no lo permiten.

Esperamos en el futuro poder tal vez dedicarnos a un estudio más acabado de este tema, por el momento nos sentiremos satisfechos si las líneas que hemos escrito y la investigación realizada es de utilidad para alguien más que nosotros.

II. Los Delitos Informáticos.

1.- Generalidades:

Tal vez uno de los mayores inconvenientes presentados al momento de abordar el estudio de los delitos informáticos, sea el hecho de la existencia de una demasiado amplia y poco sistemática cantidad de conceptualizaciones que se dan respecto al término, lo cual puede crear una gran sensación de confusión en quién se acerque por primera vez a estas materias.

A juicio de los autores HUERTA Y LÍBANO, el anterior fenómeno se puede explicar por el hecho de que "cada profesión o ciencia ha entregado conceptos diversos de lo que entienden por delito informático de acuerdo a sus propios lenguajes y propósitos, investidos de terminología informática, muchas veces, sólo regularmente empleada, situación que de acuerdo a Sneyers acarrearía una falta de soltura en materia informática (Computer Literacy), lo que impediría la existencia de una sola definición

para el delito informático que sea operativa y flexible en el sentido de permitir la incorporación de nuevos elementos"[1]

A lo anterior se suma, dentro del ámbito estrictamente jurídico, el hecho de que aún subsistan múltiples posturas doctrinales que pretenden explicar el fenómeno de la criminalidad informática desde distintas ópticas, siendo aquellas principales las representadas, desde un lado, por la ya vieja tendencia a intentar asimilar los delitos informáticos a algunas de las clasificaciones y nociones clásicas o tradicionales del Derecho Penal, negando a este tipo de ilícitos la existencia como ámbito jurídico independiente y limitándose a aceptar, a lo más, la existencia de "una pluralidad de ilícitos con una única nota común: su vinculación con el ordenador"[2]. Es decir, se asimila esta clase de ilícitos a las conductas criminales tradicionales, con la sola diferencia de que en este caso se establece un nuevo *modus operandi,* esto es, "el ser cometidos por medios

---

[1] HUERTA MIRANDA, MARCELO Y LIBANO MANSSUR, CLAUDIO, Delitos Informáticos. Segunda Edición Complementada y Actualizada a 1998. Editorial Jurídica Conosur Ltda.., Santiago, Chile, 1998. Pág. 110-111.

[2] ROVIRA DEL CANTO, ENRIQUE, Delincuencia Informática y Fraudes Informáticos. En Estudios de Derecho Penal dirigidos por Carlos María Romeo Casabona, Editorial Colmenares, España, 2002. Pág. 65.

informáticos, o como 'delitos contenidos en la vigente legislación cometidos a través de medios informáticos'"[3].

ROVIRA, en su obra ya citada, nos menciona como ejemplos de autores ligados a esta postura a NIMMER, para quien la delincuencia informática sería equiparable a la delincuencia financiera; RUIZ VADILLO, quién postula que estos ilícitos son una forma de delincuencia económica, al igual que hacen MÖHRENSCHLAGER y GÓMEZ PERAL. Este último concebiría al delito informático como "el conjunto de acciones dolosas que provoca un perjuicio a personas físicas o entidades, sin que sea necesario que ello conlleve un beneficio material para su autor, o viceversa, produce un beneficio ilícito a su autor aún cuando no perjudique de forma ostensible a la víctima"[4].

Otros autores que también adhieren a esta postura son: MIGUEL ANGEL DAVARRA RODRÍGUEZ, para quien el delito informático es "la realización de una acción que reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea el

---

[3] Ibíd.., Pág. 66.
[4] Citado por ROVIRA DEL CANTO, ENRIQUE, Ob. Cit. Pág. 67.

hardware o software"[5]; y TÉLLEZ VALDÉS, para quien "los delitos informáticos son actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)"[6].

En la vereda opuesta a la anterior postura doctrinal, encontramos a aquellos que reclaman para la delincuencia informática una caracterización propia, nueva y separada de las nociones tradicionales de delito. Para éstos, no es suficiente el querer asimilar los delitos informáticos a las categorías clásicas que conoce el Derecho Penal, puesto que al intentar subsumir estos ilícitos a otros tipos como el fraude, el hurto, los daños, etc., se estaría atentando no sólo en contra del principio de legalidad, *nullum crime sine lege*, puesto que se pretendería aplicar por analogía sanciones penales para conductas no específicamente contemplada en la ley, sino que, además, con ello se estaría obviando la existencia de intereses jurídicos nuevos derivados de la actual realidad del entorno tecnológico y del uso de los sistemas

---

[5] DAVARRA RODRÍGUEZ, MIGUEL ANGEL, Citado por RAPP ORTEGA, RAINER, El Delito Informático en Chile y en el Derecho Comparado. Memoria de Prueba, Facultad de Derecho Universidad de Chile, 2001. Págs., 112-113.

[6] TÉLLEZ VALDES, JULIO, Citado por RAPP ORTEGA, RAINER, Ob. Cit., Pág.113

informáticos y de telecomunicaciones, los cuales requieren regulación y protección por el Derecho. En este caso se tiende a reconocer a lo informático no sólo como un medio más de comisión de delito, sino como un fin en sí mismo, como bien jurídico que debe ser reconocido y protegido.

Adhiriendo a esta última postura ROVIRA señala, "Hoy en día no solo puede hablarse de la existencia de meros abusos informáticos derivados del uso y utilización de los sistemas informáticos y de telecomunicaciones, sino también de comportamientos ilícitos informáticos derivados de la propia sociedad global del riesgo informático y de la información, y que, en cuanto adquieren la suficiente entidad y gravedad como para constituir ataques serios a intereses jurídicamente protegidos y protegibles, tradicionales y nuevos, deben ser contrarrestados con medidas que superen los meros ámbitos de la autorregulación, del derecho administrativo y del derecho civil, requiriendo la intervención del derecho penal, se constituyen en lo que podemos denominar 'delitos informáticos'. En consecuencia , podemos no sólo afirmar la existencia del delito informático como manifestación global y genérica de la criminalidad informática originada por el riesgo propio del uso y utilización de la informática y de la información en la actual sociedad,

sino incluso el utilizar correctamente el término de *delito informático* no sólo como categoría funcional sino incluso para referirnos al conjunto de figuras sustantivas normativas que conforman el núcleo de lo que hemos venido a denominar Derecho penal global del riesgo informático y de la información"[7].

En la doctrina nacional también encontramos autores que adscriben a esta tendencia sobre la necesidad de tratamiento independiente para los delitos informáticos. Así, RAINER RAPP ORTEGA, en su Memoria de Prueba ya citada, luego de efectuar un análisis detallado de los delitos informáticos comparándolos con aquellos otros delitos de la esfera tradicional con los que comparten características, llega a la conclusión de que si bien, "ciertas conductas de los llamados delitos informáticos, podrían ser subsumidas, sin mayor dificultad, dentro de la descripción típica de las categorías tradicionales que se manejan en nuestro Código Penal, como lo sería por ejemplo algunos casos de sabotaje informático dentro del ámbito de daño. Pero es un hecho patente que la norma general sea el caso contrario. Dicha subsunción, no será posible debido a la falta definitiva de

[7] ROVIRA DEL CANTO, ENRIQUE, Ob. Cit. Pág. 68.

uno o más de los elementos objetivos o subjetivos exigidos en la descripción típica de los delitos que contempla el Código Penal. Ello nos hace afirmar con absoluta certeza la existencia de una categoría de ilícitos, delitos especiales y diversa de los tipos tradicionales, denominados Delitos Informáticos"[8].

El mismo autor más adelante se encarga de reafirmar la anterior idea al aseverar que no puede considerase a toda conducta ilícita en que se vea involucrado un sistema informático como un delito informático propiamente tal, ya que es posible encontrar en la actualidad un sinnúmero de actos delictivos en los cuales se ven utilizados este tipo de medios, pero sólo como una forma peculiar o novedosa de comisión de alguno de los delitos ya contemplados en las clasificaciones clásicas del derecho penal, como podría ser para cometer un fraude, hurto, falsificación, etc. Sin embargo, en dichos casos señala que difícilmente podría afirmarse que "nos enfrentamos a un nuevo ilícito que no esté contemplado en nuestra legislación penal. Cierto es, que la perpetración de este ilícito presenta un elemento nuevo e informático, cual es el uso de un computador como

[8] RAPP ORTEGA, RAINER, "El delito Informático en Chile y en el Derecho Comparado". Memoria de Prueba, Facultad de Derecho. U. De Chile, Pág. 108-109.

instrumento o medio para su realización, pero no basta esa sola circunstancia, a nuestro juicio, para sostener la presencia de un delito informático. Ciertamente en estos casos, y así lo estima la doctrina, es más acertado hablar de **delitos computacionales** o de la **informatización de tipos penales**, reconociendo en estos ilícitos ya contemplados en el Código Penal o, que en el caso de no ajustarse plenamente a la conducta descrita, solamente requieren de la ampliación del tipo penal ya establecido para contemplarlos, pero que en ningún caso haría necesario la creación de tipos penales nuevos".[9]

Coincidentes, en particular con esta última afirmación, HUERTA Y LÍBANO, luego de señalar que únicamente habrá delito informático cuando la acción u omisión típica sólo pueda realizarse por medio, en utilización o en contra de un sistema informático, y que no puede considerarse como uno de estos ilícitos los actos perpetrados en contra de los elementos físicos, palmarios del sistema informático, como destruir un diskette, robar un ordenador, etc.; afirman que tampoco puede catalogarse como delito informático el hecho de que el delincuente utilice, como medio para facilitar

[9] RAPP ORTEGA, RAINER, Ob. Cit., Pág. 110.

su acto delictivo, un sistema informático. Sobre el particular afirman que "no es buena una técnica legislativa que 'informatice' los delitos comunes ya que de tal forma se menoscaba el carácter especialísimo de los delitos informáticos. Es evidente que algunos delitos comunes se facilitan al cometerse por medios informáticos. En este punto debemos reparar en la licitud o ilicitud de la acción u omisión informática, herramienta de comisión de un delito como sería, por ejemplo, la estafa. Si la conducta informática es lícita y la estafa se consuma, habrá pura y simplemente una estafa que se sancionará de acuerdo a las prescripciones del Código Penal. ¿Pero que ocurre si la acción u omisión informática es ilícita y así es tipificada en una ley especial? Sobre el particular, pueden darse dos situaciones: la primera sería que la estafa se consume y la segunda que tal delito no llegue a producirse. En la primera hipótesis estamos frente a un delito informático puro que consiste en una conducta tipificada por la ley y por ello se sancionará en conformidad a lo que ordene el precepto regulador. En la segunda, se ha producido igualmente el ilícito informático que deberá sancionarse como tal y al mismo tiempo se ha consumado una estafa que es un delito diverso. La acción del delincuente ha sido sólo una y ella consta de un delito informático que ha servido de medio para cometer

otro que es la estafa. Consideramos que esta es una situación ya regulada por el Código Penal chileno en su Art. 75, por lo que deben aplicarse las indicaciones de la norma en lo que la doctrina ha llamado el Concurso Ideal de Delitos"[10].

Nosotros también nos sentimos inclinados a adscribir a esta segunda postura doctrinal. Creemos que lo informático es una nueva realidad, con características muy particulares y, en general, no previstas por la legislación clásica del Derecho Penal. En este caso nos enfrentamos a un fenómeno que requiere un estudio y tratamiento independiente, que debe ser asumido en su particular dimensión puesto que posee bienes jurídicos que le son propios y que deben ser salvaguardados por el Derecho. Esto se hace aún más patente tratándose de los delitos informáticos cometidos a través o en el ciberespacio, en particular cuando nos referimos a las conductas de Hacking, pues, como veremos más adelante, en estos casos, principalmente tratándose del llamado Hacking blanco, no nos enfrentamos a la existencia de una acción ilícita que pueda resultar en daños efectivos o palpables para la víctima, sino que en ellos la sola realización de la conducta entraña en sí

---

[10] HUERTA MIRANDA, MARCELO Y LIBANO MANSSUR, CLAUDIO, Ob. Cit., Págs., 109-110.

ya un riesgo, el cual puede ser la antesala de la comisión de delitos de mayor gravedad, situación que podría ocurrir si sobre el mismo sistema vulnerado originalmente se realiza una conducta de Cracking o incluso de ciberterrorismo. Empero, cuando reclamamos este tratamiento independiente para los delitos informáticos, con ello nos referimos sólo a aquellos delitos cuyo medio o fin necesariamente se halla en lo informático y no a aquellos actos que puedan facilitar la realización de un crimen o simple delito de los clasificados dentro de la doctrina tradicional del Derecho Penal. Estos últimos deberán ser analizados como cualquier otro medio utilizado para facilitar la comisión de un delito, pudiendo servir incluso como calificante para un delito tradicional, aunque no por ello será un delito informático. Además, como sucede con todas las áreas del Derecho Penal, es menester también en este caso respetar el principio de legalidad, en cuanto para que sea factible perseguir estos ilícitos será necesaria la existencia de una conducta que se encuentre previamente tipificada en la ley, pues no puede ser que, so pretexto de la necesidad de sancionar conductas que a todas luces sean punibles, se intente aplicar figuras clásicas en forma analógica o mediante una interpretación demasiado amplia de ellas. Es cierto que en muchas situaciones el Derecho

ha demostrado su impotencia para perseguir actos delictivos cometidos en el entorno digital, principalmente debido a la realidad esencialmente dinámica de este entorno, pero para subsanar esta deficiencia es menester hacer uso de la técnica legislativa, pues son los legisladores quienes deben dotarnos de normas lo suficientemente adecuadas para perseguir y sancionar estas conductas, y ello tomando justamente en consideración el que en estas materias no siempre será necesario la existencia de un daño para que la conducta sea lesiva. El hecho de que la penetración de un hacker en un sistema informático no acarree ningún daño directo para la víctima, no significa que a dicha actividad se la pueda considerar sólo como un acto preparatorio o como un delito frustrado de un daño directo. Es por ello que también compartimos la tesis de la importancia de que en estos casos estamos frente a un derecho penal de riesgo, y no necesariamente de resultado, por lo cual se hace necesario el adelantar la barrera jurídica y no juzgar al acto únicamente por su consecuencia final sino como acto en sí mismo, el cual pensamos que es justamente el camino adecuado para comenzar la protección de esta área de la realidad social. En este sentido, nos hacemos eco de lo señalado por ESTHER MORON, en cuanto "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."[11]

Sobre el particular, podemos agregar además lo dicho por ROVIRA, en cuanto a que "en la configuración de un Derecho Penal del Riesgo informático y de la información, creo que para la formulación dogmática de una conceptuación actual del delito informático en general, con las salvedades propias de toda excepción a la regla, la punibilidad debe venir determinada, en este ámbito, por la potencialidad de las conductas o comportamientos en afectar gravemente la información en sí misma como bien jurídico supraindividual y el interés colectivo en la seguridad y fiabilidad de los sistemas y redes de almacenamiento, tratamiento, procesamiento y transferencia de la misma, siendo por tanto el método a utilizar el de formulación de *tipos delictivos de peligro abstracto* en cuanto a la grave afectación de estos nuevos bienes jurídicos, con independencia del requerimiento por alguna figura concreta, además, y en su caso, de un

[11] MORON LERMA, ESTHER, Internet y Derecho Penal: «Hacking» y otras Conductas Ilícitas en la Red. Editorial Aranzadi, 1999, Pamplona, España. Pág. 64.

resultado perjudicial, lesivo o dañino de un bien jurídico tradicional, individual o colectivo, también protegido o concurrente"[12].

Cabe señalar que en el supuesto anterior, el autor además destaca que para que un delito informático pueda ser considerado como tal es menester que exista la posibilidad, directa o indirectamente, de una grave afectación de la información, puesto que si no concurren estos presupuestos sería procedente sólo aplicar sanciones administrativas, como postula MORON LERMA[13] para aquellas conductas que sólo constituyen mero intrusismo o acceso informático, y realizadas sin otro móvil que la curiosidad o la diversión. No obstante, el autor precisa que incluso en tales supuestos, "frente a las conductas que aún suponiendo inicialmente un quebranto leve de la información como bien o valor de interés supraindividual, si traen consigo indisolublemente una potencialidad o peligrosidad de quebranto de otros bienes jurídicos tradicionales, la reacción más adecuada sigue siendo la penal y no la de la mera sanción administrativa"[14].

---

[12] ROVIRA DEL CANTO, ENRIQUE, Ob. Cit. Pág. 73-74
[13] MORON LERMA, ESTHER, Ob. Cit. Pág. 73 y 140.
[14] ROVIRA DEL CANTO, ENRIQUE, Ob. Cit. Pág. 74.

2.- El Bien Jurídico Protegido en los Delitos Informáticos

En Derecho Penal, la determinación del bien jurídico protegido cumple, entre otras, con la función de servir de límite material al ius puniendi del Estado y de base para la interpretación jurídica de la norma, además de ser el punto de partida sobre el cual se erige gran parte de la sistematización de las conductas delictivas, por cuanto por su intermedio se permite ordenar las clases y familias de delitos. Es por ello que creemos importante el determinar en esta parte cuáles son los bienes jurídicos que se entienden vulnerados cuando hablamos de los delitos informáticos y que por tanto requieren una protección especial por parte del Derecho.

Ya en el apartado precedente postulamos que, entre las razones que nos llevan a adherir a la postura de considerar a los delitos informáticos como una especialidad dentro del Derecho punitivo, estaba el que opinamos que este tipo de ilícitos atentan en contra de bienes jurídicos que han aparecido en el último tiempo y que son propios de la sociedad de la información en que estamos inmersos. Sin embargo, desde ya es menester advertir que al afirmar esto en modo alguno postulamos que esta categoría de delitos atenten única y exclusivamente en contra de dichos bienes jurídicos que le son propios y que, en consecuencia, se deban excluir otros

del área de sus atribuciones, puesto que se deriva de las características propias de estos ilícitos el que, además de atentar en contra de los bienes jurídicos propiamente informáticos, también en la mayoría de los casos se deben entender involucrados otros bienes jurídicos tradicionales, como son la propiedad, la intimidad, etc. Es característico de los delitos informáticos el que sean pluriofensivos, es decir, que atenten en contra de más de un bien jurídico, sean ellos propios de la realidad informática o pertenezcan a las categorías tradicionales, aunque, claro está que, para ser considerados como tales estos ilícitos deben necesariamente atentar en contra de los primeros, en cambio el que atenten en contra de un bien jurídico tradicional es algo que puede o no ocurrir, cuestión que no afecta en nada su clasificación como delito informático.

Ahora bien, en cuanto a la determinación de cuál o cuales son estos bienes jurídicos que el área punitiva del derecho informático debe proteger, los autores HUERTA Y LIBANO señalan que ellos dependerán con mucho del sistema que se siga para incorporar estos ilícitos a la legislación, ya sea por la vía de su asimilación a alguna de las categorías clásicas de ilícitos penales, como en general ha ocurrido en Europa, en donde incluso ha existido la tendencia a "informatizar" las figuras delictivas tradicionales, o

estableciendo una tipología independiente para estas situaciones. Estos autores, trayendo a colación el modelo Europeo, señalan que son bienes jurídicos protegidos con la incorporación de estos tipos penales de la informática:

- "El patrimonio, en el caso de amplia gama de fraudes informáticos y las manipulaciones de datos a que da lugar;
- "La privacidad, intimidad y confidencialidad de los datos, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general especialmente en el caso de los bancos de datos y el espionaje;
- "La seguridad y fiabilidad del tráfico jurídico y probatorio en el caso de falsificaciones de datos probatorios vía medios informáticos;
- "El derecho de propiedad sobre la información y sobre los elementos físicos, materiales de un sistema informático, en el caso de los delitos de daños"[15].

[15] HUERTA MIRANDA, MARCELO Y LIBANO MANSSUR, CLAUDIO, Ob. Cit., Pág. 118.

Aunque puede parecer propia y ajustada esta clasificación que de los bienes jurídicos hacen HUERTA Y LIBANO, necesariamente ello es sólo aparentemente, puesto que ella más corresponde a una informatización de los bienes jurídicos tradicionales, lo cual arranca justamente del carácter pluriofensivo de estos delitos, que un verdadero intento por determinar los bienes jurídicos que son propios de esta área, independientemente de la posibilidad de que en la comisión de alguno de los ilícitos por ellos mencionados se vea envuelto, además, otro bien jurídico como la propiedad, la privacidad, el patrimonio, etc.

Nosotros creemos que el principal bien jurídico que está llamada a proteger la incorporación de los tipos penales informáticos no es otra que la información, pues ella constituye el nuevo fenómeno no contemplado por los tipos penales clásicos. Claro que no cualquier tipo de información, sino que la información digital, por cuanto es ella la que constituye la base de la informática, y seguidamente podríamos agregar como bienes, los datos informáticos, las redes, las telecomunicaciones informáticas, etc. por cuanto ellos no constituyen sino formas en que la información se plasma, circula y utiliza en el nuevo entorno tecnológico.

En este mismo sentido ROVIRA ha señalado: "sostengo como principal bien jurídico protegible la información, y secundariamente los datos informáticos en sí mismos o los sistemas y redes informáticos y de telecomunicaciones, pues los primeros no constituyen más que la representación electrónica, incluso digital, de la primera, con un valor variable, y los segundos los mecanismos materiales de funciones automáticas de almacenamiento, tratamiento, transferencia y transmisión de aquella, cuya afectación o no, de cualquiera de ellos, datos o elementos, pueden servir normalmente más no necesariamente, para la configuración de algunas modalidades o tipos de delitos informáticos"[16].

3.- Características Generales de los Delitos Informáticos

3.1.- Permanencia del hecho:

Tal vez la principal y más distintiva característica de los delitos informáticos es que ellos puedan repetirse continuamente en el tiempo. Un sujeto que ha descubierto una falla de seguridad o una puerta de entrada y que ha través de ella ha penetrado en un sistema, generalmente volverá a hacerlo mientras la falla permanezca o no sea descubierta su presencia de

[16] ROVIRA DEL CANTO, ENRIQUE, Ob. Cit. Pág. 72.

alguna forma. De hecho tratándose particularmente de los delitos de Hacking, es casi una premisa el que el hacker, luego de haber entrado a un sistema se agencie los medios para poder dejarlo configurado de tal forma que le permita volver a ingresar a éste cuantas veces así lo desee. Incluso en ocasiones el sistema puede ser manipulado para que no sea necesaria la entrada directa en él, sino que mediante un proceso automatizado los datos puedan ser enviados directamente a un destino que el hacker determine. Lo anterior lleva a que entonces este tipo de delitos, desde el punto de vista del derecho penal sustantivo, se caracterice en cuanto a sus modalidades por ser de comisión instantánea y de efectos permanentes.

3.1.- Es un delito altamente técnico:

En general el sujeto activo de los delitos informáticos debe estar constituido por un individuo que tenga conocimientos bastantes más avanzados en sistemas computacionales que el que habitualmente posee un usuario medio. Si bien es cierto que en la actualidad la mayoría de las herramientas para cometer ilícitos de este tipo se hallan a disposición de cualquiera que se encuentre interesado, no es menos cierto que en la elaboración de esos medios han debido intervenir personas con

conocimientos informáticos muy amplios, puesto que no cualquiera puede, por ejemplo, crear un virus o un crack para vulnerar la seguridad de un programa computacional. Y quien hace uso de esas herramientas tampoco puede ser un lego, puesto que no sólo hay que saber donde encontrarlas, sino que también hay que saber usarlas evitando que el daño se le revierta a uno mismo, como ocurriría por ejemplo al hacer la manipulación errónea de algún virus.

3.2.- Son pluriofensivos:

Como ya señalamos anteriormente, habitualmente la comisión de un delito informático no atenta en contra de uno sino de varios bienes jurídicos protegidos, sean ellos de carácter propiamente informáticos o tradicionales.

3.3.- Son delitos masivos, colectivos o difundidos:

Atendiendo a las particularidades propias de algunos delitos, hay autores que han querido caracterizar a los delitos informáticos como delitos masivos, colectivos o difundidos, por cuanto su comisión afecta a un número indeterminado de personas, el que habitualmente puede ser muy alto. Particular ejemplo de esto son los virus computacionales, los cuales

pueden dañar las bases de datos de miles de personas sólo en unos pocos días, pese a haber sido el producto del trabajo de sólo un sujeto activo.

3.4.- Son delitos de mera actividad

Como señala RAINER RAPP, estos delitos pueden revestir el carácter de "delito formal o de mera actividad, que se perfecciona por la sola acción u omisión del sujeto activo (como ejemplo cabe señalar el caso del acceso indebido), como el de delito material, cuyo perfeccionamiento el legislador lo ha condicionado a la obtención del resultado ilícito de parte del agente (cabe señalar el caso del sabotaje informático)"[17].

Como ya antes hemos señalado, a este respecto nosotros nos inclinamos por adelantar en el caso de los delitos informáticos la barrera de protección, puesto que existen numerosas actividades ilícitas que no requieren la realización de un daño directo para ser consideradas como delictivas. Esto ocurre en particular tratándose del mero acceso no autorizado o hacking blanco, en que el sujeto activo no produce ningún perjuicio directo al afectado, salvo el hecho de que en éste provoca una sensación de inseguridad en los casos en que se logra detectar al intruso,

sabiendo que la información que se posee no está segura y a salvo de miradas extrañas. Además, también hemos visto que muchas veces el mero acceso es sólo la antesala de actividades de mayor envergadura y que si pueden implicar perjuicios directos para el afectado, como ocurre cuando, una vez descubierto el agujero de seguridad se utiliza éste para robar información o para mantener un control o vigilancia sobre todas las actividades que se lleven a cabo en el computador accesado.

Es por lo anterior entonces, que nosotros estamos por clasificar directamente a los delitos informáticos, y en particular al hacking como delitos de mera actividad, no siendo necesaria la existencia de un daño palpable para que el derecho se encuentre en la obligación de castigar la conducta ilícita.

3.5.- Son delitos de muy difícil averiguación y comprobación:

Como dijimos anteriormente, en general quienes cometen delitos informáticos poseen los conocimientos técnicos necesarios para lograr que sus actos se mantengan en el anonimato, ocultando la ocurrencia del hecho y borrando todas las huellas que pudieren implicar al sujeto activo con el

---

[17] R ORTGA, RAINER, Ob. Cit. Pág. 128

acto en cuestión. Facilita esta situación el hecho de que al ir evolucionando tan aceleradamente el entorno tecnológico, por esta vía también cada día vayan apareciendo nuevas herramientas para cometer delitos progresivamente más "perfectos", incluso sin necesidad de recurrir al uso de programas realizados con el sólo fin de permitir la consumación de un delito, sino que echando mano a programas o sistemas cuyo objetivo original es proteger justamente a los usuarios de dichas actividades. Un ejemplo viene dado por el uso de servidores proxys, los cuales, concebidos originalmente como un sistema de seguridad para los usuarios y una forma de garantizar su confidencialidad, son habitualmente utilizados por crackers con el objeto de no ser detectados a la hora de violar los mecanismos de seguridad de los diferentes sitios web, particularmente de aquellos que ofrecen servicios que son pagados. En este caso el proxy funciona como una barrera entre el delincuente y la víctima, mediante la cual el segundo se encuentra en la imposibilidad de determinar la dirección IP desde la cual ha sobrevenido el ataque, puesto que en la mayoría de los casos estos servidores proxys son del tipo anónimo y no dejan registro alguno de la dirección que le ha visitado.

3.6.- Alto volumen de cifra oscura:

Íntimamente ligada con la anterior característica se encuentra ésta, la cual significa que, pese al alto volumen de delitos informáticos que cada día se perpetran, un gran volumen de ellos, y nos atreveríamos a afirmar que la mayoría, no salen a la luz pública y no pueden, por tanto, ser perseguidos por las autoridades correspondientes. ROVIRA sobre el particular nos señala que "con la mejora y avances en las técnicas de investigación, lo cierto es que en base a los estudios empíricos más recientes efectuados a nivel internacional, se reafirman las tres clásicas apreciaciones de que el número de los delitos informáticos comprobables no es excesivamente alto, ello no obstante el número de los casos que verdaderamente tienen lugar no es ni mucho menos escaso, y ello debido a que *la cifra oscura* en el ámbito de la criminalidad informática es efectivamente excepcionalmente alta"[18]. El mismo autor nos señala como causas de lo anterior las siguientes:

1) Las ya mencionadas dificultades de averiguación y de comprobación de este tipo de delitos;

[18] ROVIRA DEL CANTO, ENRIQUE, Ob. Cit., Pág. 87.

2) El desconocimiento e ignorancia del sujeto pasivo de haber sido objeto de un ataque informático;

3) El que muchos de aquellos delitos que efectivamente son descubiertos no sean posteriormente denunciados; y

4) El que en las situaciones en que la denuncia se materializa, estos ilícitos se presenten emboscados entre casos de delitos tradicionales (estafa, robo, etc.), "ya que el concepto criminológico de criminalidad informática no aparece como tal en las estadísticas de las correspondientes Fiscalías Generales o Administraciones de Justicia de cada país, ni muchas veces en las de los cuerpos y fuerzas policiales o de investigación criminal"[19].

3.7.- Son delitos de creciente frecuencia, diversidad y peligrosidad:

El conjunto de características anteriormente expuestas en cierta medida explican el que se haya manifestado, hasta el momento, un creciente y progresivo aumento de la delincuencia informática, cuestión que parece no detenerse. A esto se suma el hecho de la vertiginosa celeridad con que se desarrollan los adelantos tecnológicos, y el que estén cada día más los

[19] Ibíd.., Pág. 91.

computadores al alcance de porciones mayores de población; todo esto, en conjunto, no sólo aumenta la cantidad de posibles ciberdelincuentes entre sujetos que se encontraren predispuestos a delinquir, sino que, además, incluso personas comunes y corrientes se ven a diario tentadas a cometer actos reñidos con la legalidad y, por tanto, a perpetrar delitos informáticos. Ocurre ello, por ejemplo, entre personas que si bien no pueden considerarse como delincuentes informáticos habituales, se ven tentados a conseguir el número de serie, o el crack para poder utilizar permanentemente aquel programa shareware que bajaron algún día por la utilidad que les prestaba y que, transcurrido el tiempo de prueba del mismo se ha vuelto inutilizable, pero respecto del que sólo basta bajar un archivo para que vuelva a ser plenamente funcional; disyuntiva a la que el sujeto se enfrenta habitualmente en la intimidad de su hogar o de su trabajo, sabiendo que difícilmente alguien lo vigila, y que, pese a ser al inicio casi un juego, al poco tiempo se transforma en una práctica habitual, dejando ese individuo de pagar para adquirir un software determinado pues sabe que sólo basta una conexión a Internet y saber donde buscar para hacerse con lo último en herramientas informáticas, con lo cual se transforma en un delincuente habitual que sabe que difícilmente será sancionado, ya que, como él, hay

millones en el mundo y los sistemas judiciales se encuentran impotentes frente a ellos.

3.8.- Ellos son habitualmente transfronterizos:

Esto viene dado principalmente a partir de la fuerte irrupción de Internet. "Es decir, como consecuencia de la posibilidad de distanciamiento espacial, y en virtud de las redes informáticas internacionales, el alejamiento entre el lugar donde se encuentra el autor de la acción, o donde ésta se realiza, y la del lugar donde va a producir sus efectos o consecuencias, aparece la superación de las barreras nacionales"[20].

4.- Clasificación de los Delitos Informáticos

Atendiendo a las diversas posiciones que se tomen sobre el carácter de los delitos informáticos, su naturaleza jurídica, bien jurídico protegido y al hecho de si se piensa o no en él como una tipología nueva de ilícitos con características que le son propias y que por tanto requieren de una regulación especial, es que se ha concebido una buena cantidad de

[20] Ibíd.., Pág. 99.

clasificaciones respecto de ellos. A continuación nosotros rescataremos aquellas que nos han parecido más relevantes para nuestro trabajo.

4.1.- Clasificación de TÉLLEZ VALDÉS

Este autor, en su obra "Derecho Informático"[21], realiza una clasificación de los delitos informáticos adoptando una diferenciación entre "lo informático" como instrumento medio y como objetivo o fin. De acuerdo a esto, distingue entre dos tipos de conductas:

a. Conductas criminógenas que utilizan a los computadores como método o medio en la comisión del delito, entre las cuales se pueden señalar: la falsificación de documentos por vía computarizada; la lectura, sustracción o copiado de información confidencial; el aprovechamiento indebido o violación de código para penetrar a un sistema introduciendo instrucciones inapropiadas; el acceso no autorizado; el uso no autorizado de programas computacionales, etc.

[21] TÉLLEZ VALDES, JULIO, Derecho Informático, Universidad Autónoma de México, México, 1987, Pág. 106.

b. Conductas criminógenas en que el computador, sus accesorios o programas como entidad física, son el objetivo o fin de ellas, entre las cuales se pueden mencionar: la destrucción de programas; el atentado físico contra la máquina o accesorios, secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje, etc.

4.2.- Clasificación de HUERTA Y LÍBANO

En la doctrina nacional, los autores HUERTA Y LÍBANO han elaborado una clasificación de los delitos informáticos basada fundamentalmente, como ellos advierten[22], en la experiencia del derecho comparado, y la cual sigue, en términos generales, la dada por SIEBER, la que a su vez sigue aquella que hiciera el jurista alemán LAMPE. Dicha clasificación agrupa a los delitos informáticos en las siguientes categorías:

a.- **Manipulación indebida de datos a través de la utilización de un sistema de tratamiento de la información. Fraude Informático.** Esta constituye la

[22] HUERTA MIRANDA, MARCELO Y LIBANO MANSSUR, CLAUDIO, Ob. Cit., Pág. 123.

forma más habitual de comisión de delitos informáticos, la cual puede ser caracterizada como "aquella impropia utilización de un sistema de tratamiento de datos, cuyo resultado se traduce en la desviación o alteración de la sana técnica informática, desnaturalizando los datos contenidos en el sistema, en cualquiera de las fases de su tratamiento, con o sin ánimo de lucro, y en perjuicio de terceros"[23].

b.- **Delitos de espionaje informático.** Los autores definen a estos ilícitos como "toda conducta típica, antijurídica y culpable que tiene por finalidad la violación de la reserva u obligación de secreto de la información contenida en un sistema de tratamiento de la información"[24], o dicho de otra forma, "aquel delito que consiste en obtener una información de forma no autorizada, sea por motivo de lucro o de simple curiosidad, hecho que implica espiar y procurarse una

[23] Ibíd.., Pág. 124.
[24] Ibíd.., Pág. 132

comunicación o bien una utilización de un sistema de tratamiento de la información en forma desleal, no autorizada"[25].

a. **Delitos de sabotaje informático.** Son definidos por los autores, desde la perspectiva del derecho comparado, como "toda conducta típica, antijurídica y culpable que atenta contra la integridad de un sistema de tratamiento de información o de sus partes componentes, su funcionamiento o de los datos contenidos en él"[26]. Se dividen en delitos de destrucción de los elementos físicos del sistema y delitos de destrucción de los elementos lógicos del sistema.

b. **Delitos de piratería de programas.** En este caso se trata de delitos informáticos en los cuales "el sujeto activo se aboca a la tarea de reproducir, plagiar, distribuir, comunicar, transformar, y/o exportar o importar material software, sin estar autorizado para

[25] Ibíd.., Pág. 132-133
[26] Ibíd.., Pág. 139.

ello, con o sin ánimo de lucro, a través de un sistema de tratamiento de la información, y en perjuicio del legítimo derecho de la persona natural o jurídica, o grupos de personas naturales o jurídicas ligadas por un contrato de colaboración, fabricantes del software"[27].

c. **El delito de hacking o acceso no autorizado a sistemas informáticos en sus diversas manifestaciones.** De acuerdo a los autores, el delito informático de hacking consiste en acceder de manera indebida , sin autorización o contra derecho a un sistema de tratamiento de la información. En virtud de las motivaciones que llevan al sujeto activo a realizar dicho ilícito, este delito puede dividirse en: hacking directo o propiamente dicho, en el cual la única motivación del autor es lograr una satisfacción de carácter intelectual por haber logrado burlar un sistema de seguridad o por mera diversión; y hacking como medio de comisión de

[27] Ibíd.. Pág. 156.

otros delitos, como fraude, sabotaje, piratería o espionaje.

4.3.- Clasificación de RAINER RAPP

Este autor nacional, en su Memoria de Prueba antes citada, divide a los delitos informáticos en las siguientes categorías:

a. **Fraude informático:** es decir, "la manipulación fraudulenta de un sistema de tratamiento de la información, realizada con ánimo de lucro y en perjuicio de un tercero, por medio de la alteración de datos que maneja dicho sistema en cualquiera de sus tres fases: introducción de datos, procesamiento y salida de los mismos"[28].
b. **Sabotaje informático:** el cual es definido como la "destrucción o inutilización dolosa del hardware o equipo computacional propiamente tal, o la destrucción o inutilización dolosa del software"[29].

[28] RAPP ORTEGA, RAINER, Ob. Cit. Pág. 160
[29] Ibíd..

c. **Espionaje informático:** consistente en "el acceso y/o obtención dolosa de datos u información de acceso reservado almacenada en un sistema de tratamiento automatizado de la información"[30].

d. **Delito de acceso no autorizado:** el cual se refiere a la "acción de acceder dolosamente, sin autorización, a un sistema de tratamiento automatizado de la información, sin producir daño a los datos o información contenidos en éste"[31]. En término generales, dentro de esta categoría se encontraría contemplado, como veremos, el fenómeno del hacking.

e. **Falsificación de documentos informatizados:** En este caso el autor se refiere a la "acción consistente en falsificar, con intención de causar un perjuicio a un tercero, documentos informatizados, esto es, de documentos, sin materialidad palpable, que se

[30] Ibíd.., Pág. 161
[31] Ibíd..

encuentren archivados electrónicamente en un sistema de tratamiento automatizado de la información"[32].

f. **Delito de piratería informática:** el cual, según definición dada por este autor, consiste en la acción de "utilizar, reproducir, plagiar, transformar, distribuir, comercializar, importar o exportar, sin autorización, con o sin ánimo de lucro y en perjuicio de un tercero, por medio de un sistema de tratamiento automatizado de la información, todo o parte de un software o programa computacional"[33].

4.4.- Clasificación de ENRIQUE ROVIRA

El autor español ENRIQUE ROVIRA, previo a entregarnos su clasificación respecto de los delitos informáticos, señala que es menester distinguir en esta materia entre tres grupos de ilícitos, atendiendo a si atentan o no efectivamente en contra de uno de los bienes jurídicos protegidos por el Derecho Penal Global del Riesgo Informático. Tenemos

[32] Ibíd..
[33] Ibíd.., Pág. 162

entonces que a su parecer es posible distinguir entre los siguientes ámbitos de delitos vinculados con la informática:

1) Delitos no informáticos vinculados a la informática, los cuales define como "comportamientos delictivos que recaen sobre elementos físicos informáticos (hardware), o que utilizándose medios o sistemas informáticos o telemáticos para su comisión no tiene afectación alguna la información en sí misma, los datos o tales medios o sistemas, siendo objeto de ataque y quebranto exclusivamente un bien jurídico tradicional"[34]. En este caso, a juicio de Rovira, no nos encontraríamos en presencia de delitos informáticos en sentido estricto, y por tanto no deben ser ellos objeto de estudio por parte del Derecho Penal Global de Riesgo Informático y de la Información, sino que deben ser tratados como parte de las figuras delictivas tradicionales.

2) Delitos informáticos impropios, los cuales son caracterizados como "comportamientos delictivos en los

[34] ROVIRA DEL CANTO, ENRIQUE, Ob. Cit. Pág. 130.

que la utilización de los sistemas y medios informáticos y de telecomunicaciones suponen además de un quebranto o peligro a un bien jurídico tradicional, una afectación de la información en sí misma, directamente, o de forma indirecta al quebrantarse la fiabilidad y seguridad de su medio de representación o de los sistemas para su procesamiento y/o trascendencia."[35] Estos ilícitos sí los considera Rovira como objeto de estudio para el Derecho Penal Global del Riesgo Informático y de la Información, por cuanto poseen un carácter pluriofensivo en el que, si bien no es la información el principal bien jurídico vulnerado, por las características que los individualizan se hace necesario un tratamiento jurídico diferenciado, que vaya más allá de las correlativas figuras delictivas clásicas.

3) Delitos informáticos propios, los cuales son "comportamientos delictivos, cualquiera que sea el medio o mecanismo utilizado, en los que resulta afectada la

[35] Ibíd.., Pág. 131.

información y los datos informáticos en sí mismos, como nuevos bienes o valores jurídicos principalmente protegidos, sin perjuicio de la presencia de otros bienes jurídicos tradicionales merecedores de protección conjunta, pero siempre de forma secundaria o de menor importancia". Son estos delitos los que constituyen el objeto específico del Derecho Penal Global del Riesgo Informático y de la Información.

Una vez realizada esta primera división, ROVIRA nos señala que tratándose de los delitos informáticos propios e impropios, los únicos que, a su entender, son relevantes para el Derecho Penal Global del Riesgo Informático y de la Información, pueden ellos a su vez ser divididos en cuatro grandes áreas de ilícitos:

a. **Infracciones a la Intimidad y Privacidad**, entre las cuales es posible a su vez encontrar: Infracciones de los derechos sustantivos de la intimidad, como el descubrimiento, difusión, obtención o acceso de forma ilegal a datos personales, su uso ilícito, la entrada modificación ilegal y/o falsificación de éstos con la

intención de causar un perjuicio, etc.; Infracciones de los requisitos formales legales impuestos por las autoridades administrativas supervisoras de las actividades informáticas o telemáticas, o por disposiciones civiles o administrativas; Infracciones de los derechos de acceso a la información o a la libertad de información, como dar información falsa o negar información a la que se tiene derecho; y Negligencia en la adopción de medidas de seguridad informática.

b. **Ilícitos en el ámbito económico**, entre los cuales se comprenden: el acceso informático ilegal o hacking; el espionaje informático; la piratería de software y otras formas de piratería de productos; el sabotaje informático y la extorsión informática; y el fraude informático.

c. **Ilícitos de comunicación telemática, o de emisión y difusión de contenidos ilegales y nocivos**, como la pornografía infantil, instrucciones para confeccionar bombas, producir drogas ilegales, pirateo de tarjetas de

crédito, difusión no autorizada de obras protegidas por el derecho de autor, etc.

d. Otros ilícitos.

5.- Sujetos Activo y Pasivo en los Delitos Informáticos

5.1.- El Sujeto Activo:

La caracterización del delincuente perpetrador de delitos informáticos sin duda es una cuestión compleja, como la mayoría de las que tienen que ver con el derecho penal informático. Tradicionalmente dentro de las teorías criminológicas se ha venido a considerar al delincuente como un marginado social, habitualmente perteneciente a los estratos más bajos de la comunidad que, por diversas razones, se ve impelido a cometer actos delictivos, habitualmente como forma de subsistencia. No obstante ello, también en el área de los delitos tradicionales, ya desde antiguo se ha caracterizado a un tipo de criminal que, por el nivel social o de educación que posee y por la forma y el tipo de ilícitos que comete escapa a esta caracterización tradicional, denominándoseles normalmente como delincuentes de "cuello blanco", los cuales se dedican especialmente a la comisión de delitos vinculados al área económica, como las estafas, los

fraudes tributarios, etc. Ahora bien, tratándose de los delitos informáticos, también nos encontramos frente a una tipología de sujeto que, en cierta medida, escapa a los cánones tradicionales.

Por una parte, en este caso nos topamos con sujetos que, debido a las necesidades propias del entorno informático, pertenecen a los niveles medios o altos del escalafón social, los cuales, deberán poseer, además, conocimientos bastante avanzados de informática.

Por su parte, la Dra. MARÍA JOSÉ VIEGA RODRÍGUEZ agrega a lo anterior que en este caso los delincuentes pueden "ocupar lugares estratégicos en su trabajo, en los cuales se maneja información de carácter sensible (se los ha denominado delitos ocupacionales ya que se cometen por la ocupación que se tiene y el acceso al sistema)"[36].

No obstante que las anteriores premisas pueden ser válidas en la mayoría de los delitos, creemos que es desconocer la realidad actual de la delincuencia informática el restringir la tipología de estos delincuentes a sólo personas pertenecientes a determinado rango educacional o social. Como señala ROVIRA DEL CANTO, "en la actualidad la caracterización

---

[36] VIEGA RODRÍGUEZ, MARÍA JOSÉ, Delitos Informáticos, Revista Electrónica de DerechoInformático,Nº9,http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107138

del sujeto activo del delito de riesgo informático y de la información ha evolucionado hasta tal punto que *cualquiera puede tener la condición potencial de serlo, tanto una persona física, como una persona jurídica a través de sus órganos, como entidades, agrupaciones, grupos del crimen organizado, agencias gubernamentales o los servicios de espionaje de un Estado*, con lo que desde este punto de vista, la formulación de tipos delictivos debe tener presente tal diversidad y la imposibilidad de otorgar ubicar en base a ello al sujeto activo en una de las categorías tradicionales de delincuentes, sino en una *nueva categoría sui generis, en donde la personalidad del mismo no es ningún factor determinante, pero sí sus móviles.*"[37]

En efecto, hoy en día debido a lo masificado del uso de los sistemas computacionales, en particular de los computadores personales, y al acceso cada vez más expedito a formas de comunicación en red, como Internet, cualquier persona puede transformarse potencialmente en un delincuente informático. No se necesitan más que unos cuantos conocimientos básicos, que van desde saber encender un PC hasta instalar un simple programa,

[37] ROVIRA DEL CANTO, ENRIQUE, Ob. Cit., Pág. 108.

para estar ya en un mundo virtual que ofrece posibilidades delictuales insospechadas.

Cualquiera que necesite un programa como, por ejemplo, el Winzip, el compresor más famoso del mercado, el cual es muy útil y hasta imprescindible para navegar por sitios que ofrecen descargas de productos, sean estos libros, programas, juegos, fondos de escritorio, utilidades, etc., no tiene que hacer otra cosa que ir al sitio oficial de los desarrolladores del software y "bajarlo" a su computador. Habitualmente programas como estos le ofrecen a los navegantes la posibilidad de descargarlos gratuitamente con el objeto de que éste los pruebe y cree una necesidad de ellos, real o ficticia, ya que si hay algo cierto en Internet es el consumismo compulsivo de los navegantes por descargar cosas desde los más diversos sitios. Ahora bien, estos programas de evaluación, técnicamente llamados shareware, habitualmente tienen una limitación temporal, 7, 15 o 30 días, período al termino del cual éste se vuelve inútil. Ahora bien, ¿qué ocurre con aquella persona que ha descargado el programa, lo ha usado, le ha gustado, le ha servido, al término de dicho período?, pues habitualmente tendrá que comprarlo o encontrar otro que cumpla similares funciones y que sea gratuito, lo que no siempre es posible hallar. Sin embargo, puede ocurrir

que navegando por Internet, se encuentre con algún sitio en el cual, sin pedirle nada a cambio le ofrezcan un número de serie que puede ser utilizado para registrar el programa y que éste vuelva a ser totalmente funcional. No estamos hablando aquí ni de un experto en informática, ni de un programador, ni de un ingeniero en computación, estamos simplemente hablando de una persona inexperta, que tal vez lleve sólo unos meses descubriendo el mundo virtual de la red. Esa persona puede optar por probar el serial que le ofrecen, tal vez por simple curiosidad, a ver si funciona, y de pronto constata que el ofrecimiento que le hacían era totalmente real, y que el software en cuestión se ha transformado en completamente funcional. Pues esa persona, tal vez sin quererlo está cometiendo un delito, pues está infringiendo el derecho de propiedad intelectual que acompañaba a la aplicación y que pretendía ser salvaguardado con la incorporación de un sistema de password. Cuestiones como ésta, que pueden parecer tan burdas, ocurren a diario en la red. De hecho el caso no lo hemos inventado, sino que le ocurrió exactamente como lo hemos relatado a una persona que conocemos, quien cuenta que, desde ese día, no ha vuelto a pagar por aplicación alguna de las que va necesitando en su viaje por la red.

Incluso, si no se sabe bien cómo conseguir aplicaciones que son más complejas, y en donde ya se hace más difícil el encontrar las herramientas para vulnerar los sistemas de seguridad de ellas, como ocurriría con sistemas operativos como Windows[38], o programas altamente sofisticados como los que ofrecen empresas como Adobe[39] o Macromedia[40], siempre le queda al usuario interesado la opción de comprar en las calles del centro de nuestra ciudad o en sectores especializados en la venta de software "pirata" las aplicaciones que necesita, por valores que en ocasiones no alcanzan ni al 1% de su valor real. Y en este caso, al igual que en el anterior, también el usuario lego se transforma, consciente o inconscientemente, en un delincuente informático, pues lo es no sólo quien distribuye ilegalmente un programa, sino también quien lo adquiere y usa.

---

[38] Windows es el sistema operativo más famoso y utilizado del mercado perteneciente a la empresa Microsoft, http://www.microsoft.com

[39] Adobe es una empresa que ha desarrollado una amplia gama de herramientas de diseño y multimedia, entre las que destacan Adobe Photoshop, el más potente editor de imágenes del mercado, Adobe PageMaker, herramienta imprescindible dentro del campo de la publicidad y Adobe Acrobat, software utilizado para crear documentos PDF, el formato más usado para crear ebooks. http://www.adobe.com

[40] Macromedia es una empresa especializada en el ámbito del diseño web, con productos muy potentes como Dreamweaver, especial para crear páginas web de alta calidad y Fireworks, utilidad para editar imágenes para la web. http://www.macromedia.com

5.2.- El Sujeto Pasivo

Respecto del sujeto pasivo en los delitos informáticos, es decir, del titular del bien jurídico protegido por el ordenamiento jurídico[41], lo es toda persona, natural o jurídica, pública o privada, que posea un sistema automatizado de tratamiento de la información y que vea amenazados o transgredidos sus derechos informáticos debido al uso ilícito de sistemas computacionales.

En este caso, como señalamos anteriormente, los delitos informáticos pueden afectar tanto a personas individuales, como a grupos o a los usuarios todos que tengan un sistema al cual es posible acceder remotamente o que pertenece a una red, sea de Intranet o de Internet, como sucede por ejemplo en el caso del uso de virus computacionales difundidos a nivel global.

Ahora bien, aún cuando potencialmente cualquier acto ilícito realizado por medios informáticos puede llegar a constituirse en delito informático, coincidentes con lo hasta ahora expresado tenemos que concluir que para que una persona sea considerada sujeto pasivo de un delito informático, además de haber sido atacada a través de un mecanismo

computacional, también el bien jurídico que en este caso se ha agredido debe estar constituido por aquel que hemos caracterizado como propio y distintivo en este tipo de ilícitos, es decir, la información y los datos informáticos en si mismos, aun cuando con el ataque también puedan verse vulnerados otros bienes jurídicos de carácter tradicional.

Respecto de los ámbitos en que este sujeto puede ver vulnerados sus derechos informáticos, como veremos más adelante ellos son variados, no existiendo otra limitante que los medios usados para perpetrar el acto y el bien jurídico que se afecta en cada caso. Es así que con un ataque o delito informático se puede ver afectada la intimidad, la imagen, el honor, la propiedad civil, la propiedad privada, el orden público, la seguridad interior del Estado, etc.

---

[41] El que en modo alguno debe ser confundido con el sujeto perjudicado, pese a que en una gran cantidad de casos sean la misma persona

III. Delitos Informáticos e Internet

De acuerdo al séptimo Informe sobre Seguridad y Delitos Informáticos, del año 2002, elaborado por el FBI y el Instituto de Seguridad en Computadoras (CSI)[42], entidad norteamericana abocada al tratamiento de este tema, el 90% de las empresas encuestadas detectó agujeros de seguridad, al tiempo que el 80% registró pérdidas económicas por este motivo, elevándose el monto por las pérdidas a la no despreciable suma de US 455,848,000. Según la respuesta de 41 participantes, el robo de información confidencial fue el que más impacto tuvo –170.827.000 dólares–, seguido del fraude financiero –115.753.000 dólares–. En opinión del 74% de los entrevistados la conexión a Internet se situó como la principal vía empleada para llevar a cabo los ataques, mientras que el 33% considera que los de origen interno fueron más frecuentes.

Como podemos observar, debido a la masificación del uso de Internet y a que ésta es cada vez más imprescindible como herramienta dentro del mundo de los negocios, es que también la importancia que esta adquiere como medio adecuado para cometer determinados delitos se transforma día

a día en una cuestión preocupante, existiendo un sin fin de ilícitos que la requieren necesariamente para poder ser perpetrados.

Pero ¿qué es Internet? A continuación intentaremos responder de un modo sencillo a esta pregunta, pese a que el tema en sí es considerablemente técnico y complejo.

1.- Internet

Aunque los orígenes de Internet se remontan hasta la década de los '50, cuando el presidente norteamericano Dwight Einsenhower ordenó la creación del proyecto ARPA (Agencia de Proyectos Avanzados de Investigación), con el objeto de hacer frente a la avanzada tecnológica soviética que había logrado colocar el primer satélite en órbita, el Sputnik, no es sino hasta 1962, con la llegada del psicólogo e informático J.C.R. Licklider a dicho proyecto que puede hablarse más propiamente del nacimiento de lo que hoy conocemos como Internet. Licklieder "creía que los ordenadores se podrían utilizar para aumentar el pensamiento humano y sugirió que fuera establecida una red de ordenadores para permitir a los investigadores de ARPA comunicar información con los otros de modo

eficiente"[43] Él concebía una red interconectada a través de la cual cada persona pudiera acceder desde cualquier sitio a programas, datos, etc., y aunque nunca pudo materializar su idea mientras trabajó en ARPA, cuando dejó esta institución en 1964, su idea se mantuvo presente, siendo ella la que finalmente daría origen a la llamada ARPANET.

Es en 1965 que se logra realizar la primera red interconectada de ordenadores mediante el enlace, a través de una línea telefónica, entre un computador TX2, ubicado en Massachussets, con un Q-32 que se encontraba en California. Dicha prueba estuvo a cargo del investigador Lawrence G. Roberts, quien en 1966 se trasladó a trabajar a DARPA, en donde se avocó a desarrollar el concepto de red de ordenadores y a confeccionar su plan para ARPANET, el cual publico en 1967. Paralelamente a esto, ya desde 1961 se venía desarrollando un concepto que habría de ser vital en el posterior desarrollo de ARPANET, esto es, el de la conmutación de paquetes, cuyo primer desarrollador fue Leonard Kleinrock, y que básicamente consiste en dividir la información en pequeños paquetes cada uno de los cuales contenía la dirección desde donde

[43] Historia de Internet, en el sitio Entender Internet: http://internet.fiestras.com

era enviado, la dirección de destino, el número de secuencia y una cierta parte de la información. Al llegar a su destino, dicho paquete se ordenaba en base al número de secuencia de cada uno y se juntaban para volver a reconstruir la información originalmente enviada.

Al cabo del tiempo, y utilizando el mismo método creado por Kleinrock, se fueron uniendo de este modo varios ordenadores con lo cual se creó la llamada ARPANET, la cual poco a poco fue extendiéndose por todo el territorio de EE.UU. Hará unos 15 años se conectaron las instituciones públicas como las Universidades y también algunas personas desde sus casas. Fue entonces cuando se empezó a extender Internet por los demás países del Mundo, abriendo un canal de comunicaciones entre Europa y EE.UU.

Pero, ¿qué es en los hechos Internet?

Como anteriormente dijimos, desde hace ya muchos años uno de los métodos utilizados con el objeto de, por ejemplo, centralizar o transmitir información entre distintos ordenadores para así facilitar y hacer más eficiente el trabajo en una empresa, oficina, organismo público, etc., es el de unir varios computadores a través de una red de área local (LAN). Y, en términos generales, esto es Internet, muchos computadores personales

unidos mediante una network para intercambiar información, archivos, documentos de usuario, etc. Sin embargo, el decir esto no nos hace aclarar, ni cercanamente, lo que realmente Internet significa hoy en día. Internet no son sólo computadores unidos en red, sino que Internet es la llamada "red de redes", pues por medio de ella no son cientos, ni miles, sino millones los ordenadores enlazados a través de todo el mundo, cifra que día a día va aumentando en cantidad y en la importancia de la información compartida. Como señala JOSÉ DANIEL SÁNCHEZ NAVARRO en su libro "El Camino fácil a Internet", es ésta "Una gran comunidad de las que forman parte personas de todo el mundo, que usan sus computadoras para interactuar unas con otras, y con la posibilidad de obtener información".[44]

Ahora bien, para lograr lo anterior, ha sido menester la creación de un mismo lenguaje o protocolo a utilizar entre los distintos computadores para que el enlace y el intercambio de la información sea posible, destacando, de entre los múltiples lenguajes hoy en día disponibles el llamado TCP/IP, el que es estándar y no pertenece a ningún fabricante en particular.

---

[44] Franklin Sandoval, "Internet el arte de romper paradigmas". Disponible en Monografias.com (http://www.monografías.com)

El TCP/IP es la sigla identificadora de “Transfer Control Protocol / Internet Protocol”, que engloba en sí dos elementos:

a) **El Protocolo IP:** define una red de conmutación de paquetes donde la información que se quiere transmitir está fragmentada en pequeñas porciones. Cuando un ordenador quiere mandar a otro un fichero de datos, lo primero que hace es partirlo en trozos pequeños (alrededor de unos 4 Kb) y posteriormente envía cada trozo por separado. Cada paquete de información contiene la dirección IP donde ha de llegar, y también la dirección de remitente, por si hay que recibir contestación. Una dirección IP es un número de identificación único de la computadora tal como es reconocida por las demás computadoras en Internet. Las direcciones IP constan de cuatro números de 32 bits separados por puntos, sin embargo, dichos números no es menester colocarlos cada vez que queramos acceder a Internet, puesto que sería muy complicado que recordáramos todos y cada uno de ellos, ya sea el nuestro o el de cada uno de los computadores (también llamados host) a que queramos conectarnos. Para facilitar esta tarea, la dirección

IP asignada al lugar en que estemos buscando la información (servidor) es traducida en un "dominio" (DNS) que representa el nombre para un host determinado, el cual va asociado a una dirección IP concreta y a una URL (Localizador Uniforme de Recursos) que es el método estándar empleado para especificar la ubicación de los recursos de Internet. Por su parte, en el caso del "cliente" (es decir de nuestro computador), a él le será asignada automáticamente una IP cada vez que se conecte a Internet, siendo ella distinta en cada ocasión (para el caso de conexión vía modem) o permanente (en el caso de otros medios como el cable o el ADSL). Cada computador puede tener una, y sólo una, dirección IP. La característica principal de los paquetes IP es que pueden utilizar cualquier medio y tecnología de transporte. Los equipos que conectan las diferentes redes y deciden por donde es mejor enviar un paquete según el destino, son los routers o direccionadores.

b) **El Protocolo TCP:** Es éste el encargado de subsanar las deficiencias en la llegada de los paquetes de información a su destino, para conseguir un servicio de transporte fiable. El

protocolo de control de transmisión define la manera en que la información será separada en paquetes y enviada a través de Internet, se asegura también de que cada paquete sé recombine en el orden correcto y también los revisa para localizar posibles errores en la transmisión.

Quizá ahora quede un poco más claro por qué se dice que Internet es la red de redes: miles de redes de computadoras en todo el mundo, interconectadas a través de diferentes medios físicos de transmisión, todas utilizando el protocolo de comunicación TCP/IP.

Tenemos entonces, que una de las mayores características de Internet es el hecho de que día a día, minuto a minuto, existen millones de usuarios conectados a esta gran red, por medio de la cual se intercambian contenidos, mensajes, archivos, conocimientos e información de todo tipo. Tal vez este vertiginoso proceso de globalización en el que el mundo se ha visto envuelto estos últimos años no habría sido posible, al menos en su actual magnitud, sin la existencia de este impresionante medio de comunicación. En la antigüedad, cuando alguien quería saber algo de lo que ocurría en alguna otra parte del mundo, muchas veces debía esperar días, semanas y hasta años para acceder a alguien que contara la historia (como en la edad

media hacían los trovadores), o para poder adquirir diarios, revistas o libros que dieran cuenta del devenir de la humanidad. No hace mucho tiempo (e incluso hoy mismo), era difícil encontrar en buena parte de las capitales del mundo periódicos provenientes de otras latitudes, los cuales, generalmente, sólo daban cuenta de noticias ya atrasadas por lo difícil que era su circulación (y para que hablar del caso de ciudades más pequeñas, principalmente provenientes de países del tercer mundo, en las cuales las noticias llegaban con un retraso quizá difícil de dimensionar en la actual circunstancia histórica. La situación de muchos ciudadanos del mundo era casi como aquella que Emir Kusturica grafica en su película Underground, en la cual el protagonista sólo se entera del término de la Segunda Guerra Mundial muchos años después de que ella haya ocurrido al estar absolutamente aislado del resto de la humanidad).

Sin duda la televisión vino en cierta medida a remediar este escenario, haciendo mucho mas asequible la información a las masas, aunque en este caso dicho medio tiene una gran limitante, cual es la de que en él sólo es factible enterarse de los acontecimientos más relevantes y con un sesgo muy marcado y determinado por los intereses que dicta el mercado y los de las grandes cadenas informativas. Cuestión distinta ocurre quizá

con la radio, la cual también tiene la característica de la variedad y la instantaneidad de la información, aunque presenta la dificultad de que pierde mucha riqueza al ser solamente un medio "auditivo", en un mundo en que nos hemos acostumbrado mucho más a ver que a escuchar.

Internet ha venido a representar una verdadera revolución en todo lo que a temas comunicacionales se refiere, poniendo a disposición de cualquiera que cuente con un ordenador y una conexión a la red de una inconmensurable gama de recursos que abarcan los más diversos temas, pudiendo hallar en esta gran autopista desde la noticia, casi instantánea, de lo que está ocurriendo en cualquier punto del orbe, hasta el ensayo, el poema, o la obra del más oscuro de los autores que desee dar a conocer al mundo su creación. Lo que antes demandaba horas y horas de exhaustiva investigación en bibliotecas o centros de estudio hoy está, sabiendo buscar, casi al alcance de la mano, o más bien a sólo unos clicks de ratón. En Internet el desarrollo de los acontecimientos es vertiginoso, y muchas veces caótico, pudiendo representar casi un verdadero monstruo de infinitas cabezas para el navegante inexperto, que al intentar buscar el dato más sencillo se encuentra con cúmulos y cúmulos de información que a veces emborracha el entendimiento, al no saber por donde empezar a revisar o

cual será el sitio más confiable y seguro desde el cual extraer los datos requeridos. Por ejemplo, buscando algo tan simple como la biografía de Pablo Picasso, el internauta se encuentra con más de cinco mil referencias a las cuales puede acceder, y ello sólo ingresando un par de palabras clave en uno de los motores de búsqueda más conocidos como es Google[45].

Ahora bien, el hecho de que Internet sea una verdadera autopista de la información en ningún caso significa que lo que ella nos ofrece sea siempre de una calidad óptima. Quizá uno de los principales inconvenientes que presenta Internet, es el hecho de que muchos de los datos que en ella podemos encontrar son a veces muy fragmentarios, privilegiándose con mucho la presentación gráfica por sobre los contenidos de peso, profundos, realmente documentados. Por el momento Internet, en su mayoría, es el acceso a la información rápida, escueta, de entrada, por lo cual aún no representa un verdadero peligro a los contenidos impresos, los cuales, con mucho permiten abordar los temas desde diferentes ópticas, con un desarrollo acabado y de mucho más cómodo análisis, pues quizá otro de los grandes problemas de Internet, es el hecho de que muchas veces es muy

[45] http://www.google.com

fatigoso el tener que pasar horas y horas frente a una pantalla con el objeto de obtener la información requerida, pues los avances tecnológicos aún no permiten el desarrollo de un interfaz de usuario lo suficientemente cómodo como para no tener que recurrir, imperiosamente, a la impresión del material hallado para poder consultarlo off line y de una forma mucho más cómoda y menos dañina para nuestros sentidos.

Se suma al anterior inconveniente, el hecho de que Internet es, todavía, y sobre todo para los países en desarrollo, un medio muy elitista al cual sólo tienen acceso segmentos limitados de la población, por lo caro que resulta aún tanto la adquisición de equipos como los servicios de conexión. Situación, en todo caso, que ha ido variando con el paso de los años. Además, como generalmente ocurre con los adelantos tecnológicos de punta, ésta presenta un fuerte rechazo entre muchos sectores, que aún no se acostumbran a la utilización de un medio que recién comienza a escribir su historia.

2.- Internet y el derecho

Más allá de las innegables bondades que conlleva Internet, la cual ha facilitado en muchos aspectos la vida de millares de personas, es un hecho

que ella presenta, en cuanto fenómeno relativamente nuevo, también un sinnúmero de desafíos a la ciencia jurídica. La expansión de Internet, a la que hemos hecho reiteradamente mención, en cierto sentido es, además de vertiginosa, caótica.

En 1996 se calculaba en 61 millones las personas en el mundo que hacían uso de este servicio, aumentando la cifra a 147 millones en 1998 y a 407.1 millones en el año 2000, es decir, en apenas cuatro años se había más que sextuplicado el número de usuarios, y las cifras han seguido aumentando. Dicha situación se entiende, entre otros factores, por la baja en el costo tanto de los equipos como de los sistemas de conexión, y por la necesidad cada vez mayor que tienen los sujetos de hacer uso de este sistema de comunicación..

Como señala ESTHER MORON, "Todas las ventajas ofrecidas por los ordenadores (su alta velocidad, su bajo coste por operación unitaria, su inagotable precisión y la variedad de trabajos para los que se les puede programar) se multiplican cuando se produce la denominada «explosión o eclosión informática». Hasta la década de los setenta, la informática era cara, poco eficiente y se circunscribía a un número restringido de usuarios (fundamentalmente, empresas) y de funciones. Se trataba de una

informática de élites. No obstante, comienza entonces un período de expansión del fenómeno informático, favorecido y caracterizado por unos ordenadores cada vez más pequeños y económicos, conectados entre sí por medio de redes. Se ha consolidado la transición a una informática de masas, que ha invadido a toda la sociedad, como en su tiempo lo hiciera la electricidad, con la diferencia de que, la telemática no transmite una corriente inerte, sino información, esto es poder"[46].

Por su parte, desde el punto de vista jurídico penal, este aumento en el uso y la difusión de Internet ha traído aparejado el desafío tanto para legisladores, como para los interpretes de la ley, de crear las bases de un sistema jurídico moderno que sea capaz de dar respuestas a las nuevas particularidades del entorno tecnológico, ya sea adecuando las normas tradicionales existentes o creando unas nuevas, especiales para esta nueva realidad.

Internet ha servido de medio para que se produzca una diversificación de la actividad delictual impensada hasta hace algunos años, lo cual se hace

[46] MORON, ESTHER, Ob. Cit., Págs. 83-84.

más patente, según señala JUAN LÖPEZ MORENO[47], fundamentalmente, en seis ámbitos:

a. En el ámbito de la intimidad, la imagen y el honor de las personas, particularmente a través de la posibilidad que existe de que los datos personales, almacenados hoy en día en múltiples bases de datos, puedan ser utilizadas por terceros que no tienen legítimo derecho a ellos, o para fines distintos de los originalmente previstos.
b. En el ámbito de la libertad sexual, puesto que Internet se ha transformado en el vehículo idóneo para la proliferación de un conjunto de conductas bastante más restringidas y controladas en el entorno no virtual, como son la pornografía infantil, actos sexuales violentos o forzados, prostitución, pederastia, etc.
c. En el ámbito de la propiedad intelectual e industrial, por cuanto Internet es hoy en día uno de los vehículos más idóneos para traficar con obras protegidas de los más

[47] LOPEZ MORENO, JUAN, Comunicación, La World Wide Web como Vehículo de Delincuencia: Supuestos Frecuentes. En "Internet y Derecho Penal", Varios Autores. Escuela

diversos tipos, los que van desde softwares y otras creaciones propiamente informáticas, hasta música, obras literarias, científicas, etc.

d. En el ámbito del orden público y la seguridad interior de los Estados, los cuales son atacados a través de la difusión incontrolada de ideas métodos o doctrinas terroristas o de grupos violentistas, o racistas, o de espionaje entre países, etc. De hecho, se dice que Internet cumplió también una función importante durante la preparación de los atentados a las torres gemelas de Nueva York, por cuanto quienes habrían preparado este acto utilizaron Internet como medio de comunicación y coordinación entre ellos.

e. En el ámbito de las defraudaciones a la hacienda pública, en cuanto existen páginas web que permiten efectuar transacciones comerciales que eluden el pago de impuestos, mediante el ocultamiento o no identificación del lugar físico en que se realizan. Además, muchas de las empresas existentes en Internet, al no tener existencia

material, sino meramente virtual, son muy difíciles de fiscalizar. Cualquier persona puede comenzar una venta de productos vía Internet y no pagar por ello ninguna de las cargas impositivas que en dichos casos serían aplicables al tratarse de una empresa o negocio tradicional, como podría ser el IVA.

f. Finalmente, también en el ámbito comercial Internet se presenta como un medio adecuado para cometer actos ilícitos, fundamentalmente debido al desarrollo del comercio electrónico, lo cual ha traído aparejado un aumento y una diversificación en delitos hoy tan extendidos como el fraude o la estafa mediante sistemas informáticos.

Ahora bien, es necesario hacer notar que la anterior enumeración de ámbitos en los cuales Internet presenta desafíos al derecho sancionatorio en modo alguno puede entenderse como taxativa, puesto que las posibilidades que otorga este medio para quienes tienen el objetivo de burlar la ley son prácticamente ilimitadas, expandiéndose con la misma velocidad con la que el uso de Internet lo hace. Sin embargo, siguiendo la línea de la tesis

acogida en este trabajo, nosotros pensamos que no deben mezclarse dentro de la órbita del derecho penal informático o del riesgo informático, elementos que en general no le son propios. Para muchas premisas y actos delictivos cometidos en el ámbito informático el derecho penal tradicional ya cuenta con las herramientas necesarias para llevar adelante su persecución o es menester sólo una adecuación de las mismas para que ello sea posible, por cuanto los sistemas informáticos en este caso no atacan al bien jurídico especial que debe proteger el derecho penal del riesgo informático, sino que sólo vulnera bienes jurídicos tradicionales, los cuales son atacados utilizando otros medios, distintos a los conocidos tradicionalmente, esto es, medios informáticos.

Hemos dicho que el bien jurídico que especialmente debe proteger el derecho penal del riesgo informático es la información en sí misma, o bien a los datos programas, sistemas o redes informáticos y de telecomunicaciones, en cuanto sean susceptibles de afectar a ella, a su seguridad y al pacífico uso que de ésta puede hacerse, teniendo en este caso el bien jurídico que el derecho penal del riesgo informático protege un carácter pluriofensivo, ya que aunque pueden existir otros bienes jurídicos tradicionales vulnerados es la información lo que le da su tinte

identificatorio. Además, su naturaleza debe ser considerada como la de un delito de riesgo abstracto, por cuanto no sólo deben ser sancionados los resultados dañinos que de la conducta se pudieren derivar, sino también los actos que ponen en riesgo, grave y serio, a este nuevo bien jurídico. Como veremos más adelante, esta cuestión cobra vital importancia sobre todo tratándose de las conductas llamadas de "hacking blanco", por cuanto en ellas habitualmente no existe un daño efectivo para el sujeto pasivo, sino sólo una situación de riesgo, la cual, pensamos, que también debe ser sancionada.

3.- La dificultad de sancionar los actos ilícitos cometidos a través de Internet

Un aspecto que caracteriza a Internet, desde el punto de vista del derecho informático sancionatorio, es el que dice relación con la gran dificultad que existe, tanto para descubrir, como perseguir y sancionar a quienes cometen actos ilícitos a través de la red.

Hasta el momento, Internet carece de organismos efectivos que controlen lo que sucede en ella. Si bien esto es una virtud, defendida sobre todo por aquellos que abogan por los llamados Derechos del Ciberespacio,

quienes se niegan a que existan organismos censores que puedan dictaminar lo que puede y no hacerse en esta infopista, es un hecho de que ello también se transforma en un problema, puesto que el grado de excesiva libertad ha traído aparejado justamente el que este importante medio se utilice para la realización de las actividades delictivas más variadas, sin que sea posible controlarlas de manera efectiva. Es así que organizaciones del tipo terrorista o que trafican sexualmente con niños, pueden moverse por la red casi sin problemas.

Como señala LOPEZ MORENO, "La gran virtud de Internet, que es su independencia de los núcleos ordinarios de poder, se convierte en uno de sus mayores defectos: Internet es un proyectil muchas veces incontrolado, y su gran capacidad de comunicación le convierte en un gran peligro y en un gran foco, un tremendo foco de delincuencia"[48].

Ahora bien, en modo alguno creemos que esta dificultad presentada por Internet deba traducirse en la instauración de entes centralizados y con facultades de censura, quienes puedan decidir todas aquellas cosas que pueden o no mostrarse a través de la red. Tomar este camino, además de

[48] LOPEZ MORENO, JUANA, OB. Cit. Pág. 404.

peligroso y muy difícil de llevar a la práctica, podría fácilmente transformarse en atentatorio en contra de las libertades más fundamentales de los individuos. La solución a este aspecto sin duda es difícil, toda vez que el tema es altamente sensible para todos aquellos quienes encuentran en Internet una forma de acceder a contenidos e información que de otra forma sería muy difícil conseguir. Creemos que es menester encontrar las solución a esta cuestión por la vía del derecho, estableciendo legislaciones claras a nivel nacional e internacional, que permitan, no por la vía de la censura previa, sino mediante la represión de conductas claramente delictivas, sobre las cuales exista un consenso generalizado de que deben ser sancionadas, y que se encuentren expresamente establecidas en los sistemas formativos, puesto que no puede, en pos de alcanzar la erradicación de los delitos en el ciberespacio, pasar por encima del principio de legalidad, ampliamente reconocido como una de las bases de la libertad de los individuos y un freno en contra de las arbitrariedades que en este sentido se pudieren cometer.

Justamente este último punto nos lleva a otro que hace difícil la persecución de las actividades delictivas en la red, y es la inexistencia de leyes claras y modernas que permitan hacer frente al cibercrimen de manera efectiva.

Sobre este punto existe básicamente dos posturas, en cierto modo antagónicas, entre quienes creen que los delitos del ciberespacio son solamente una modalidad más de los delitos tradicionales, y que por lo tanto sólo es menester una adecuación de las normas ya existentes para perseguirlos y los que piensan que estamos frente a una categoría nueva de ilícitos, que requieren un tratamiento especial por parte del derecho.

Nosotros estamos por inclinarnos por una tesis algo más ecléctica que rescate lo mejor de ambas posturas, ya que si bien en cierto sentido es verdadero que en muchas ocasiones los delitos cometidos por medio de Internet no son más que una variación de ilícitos cometidos tradicionalmente, en el que el aspecto informático no es otra cosa con un medio más de comisión de los actos ya reconocidos y sancionados por el Derecho, también es verdad que en otros casos estamos frente a fenómenos nuevos que requieren un tratamiento pormenorizado.

Pensamos que la mejor forma para partir abordando este punto es el lograr una definición más o menos consensuada de lo que el delito informático es, de cuales son sus características y, particularmente, de cual es el bien jurídico protegido en este caso, para a continuación llevar adelante la labor legislativa que sea menester, ya sea, en algunos casos,

mejorando la normativa existente para que abarque también los ilícitos cometidos a través de la red, y en otros creando formativas nuevas, con estudios particulares que hagan frente a cuestiones que en modo alguno responden a las conductas que tradicionalmente han sido consideradas como delitos. Pensar que sólo adecuando las normas existentes se puede hacer frente al fenómeno creemos que es una equivocación, la cual mucha veces parte de la ignorancia y de la incomprensión de lo que el fenómeno tecnológico y particularmente de la red, significa. El tratamiento de esta temática necesita un estudio multidisciplinario, que incluya no sólo a legisladores, jueces y abogados, sino también a personas que provenientes desde el mundo técnico e informático sean capaces de dar luces ciertas en torno a lo que se encuentra envuelto en cada acto llevado a delante a través de Internet. A esta discusión, sin duda, también se debe convocar a la sociedad civil, la cual habrá de ser el ente más afectado en caso de que se tome cualquier resolución a este respecto.

Lo que si no se puede hacer, es dejar que la situación se mantenga como hasta ahora, pues ha quedado claro, y los jueces así lo han declarado, que no se cuenta con las herramientas necesarias para hacer frente a este fenómeno, como ha quedado claro incluso en nuestro país cuando se ha

intentado juzgar, por ejemplo, a personas que se mueven dentro del mundo del comercio sexual infantil en Internet, ya que en nuestro país no existen las normas que sancionen expresamente este tipo de conductas.

Sobre lo anteriormente dicho, la autora española ESTHER MORON nos dice: "seguir planteando el conflicto «liberalización 'versus' control» o «Estado 'versus' usuarios» resulta, a estas alturas, una intolerable simplificación. En la infopista, el orden no puede correr a cargo sólo de los usuarios, quienes, por muy responsables que sean, pueden tener intereses contrapuestos a los otros. Está fuera de toda duda que las redes mundiales de información necesitan, para su fomento y desarrollo, infundir confianza a los distintos operadores del mercado, protegiendo los intereses de productores y consumidores, para los cual deviene imprescindible la existencia de normativa adecuada. La transmisión de datos, ya sea con fines comerciales o para uso estrictamente privado, por cualquier medio, necesita de alguna regulación, por mínima que sea. A mayor abundamiento, no pueden ignorarse los aspectos negativos de Internet por la trascendencia que en el orden público puede llegar a tener la transmisión de contenidos potencialmente ilícitos o nocivos y su utilización como vehículo de actividades delictivas. Así pues, el arbitrio de una solución que conjugue, en

correcto equilibrio, la garantía del libre flujo de información y la protección del interés público, deviene imprescindible.

"En el binomio libertad-control, por tanto, la cuestión no incide tanto en la conveniencia de su regulación, sino en el cómo, dadas las particularidades de la red. El carácter internacional de Internet y sus exclusivas características (descentralización, alcance global, uso general, amplitud y diversidad de contenidos, alto grado de automatismo) acarrean problemas específicos. Ello conduce al planteamiento del carácter que deberá asumir la respuesta normativa: regulación nacional, supranacional o bien soluciones coordinadas a nivel comunitario e internacional. Para poder afrontar el entramado de un hipotético estatuto jurídico de Internet, hay que analizar previamente la convergencia de tecnologías (telecomunicaciones, informática y radiodifusión) que conllevan las nuevas tecnologías y, por antonomasia, Internet"[49].

Uno de los puntos tratados por la autora en el párrafo recién trascrito, nos introduce en otro aspecto que hace que los delitos cometidos en Internet

[49] MORON, ESTHER, Ob. Cit. Págs. 109-111.

sean de tan difícil persecución y sanción, nos referimos al carácter transnacional que ellos habitualmente tienen.

En efecto, en la mayoría de los casos de hechos ilícitos cometidos en el ciberespacio se ven presentes conductas que incluyen a las jurisdicciones de más de un Estado, puesto que al no tener Internet una presencia física real, y estar expandido su uso por todo el globo, es fácil que un sujeto ubicado en cualquier parte del mismo cometa sus actos en un país muy distante a aquel en que él se encuentra en el momento de cometer el crimen, e incluso puede que use recursos provenientes de varias naciones para hacerlo.

Un ejemplo nos puede servir para graficar mejor este hecho.

Pongámonos en el supuesto de que un tipo gusta de la pornografía infantil y decide montar un sitio sobre este tema, en el cual no sólo distribuye fotografías, sino que además toma contacto con otras personas para conjuntamente entrar de manera ilegal a otros sitios dedicados al mismo tema y que son pagados. Esta persona, por ejemplo, puede decidir encontrarse, al momento de crear las páginas web en Japón, un país en el que se gusta mucho de las fotos de menores y del sexo violento. Este sujeto utiliza para poner en la web sus contenidos un servidor que está ubicado en

Italia, al cual accede, con el objeto de evitar ser rastreado, mediante un servidor proxy ubicado en Groenlandia. Mientras que los sujetos a los que le es enviado el material acceden desde ordenadores ubicados, en Estados Unidos, Suecia y Chile. ¿Qué legislación le es aplicable al sujeto en este caso? Podría decirse que la del país desde el cual el accede a Internet, sin embargo, ¿que ocurre si en ese país las normas son más permisivas a este respecto que aquellas que rigen en el país del servidor proxy utilizado para borrar el rastro o las del país en que se encuentra ubicado el servidor donde el material es exhibido? ¿Debe entonces el sujeto quedar impune por estar favorecido por la legislación de su país? Y los sujetos que acceden al material, quienes no han hecho otra cosa que bajar algo que es público y que está en Internet, proveniente de otro lado del mundo en que, tal vez dicho material no es objeto de la misma sanción de la que sería en el país en el que él está ubicado? ¿a ellos se les aplica su propia ley, o las de aquellos otros países involucrados?

Situación más compleja aún se produce con los derechos de la propiedad intelectual, en donde, por ejemplo, un autor inglés, ve reproducido ilegítimamente sus libros por un lector australiano, quien para difundirlos usa un servidor chino, para que los baje un lector argentino.

¿Que normativa se debe aplicar para salvaguardar los derechos del autor inglés, toda vez que a este respecto la Convención de Berna faculta a los Estados para poner normas más estrictas que las por ella contempladas? situación que podría ocurrir en este caso. ¿Cuál es la jurisdicción que se deberá aplicar en casos como estos que ocurren todos los días en Internet?

Refiriéndose a este punto, LOPEZ MORENO señala que "en todos los casos, el carácter trasnacional de las conductas hace muy difícil no ya su descubrimiento, sino su castigo, siendo frecuentes los problemas de jurisdicción competente, así como el hecho de que es verdaderamente difícil determinar la identidad de los delincuentes. Internet presenta una capacidad ilimitada para ser un medio y un vehículo de delincuencia, mientras que la capacidad de los Estados es infinitamente menor, y se haya limitada por las fronteras exteriores, que no existen en Internet"[50].

Ahora bien, cada día más en el mundo se hacen esfuerzos por salvar este problema del derecho para perseguir los delitos ciberneticos, siendo uno de los más serios del último tiempo la adopción de la Convención sobre el Cibercrimen, adoptada en Budapest el 2001, la cual pretende justamente

[50] LOPEZ MORENO, JUANA, Ob. Cit., Pág. 409.

coordinar a los Estados en la lucha en contra de este flagelo de la red. Sin embargo, ella aún no entra en funciones debido a que no ha contado con el número de ratificaciones necesarias para que lo haga. "El planteamiento de la Convención se basa en el reconocimiento fundamental de que se necesita armonizar las leyes nacionales. En años recientes, se ha logrado la cooperación internacional en materia de aplicación de la ley mediante una serie de tratados de extradición y ayuda jurídica mutua, que permite a los gobiernos intercambiar información y pruebas. Sin embargo, para que los tratados de extradición y ayuda jurídica mutua entren en vigor, generalmente existe un requerimiento de criminalidad doble (es decir, el acto delictivo debe ser calificado como tal en ambas jurisdicciones). En otras palabras, la cooperación internacional se facilita enormemente con la convergencia de lo que es penalizado en las jurisdicciones nacionales.

"Además, según lo señaló ERNESTO SAVONA, director del Centro de Investigación de Crímenes Transnacionales en Trento, Italia, la imposición de leyes similares en varios países propaga los riesgos que las organizaciones delictivas deben confrontar y al mismo tiempo sirve para igualar los riesgos a través de las jurisdicciones. De hecho, cuanto más alcance tengan las leyes, tanto menor será el número de refugios desde los

que los piratas controlados por el crimen organizado (o en efecto piratas individuales) puedan operar con impunidad.

"La armonización es necesaria tanto para las leyes substantivas como las procesales. Todos los países deben reevaluar y revisar sus reglamentos acerca de las pruebas, el registro y decomiso, la escucha electrónica oculta y otras actividades similares, que abarquen la información digital, los sistemas modernos de computación y comunicación y la naturaleza mundial de la Internet. Una mayor coordinación de las leyes procesales facilitaría, por lo tanto, la cooperación en las investigaciones que trasciendan jurisdicciones múltiples.

Además de tener las leyes apropiadas, es importante también que los gobiernos y las instituciones de aplicación de la ley desarrollen la capacidad para poner en vigor esas leyes. Esto requiere que se adquiera experiencia en el área del crimen cibernético y que también se establezca un intercambio eficaz de información entre las instituciones, tanto dentro de un país como a través de las fronteras nacionales. Asimismo, este intercambio deberá extenderse más allá de los organismos tradicionales de aplicación de la ley y deberá incluir a los organismos de seguridad nacional y de inteligencia.

"Es esencial también que se formen unidades policiales especializadas para abordar cuestiones del crimen cibernético a nivel nacional. Estas unidades pueden servir también de base tanto para una cooperación internacional formal o una cooperación informal basada en redes transnacionales de confianza entre los agentes de aplicación de la ley. La cooperación ad hoc y los grupos especiales multinacionales pueden resultar ser particularmente útiles - y ya hay casos en que la cooperación internacional ha sido muy efectiva. De hecho, la cooperación puede engendrar emulación y éxitos adicionales"[51].

Nosotros volveremos sobre la Convención del Cibercrimen más adelante en este trabajo.

Finalmente, otro de los aspectos que limita o hace más difícil la posibilidad de perseguir y sancionar los delitos informáticos cometidos a través de Internet, es el aparente anonimato de los usuarios de la red.

Una de las características de Internet que más atrae a muchos usuarios, es que en el entorno virtual los individuos carecen de una identidad real, siendo considerado esto prácticamente un derecho por parte

---

[51] WILLIAMS, PHIL, Crimen Organizado y Crimen Cibernetico: Sinergias Tendencias y Respuestas. http://usinfo.state.gov/journals/itgic/0801/ijgs/gj-7.htm

de los cibernautas, quienes se niegan a la posibilidad de que sus conductas en Internet puedan ser rastreadas, llevándose un control de sus intereses y preferencias, ni de su historial de navegación.

Ahora bien, este derecho, cuya consagración es entendible y necesaria en multitud de casos, pues va unido a otros derechos consagrados universalmente como la libertad y la protección de la intimidad, sirve para que, sujetos inescrupulosos, amparados en este anonimato virtual, y utilizando uno de las múltiples identidades de este entorno se sienta seguro para cometer actos ilícitos de todas las clases, como vulnerar passwords, e-mails, introduzca imágenes de pornografía infantil, intercambie programas y obras protegidas por la propiedad intelectual sin contar con los debidos permisos, etc. Además estos mismos individuos también hacen uso de herramientas sofisticadas que han sido pensadas para proteger este anonimato de los navegantes, como son los servidores proxy, los cuales consisten en sistemas de redirección de la información que ponen barreras entre el usuario y el lugar de destino. Dichas barreras en algunos casos son infranqueables, pues resulta casi imposible determinar que individuo ingresó a un sistema determinado puesto que el servidor proxy utilizado ni siquiera guarda un registro de los usuarios que han hecho uso de sus

servicios, siendo estos los más utilizados por hackers y crackers, quienes crean las formas de intercambiar periódicamente la información acerca de los proxys que actualmente están guardando el absoluto anonimato, pues ello cambia periódicamente, incluso de una hora a otra.

En términos muy generales, y para que el lector se haga una idea de que son estos mecanismos llamados proxy, vamos a dar un ejemplo:

Supongamos que un cracker, desea vulnerar los passwords de una página web de sexo, que son las más craqueadas de la red. Lo natural, y que haría cualquier persona que quisiera acceder a esa web es que se conectara a Internet, escribiera la URL correspondiente y así pudiera acceder a los contenidos ofrecidos por el sitio en cuestión. Sin embargo, en este caso, la página web de destino guardaría un registro de la dirección IP de este sujeto, y en caso de que él deseara realizar cualquier actividad delictiva podría ser rastreado para denunciarle ante las autoridades policiales correspondientes. Entonces que hace el cracker, como sabe que no puede ingresar directamente al sitio, ubica un servidor proxy que guarde totalmente el anonimato, introduce esos datos en el programa que esté usando para realizar la actividad de hacking, habitualmente el Accesdriver, un programa para realizar cracks que utiliza la fuerza bruta, tratando de

descubrir entre millones de combinaciones de palabras cuál es aquella que corresponde para poder entrar a un sistema. Entonces el programa ingresará directamente al servidor proxy y desde allí ingresará a la web objetivo del crackeo, no quedando registro alguno de esta actividad. Incluso, un cracker más experimentado utilizaría varios proxys sucesivos con el objeto de que así fuera aún más difícil el crackeo, con lo cual para ingresar a una web dada podría ir recorriendo casi todo el mundo en su afán de quedar impune. Tal vez lo más pintoresco de todo esto, es que la función de los servidores proxy es justamente de seguridad, para evitarle a los usuarios que su máquina sea detectada en Internet por hackers y Crackers y que pudiere así ser objeto de algún ataque.

Tenemos entonces que, la protección de este derecho al anonimato, en muchas ocasiones válido, sobretodo para los millares de usuarios que navegan en Internet sin la intención de cometer actos delictivos, ampara asimismo a los delincuentes, pues en pos de salvaguardar esta libertad se le niega a los organismos encargados de velar por el cumplimiento de la ley herramientas que le serían útiles a la hora de detectar y perseguir a los cibercriminales.

A este respecto, es sin duda necesario el encontrar una solución que, por una parte, permita mantener a los usuarios legítimos su anonimato y, por otra, faculte a los organismos judiciales para poder realizar actividades de monitoreo con el objetivo de detectar más eficazmente los actos delictivos que se cometan, para garantizar así su persecución y sanción.

A juicio de ESTHER MORON, "La sociedad digital ha fomentado el mito *orwelliano* del *Big Brother* y así Theodore Loti sostiene que «un escenario como el de 1984 será el resultado más probable si se permite que las cosas se desarrollen al ritmo actual y no se presta atención a la revolución de la información». Esta reivindicación casi constante y con cariz alarmista de la *privacy* en la Red desvela la tensión existente entre los intereses en pugna, lógicas contrarias subyacentes a un conflicto histórico pero robustecido por los avances tecnológicos. De una parte, la defensa de los derechos fundamentales y libertades públicas y, en concreto, el derecho a la intimidad; de otra parte, la necesidad estatal de proteger la seguridad nacional (a estas alturas, los proyectos euro-norteamericanos conducirán a una proyección de facto «global») y, en consecuencia, creciente ampliación de las capacidades de vigilancia en la lucha contra una criminalidad, dados los vertiginosos cambios que se suceden en las infraestructuras de

telecomunicaciones, transfronteriza. Se trata de un conflicto, pues, que no puede ventilarse sin parar mientes en los excesos en que el antecitado interés en pugna puede concluir. En efecto, la incuestionable necesidad de velar por la defensa nacional y la seguridad pública (¿mundial?) puede facilitar un paraguas, que cobije no sólo propósitos de lucha contra el terrorismo o el blanqueo de dinero, sino también intolerables conductas de espionaje económico o irreparables atentados contra la privacidad de las personas."[52]

Como se ve, nos encontramos frente a un tema altamente sensible, el cual sin duda en el corto plazo será muy debatido, en especial con la adopción de la Convención contra el Cibercrimen, la cual, ya ahora, antes de que entre en funciones, ha sido criticada como un atentado en contra de las libertades individuales. Igual cosa sucede con la nueva normativa estadounidense sobre la materia, la cual adoptada luego del atentado a la torres gemelas, también provoca fuertes rechazos en quienes ven en dichas normas una oportunidad más para que el poderoso país del norte imponga sus dictados por sobre el resto de las naciones.

---

[52] MORON, ESTHER, OB. Cit. Págs. 29-30.

IV. Hacking, Cracking y otros ilícitos cometidos en Internet

Ya anteriormente nos hemos referido a que tal vez uno de los mayores inconvenientes a que se enfrentan los operadores jurídicos a la hora de analizar y actuar respecto del mundo de la informática, es el poco conocimiento que en esta área se posee, principalmente debido a que, en general, se considera a éste un mundo más propio de las ingenierías y las matemáticas que de las humanidades que es el ámbito natural donde el hombre de derecho está acostumbrado a desenvolverse. Expresión de lo anterior la encontramos en el hecho de que, en la mayoría de la bibliografía especializada consultada en el curso de esta investigación, en general se le dediquen líneas muy breves y escuetas al tratamiento de los diferentes aspectos y caracterizaciones de los delitos informáticos, centrándose la mayoría de las veces el análisis en los aspectos netamente jurídicos de los mismos, y en particular en su consagración legal, sin adentrarse más a fondo en lo que este nuevo ámbito del conocimiento significa, en sus particularidades, en sus antecedentes y explicaciones no sólo jurídicas, sino también sociales, culturales e incluso filosóficas, puesto que de lo que

hablamos no sólo es de la regulación de un sector más del acontecer social, sino que hablamos de todo un mundo nuevo, esencialmente dinámico, revolucionario, con sus propios rasgos distintivos de interacción y comportamiento; un espacio esencialmente globalizado, en el cual se han demostrado insuficientes los intentos meramente nacionales por regularlo, y en el que se hace imprescindible una acción conjunta de los diferentes países para darle un estatuto jurídico verdaderamente aplicable, real, eficiente y eficaz, que responda a sus propias particularidades, puesto que ya desde antaño se ha constatado que no es el derecho el capaz de transformar, por si solo, las realidades sociales, sino que éste debe adecuarse a ellas, cuestión que tratándose de Internet es aún un desafío a cumplir.

Es debido a lo anterior, que en este apartado en el que pretendemos caracterizar los principales ilícitos que se cometen en Internet, hemos preferido guiarnos entonces no sólo por la bibliografía jurídica atingente al caso, la cual es necesario acotar que en general es escasa, al menos en nuestro país, sino que nos hemos remitido fundamentalmente a textos más centrados en el análisis propio de estos fenómenos, para intentar realizar, aunque sea someramente, una caracterización de ellos que apunte más a su

entendimiento en el medio en que ellos se llevan a cabo que a una simple y escueta definición de los mismos, que es el camino comúnmente seguido en esta materia. De todas formas, creemos importante sobre este punto advertir que no es nuestra intención el pretender el realizar aquí un análisis totalmente acabado sobre este fenómeno, puesto que ello escapa, por el momento, tanto a nuestras posibilidades como a las pretensiones de esta memoria, puesto que para esto sería menester el contar con el apoyo de un equipo interdisciplinario que fuese capaz de ir abordando desde distintas ópticas el asunto, realizando las explicaciones técnicas, jurídicas, sociales y culturales que fuesen menester para comprender el asunto en su real dimensión y así poder realizar un análisis profundo y acabado de una materia de por si compleja y que cruza, con mucho, las particularidades de una sola disciplina. En Internet se cometen día a día, minuto a minuto, miles o tal vez millones de actividades que lindan con lo ilícito, principalmente en lo que dice relación con los derechos derivados de la propiedad intelectual, y con el intrusismo informático, pero ello analizado desde la óptica propia del mundo real, del convencional, puesto que a la luz de la práctica y las particularidades propias del entorno digital, en muchas de esas ocasiones se trata de actividades normales, comunes e incluso necesarias para la

realización de la función tecnológica, razón por la cual ellas deben ser observadas en cuanto tales, tratando de evitar los prejuicios a su respecto y buscando la forma de conciliar tanto las necesidades de este nuevo mundo con las necesidades propias que el derecho trata de satisfacer.

1.- Hackers, Crackers y el resto de la familia underground

Como bien relata Bruce Sterling en su libro The Hacker Crackdown[53], "El término *hacking* se ha usado rutinariamente hoy en día por casi todos los policías, con algún interés profesional en el abuso y el fraude informático. La policía americana describe casi cualquier crimen cometido con, por, a través, o contra una computadora, como *hacking*.

"Más importante aún, *hacker* es lo que los asaltantes informáticos eligen para describirse a ellos mismos. Nadie que asalte un sistema de

[53] STERLING, BRUCE, "The Hacker Crackdown", traducción hecha por el equipo de Kriptópolis, http://www.kriptopolis.com. Es importante señalar que a este libro, como a varios otros utilizado en el curso de esta investigación sólo hemos tenido acceso mediante sus copias electrónicas y sin que se pueda especificar en cada caso el origen específico del texto. Tratándose de este libro en particular, el autor, siguiendo en todo el espíritu hacker, ha señalado que su reproducción y difusión electrónica es totalmente permitida, siempre y cuando ello se realice de manera freeware, es decir, gratuita. Sin embargo, en un interesante prólogo, también advierte que el hecho de que el libro en sí pueda ser distribuido en la forma que los usuarios encuentren conveniente no significa en modo alguno que lo puedan comercializar, puesto que él no ha cedido sus derechos de copyright sino que únicamente ha autorizado su libre y gratuita distribución. Nosotros hemos tenido acceso a este libro a través de un canal del IRC en la red Undernet llamado #biblioteca, el cual, creemos es el mayor centro existente de distribución de obras en formato digital en español, estén ellas o no con los derechos de propiedad intelectual vigentes.

buena gana, se describe a él mismo —raramente a ella misma— como un *asaltante informático, intruso informático, cracker, wormer, hacker del lado oscuro o gángster callejero de alta tecnología*. Se han inventado algunos otros términos degradantes con la esperanza de que la prensa y el público dejaran el sentido original de la palabra sola. Pero en realidad pocas personas usan esos términos. —Excluyo el término *cyberpunk*, que usan algunos *hacker* y gentes de la ley—. El término *cyberpunk* está extraído de la crítica literaria y tiene algunas extrañas e improbables resonancias, pero, al igual que *hacker*, *cyberpunk* también ha llegado a ser un peyorativo criminal hoy en día"[54].

Ahora bien, ¿es propio entonces el utilizar el término hacker o hacking para denominar a todas las actividades ilícitas o reñidas con la ley que se cometen en Internet? Después de nuestro estudio e investigación debemos concluir necesariamente que no. El confundir al hacker con un cracker o incluso con un simple lammer es un error que habitualmente se comete y el cual puede llevar a confusiones que hagan imposible la lucha en contra de los reales delincuentes del ciberespacio.

---

[54] Ibíd..

Es por ello entonces, que creemos importante antes de comenzar el análisis particular de las conductas de hacking y cracking, el realizar una breve a aproximación a cuáles son los distintos sujetos que se encuentran en el ciberespacio o, como algunos gustan llamarse, cuales son los miembros de la gran ciberfamilia underground, para lo cual justamente nos remitiremos a The Jargon File[55], la Biblia de los hackers, un diccionario creado por Eric S. Raymond[56], que ya va en su versión 4.3.3

1) **Hacker:** Dentro de esta familia del underground digital, sin duda el puesto más elevado lo ocupan los denominados hackers. Como ocurre con muchas de los vocablos utilizados en este nuevo entorno, no existe una definición exacta de lo que ello significa, y menos aún existe una traducción de la misma al español. Se dice que originalmente con el término hacker se quería hacer referencia a personas que fabricaban muebles a hachazos, mientras otros hacen referencia a que este era el término reservado para denominar durante la década de los '50 en Estados

[55] RAYMOND, ERIC S, The Jargon File 4.3.3, http://www.catb.org/~esr/jargon/

[56] RAYMOND, ERIC S., programador e impulsor de GNU y del Open Source Initiative, que promueven el desarrollo de código y software libre, como Linux. Para ser usados gratuitamente. Página personal http://www.catb.org/~esr/

Unidos a los reparadores de cajas telefónicas, quienes para cumplir con su cometido habitualmente le pegaban un golpe seco (hack) al aparato que presentaba las fallas. Con todo, es sin duda a partir de los años 60 en que el término comienza a acuñarse en la acepción relativamente general que conocemos, en cuanto ella se empezó a usar para referirse a un grupo de individuos maravillados por la recién naciente informática y la computadora TX-0 y que se encontraban agrupados en el Massachussets Institute of Tecnology (MIT).

Ahora bien, ¿cómo puede hoy en día ser definido un hacker?

> Para HUGO DANIEL CARRION, rescatando tal vez una de las acepciones más comunes del término, los hackers pueden ser definidos 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."[57]

Por su parte CLAUDIO HERNANDEZ, autor del libro "Hackers, los Piratas del Chip y de Internet", describe a estos sujetos como "expertos en sistemas avanzados. En la actualidad se centran en los sistemas informáticos y de comunicaciones. Dominan la programación y la electrónica para lograr comprender sistemas tan complejos como la comunicación móvil. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos. Les encanta entrar en ordenadores remotos, con el fin de decir aquello de "he estado aquí" pero no modifican ni se llevan nada del ordenador atacado. Normalmente son quienes alertan de un fallo en algún programa comercial, y lo comunican al fabricante. También es frecuente que un buen Hacker sea finalmente contratado por alguna importante empresa de

[57] CARRION, HUGO DANIEL, Presupuestos para la Incriminación del Hacking. Obtenido desde el sitio web "Delitos Informáticos", http://www.delitosinformáticos.com.

seguridad. El perfil del Hacker idóneo es aquel que se interesa por la tecnología, al margen de si lleva gafas, es delgado o lleva incansablemente encima un teléfono celular de grandes proporciones o emplea muchas horas delante del ordenador, pero para nada debe ser un obsesivo de estas maquinas. No obstante puede darse el caso. Este grupo es él mas experto y menos ofensivo, ya que no pretenden serlo, a pesar de que poseen conocimientos de programación, lo que implica el conocimiento de la creación de Virus o Crack de un software o sistema informático"[58].

Por su parte, en lo que tal vez es la acepción más respetada de lo que por un hacker debe entenderse dentro del underground digital, ERIC S. RAYMOND, en su *Jargon File* antes citada, señala que este tipo de sujetos puede ser definido de varias maneras:

[58] HERNÁNDEZ, CLAUDIO, "Hackers, Los Piratas del Chip y de Internet", libro electrónico gratuito disponible en http://.perso.wanadoo.es/snickers

- Alguien que disfruta explorando los sistemas y programas y sabe cómo sacarles el máximo provecho, al contrario que la mayoría de los usuarios que prefieren conocer sólo lo imprescindible.
- Entusiasta de la programación (a veces de forma obsesiva).
- Alguien que aprecia el valor de hackear.
- Persona que es buena programando de forma rápida.
- Experto en un programa concreto o que es especialmente hábil en el manejo de un programa dado (e.j.: 'un *hacker* de UNIX'). *Las definiciones 1 a 5 comprenden un grupo de gente que se une para compartir sus habilidades.*
- Experto o entusiasta de cualquier clase.
- Alguien que disfruta con el desafío intelectual de superar las dificultades de forma creativa.
- [objetable] Mala persona que trata de descubrir información secreta. De ahí viene password hacker y network hacker. En este caso debe utilizarse cracker.

Asimismo, dentro de esta categoría de los hackers, es posible a su vez encontrar a otros sujetos, que son hackers, pero con particularidades propias. Dentro de ellos destacan:

- **Los Samurai.** Hackers que "crackean", es decir, violan sistemas, amparados por la ley y/o la razón, normalmente es alguien contratado para investigar fallos de seguridad, que investiga casos de derechos de privacidad, esté amparado por la primera enmienda estadounidense o cualquier otra razón de peso que legitime acciones semejantes. Los samurais desdeñan los crackers y a todo tipo de vándalos electrónicos.
- **Los *Sneaker.*** Aquellos individuos contratados para romper los sistemas de seguridad por las empresas e instituciones con la intención de subsanar dichos errores.

2) **Los crackers.** Como tuvimos oportunidad de ver más arriba, cuestión sobre la que volveremos en el desarrollo de este trabajo, los hackers niegan respecto de sí la mayoría de las acusaciones que recaen sobre ellos por parte de los organismos policiales y la prensa, quienes habitualmente utilizan este término para señalar todas las actividades que pudieren tener algún grado de ilicitud y

que se encuentren vinculadas a la informática, ya sea que se realicen dentro o fuera de la red. A juicio de los hackers esta confusión nace de la ignorancia y al difundir este error también hacen caer en él al común de las personas, quienes tienden a asociar hacker con actividades reñidas con la ley. Es por ello que a mediados de los años ’80 desde el mundo hacker se comenzó a acuñar un nuevo término, el de cracker. Dicha palabra, dentro del mundo *underground* de los hackers, tiene una connotación peyorativa, y la usan para referirse a aquellos sujetos que usan sus conocimientos no para descubrir la verdad del cibermundo sino para lucrar, destruir o dañar a otros, violando con ello los principios básicos de la ética hacker. Sin embargo, pese a los esfuerzos desplegados por los hackers para que los diferencien de estos no ha tenido mucho resultado pues es habitual que se los confunda. Dentro de la jerga especializada también se les ha denominado “hackers del lado oscuro” en clara alusión a la película de Lucas Star Wars. Entre las variantes de crackers maliciosos están los que realizan Carding (Tarjeteo, uso ilegal de tarjetas de crédito), Trashing (Basureo, obtención de información

en cubos de basura, tal como números de tarjetas de crédito, contraseñas, directorios o recibos) y Phreaking o Foning (uso ilegal de las redes telefónicas).

CLAUDIO HERNANDEZ define a los crackers como "'Hackers de élite rebeldes' que emplean sus conocimientos para difundirlos en la red en forma de Software que otros utilizaran indebidamente. Los Crackers revientan sistemas y roban la información del ordenador ajeno"[59].

Por su parte, en el glosario de términos informáticos del portal de Terra, los crackers son definidos como "alguien que entra subrepticiamente en el sistema de ordenadores de otra persona, con frecuencia en una red. Un cracker puede hacer esto por ganancias materiales, malintencionadamente, por algún propósito o causa altruista o por el placer del desafío. Parte de estos allanamientos se han emprendido de manera ostensible para destacar las debilidades en el sistema de seguridad de algún sitio"[60].

---

[59] HERNANDEZ, CLAUDIO, Ob. Cit.
[60] TERRA.COM, Cibercultura, http://www.terra.com/informatica/que-es/cracker.cfm

Definiciones como las anteriores podemos encontrar por montones en la red, incluso en la Jargon File, la Biblia hacker podemos encontrar una hecha en el mismo sentido y en la cual se grafica el desprecio que los hackers sienten por los cracker. Dicho documento se refiere del siguiente modo a este término:

"Cracker n. El que rompe la seguridad de un sistema. Acuñado hacia 1985 por hackers en defensa contra la utilización inapropiada por periodistas del término hacker (en su acepción número 8[61].) Falló un intento anterior de establecer "gusano" en este sentido en 1981-1982 en Usenet.

"La utilización de ambos neologismos refleja una fuerte repulsión contra el robo y vandalismo perpetrado por los círculos de crackers. Aunque se supone que cualquier hacker auténtico ha jugado con algún tipo de crackeo y conoce muchas de las técnicas básicas, se supone que cualquier que haya pasado la etapa larval ha desterrado el deseo de hacerlo con excepción de razones prácticas inmediatas (por ejemplo, si es necesario pasar por alto

61 Liante malicioso que intenta descubrir información sensible cotilleando por ahí. De ahí vienen Hackers de contraseñas" y "hackers de redes". RAYMOND ERIC, The Jargon File.

algún sistema de seguridad para completar algún tipo de trabajo.)

”Por lo tanto, hay mucho menos en común entre el mundo de los hackers y de los crackers de lo que el lector mundano, confundido por el periodismo sensacionalista, pueda suponer.

“Los crackers tienden a agruparse en grupos pequeños, muy secretos y privados, que tienen poco que ver con la poli-cultura abierta y enorme que se describe en este diccionario; aunque los crackers a menudo se definen a sí mismos como hackers, la mayor parte de los auténticos hackers los consideran una forma de vida inferior.

“Consideraciones éticas aparte, los hackers consideran que cualquiera que no sea capaz de imaginar una forma más interesante de jugar con su ordenador que romper los sistemas de alguien ha de ser bastante perdedor”[62].

Ahora bien, lo anterior es lo que dicen los hackers respecto de los crackers y lo que, en cierta medida han logrado imponer dentro del mundo meridianamente informado sobre la materia. Sin

[62] RAYMOND, ERIC S, The Jargon File 4.3.3, http://www.catb.org/~esr/jargon/

embargo, los crackers tienen una visión de si bastante distinta. Ellos se consideran en muchos casos los nuevos rebeldes, los negadores del sistema tal y cual está establecido y por eso es que realizan su labor, para liberar la información y ponerla al alcance de todos, de cualquiera. KING FISHER, un reconocido cracker, en un texto denominado "La Conciencia de un cracker" se refiere a este punto señalando lo siguiente: "Dicen que un nihilista es una persona que reniega los valores. No es del todo verdad. Un nihilista es alguien que reniega ciertos valores, y construye nuevos. Alguien que únicamente reniega los valores, y solo quiere destruir la sociedad, es más bien un anarquista, o simplemente un vándalo, un profeta de la carencia de valores. Para mi, prefiero llamarme un adherente a la filosofía Zen, la Falibilidad, o sencillamente: una persona que cree que no hay entidades fijas tales que "El Bien", "El Mal" o "La Propiedad Privada", todos conceptos que tan solo son construcciones momentáneas del espíritu humano. Por una parte soy de la banda de Nietzsche, pero quiero llegar más allá de Nietzsche, pues el Nihilismo siempre es creativo.

"Dicen que los crackers son escarabajos maléficos que quieren arruinar las compañías de softwares y robar el dinero que cobran los desdichados programadores. Lo que digo yo, es que la información es de todos, como el aire que nos rodea, y que nadie tiene derecho de esconder tras las paredes. Si pensáis que los crackers tan solo son un grupo de anarquistas listos a ponerlo todo a sangre viva porque eso les divierte, os equivocáis de lleno. De hecho, somos peor que eso.

"Ponemos todo patas arriba, cierto, pero estamos orgullosos de ello, y lo hacemos porque tenemos que hacerlo. Alguien tiene que liberar la información. No pirateo porque odio la sociedad, sino porque la amo y deseo que evolucione. Considero el pirateo una acción altamente política, y estoy firmemente convencido que es JUSTO piratear!"[63].

Volveremos más adelante sobre este punto y la diferencia entre hackers y crackers.

---

[63] KINA FICHER, La Conciencia de un Cracker, traducción de Katia Coen, http://www.df.lth.se/~triad/triad/3words/Consesp.html

3) Así como reza el dicho popular que "no todo lo que brilla es oro", en el mundo *underground* del ciberespacio junto con hackers y crackers, que vendrían a ser como el escalafón más alto de esta sociedad virtual, también conviven otro tipo de sujetos, en general de conocimientos informáticos muchos menos sólidos que los que tienen hackers y crackers verdaderos y, en ocasiones, mucho más dañinos para la red de lo que podrían llegar a serlo los miembros más avanzados de esta familia.

A continuación, y guiándonos por la amplia clasificación dada en la *Jargon file* sobre esta materia, señalaremos algunos de los sujetos más relevantes que también viven en el submundo digital, quienes arrancan sus denominaciones muchas veces de la ciencia ficción, la literatura fantástica, el rol y los juegos de ordenador

- **Wannabes.** Alguien que podrá llegar a ser un hacker, pero que aún no lo es. Todos los hackers han pasado por esta etapa. Un *wannabe* adquiere el estatus de hacker cuando los veteranos deciden empezar a considerarle uno de los suyos, puesto que en el mundo hacker la pertenencia se gana sólo por los conocimientos demostrados y se llega a ser hacker, o

cracker en su caso, sólo cuando la comunidad considera como tal al sujeto en cuestión. Podría incluso afirmarse que, en el *underground* digital impera una férrea "meritocracia"

- **Newbie.** Algo muy similar a w*annabe*: un novato. Originariamente esta palabra procede de Inglaterra y se aplicaba a los recién llegados a los colegios y a las academias militares. Hay que tener presente en todo momento que estos aprendices de hackers pueden ser unos seres inofensivos en determinados círculos, principalmente en el de los que son más avanzados en el conocimiento informático, pero que pueden llegar a jugar muy malas pasadas a los usuarios comunes y corrientes, a la "plebe" informática.
- **Esado larval.** Para entrar en este comando de elite dentro de los guerreros de los bits hay que pasar por diferentes estadios de desarrollo. Uno de los periodos más frecuentes es el larval (larval stage), que oscila entre los 6 meses y los dos años y en el que el sujeto se encierra en su habitación a escribir código e ignora en mayor o menor medida la realidad que le rodea.

❖ **Bogus (farsante)**. Ser hacker es un honor que hay que ganar y que la comunidad hacker concede. Uno no puede empezar a proclamar que lo es sin la aquiescencia de dicha comunidad a menos que quiera ser mirado con desprecio y pasar a formar parte de la tribu de los hackers de pacotilla, los farsantes conocidos como *bogus*.

❖ **Mundane (mundano)**. Cualquier persona no iniciada en este mundo *underground*. Es decir, el común de los mortales.

❖ **Lamer,** sinónimo de ***Leecher*** y de ***Luser*** (mezcla entre *user*, usuario, y l*ooser*, perdedor), empleado más frecuentemente entre los crackers que entre los hackers. Es aquella persona que se aprovecha de los recursos que ofrece la comunidad *underground* sin aportar nada a cambio. Alguien que, por poner un ejemplo, descarga *cracks* sin cesar pero nunca desarrolla uno. Los crackers a veces designan con esta palabra a los *wannabes* de crackers.

❖ **Muggle.** Denominación inspirada en los personajes carentes de poderes mágicos de la serie de libros de Harry Potter que convivían en el mismo mundo que los magos, pero

ignorantes de la existencia y los poderes de estos últimos. Es decir, de nuevo el común de los mortales.

❖ **Weenie.** El típico *weenie* es ese adolescente aficionado al rol y a la música *metal* y con escasas aptitudes sociales que pulula y puebla parte del universo *underground*.

❖ **Bigot (fanático)**. Una persona que es férrea partidaria de un lenguaje de programación, de un particular sistema operativo o una computadora en concreto. Aplicable a los hackers y a la familia circundante.

❖ **Geek** Una persona que ha elegido la concentración más que el conformismo; un sujeto que persigue la habilidad (especialmente habilidad técnica) y la imaginación, sin importarle la aceptación social. Los Geeks tienen habitualmente un caso fuerte del "neophilia", es decir un gusto compulsivo por lo nuevo, por aquello que les resulta novedoso, lo cual ha sido considerado una enfermedad emergente en nuestros días. La mayoría de los geeks son peritos con las computadoras y tratan a los hacker de manera respetuosa, pero ellos mismos no necesariamente son hackers,

e incluso, la relación de respeto es tal que aunque algunos puedan en los hechos ser hackers de todas formas se siguen autodenominando geeks en el entendido (correcto) de que esta denominación no es algo que uno se da a sí mismo, sino que debe ser otorgada por el resto

❖ **Spod.** Alguien que reúne todos los aspectos negativos de un g*eek*, pero que no cuenta con ninguna de sus ventajas, se mueve por la Red aprovechando sus ventajas pero sin interesarse lo más mínimo en su funcionamiento o en ningún tipo de filosofía. Generalmente es despreciado.

❖ **Lurker.** Un término que no es en absoluto peyorativo y que se refiere a la mayoría silenciosa que sólo participa en los foros muy de vez en cuando. Cabe en este punto señalar que los foros o BBS son puntos habituales de encuentro de hackers, en los cuales intercambian experiencias y conocimientos.

❖ **Twink.** Un usuario 'repelente'. En las partidas de rol es aquel jugador que ignora todas las reglas y convenciones sociales para hacer alarde de sus superpoderes.

Como podemos observar, la familia del *underground* digital es muy variada, y no siempre es fácil distinguir a unos sujetos de otros, en particular tratándose de aquellos que actúan como hackers o crackers sin en realidad serlo. Tal vez son estos últimos sujetos quienes más problemas provocan a la hora de tratar la temática hacker, en particular porque su accionar es el más vistoso y difundido y ello ayuda a que los verdaderos hackers vean enlodado su nombre sin que en verdad sean ellos los que cometen muchas de las fechorías que se les atribuyen. De los anteriores, tal vez los sujetos más perniciosos en la red sean los llamados lammers, término que ya se encuentra muy extendido en el Internet, y que se usa habitualmente para referirse, entre quienes meridianamente conocen el tema, a aquellos individuos que gustan molestar al resto y que se ponen a manejar herramientas y causar daño sin ni siquiera conocerlas, y es éste el grupo más grande.

Ser un hacker o un cracker es algo que demanda mucho estudio, y habilidades especiales para la informática, ser un lammer no. Cualquiera que así lo desee puede a través de Internet hacerse con herramientas muy peligrosas de hack y crack, así como con virus, troyanos, etc., las cuales pueden ser muy fáciles de utilizar para un usuario medio, pero con ello

puede causar daños que ni siquiera ellos se imaginan. De hecho, alguna vez en el *Direct Connect* uno de los múltiples sistemas *peer to peer* existentes en Internet, es decir de intercambio de archivos persona a persona, tuvimos oportunidad de ver una conversación entre dos sujetos que decían ser hackers, pero que a todas luces no lo eran sino simples lammers, en la cual se entretenían contándose mutuamente historias sobre las "travesuras" que habían hecho el último tiempo. En una de las tantas que tuvimos oportunidad de leer, uno le contaba a otro lo mucho que se había entretenido introduciendo un troyano en el computador de una oficina y molestando a la secretaria abriéndole remotamente el programa *Paint* de Microsoft para escribirle insultos y groserías. Lamentablemente cuestiones como esta ocurren a diario y no es necesario ser un genio de las computadoras para poder hacerlas, sino que basta con leerse unos cuantos manuales, tener conocimientos medios de informática y hacerse con algunos de los muchos programas que hay en la red para realizar este tipo de actos, nada más. Claro, en el anterior caso no eran más que un par de jóvenes tratando de divertirse, pero eso es el primer paso para provocar graves daños a terceros sin haber un motivo real detrás.

En el entendido que los anteriores sujetos, los *lammers* o afines, son simples ciberdelincuentes cuya criminalidad y peligrosidad no está en duda, puesto que además son individuos sin escrúpulos que juegan a aparentar ser algo que no son, nosotros a continuación nos ocuparemos del tratamiento de la primera escala de la familia del *underground* de Internet, de Hackers y Crackers, puesto que su incriminación, sobre todo en el primer caso es algo que ha sido difícil de abordar, incluso ahora, y tratándose de los segundos, nos es imperioso referirnos a ellos para distinguirlos de los llamados "hackers blancos" o simplemente "hackers" y también porque creemos importante explicar un poco más su comportamiento y

2.- Los Hackers

De todas las definiciones citadas en el acápite anterior, uno de los elementos que es común a todas ellas es que cuando hablamos de un hacker no nos referimos a un simple aficionado a las computadoras, sino a todo un experto en ellas, sea que se trate de una especialización en un sistema operativo en particular o que se sea hábil en el uso informático en general. Tal vez como dato, podríamos decir que los hackers prefieren para ellos mismos usar sistemas operativos de software libre, como Linux, ya que

además de ser gratuito es más seguro. Sin embargo un hacker que se precie de tal deberá tener sólidos conocimientos también de Windows, pues es el sistema operativo más extendido y ha demostrado ser, a su vez, el más vulnerable.

Otra característica que es a su vez común en las definiciones dadas anteriormente, es que los hackers deberían ser, a su vez, definidos en base a su curiosidad extrema y al deseo de superación y de ahondar en un conocimiento sin límites. Destacamos en particular esta característica porque se ha dicho que el ser un hacker no es tanto una cuestión de conocimientos sino de actitud, y es ésta la que lleva finalmente al saber, debiendo estar ambos aspectos muy interrelacionados, puesto que el ser hacker es una cuestión de reconocimiento entre pares, como miembros de una elite, pero al decir de los entendidos la actitud hacker no sólo es posible verla en el mundo de los computadores, sino que también en la vida real en aquellos que tienen una sed incontenible de conocimiento, un ansia casi patológica por saber, por descubrir cómo funcionan las cosas.

CLAUDIO HERNÁNDEZ lo grafica del siguiente modo:

"*...Papa, que hay dentro de la televisión?.-Sus ojos brillantes mostraron un rostro encogido por la curiosidad y añadió.-Que hay dentro de tu ordenador.*

El padre del chico sé encogió de hombros. Era evidente que le había dejado en un compromiso o como solían decir los Kensit, sé había quedado colgado como el sistema operativo de Bill Gates. Llevaba años manejando el ordenador y apenas si sabia que dentro de él, había unas cuantas cucarachas, como las solía llamar él.

Después de un largo lapso de tiempo, interminable para el chico, dijo.-No sé exactamente lo que hay dentro. Pero tengo la certeza de que debe de haber mucho que contar de lo que hay allí dentro. Pero eso, es algo que se me escapa a mis conocimientos.

-Bien, al menos has sido sincero.-Explicó el chico y añadió.-Lo descubriré yo mismo, un día de estos.

Entonces el chico era un Hacker..."[64]

En la anterior "fábula", justamente se hace hincapié en aquello que veníamos diciendo, el hacker lo es porque necesita descubrir el mundo, y

[64] HERNÁNDEZ, CLAUDIO, Ob. Cit.

ese mundo son los computadores, por eso que para ser hacker se necesitan conocimientos sólidos, pero ellos no necesariamente son de aquellos conocimientos que se adquieren en una universidad o instituto, sino que es habitual que los hackers, los mejores de entre ellos, sean autodidactas, porque ello va en el espíritu mismo de ser hacker.

Asimismo, es necesario destacar de los anteriores conceptos el que, para hackers e investigadores ligados al tema, en modo alguno puede ser considerado como algo peyorativo, reñido con la moral o con las leyes, el ser denominado un hacker, al contrario ello es motivo de orgullo, pues como hemos reiterado, el ser considerado un hacker es una cuestión de reconocimiento entre pares. A un hacker no le interesa que lo miren como tal ni los simples usuarios de Internet, ni los organismos policiales ni el resto de la sociedad no ligada específicamente al tema, puesto que quien nada sabe o quien tiene unos conocimientos medios o limitados puede fácilmente confundirse y creer que una simple actividad, como entrar a un computador y tomar el control de él, es un gran acto de hackeo, cuando ello no es así. Lo que si interesa a los hackers es que no se los confunda con los crackers, de acuerdo a la concepción que ellos mismos han acuñado del término y que hemos expuesto más arriba.

En principio un hacker no cree que con su accionar esté trasgrediendo ninguna ley, al menos no las del ciberespacio que es el mundo que en realidad le interesa. Un hacker actuará pero sin el ánimo directo de dañar o de obtener un beneficio económico directo e ilícito. Lo que lo mueve es el conocimiento, la comprensión del mundo que lo rodea, y para ello es que gusta de intentar penetrar los diferentes sistemas informáticos, para descubrir sus fallas y errores, cuestión que por lo demás ha sido de mucha utilidad en algunas ocasiones para las empresas, no por nada es habitual ver a gigantes corporativos que contratan a verdaderos hackers con el objeto de que se encarguen de perfeccionar sus sistemas informáticos o para que les diseñe un plan de seguridad fiable.

Es más, en la mayoría de las oportunidades es muy difícil determinar que un determinado sistema fue hackeado, y ello porque un verdadero hacker rara vez deja huellas perceptibles de su ingreso y accionar dentro de alguno de ellos, pese a que, también, la mayoría de las veces se encargan de generar las herramientas y condiciones que les permitan reingresar libremente y la cantidad de veces que quieran. Esto último, es lo que justamente lleva a algunos autores como ROVIRA a calificar al delito de hacking dentro de los llamados delitos de riesgo penal informático, puesto

que si bien en una primera oportunidad puede que no se realice ninguna actividad realmente dañina para el afectado, nada garantiza que en el futuro ello no suceda.

En base a esta distinción, basada en que un acto de hacking pueda o no servir para lo comisión de futuros delitos informáticos de mayor gravedad, es que en la doctrina nacional los autores HUERTA Y LÍBANO clasifican el hacking en dos grupos:

1) **Hacking propiamente dicho o hacking directo**, el cual a su entender es "un delito informático quie 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 curosear o divertirse de su autor"[65]. Como más adelante agregan estos autores en estos casos la motivación del hacker "no es la de causar daño, sino que se trata de obtener personales satisfacciones

[65] HUERTA MIRANDA, MARCELO Y LIBANO MANSSUR, CLAUDIO, Ob. Cit. Pág., 172

y orgullos, basados principalmente en la burla de los sistemas de seguridad dispuestos. Por ello, el hacker siempre buscará notoriedad pública desde el anonimato. Asimismo, perseguirá objetivos cada vez más difíciles de vencer, y elegirá sus víctimas entre empresas y organismos de trascendencia nacional e incluso internacional"[66].

2) **Hacking como medio de comisión de otros delitos o hacking indirecto.** Como de su nombre claramente se desprende, en este caso el hacking o accesos indebido a un sistema, que es la acepción que rescatan estos autores, no es el objetivo de la actividad en sí, sino que ello es únicamente utilizado como medio para cometer otro tipo de delitos de mayor gravedad, como fraudes, sabotaje, espionaje, etc. En este caso, para los autores, "lo que determina si el hacking es propiamente dicho o medio de comisión de otros ilícitos es el ánimo o motivación que induce a la comisión del delito. En el caso del hacking que tratamos, el ánimo del delincuente está determinado

[66] Ibíd..

por su intención de dañar, de defraudar, de espiar, etc. Es por ello que en el hacking indirecto el acceso indebido cede su rol protagónico frente al delito 'principal' que se busca cometer"[67].

Si bien pensamos que las caracterizaciones hechas por estos autores son correctas, nos permitimos disentir con la nomenclatura por ellos empleada, puesto que utilizan el término hacking para referirse no sólo a los actos de mero intrusismo informático, sin ánimo de dañar o lucrar, sino también a los que tienen otras motivaciones de carácter delictivo claro, y en este último caso, para evitar confusiones y siendo más propios en el uso del lenguaje usado en el ciberespacio es necesario hablar de crackers, puesto que estos individuos son a los que los mueve el ánimo delictivo propiamente tal, no a los hackers.

Por lo anterior creemos importante recalcar que cuando nosotros en este texto nos referimos al hacking, lo estamos haciendo en su significado propio de mero intrusismo informático, que como los define ESTHER MORON es el "conjunto de comportamientos de acceso o interferencia no autorizados, de forma subrepticia a un sistema informático o red de

[67] Ibíd.. Pág. 173

comunicación electrónica de datos y a la utilización de los mismo sin autorización o más allá de lo autorizado"[68].

2.1.- Los principios y la ética hacker

"Hoy han cogido a otro, aparece en todos los periódicos. 'Joven arrestado por delito informático', 'hacker arrestado por irrumpir en un sistema bancario'. 'Malditos críos. Son todos iguales'. ¿Pero pueden, con su psicología barata y su cerebro de los años cincuenta, siquiera echar un vistazo a lo que hay detrás de los ojos de un hacker? ¿Se han parado alguna vez a pensar qué es lo que les hace comportarse así, qué les ha convertido en lo que son? Yo soy un hacker, entre en mi mundo. Mi mundo comienza en el colegio. Soy más listo que el resto de mis compañeros, lo que enseñan me parece muy aburrido. 'Malditos profesores. Son todos iguales'. Puedo estar en el colegio o un instituto. Les he oído explicar cientos de veces cómo se reducen las fracciones. Todo eso ya lo entiendo. 'No, Sr. Smith, no he escrito mi trabajo. Lo tengo guardado en la cabeza'. 'Malditos críos. Seguro que lo ha copiado. Son todos iguales'. Hoy he descubierto algo. Un ordenador. Un momento, esto mola. Hace lo que quiero que haga. Si comete

---

[68] MORON, ESTHER, Ob. Cit, Pág., 42.

errores, es porque yo le he dicho que lo haga. No porque yo no le guste, me tenga miedo, piense que soy un listillo o no le guste ni enseñar ni estar aquí. Malditos críos. A todo lo que se dedican es a jugar. Son todos iguales. Entonces ocurre algo... se abre una puerta a un nuevo mundo... todo a través de la línea telefónica, como la heroína a través de las venas, se emana un pulso electrónico, buscaba un refugio ante las incompetencias de todos los días... y me encuentro con un teclado. 'Es esto... aquí pertenezco...' Conozco a todo mundo... aunque nunca me haya cruzado con ellos, les dirigiese la palabra o escuchase su voz... los conozco a todos... malditos críos. Ya está enganchado otra vez al teléfono. Son todos iguales... puedes apostar lo quieras a que son todos iguales... les das la mano y se toman el brazo... y se quejan de que se lo damos todo tan masticado que cuando lo reciben ya ni siquiera tiene sabor. O nos gobiernan los sádicos o nos ignoran los apáticos. Aquellos que tienen algo que enseñar buscan desesperadamente alumnos que quieran aprender, pero es como encontrar una aguja en un pajar. Este mundo es nuestro... el mundo de los electrones y los interruptores, la belleza del baudio. Utilizamos un servicio ya existente, sin pagar por eso que podría haber sido más barato si no fuese por esos especuladores. Y nos llamáis delincuentes. Exploramos... y nos llamáis

delincuentes. Buscamos ampliar nuestros conocimientos... y nos llamáis delincuentes. No diferenciamos el color de la piel, ni la nacionalidad, ni la religión... y vosotros nos llamáis delincuentes. Construís bombas atómicas, hacéis la guerra, asesináis, estafáis al país y nos mentís tratando de hacernos creer que sois buenos, y aún nos tratáis de delincuentes. Sí, soy un delincuente. Mi delito es la curiosidad. Mi delito es juzgar a la gente por lo que dice y por lo que piensa, no por lo que parece. Mi delito es ser más inteligente que vosotros, algo que nunca me perdonaréis. Soy un hacker, y éste es mi manifiesto. Podéis eliminar a algunos de nosotros, pero no a todos... después de todo, somos todos iguales"[69]

La anterior es la transcripción del llamado Manifiesto Hacker, escrito por MENTOR, un hacker. Hemos querido reproducirla porque tal vez en él está contenida buena parte de lo que es el pensamiento de las personas que son o quieren ser hackers, y también en él se expresa el que tal vez sea uno de lo mayores problemas de la sociedad civil para tratar jurídicamente a estos sujetos, la dificultad que se tiene para entenderlos, para comprender su filosofía, sus objetivos. Sin duda puede resultar muy sencillo el pensar que

---

[69] MENTOR, Manifiesto Hacker, http://www.sindominio.net/biblioweb/telematica/mentor.html

no son más que otros criminales y que, por tanto, deben ser condenados. Pero tal vez al actuar de este modo sólo se está incurriendo en un error que puede agravar el problema, puesto que a medida que avanza el desarrollo tecnológico y la automatización de hasta las actividades mínimas del ser humano, los hackers también van aumentando su poder. Ya han ocurrido casos en que jóvenes han ingresado a sistemas tan delicados como el Pentágono en Estados Unidos, con todas las consecuencia que ello pudo haber traído, pese a que, según fuentes oficiales, nunca lograron penetrar en ningún sistema realmente importante, pero eso lo dicen las fuentes oficiales y sabemos que aunque no hubiese sido así ese sería el discurso público que manejarían.

Antes de juzgarlos es menester tratar de conocer el mundo del *underground,* qué piensa y busca y sólo una vez hecho esto invocar todas las penas que sean menester.

Detrás de los hackers, de los verdaderos, hay toda una filosofía de vida, una ética que es la que pretendemos exponer a grandes rasgos en este apartado.

Quien crea que los hackers son sólo jóvenes desadaptados, adictos a computadores y videojuegos y que lo único que saben es de programas,

kilobytes y modems, está equivocado. Pese a ser un movimiento relativamente nuevo los hackers han ido forjando una serie de principios que, en general, son los que inspiran o deberían inspirar a todo aquel que desee adentrarse en este submundo y ser considerado como tal, y no como un simple cracker o lammer.

Tal vez el texto que mejor resume estos principios básicos de la ética hacker sea el de STEVEN LEVY[70], "Hackers: Heroes of the Computer Revolution"[71]en el cual se recogen los llamados mandamientos del hacker, inspirados en los objetivos esbozados por las primeras generaciones de hackers.

Dichos principios recogidos por LEVY *a grosso modo* son:

1) **El acceso a los ordenadores, y cualquier cosa que pueda enseñar algo sobre el funcionamiento del mundo, debe ser ilimitado y total**.

Sobre este punto LEVY señala que los hackers creen que se pueden aprender lecciones esenciales sobre los sistemas, sobre el mundo , desmantelando las cosas, viendo cómo funcionan , y

[70] LEVY, STEVEN, Página Personal, http://www.echonyc.com/~steven/

[71] LEVY, STEVEN, Hackers: Heroes of the Computer Revolution, edición digital obtenida desde el canal #bookz en el IRC en la red Undernet.

usando este conocimiento para crear nuevas y más interesantes obras. Es por ello que rechazan a cualquier persona, barrera física, o ley que pretenda impedir la consecución de este objetivo.

A juicio de LEVY los sistemas imperfectos enfurecen a los hackers, cuyo instinto principal es depurar el sistema. Esa sería una de las razones por las cuales los hackers odian conducir automóviles: el sistema de luces rojas aleatorias y calles de único sentido provoca demoras que son tan absolutamente *innecesarias* que el impulso es reorganizar los signos, abrir las cajas de control de las luces de tráfico... rediseñar el sistema completo.

Resulta curioso señalar a este respecto, que justamente por ese gusto que siempre presentó por conocer las cosas, observarlas, estudiarlas y aprender de ellas desarmándolas es que los hackers consideran a Leonardo Da Vinci como el primer hacker de la historia, puesto que como antes dijimos, el ser hacker no es sólo una cuestión que se relaciona con las computadoras, sino que es un gusto ilimitado por el conocimiento, por descubrir el mundo, por entenderlo. Sobre esto ha declarado OXBLOOD RUFFIN, líder de un grupo de hackers denominado *Cult of the Dead Cow,*

"Lo que explica el dominio supremo alcanzado por Da Vinci en lo referido a la forma humana es que, literalmente, sabía como analizarla. Y es algo de lo que los hackers pueden aprender… En la informática, hay una suerte de factor de reciprocidad que indica que cuanto más lejos se llega en el conocimiento de una máquina o de una red, más se puede alcanzar en el descubrimiento tecnológico. Esto mismo es lo que veo cuando miro la obra de Da Vinci. Era un hacker, sin lugar a dudas"[72].

2) Toda información debe ser libre.

Para los hackers, si no se tiene acceso a la información necesaria entonces es imposible mejorar las cosas. Es por ello que consideran que el libre intercambio de información, particularmente cuando la información toma la forma de un programa de ordenador, permite una mayor creatividad media.

LEVY señala en su libro que la creencia, a veces tomada incondicionalmente, que la información debe ser libre es un tributo directo a la forma espléndida de trabajar de un ordenador,

---

[72] DELIO, MICHELLE, Da Vinci, El Primer Hacker de la Historia, http://buscar2.terra.com/wired/cultura/03/01/29/cul_62114.html

o un programa: los bits binarios se mueven de la forma más simple siguiendo una lógica necesaria para realizar su complejo trabajo. ¿Qué sería un ordenador sino algo que se beneficia de un libre flujo de información? En este punto pone como ejemplo el caso de que una CPU se encontrase incapaz de obtener información de los dispositivos de entrada/salida (E/S), entonces todo el sistema se colapsaría. Es así entonces que, desde el punto de vista de un hacker, cualquier sistema podría beneficiarse de un fácil flujo de la información.

LEVY da el siguiente ejemplo sobre las bondades de este fluir libre de la información. Cuenta que en 1961, el MIT recibió gratuitamente el primer prototipo de ordenador PDP-1, un sistema antiquísimo. Su ensamblador era poco capaz, y un grupo de hackers liderados por Alan Kotok sugirieron a Jack Dennis, la persona a cargo del PDP-1, mejorar el ensamblador, lo cual no le pareció una buena idea a Dennis. Kotok, deseando tener la herramienta perfecta habría preguntado: “Si escribimos este programa durante el fin de semana y lo tenemos funcionando, ¿nos pagarías por el tiempo dedicado?". Dennis aceptó, y así seis

hackers trabajaron unas doscientas cincuenta horas en total ese fin de semana, escribiendo código, depurando, y bajando la comida china encargada con cantidades masivas de Coca-Cola. Era una orgía de programación, y cuando Jack Dennis vino el lunes se quedo estupefacto al encontrar un ensamblador cargado en el PDP-1, que como demostración estaba ensamblando su propio código a binario.

Por simple esfuerzo de hackear, los hackers del PDP-1 habían creado un programa en un fin de semana, lo que a la industria le hubiese costado desarrollar semanas, quizás incluso meses. Era un proyecto que no sería realizado por la industria sin largos y tediosos procesos de estudios, reuniones, y vacilaciones ejecutivas, probablemente arrastrando considerables compromisos durante el camino. Quizás ni siquiera se hubiese realizado en absoluto. LEVY afirma que en este caso el proyecto fue un triunfo de la Ética del Hacker.

Los hackers creen que incluso el hackear para uno mismo es productivo, pues el trabajo individual de una persona puede ser muy útil para otras sobre todo desde la óptica del software libre,

puesto que dentro de las normas de comportamiento de los hackers está el hacer accesible a quien lo desee el código fuente de sus creaciones, con el objeto de que pueda ser analizado, estudiado, para que así otros no cometan los mismos errores que ya han sido resueltos por alguien, lo cual es una forma de invertir las energías no en solucionar cientos de veces un mismo problema, sino que avanzando al siguiente sin quedarse estancado. Como señala RAYMOND "Los cerebros creativos son un recurso valioso y limitado. No deben desperdiciarse reinventando la rueda cuando hay tantos y tan fascinantes problemas nuevos esperando"[73]. Lo anterior es una gran diferencia con la lógica del software propietario, que al ser secreto su código impide que cualquier otra persona pueda abrirlo y descubrir qué está mal con él y solucionarlo. Es lo que le ocurre a Microsoft, cuyos sistemas operativos son reconocidamente de los que más fallos de seguridad y *bugs*[74] tiene, muchos más, por

[73] RAYMOND, ERIC S., How to Become a Hacker, http://www.catb.org/~esr/faqs/hacker-howto.html. Traducción obtenida del canal #biblioteca en el IRC en la red Undernet.

[74] Imperfecciones

ejemplo, que los sistemas operativos basados en UNIX[75], como LINUX, el cual es de software libre.

Respecto de este punto, creemos importante reproducir un texto de ERIC S. RAYMOND, en el que cuenta un poco la historia de LINUX y cómo un poco de código creado por un programador en un lugar muy distante se ha ido convirtiendo con el tiempo en uno de los principales competidores de Microsoft, y el cual se ha desarrollado únicamente gracias al trabajo desinteresado de cientos de programadotes alrededor de todo el mundo, quienes han actuado sin ninguna dirección central, pero que han encontrado la forma de llevar adelante un trabajo cooperativo, que sin necesidad de imposiciones se encamine hacia un objetivo común.

Esto es lo que nos cuenta RAYMOND: "¿Quién hubiera pensado hace apenas cinco años que un sistema operativo de talla mundial surgiría, como por arte de magia, gracias a la actividad hacker desplegada en ratos libres por varios miles de programadores

[75] Sistema operativo creado por AT&T (Compañía Estadounidense de telecomunicaciones) a mediados de los 70.

diseminados en todo el planeta, conectados solamente por los tenues hilos de la Internet?

"Lo que si es seguro es que yo no. Cuando Linux apareció en mi camino, a principios de 1993, yo tenía invertidos en UNIX y el desarrollo de software libre alrededor de diez años. Fui uno de los primeros en contribuir con GNU[76] a mediados de los ochentas y he estado aportando una buena cantidad de software libre a la red, desarrollando o colaborando en varios programas (NetHack, los modos VC y GUD de Emacs, xlife y otros) que todavía son ampliamente usados. Creí que sabía cómo debían hacerse las cosas.

"Linux vino a trastocar buena parte de lo que pensaba que sabía. Había estado predicando durante años el evangelio UNIX de las herramientas pequeñas, de la creación rápida de prototipos y de la programación evolutiva. Pero también creía que existía una determinada complejidad crítica, por encima de la cual se requería un enfoque más planeado y centralizado. Yo pensaba que

[76] Gnu is not Unix. Proyecto de la FSF (Free Software Foundation) para crear un sistema UNIX libre.

el software de mayor envergadura (sistemas operativos y herramientas realmente grandes, tales como Emacs) requería construirse como las catedrales, es decir, que debía ser cuidadosamente elaborado por genios o pequeñas bandas de magos trabajando encerrados a piedra y lodo, sin liberar versiones beta antes de tiempo.

"El estilo de desarrollo de Linus Torvalds[77][78] ("libere rápido y a

[77] **Linux** llegó al mundo con una declaración de Torvalds publicada en comp.os.minix en la que instaba a los programadores de todo el mundo a sumarse a su proyecto. En una parte les decía *"¿Añoras los buenos tiempos del Minix 1.1, cuando los hombres eran hombres y escribían sus propios manejadores de dispositivos? ¿No formas parte ahora de un proyecto interesante y no te mueres por hundirle el diente a un sistema operativo que puedas modificar según tus necesidades? ¿No te frustra descubrir que todo funciona bien en Minix? ¿Se acabaron los desvelos para hacer que un programejo trabaje bien? Entonces tal vez este mensaje sea para tí...".*

El 5 de octubre de 1991, Linus Torvalds anuncia la primera versión oficial de **Linux.**

"Se puede decir que creció hacker porque en su adolescencia se entretenía programando en lenguaje ensamblador, el Rolls Royce de la programación, una computadora *Commodore*. Era cosa de pocos años que llegará a estudiar en la Universidad Tecnológica de Helsinki.

"En la primavera de 1989, mientras estaba en la universidad, empezó a trabajar en el desarrollo de un kernel basado en el sistema operativo = propietario **UNIX** para computadoras con procesadores Intel. Una vez creado, lo puso a disposición del público a través de un servidor FTP de la universidad finlandesa.

"Linux era el nick (apodo) de Linus en la universidad, para evitar que lo acusaran de egocéntrico, quiso llamar a su cración *Freax (free+freak+x)* pero el webmaster decidio que le gustaba más el nombre de su amigo y usó **Linux.** El resto ya es historia.

"Ahora tocan dos pequeñas lecciones, una diferenciación de términos importante. La palabra **Linux** se refiere técnicamente sólo al kernel o núcleo del sistema operativo que es la parte que se carga primero y que permanece en la memoria principal de la máquina, por lo que es importante que sea lo más pequeña posible, y que provee a las otras partes y aplicaciones del sistema operativo de diferentes servicios esenciales como la gestión de la memoria o el almacenamiento en disco. Pero de nada sirve un kernel si no forma parte de un sistema completo, y de poco vale un sistema operativo si no cuenta con nuevas aplicaciones y sobre todo con nuevos drivers, una parte imprescindible para emplear periférico como teclados y ratones.

"Linus pronto se sumó a la filosofía del proyecto *GNU (GNU is Not Unix)* de la *Free Software Foundation*, convirtiendo a **Linux** en un producto de licencia *GPL (Licencia Pública General)*, y consiguiendo que numerosos desarrollos ya existentes lo adoptaran y que muchos programadores generaran otros nuevos.

"Es decir, lo que Linus desarrollló fue el corazón de los actuales sistemas operativos open source, que actualmente también se conocen por extensión con el nombre de **Linux**, pero que son obra del trabajo conjunto de miles de desarrolladores de todo el mundo..

"Linus dio a luz su *Kernel* a raíz del *OS MINIX*, un sistema operativo basado en **UNIX** que escribió Andrew Tanenbaum, un profesor de informática especialista en diseño de sistemas operativos. Lo desarrollo en 1987 para ayudar a sus alumnos a entender los entresijos de **UNIX**.

"Cuando Linus decidió que su creación se acogiera a la Licencia Pública General, estaba sumándose a la filosofía libertaria del software impulsada en los 80 por Richard Stallman, máximo responsable de GNU y defensor a ultranza del Free Software.

"Esta fue la proeza que convirtió a Linus Torvalds en una figura pública y en un estandarte viviente para muchos programadores. Eso sí, a menos que cambien las cosas, a diferencia de Bill Gates, Linus nunca estará en la lista de los hombre más ricos del mundo" (Linus Torvalds y Linux, http://www.informedica.org/2002/S1/files/biolinux/softlibre/torvalds.htm)

menudo, delegue todo lo que pueda, sea abierto hasta el punto de la promiscuidad") me cayó de sorpresa. No se trataba de ninguna forma reverente de construir la catedral. Al contrario, la comunidad Linux se asemejaba más a un bullicioso bazar de Babel, colmado de individuos con propósitos y enfoques dispares (fielmente representados por los repositorios de archivos de Linux, que pueden aceptar aportaciones de quien sea), de donde surgiría un sistema estable y coherente únicamente a partir de una serie de artilugios.

"El hecho de que este estilo de bazar parecía funcionar, y funcionar bien, realmente me dejó sorprendido. A medida que iba aprendiendo a moverme en ese medio, no sólo trabajé arduamente en proyectos individuales, sino en tratar de comprender por qué el mundo Linux no naufragaba en el mar de la confusión, sino que se fortalecía con una rapidez inimaginable para los constructores de catedrales.

---

[78] En la actualidad Linus Torvalds tiene 33 años.

"Creí empezar a comprender a mediados de 1996. El destino me dio un medio perfecto para demostrar mi teoría, en la forma de un proyecto de software libre que trataría de realizar siguiendo el estilo del bazar de manera consciente. Así lo hice y resultó un éxito digno de consideración"[79].

Como podemos observar, este gusto de la comunidad hacker no sólo por el software gratuito, sino que a la vez abierto, ha dado resultado y los hechos han ido demostrando que, a diferencia de lo que ha sucedido en la vida real, en la red si es posible encontrar formas organizativas absolutamente libres, sin controles, y que son capaces de encaminarse comunitariamente hacia un objetivo común. La experiencia de Linux es una clara muestra de ello, de hecho como antes dijimos este sistema se presenta como el enemigo más temible de Microsoft, puesto que su desarrollo es vertiginoso y se va perfeccionando cada día más. Como se ha señalado, el sistema de trabajo libre e independiente ha traído como consecuencia que a través de la red se junte el grupo más

[79] RAYMOND, ERIC S, La Catedral y el Bazar, texto en formato digital obtenido en su versión en español en el canal #biblioteca del IRC en la red Undernet.

selecto de programadotes, muchos de ellos hackers, trabajando mancomunadamente en un sistema del que todos se sienten dueños y padres. Sin duda a cualquier empresa le gustaría poder contar entre sus miembros a equipo tan granado, pero tal vez ni siquiera Microsoft tendría el dinero para pagar los honorarios de todos estos programadotes que tratándose de Linux trabajan gratis.

3) **Desconfiar de la autoridad: promocionar la descentralización**.

Según LEVY, el mejor medio de promocionar el intercambio libre de la información es tener un sistema abierto, algo que no presente límites entre el hacker y el trozo de información o el equipamiento necesario en su búsqueda del conocimiento, mejora, y tiempo on-line. Se rechazan las burocracias de todo tipo, ya sea corporativas, gubernamentales, o universitarias, puesto que son sistemas con errores, peligrosos en el sentido de que no pueden acomodar el impulso explorador de los verdaderos hackers. Para los hackers los burócratas se escudan tras reglas arbitrarias (a diferencia de los algoritmos lógicos que operan las

máquinas y los programas de ordenador): invocan aquellas reglas para consolidar el poder, y perciben el impulso constructivo de los hackers como una amenaza.

Sobre este punto, ERIC S. RAYMOND en su trabajo "How to Become a Hacker"[80], señala que los hackers son "naturalmente anti-autoritaristas. Cualquiera que te pueda dar órdenes, puede hacer que debas dejar de resolver ese problema con el cual estás ocupado y, debido a la manera en la cual trabajan las mentes autoritarias, encontrarán alguna razón espantosamente estúpida para hacerlo. Por eso, la actitud autoritaria debe ser combatida donde sea que se la encuentre, pues si se la deja te asfixiará, tanto a ti como a los otros hackers"[81]. No obstante esto, el mismo autor se encarga más delante de aclarar que ese rechazo a la autoridad como límite de la actividad creativa no necesariamente se expande a todos los aspectos de la vida del ser humano, es así que reconocen que la autoridad puede ser necesaria cuando se trata,

---

[80] RAYMOND, ERIC S., How to Become a Hacker, http://www.catb.org/~esr/faqs/hacker-howto.html

[81] Ibíd..

por ejemplo, de la crianza de los hijos o cuando se trata de reprimir actividades realmente delictivas.

4) **Los hackers deben ser juzgados por sus trabajos, no por criterios irrelevantes como títulos, edad, raza, o posición**.

Las personas que se presentan con credenciales aparentemente impresionantes no son tomadas en serio hasta que prueban su conocimiento en la consola de un ordenador. Esta traza meritocrática no está enraizada necesariamente en la inherente buena fe de los corazones hackers: es principalmente que se preocupan menos de las características superficiales de alguien que de su potencial para avanzar al estado general del hacking, crear nuevos programas que admirar, o hablar sobre aquella nueva característica en el sistema.

5) **Se puede crear arte y belleza en un ordenador.**

Para los hackers, el arte de programar no reside en el placentero producto que emana de una máquina. El código del programa tiene una belleza propia: una cierta estética de programación. Dada la limitada memoria de los ordenadores, valoran profundamente cualquier técnica innovadora que permite a los

programas realizar tareas complicadas con pocas instrucciones. Cuando más corto sea un programa, con mayor velocidad se ejecutará. A veces cuando no se necesita mucha velocidad o espacio, y no se piensa en arte y belleza, LEVY plantea que se puede hackear un programa “feo”, que ataca los problemas con métodos de "fuerza bruta", lo cual no es el sello distintivo de un buen hacker, es por ello que se prefiere planear cuidadosamente los algoritmos que provocan el mismo efecto, y que son más cortos y eficientes, en este caso es cuando los compañeros hackers admirarán el trabajo del sujeto que lo hace considerándolo uno de ellos

6) **Los ordenadores pueden mejorar la vida.**

A juicio de los hackers los ordenadores han cambiado sus vidas, las ha enriquecido, les ha dado un objetivo, las ha hecho más interesantes. Los ha convertido en maestros de una porción del destino. Es por ello que piensan que si todo el mundo pudiese interaccionar con los ordenadores con el mismo inocente, productivo, impulso creativo que usan, la Ética Hacker podría

difundirse por la sociedad como un fenómeno benevolente, y los ordenadores cambiarían entonces el mundo en algo mejor.

7) **Los hackers (y las personas creativas en general) nunca debieran ser sometidas a trabajos rutinarios**.

Este principio no se encuentra expresado abiertamente en el texto de LEVY, aunque se desprende de todo el contenido general de la obra a que hemos estado haciendo referencia. Por su parte, RAYMOND, quien si le dedica un apartado, señala que lo aburrido y lo rutinario es malo, tanto para los hackers como para todo aquel que desarrolla actividades creativas, puesto que en este caso no se estarían dedicando a lo que debe ser su labor fundamental: resolver nuevos problemas. No obstante lo anterior, también señala que existe una aparente excepción a esta regla, en virtud de la cual "los hackers hacen cosas a veces que pueden parecer repetitivas o aburridas pero como ejercicio para lograr limpieza mental, o para obtener cierta habilidad, u obtener cierta clase de experiencia que no podría tener de otro modo. Pero esto es una elección --ninguna persona pensante debiera nunca ser

forzada a hacer cosas aburridas."[82] Esto último, sería consecuencia lógica del hecho señalado por RAYMOND de que para ser hacker no basta con sólo querer serlo o tener una actitud para ello, sino que requiere un trabajo duro, constante y mucha dedicación.

2.2.- Requisitos para ser considerado un hacker

Como ya antes hemos señalado, el mundo hacker es en sí una especie de "meritocracia" para entrar a la cual es menester el cumplir un conjunto de requisitos, basados principalmente en la habilidad desarrollada por quien pretenda ingresar, y además es necesario tener un comportamiento acorde con aquello que los hackers consideran correcto, entre lo cual es posible encontrar, además del férreo respeto a los principios anteriormente esbozados, el desarrollo de ciertas actividades que los hackers consideran correctas y deseables en cualquiera que pretende entrar en su mundo y adquirir cierto *status* dentro de él. A continuación expondremos entonces algunos de estos requisitos para ser considerado un hacker, para lo cual nos remitiremos fundamentalmente al libro de RAYMOND "How to Become a

---

[82] Ibíd..

Hacker", ya antes citado. Es necesario eso si aclarar, como el mismo autor lo hace, que en este caso sólo nos referiremos al llamado "hacker de computadoras", puesto que ya antes hemos señalado que para esta subcultura no sólo es posible encontrar hackers dentro de esta área, sino que también en el resto de las actividades desarrolladas por el ser humano, principalmente dentro de aquellas que demandan esfuerzos altos de creatividad.

2.2.1.- Habilidades necesarias para ser considerado un hacker

RAYMOND nos señala al menos tres habilidades que son necesarias desarrollar para poder convertirse en un hacker. Ellas son:

1) **Aprender a programar.**

   Esta es considerada la habilidad fundamental de todo hacker. Para poder hacer esto, es requisito principal aprender lenguajes de programación, no uno, sino varios, como Python, Perl, etc. RAYMOND lo lleva incluso al punto de que se debe adquirir tal capacidad en el uso de los lenguajes que incluso se pueda aprender uno nuevo en un par de días, por lo que es necesario mucha práctica y dedicación. Una vez aprendidos los lenguajes es

que se puede iniciar el siguiente paso que es programar, sin embargo los hackers prestan poca atención a los métodos tradicionales de enseñanza, pues creen que ellos limitan, es por eso que estimulan principalmente en transformarse en un autodidacta, y de hecho la mayoría de los mejores hackers lo son, y esto gracias a que en la red es posible encontrar un sin fin de manuales y páginas en donde se explican los pasos básicos que dan el pie para desarrollar más.

Sobre esto RAYMOND escribe: "no puedo explicar en detalle en este documento como puedes aprender a programar – es una habilidad compleja. Pero puedo adelantarte que los libros y los cursos no servirán (muchos, y tal vez la mayoría de los mejores hackers son autodidactas). Lo que sí servirá es (a) *leer código* y (b) *escribir código*.

"El aprendizaje de la programación es como aprender a escribir bien un lenguaje natural. La mejor manera de aprender es leer algunas cosas escritas por los maestros del estilo, luego escribir algunas cosas tú mismo, leer mucho más, escribir un poco más...

y repetir esto hasta que lo que escribes empiece a mostrar la clase de fuerza y economía que ves en tus modelos."[83]

2) **Obtener, aprender a usar y a poner en funcionamiento un UNIX libre**

El sistema operativo preferido por los hackers son los basados en UNIX libres, como Linux, ello porque es el sistema propio de Internet y porque, además, permite a diferencia de los sistemas propietarios como Windows y Mac, que el usuario pueda acceder a su código fuente, estudiarlo y modificarlo a placer. Pero para un hacker no basta con tener uno de estos sistemas operativos, sino que es necesario conocerlo a fondo, aprender no sólo a instalarlo, cuestión que no es sencilla, sino también lograr que funcione a placer. Es decir, un hacker debe transformarse en una especie de "experto" en el uso de estos sistemas, ya que ellos son los que entregan las mejores herramientas para desarrollar su labor, las cuales son consideradas muy superiores a las que da, por ejemplo, Windows.

[83] Ibíd..

3) **Aprender a usar la World Wide Web y a escribir código html**

Internet es el mundo en que los hackers se sienten más cómodos, es su entorno natural, es por ello que deben conocerla a fondo, lo cual no sólo significa el aprender a navegar sino que también es menester conocer hasta los últimos aspectos de su funcionamiento. Es por ello que, además, todo buen hacker deberá saber escribir el código html, el cual es la base del funcionamiento de Internet.

Como dice RAYMOND "La mayoría de las cosas que ha construido la cultura hacker trabajan fuera de la vista del gran público, ayudando en el funcionamiento de fábricas, oficinas y universidades, y carecen de un impacto obvio en la vida de los que no son hackers. La Web es la única gran excepción, y es tan enorme y brillante este juguete de hackers que incluso los *políticos* admiten que está cambiando el mundo. Sólo por esta razón (y hay un montón de otras igualmente buenas) debes aprender como trabajar en la WWW.

> "Esto sólo no significa aprender a manejar un navegador (cualquiera puede hacer eso), sino que debes aprender a escribir HTML, el lenguaje de marcas de WWW. Si aún no sabes programar, el aprendizaje que implica la escritura de HTML te enseñará algunos de los hábitos mentales que te ayudarán luego con la programación."[84].

2.2.2.- Actividades que es necesario desarrollar para ser considerado un hacker u obtener "*status*" dentro de su ambiente.

Ya hemos dicho, los hackers adquieren su status de ser considerados como tal por otros hackers, y el ir escalando dentro de su escalafón, que significa tener más reconocimiento, es una cuestión que se obtiene en base a la labor realizada, a los programas escritos, al comportamiento respecto del resto, etc. "El hackerismo es lo que los antropólogos denominan *cultura de la donación*. Ganas status y reputación no mediante la dominación de otras personas, no por ser hermoso ni por tener cosas que otras personas desean,

[84] Ibíd..

sino por regalar cosas. Específicamente, al regalar tu tiempo, tu creatividad, y el resultado de tus habilidades"[85].

Dentro de estas actividades que es necesario implementar para ser considerado un hacker o para adquirir mayor reconocimiento dentro de su mundo, RAYMOND nos señala que algunas de ellas son las siguientes:

1) **Escribir software libre**, en particular programas que sean de utilidad para otros hackers o personas en general. Mientras más útil y de mayor capacidad el programa que se cree mayor consideración se adquirirá en el mundo hacker. Pero no basta con crear el programa, además es menester que este se ponga a disposición del resto, en la forma de código abierto, que cualquiera pueda leer y aprender de él o modificarlo de acuerdo a sus requerimientos. Es importante señalar que en Internet abundan los sitios con este tipo de softwares de código abierto y gratuito, principalmente dentro del ámbito de las herramientas necesarias para el desarrollo web, en el cual adquieren el nombre de scripts.

[85] Ibíd..

2) **Ayudar a probar y depurar software libre.** Es esta una labor que se considera casi tan importante como la anterior, puesto que como ya hemos señalado la cultura y el desarrollo hacker se nutre del trabajo corporativo, en el cual las obras creadas, en este caso programas, se van mejorando y perfeccionando mediante la labor de varios hackers que al descubrir una falla o bug en un software la analizan e intentan solucionarla, cuestión que luego también beneficia al resto. Asimismo, también es muy reconocida la labor de los llamados "*beta-testers"*, es decir, el trabajo de aquellos que toman un programa en su versión beta (de prueba) y lo usan para probar sus características e informar acerca de posibles fallos que se detecten, por cuanto ello también es una forma de ayudar al trabajo cooperativo y al perfeccionamiento de las creaciones hacker.

3) **Publicar información útil.** Tal vez una de las cuestiones que más han favorecido el hecho de que vayan apareciendo más hackers sea el que a través de Internet es factible, con cierta facilidad, encontrar documentos muy completos, en forma de

manuales o FAQS (preguntas frecuentes) con las cuales quien lo desee puede aprender los pasos básicos o perfeccionarse dentro de un área determinada gracias a la experiencia sistematizada de lo que otros hackers han hecho y descubierto. Es por eso que se valora la labor de quienes se encargan de mantener estos sitios con información técnica, cuestión que en ocasiones demanda mucho trabajo, pues ello ayuda a los hackers en su desempeño.

4) **Ayudar a mantener en funcionamiento la estructura.** Como ya se ha dicho, la cultura hacker y el desarrollo de la Internet en gran medida es posible gracias al trabajo desinteresado de muchas personas, quienes deben en ocasiones desempeñar funciones no siempre gratas o "entretenidas", como servir de moderadores en los canales de discusión, mantener listas de correo, administrar sitios donde se almacenen los softwares creados, etc. "La gente que desarrolla estas actividades goza de mucho respeto, porque todos saben que esos trabajos son grandes

consumidores de tiempo y no tan divertidos como meterse con el código. Los que lo llevan adelante demuestran su dedicación"[86].

5) **Hacer algo por la cultura hacker en sí misma.** Finalmente, según RAYMOND una cuestión importante para poder ser reconocido entre los hackers es realizar acciones que tengan por objetivo difundir su cultura, su pensamiento, sus valores. Pueden existir muchas formas de hacer esto, sin embargo sólo estará realmente autorizado a ello alguien que verdaderamente sea un hacker, sea reconocido como tal por sus pares y que haya hecho asimismo alguna de las actividades ya arriba señaladas. Es decir, no cualquier hacker puede arrogarse la atribución de hablar sobre la cultura con una carácter valorado por el resto si primero no ha adquirido un grado alto de reputación en el medio.

Como podemos observar detrás del término hacker hay bastante más que sólo jóvenes jugando a ser los nuevos "antihéroes" de Internet, al estilo de los personajes de las novelas del Far West norteamericano. El fenómeno

[86] Ibíd..

hacker es un hecho complejo que ha traído aparejado la revolución tecnológica, y aunque en este apartado sólo nos hemos dedicado a realizar una breve exposición de los principales aspectos del fenómeno hacker sistematizado por algunos de sus más destacados y conocidos teóricos, es claro que con ello sólo hemos dados una pequeña aproximación a lo que el tema en sí significa. Detrás del accionar y de la ideología hacker hay variados otros aspectos, los cuales en muchos casos responden a criterios técnicos, no propios de ser expuestos en una memoria en derecho.

Un hecho que si nos gustaría destacar, es que en ninguno de los textos que hemos revisado sobre la materia, ni en los citados ni en otros que hemos tenido a la vista para escribir estas líneas, se hace referencia a que el ingreso no autorizado a un sistema constituya una de las características propias y necesarias para ser considerado un hacker. Y ello es lógico, el fenómeno hacker tiene más que ver con una pasión, casi compulsiva, por la información y por descubrir los rincones más intrincados de la informática que con un deseo por inmiscuirse en los asuntos de otras personas. Como se puede derivar de lo anteriormente expuesto, en general cuando un hacker ingresa de manera no autorizada a un sistema es porque desea conocerlo y descubrir sus imperfecciones, pero ello no con la finalidad de robar datos o

destruir algo, sino únicamente por el deseo de sentir que se tiene la capacidad para vulnerar cualquier sistema de seguridad y para demostrar que nada es absolutamente inviolable. De hecho, esto se condice con el hecho de que en muchas ocasiones son esos mismos hackers que ingresan ilícitamente a un sistema quienes luego advierten a sus administradores de los fallos presentados por este para que sean solucionados. No por nada en habitualmente, cuando una empresa descubre a un hacker que ha violado su seguridad en vez de denunciarlo a las autoridades prefiere contratarlo y encargarle que vele por solucionar los agujeros que el sistema presente. Cabe destacar que los mejores expertos en seguridad de redes son, o han sido, precisamente hackers. Además, como nos comentaron algunos hackers (o proyectos de hackers) que hemos tenido oportunidad de conocer en el curso de esta investigación, "si los sistemas los hicieran bien no habría para que entrar en ellos para demostrar su vulnerabilidad", lo cual es principalmente válido para los productos de Microsoft, el gigante informático, que es el más atacado por los hackers, no sólo por identificarlo con el lucro indiscriminado de la informática, que a su juicio debe ser libre y gratuita, sino también porque esta empresa construye los sistemas informáticos que, aunque más difundidos, son los más vulnerables e

imperfectos. Los hackers han construido Linux, y sin duda este funciona mucho mejor que Windows, aunque no esté tan difundido.

3.- Los Crackers

Ya anteriormente hemos visto que los crackers son considerados, en términos generales, como una especie de hackers del lado oscuro o como hackers que no respetan los principios éticos que se han ido estableciendo para este tipo de subcultura. Sin embargo, ¿es entonces propio hacer coincidir los términos hacker y cracker diferenciándolos únicamente por los fines que persigue cada uno? Creemos que no, y para afirmar esto nos basaremos en los argumentos que a continuación expondremos.

En primer lugar queremos dejar fuera de la significación del término hacker todo tipo de sujetos que deambulan por Internet y cuyos conocimientos se limitan a sólo utilizar las herramientas creadas por otros (hackers o crackers) con el objeto de divertirse o causar un daño innecesario por el sólo objeto de molestar al resto, en este caso nos referimos especialmente a los individuos que hemos denominado lammers más arriba.

Asimismo, también queremos dejar fuera de este grupo del *underground* digital a los simples piratas informáticos, o individuos que se

dedican a obtener copias ilegales de programas para luego venderlas en la realidad no virtual (calles , mercados, etc.) o distribuirlas a través de Internet, puesto que en la mayoría de esos casos no se requieren conocimientos informáticos especiales de ningún tipo para cometer el delito, sino que basta con contar con las herramientas de software y hardware adecuadas para beneficiarse económicamente de la acción.

Cuando hablamos de crackers, al igual que cuando lo hicimos respecto de los hackers, nos estamos refiriendo a individuos que cuentan con niveles avanzados de conocimiento informático, aunque en este caso las motivaciones no las adquieren necesariamente del sólo afan de aprendizaje y curiosidad que vimos caracteriza a los hackers, sino que en la mayoría de estos casos lo que se persigue es algún rédito económico de la actividad de "crackear". Es cierto que en muchos casos, antes de cometer un acto ilícito, la actividad de hackers y crackers puede confundirse. Ambos pueden entrar subrepticiamente a un sistema determinado y "husmear" por entre cada uno de sus archivos hasta descubrir una información que pueda ser de utilidad. Pero mientras el hacker se limitará a sólo mirar y a sentirse satisfecho con el sólo hecho de haber logrado ingresar, el cracker buscará obtener información que luego le pueda reportar algún tipo de beneficio de tipo

material, como si logra hacerse con el diseño de un programa aún no salido al mercado, o si logra descubrir claves de tarjetas de crédito que luego pueda usar o vender, etc.

En el caso anterior, como vemos, hacker y cracker sólo se diferencian en cuanto a las motivaciones.

Sin embargo, también existen otras clases de crackers, los que tal vez no son tan conocidos por sus actividades en el "mundo real", pero que sin duda en Internet se encuentran muy difundidos y son muy conocidos. En este caso nos referimos a aquellos sujetos que más que especializarse en el ingreso no autorizado a sistemas lo que hace es dedicarse a descubrir y hacer saltar las protecciones con que cuentan algunos programas con el objeto de que ellos puedan ser usados libremente más allá de los límites permitidos por sus desarrolladores.

Daremos un ejemplo para ilustrar lo anterior.

El programa Norton Antivirus de la empresa Symantec[87] es sin duda el software para el control y la eliminación de virus informáticos más conocido y usado del mercado, además de ser una de las utilidades más

[87] http://www.symantec.com

eficaces a la hora de tratar con este tipo de plagas. Pues bien, Symantec, al igual que muchas de las empresas que operan en Internet, utiliza una forma bastante "sui generis" de difundir sus productos y crear la necesidad de ellos en los usuarios. Esto lo hace mediante la entrega de una copia de evaluación de su producto por un período de 30 días, término durante el cual el programa en cuestión es completamente funcional, perdiendo todas sus características una vez cumplido el plazo antes señalado. Ahora bien, como es prácticamente imposible navegar por Internet sin contar con un sistema antivirus, una vez cesado en sus funciones el software de evaluación el sujeto se verá obligado a comprar el producto o a instalar otro que sea similar y que generalmente también le será funcional por otros 30 días, lo cual en sí es muy molesto, ya que es menester aprender el manejo de un nuevo programa y además no siempre se obtiene de esta forma una protección óptima. Ahora bien, en este momento es que cobra relevancia la labor de los crackers. Lo más seguro es que al tiempo en que el individuo vea caducado su derecho a usar lícitamente del programa en cuestión (o incluso desde antes), ya exista en Internet una aplicación que le permita eliminar la limitación de los 30 días que el software trae, habilitándolo para ser plenamente funcional por el lapso de tiempo que el sujeto elija,

generalmente de un año, hasta que aparezca una nueva versión del programa. A esta aplicación se le denomina crack, porque rompe el mecanismo de seguridad transformándolo en inservible. Y lo que hemos dicho es válido para la mayoría de los programas que hay en Internet, salvo para algunos de los que no es posible obtener copia de evaluación, pero los cuales de igual forma pueden ser adquiridos ilícitamente en la red, ya sea a través de algún sitio de warez (lugar en que puede obtenerse una copia completa del programa, no de evaluación) o mediante algún programa de intercambio peer to peer, como el Kazaa o el Edonkey.

Acá encontramos entonces otro tipo de cracker, uno cuya finalidad aparentemente es más "altruista", poner al servicio de todo el mundo todas las aplicaciones que le sean necesarias, y ello sin tener que desembolsar nada de dinero. De hecho es esta labor la cual le reporta más pérdidas a la industria del ramo, puesto que cualquiera con los conocimientos mínimos necesarios puede hacerse con todos los programas que necesite o sólo desee y sin necesidad de comprar ninguno, puesto que tan pronto como un programa sale al mercado, o incluso antes, los crackers encuentran la forma de vulnerarlo o de hacerlo circular en forma gratuita.

Es por lo anterior que entonces hay que tener cuidado al hablar de los crackers y mirarlos sólo como un grupo de individuos ávidos de enriquecerse a costa del daño de terceros, puesto que esta fama viene más bien de los hackers o de algunos autores que no saben distinguir entre los distintos tipos de sujetos que pueblan el ciberespacio.

Sobre el punto un cracker ya anteriormente citado señala lo siguiente:

"En este año 1995, puedo entrar en cualquier biblioteca, coger CUALQUIER libro, fotocopiar todas las páginas si lo deseo. Todo esto es perfectamente legal, por lo menos aquí en Suecia. El estado sueco (como tantos otros) a decidido que sus ciudadanos tenían el derecho de copiar los libros.

"Ahora, vuelvo a casa. Miro mi lector de CD. No tengo derecho de hacer una cinta de mis fragmentos favoritos. Es ilegal. Miro mis cintas de video. No tengo derecho de copiarlas. Es ilegal. Miro mis cajas de disquettes que contienen los softwares Microsoft que he comprado. Pues si, tengo derecho de hacer copias de salvaguarda, pero no de dárselas a mis amigos. Es ilegal.

"Me pone enfermo! Qué diferencia hay, entre los softwares, los CD, las cintas de video y los libros que he tomado prestados a la biblioteca del

barrio? Por Dios, todo eso es información! En este caso, el problema no es la información en si. El problema es que esta sociedad me ha condicionado a creer que teníamos derecho de poseer la información, como la tierra o el dinero, o como los Griegos o los criadores del sur de algodón que pudieron creer que tenían el derecho de poseer LA GENTE. A eso le llamaban la esclavitud. Me doy cuenta que soy un esclavo de la sociedad que controla la información. Porque de eso se trata. De controlar. Completo absoluto indiscutible control.

"No os estoy diciendo que quiero que la leyes sobre los derechos de autores sean reemplazadas por el caos. Si así lo deseará, sería una bestia destructiva y no un ciudadano constructivo. Amo nuestra sociedad, y pienso que es una de las mejores al mundo. Amo todavía más las comunidades del cyberespacio como la escena o Usenet, porque son internacionales y multiculturales. Eso es el porqué quiero decirle a la sociedad que algo no funciona. Quiero dar un toque de silbato mientras hay tiempo.

"No tengo nada en contra de las compañías de softwares y no las odio. De hecho, quiero que existan compañías de softwares. Lo que no me gusta, es la estructura social y el desarrollo económico que gobierna la gente como las empresas, y a las cuales deben obedecer. Al igual, pienso

que tanto las empresas como la gente esta cautivada por este sistema. Decís que alguien tiene que pagar. Por qué? De todos modos, en qué consiste este pago? Qué es el "saber bajo licencia" y el "saber en el ámbito público" ? O bien, para utilizar el propio lenguaje de la autoridad: en qué consiste este timo de la "propiedad intelectual" alrededor de la cual hacéis tanto escándalo? Qué información tengo derecho de poseer? Qué información tengo derecho de arrebatar en mi cabeza?

"Para los partidarios de la economía posmoderna, la propiedad y el derecho sobre la información son una religión. Siguen los dioses de la economía y piensan que estarán en el paraíso el día en el cual se convertirán en yuppies con traje y corbata. Para ellos, el tío que muera dejando un máximo de coches y de artilugios electrónicos tras el, habrá sido el más listo del grupo. Por Dios, odio estos semidioses. No hay nada con cabeza cuadrada, que no sea información, yuppies. Tal vez el único en darse cuenta, haya sido William Gibson, en 1982. Sin embargo, poca gente entendió lo que quería decir. Tal vez, ni siquiera, el mismo estaba conciente de ello.

"El cambio necesario en esta sociedad, es arrebatar lo adquirido del control de las grandes compañías y del estado para devolverlo a la gente a

quién le pertenece, a defecto de que el mundo tenga todo lo necesario para parecerse al mundo que describía Gibson en "Neuromante".

“Es por lo que tomamos el nombre de cyberpunks. Somos gente al margen de la ley , enchufados y conectados. Haremos nacer una nueva era. A nuestro parecer, la información electrónica no es un símbolo o un estatus, o una forma de ganar dinero así como la consideración general, pero una extensión del espíritu humano. Por eso, Timothy Leary a dado el nombre de LSD al micro- ordenador de los años 90 - los ordenadores parecen ensanchar el campo de visión de la gente.

“Por dios, no queremos robar las empresas. Sencillamente, queremos que nos devuelvan nuestros derechos de ciudadanos. Si tengo en mi posesión un poco de información, quiero tener el derecho de copiarlo. Y si intenta impedírmelo, seguro que me sacará de quicio. No toquen a mi vida privada! Larguense de mi vida!

“Para mi, mi ideología arde como una linterna en la oscuridad. No es una ideología de liberalismo, ni el socialismo, el conservatismo, el comunismo o todas estas ideologías que nos enseñan en la escuela. Mi ideología se llama Cyberpunk.

"Los mafiosos que se acaparan las tierras, los piratas que ganan unas fortunas vendiendo juegos a unos desdichados locos del ordenador, los que se ganan la vida siendo parásitos de la sociedad, todos estos, los podéis volatilizar e incluso matarles si os place. Nadie los echará de menos. PERO, SOBRE TODO, NO TOQUEIS LOS CRACKERS Y LOS SWAPPERS, pues, ellos no son vuestros enemigos. Un verdadero cyberpunk jamás haría pagar una información. Simplemente intercambia, y pienso que tiene todo el derecho. No quiero destruir, quiero crear"[88].

Como podemos desprender de lo anterior, lejos están este tipo de crackers, como a su vez también vimos en los hackers, de creerse alguna especie de bandido del ciberespacio ansioso por obtener dinero de una forma fácil. Los crackers también cuentan con una ideología en la cual fundamentan su actuar y de acuerdo a ella en modo alguno lo que ellos hacen puede considerarse dañino, sino que se ven a sí mismos como una especie de paladines de la liberalización de la información, que no otra cosa son, en resumidas cuentas, los programas.

---

[88] FISHER, KING, La Conciencia de un Cracker, http://www.df.lth.se/~triad/triad/3words/Consesp.html

Lamentablemente, a diferencia de lo ocurrido respecto de los hackers, en el caso del estudio de los crackers fue prácticamente imposible encontrar una cantidad de textos mayor que nos permitieran adentrarnos con paso más seguro en el submundo de esta rama de la familia del *underground* digital. Sin embargo, como podemos observar en la declaración trascrita de FISHER, él se define a sí mismo y a los crackers como "*cyberpunks"* lo cual puede arrojar algunas otras luces respecto del pensamiento cracker. El movimiento cyberpunk nace principalmente desde la literatura, como un área desprendida de la ciencia ficción tradicional, y la cual centra su polo de atención en la revolución informática y en las consecuencias de ello para la vida de las personas. Los principales autores cyberpunk fueron WILLIAM GIBSON y el ya nombrado BRUCE STERLING. Desde un punto de vista político ideológico los cyberpunks han planteado los peligros que entraña el manejo de la información y el alto grado de control de las personas que se puede lograr a través de ello, lo cual permitiría a los centros de poder dirigir y conocer hasta los aspectos más íntimos de la vida de los individuos. Frente a ello es que se en primer lugar se rebelan los cyberpunks, puesto que parar ellos la tecnología y la información no puede transformarse en una nueva herramienta de dominación sino que deben estar al servicio de

las personas mejorando sus niveles de vida. En este punto lo planteado por los *cyberpunks* se parece bastante a lo señalado por los hackers, quienes también creen en la libertad de la circulación de la información y ven a la revolución tecnológica como un medio de elevar los niveles de vida de las personas.

El asunto es, sin embargo, que las respuestas dadas frente a la realidad de los intentos por ejercer por parte de los Estados u otros centros de poder, cada vez mayores niveles de control por sobre lo que circula y se hace en la red, son distintas. Mientras los hackers se manifiestan sólo a favor de conocer y descubrir los mecanismos sin luchar directamente en contra de ellos, los crackers toman una posición más bien activa y pretenden luchar en contra del establishment existente, para lo cual no se niegan, en general, al uso de ninguna de las herramientas que el mismo entorno informático les brinda.

Tenemos entonces que, a diferencia de lo que tratan de hacernos creer los hackers y los autores que no se han adentrado demasiado en el mundo cracker, estos individuos si tendrían una vertiente que poseería un carácter más bien altruista y con una posición política e ideológica meridianamente definida, la cual gira particularmente en torno a la información y a libertad

de que debe gozar la circulación de esta como medio de favorecer el desarrollo de la humanidad y el mejoramiento en las condiciones de vida de los individuos. Este sector de los crackers toma una posición dentro del ciberespacio y su labor adquiere expresión principalmente en el área de la liberación de los programas informáticos, desarrollando las herramientas necesarias para que éstos puedan ser asequibles a cualquier persona, no importa el lugar del mundo en el que se encuentre, siempre y cuando cuente con un acceso a la red. De hecho, nuestra experiencia personal mientras desarrollábamos esta investigación, es de que en términos generales los medios de difusión de la actividad cracker y de las herramientas desarrolladas por estos en modo alguno pueden ser consideradas como unas máquinas para crear dinero, puesto que contrariamente a lo que uno podría pensar al leer alguna literatura, los sitios crackers son la mayoría de las veces sitios de acceso gratuito, en los cuales ni siquiera es menester dejar una dirección de email para obtener las utilidades que en ellos ofrecen. En algunos de esos sitios, tal vez la única fuente de ingresos que se ve a simple vista es la publicidad, sin embargo ello no creemos que sea motivo suficiente para considerarlos una especie de “ciberambiciosos” o de sujetos cuyo único móvil sería el enriquecimiento fácil, rápido y habitualmente por

medios ilícitos. Sin embargo, frente a esta misma vertiente existen otros sujetos también llamados crackers que en su actuar responden a todos los calificativos empleados tantos desde la órbita hacker como desde el mundo no virtual, los cuales carecen en absoluto de algún tipo de objetivo o ideología que no sea la de causar daños innecesarios o el de enriquecerse ilícitamente. Lamentablemente creemos que son estos últimos quienes crean un mayor manto de mala reputación entre la familia cracker, sin que necesariamente sea propio considerarlos dentro de tal entorno, puesto que más que crackers son habitualmente simples y burdos piratas informáticos, ladrones o ciberterrorístas, que en nada responden al pensamiento de los otros crackers que hemos hablado, sin embargo dichos ciberdelincuentes son los más reconocidos no sólo por el mundo real sino también por el virtual y a ellos es a quienes se les aplica el apelativo de crackers en la acepción más usada a que ya antes nos hemos referido, y aunque creemos que no siempre es propio hablar de crackers en este sentido, hemos preferido en el resto de este trabajo mantener la nomenclatura "oficial" y seguir llamando crackers a estos piratas informáticos, aunque en cada oportunidad que sea menester haremos la distinción con los otros crackers,

esos que los son por una postura ideológica y no por la mera persecución de intereses egoístas.

V. Hackers y crackers ante el derecho

En los acápites anteriores, hemos realizado una aproximación general a lo que el fenómeno hacker y cracker significa, privilegiando el uso de la información que pueda llevar a una comprensión de lo que son estos fenómenos más completa y ligada al mundo propio de Internet, a diferencia de lo que ocurre habitualmente en los textos nacidos sobre el tema desde la esfera jurídica, en los cuales se atiende en variadas ocasiones más a una repetición casi mecánica de conceptos que a un verdadero esfuerzo por descubrir lo que hay realmente detrás de estas conductas, los sujetos que intervienen y los móviles que las inspiran.

Ahora bien, determinado lo que hackers y crackers son, es tiempo de ver cuál es el tratamiento que de estos comportamientos se ha hecho en la legislación, especialmente nacional, puesto que más allá que en ocasiones pueda apelarse a legítimos intereses o loables motivaciones a la hora de llevar adelante algunas de estas conductas, es un hecho que, principalmente tratándose del cracking, ellas involucran atentados graves y directos a bienes jurídicos que el derecho debe proteger, cuestión que no siempre ocurre, o que, de hacerlo, no en todos los casos es con un manejo de la

técnica legislativa que en verdad garantice los derechos de quienes se ven afectados por este tipo de actos.

1.- Hackers y crackers en el derecho internacional. La Convención Internacional contra el Cibercrimen

Aunque es necesario reconocer que, hasta el momento, en el mundo se ha avanzado a pasos agigantados en la persecución y sanción de los delitos conocidos como cibercrimen, es un hecho que en este camino aún queda mucho por recorrer. Todavía existen un sinnúmero de debilidades que es menester subsanar para que los esfuerzos invertidos en este ámbito no queden sólo en declaración de buenas intenciones, y para que la lucha en contra de este nuevo flagelo se transforme en eficiente y eficaz. Una de ellas es la ya vista dificultad en alcanzar consensos en cuanto a la definición y caracterización de lo que son los delitos informáticos, en particular de aquellos que dicen relación con Internet. No es posible el lograr una verdadero combate en contra de estos ilícitos si no se cuenta con tipos penales claros que faciliten la labor de quienes tienen a su cargo el llevar adelante la aplicación de las normas. “En el contexto global en que vivimos los países deben estar necesariamente de acuerdo de qué se trata el delito

informático para poder enfrentarlo. Sobre este punto no hay mucho acuerdo todavía"[89].

Lo anterior, se hace mucho más patente tratándose del contexto del derecho penal informático, por cuanto, como ha sido ya ampliamente destacado en la doctrina, no es posible aplicar este sistema sancionatorio sin respetar el básico principio de la legalidad, *nulla poena sine lege*, de acuerdo al cual nadie pueda ser culpado ni condenado sino en virtud de una ley dictada con anterioridad a la comisión del delito que se imputa.

Otra debilidad del sistema legal para combatir el cibercrimen se encuentra en lo anacrónicas de muchas de las normativas que se deben aplicar a su respecto. Pese a que algunos países, como el nuestro, han ido creando una legislación más actual, que sea capaz de hacer frente a las particularidades de este tipo de ilícitos, es claro que lo nuevo del tema y el hecho de que él se desarrolle a un ritmo vertiginoso provoca que muchas de las normas que se dictan especialmente a este efecto queden rápidamente en la obsolescencia o se transformen en letra muerta, inútil o imposible de aplicar, situación a la que también coopera el hecho de que quienes están

---

[89] El Problema Legal de Combatir el Crimen Cibernético, http://www.ciudadfutura.com/internet/cibercrimen13.htm.

encargados de velar por la aplicación de estas normas, en la mayoría de los casos, carecen de los conocimientos técnicos necesarios para hacerlo. Y con esto nos referimos no sólo a los investigadores, sino que a todo el sistema jurídico penal, por cuanto en los juzgados y entre los abogados aún hay sujetos que ni siquiera poseen los conocimientos básicos que le permitan acercarse sin temor a un computador, con lo cual difícilmente podrían entonces estos comprender en su real dimensión lo que el fenómeno del cibercrimen significa, sus principios, alcances y características, así como la forma de perseguirlo y prevenirlo.

En atención a lo anterior, y a que las deficiencias legislativas respecto del cibercrimen se presentan no sólo a nivel nacional, sino también internacional (y quizá con más fuerza en este último ámbito, ya que una de las características del cibercrimen es que él se lleve a cabo, en todos los pasos hasta su consumación, involucrando no sólo a un Estado, sino que a varios, puesto que para realizarse utilizan sus autores la Internet, la cual no tiene nacionalidad ni residencia, sino que es un espacio que trasciende a lo local situándose en la globalidad, en donde el grado de indefensión de las posibles víctimas es aún mayor), es que en noviembre del 2001 se adoptó por más de 30 países la Convención contra el Cibercrimen, la cual pretende

ser el marco regulatorio internacional que sirva de base para llevar adelante la lucha en contra de estos ilícitos.

1.1.- Antecedentes

En noviembre de 1996, por decisión CDPC/103/211196, el European Committee on Crime Problems (CDPC) ordenó establecer un comité de expertos cuya labor central estaba destinada a estudiar la problemática del cibercrimen y su forma de regulación. El motivo para adoptar esta resolución fue fundamentado de la siguiente forma:

"Los rápidos progresos en el campo de la tecnología de la información tienen un impacto directo en todas las áreas de la sociedad moderna. La integración de los sistemas de telecomunicación y de información permiten el almacenamiento y la transmisión, sin importar la distancia, de toda clase de comunicaciones lo cual abre un abanico de nuevas posibilidades. Estos progresos fueron estimulados por la aparición de las autopistas y de las redes de información, incluyendo el Internet, a través del cual virtualmente toda persona podrá tener acceso a cualquiera de los servicios de la información electrónica, independientemente del lugar del mundo en que esté situado. Conectándose con los servicios de la

comunicación y la información, los usuarios crean una clase de espacio común, llamada "Ciberespacio", que puede ser utilizado para propósitos legítimos pero que también puede ser objeto de un uso indebido. Estos "delitos del Ciberespacio" son habitualmente cometidos en contra de la integridad, disponibilidad y confidencialidad de los sistemas informáticos y redes de telecomunicación o ellos consisten en el uso de tales redes o de sus servicios para cometer delitos tradicionales. El carácter transfronterizo de tales delitos, v. gr. cuando son cometidos a través del Internet, está en conflicto con la territorialidad del derecho nacional que deben aplicar las autoridades.

El derecho penal debe por tanto mantenerse al corriente de estos adelantos tecnológicos, los cuales ofrecen oportunidades altamente sofisticadas para hacer un mal uso del ciberespacio y causar daño en intereses legítimos. Dada la naturaleza transfronteriza de las redes de información, un esfuerzo internacional concertado es necesario para ocuparse de tales usos indebidos. Mientras que la Recomendación No. (89) 9 ha resultado en la aproximación de los conceptos nacionales respecto a ciertas formas de uso indebido del ordenador, solamente un instrumento internacional obligatorio puede asegurar la eficacia necesaria en la lucha

contra estos nuevos fenómenos. En el marco de tal instrumento, deben ser tratados, además de medidas de cooperación internacional, las cuestiones de la ley substantiva y procesal, como también materias que están conectadas de cerca con el uso de la tecnología de la información"[90].

De acuerdo a la Decisión antes señalada, la labor de este Comité de expertos, el cual se estableció por Decisión Nº CM/Del/Dec(97)583 y fue denominado Committee of Experts on Crime in Cyber-space (PC-CY), debería estar centrada en el análisis, a la luz de las Recomendaciones Nº R (89) 9 y Nº R (95) 13, de las siguientes cuestiones[91]:

1. Los delitos del ciberespacio, en particular aquellos cometidos mediante el uso de redes de telecomunicación, entre los que se entiende incluido Internet, como transacciones ilegales de dinero, ofrecimiento de servicios ilegales, violación de los derechos de la propiedad intelectual, etc.

2. Otros aspectos de derecho penal sustantivo en donde fuese necesario realizar un acercamiento para perfeccionar la

---

[90] COMITÉ DE MINISTROS DEL CONSEJO DE EUROPA, Convention on Cibercrime, Explanatory Report adoptado en noviembre 8 del 2001. (La traducción es nuestra). http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[91] Ibíd..

cooperación internacional, como definiciones, responsabilidad y sanciones de los actores del ciberespacio, etc.

3. El uso, incluyendo la posibilidad de usos transnacionales, de medidas coercitivas en el ambiente tecnológico, como la intercepción de telecomunicaciones y vigilancia electrónica de redes de información, la búsqueda e incautación de sistemas de procesamiento de información (incluyendo sitios de Internet), etc.

4. La cuestión de la jurisdicción en relación a los delitos de la tecnología de la información, por ejemplo para determinar el lugar en donde el delito fue realizado (*locus delicti*), y que ley se debe aplicar consiguientemente, incluyendo el problema del *non bis inidem* en el caso de que múltiples jurisdicciones puedan ser aplicables. También se debería analizar la cuestión de cómo solucionar conflictos positivos de jurisdicción y cómo evitar conflictos negativos de la misma.

5. Asimismo, también debería analizar las cuestiones relativas a la cooperación internacional en la investigación de los delitos del ciberespacio, ello en estrecha cooperación con el Committee of

Experts on the Operation of European Conventions in the Penal Field (PC-OC).

6. Finalmente, estaría dentro de las funciones de este Comité el realizar el borrador de un instrumento jurídico obligatorio, tan pronto como le fuere posible, en el que se incluyeran los anteriores puntos, poniendo un énfasis especial en las cuestiones internacionales, además, de ser ello posible, también debería realizar recomendaciones accesorias respecto a políticas específicas que fueren necesarias de acuerdo a la evolución del entorno tecnológico.

El Comité comenzó sus labores en abril de 1997, y estaba presupuestado que estas concluyeran, a más tardar, el 31 de diciembre de 1999. Sin embargo las negociaciones en modo alguno fueron fáciles, debido a que los temas tratados durante ellas estaban ligados a muchos derechos considerados como fundamentales, como la libertad, la intimidad, etc., surgiendo desde diversos sectores voces disidentes que abogaban porque la normativa no fuera adoptada, al menos no en los términos en los que estaba siendo concebida. Es por ello que en la Decisión de los Ministros Nº

CM/Del/Dec(99)679, se acordó extender las discusiones sobre el tema hasta el 31 de diciembre del 2000.

Entre abril de 1997 y diciembre del 2000, el Comité PC-CY celebró 10 reuniones en sesión plenaria y 15 en su función de redactor del borrador para el Convenio. Además, una vez cumplido el plazo extendido que le había dado el Consejo de Ministros, realizó 3 sesiones más para concluir el memorando explicativo del borrador y revisar el proyecto de Convención a la luz de la opinión de la Asamblea Parlamentaria. La Asamblea, en abril del 2001, a solicitud del Comité de Ministros, adoptó una opinión respecto al borrador del Convenio.

El proyecto de Convención revisado y concluido y su Memorando Explicativo fueron sometidos para la aprobación al CDPC en su 50.a sesión plenaria en junio del 2001, y a continuación el texto del proyecto fue sometido al Comité de los Ministros para la adopción y la apertura para la firma. El 23 de noviembre del 2001, en Budapest, el Convenio se abrió para la firma de los Estados miembros y para la de los Estados no-miembros que participaron en su elaboración, y para la accesión por parte de otros Estados no-miembros, necesitando de la ratificación de 5 Estados para que él entre

en vigencia, debiendo ser al menos 3 de ellos miembros del Consejo de Europa.

Al momento de escribir estas líneas, 31 Estados habían firmado el Convenio, entre los que se cuentan, además de los Estados miembros del Consejo de Europa, Canadá, Japón, Sudáfrica y Estados Unidos, pero ninguno lo había aún ratificado.

1.2.- Objetivos y estructura de la Convención

En cuanto a su estructura, la Convención consta de cuatro capítulos, distribuidos de la siguiente forma:

a. El Capítulo I, el cual consta de un solo artículo y se aboca definir determinados términos, como sistema computacional, proveedor de servicios, etc.

b. El Capitulo II, denominado "Medidas para ser tomadas a nivel nacional", consta de 3 secciones. La primera de ellas está referida a los aspectos de la ley penal sustantiva, en la cual se definen varios delitos, la mayoría de ellos relacionados con conductas tradicionalmente consideradas de hacking o cracking; la segunda sección se refiere a las

normas de procedimiento, las cuales en su aplicación van más allá que solamente los delitos contemplados en la sección primera, sino que ellas son validas para toda conducta ilícita realizada mediante un sistema informático; finalmente, la tercera sección se refiere a las normas sobre jurisdicción.

c. El Capítulo III denominado "Cooperación Internacional", se aboca al tratamiento de la ayuda mutua que se deben prestar los Estados Miembros de la Convención en la lucha en contra de las actividades ciber-delictivas, así como a las reglas sobre extradición.

d. Finalmente el Capítulo IV contiene las cláusulas finales que en términos generales, y salvo algunas excepciones, repite las provisiones comunes utilizadas para los tratados del Consejo de Europa.

En cuanto a los objetivos perseguidos por la adopción de esta Convención, ellos se encuentran fundamentalmente expresados en el Preámbulo de la misma, pudiendo destacarse:

1) Armonizar las normativas nacionales en el ámbito del derecho penal sustantivo en aquellas materias que estuvieren vinculadas con el cibercrimen.

2) Proveer a los sistemas nacionales de normas de procedimiento que posean los poderes suficientes para llevar adelante la investigación y persecución de aquellos ilícitos cometidos por medios informáticos o relacionados con ellos.

3) Establecer un régimen rápido y efectivo de cooperación internacional.

1.3.- La Convención sobre el Cibercrimen y las conductas de hacking y cracking

Como antes hemos hecho notar, gran parte de las normas sustantivas de derecho penal contenidas en el Capítulo I de la Convención se encuentran destinadas a conseguir una efectiva sanción de conductas que caen dentro de lo que tradicionalmente es considerado como conductas de hacking y cracking.

Respecto de lo que normalmente se considera como hacking, es decir el acceso no autorizado a un sistema informático, el artículo 1º de la

Convención señala que cada una de las Partes deberá adoptar las medidas legislativas y otras que sean necesarias conformes a hacer perseguible dentro de su ordenamiento interno el acceso voluntario a todo o parte de un sistema computacional[92], entendiéndose a éste como cualquier dispositivo, o grupo de dispositivos interconectados o relacionados, uno o varios de los cuales realiza un tratamiento automático de datos[93]. Dicho acceso debe ser realizado por quien carezca del derecho a hacerlo, con lo cual, obviamente se excluyen todos aquellos casos en que es permitido y legítimo realizar el acceso, como sería por ejemplo el entrar en un sistema de FTP poseyendo las claves y autorizaciones necesarias para hacerlo.

Ahora bien, la norma en cuestión más allá de los elementos obligatorios que deberá contener la normativa armonizada que los países en su virtud adopten, es decir, la necesidad del acceso voluntario y que este sea no autorizado, establece la facultad para los Estados Parte de señalar otros requisitos para sancionar este tipo de conductas, como pueden ser el que el acceso sea realizado mediante violación de sistemas de seguridad, como sería forzar un sistema protegido por password; que sea realizado con

---

[92] CONVENCIÓN CONTRA EL CIBERCRIMEN, artículo 2º.
[93] Ibíd.., Artículo 1ª.

la intención de obtener datos del ordenador u otra intención deshonesta, con lo cual se agregaría un elemento volitivo al mero acceso o que se realice a un ordenador interconectado con otro mediante algún sistema de red, sea de área local o de acceso remoto como Internet[94].

Como podemos observar, a este respecto la comisión redactora de la Convención y los Estados que concurrieron a su firma dan cuenta de un hecho que causa aún mucha discusión en los círculos vinculados a estas temáticas, el de si el mero acceso o intrusismo, es decir, el simple hacking en su acepción normal, constituye o no específicamente un delito. En ello se ha tomado en consideración el hecho de que en muchas ocasiones con el mero acceso no se provoca un daño real ni en el ordenador en que se entra ni a su dueño o administrador, sino que en incluso ello puede ser hasta un factor determinante a la hora de descubrir fallas de seguridad en los sistemas. De hecho muchas legislaciones, entre ellas la nuestra, no consideran hoy por hoy el hacking como un delito, sino únicamente cuando él es realizado con la intención clara de producir un daño por su intermedio, cuestión que en modo alguno podemos compartir en virtud de la acepción

[94] Ibíd..

que de delito informático adoptamos en la primera parte de este trabajo, por cuanto en este caso se está poniendo en peligro un bien jurídico que el derecho debe cautelar, el de la intimidad de las personas y sus datos, dentro de los cual claramente está el derecho a mantener información de carácter privado en un ordenador y esperar a que nadie acceda a ella sin estar expresamente facultado para hacerlo. Asimismo también se debe cautelar un bien jurídico nuevo, cual es el de la confianza en el correcto y seguro funcionamiento de las redes computacionales.

Además, creemos que en este caso es plenamente aplicable el criterio de considerar a estos actos como ilícitos de riesgo informático, puesto que en un porcentaje alto de los casos, el individuo que accede al computador creará las condiciones para poder volver a ingresar a su antojo y cuantas veces quiera, no estando garantizado que en el futuro su accionar sea tan "inocente" , sino que constituya un medio para provocar daños directos al afectado.

En lo que si podríamos compartir, es que este tipo de ilícitos obtengan una graduación en la pena menor que aquellos accesos realizados con la intención clara de producir un daño, puesto que en dicho caso estaríamos hablando de un delito agravado o el hacking pasaría a

convertirse más bien en el medio para cometer otro tipo de ilícitos, más propiamente delitos de cracking.

Respecto de las conductas de cracking propiamente tal, la Convención obliga a sus Estados Parte a adoptar las medidas legislativas u otras necesarias para sancionar dentro de sus fronteras varios ilícitos que caen dentro de esta categoría de actividades, entre las que destacan:

> 1) La Interceptación de datos no públicos realizada de manera intencional y careciendo de las facultades para hacerlo[95]. Dicha interceptación debe ser realizada mediante herramientas electrónicas e incluye los datos transmitidos de, hacia o entre distintos ordenadores, contemplándose asimismo las emisiones electromagnéticas de un ordenador que lleva tales datos. En este caso, al igual que ocurre con las conductas de intrusismo, los Estados se ven en la obligación de sancionar la conducta, sin embargo pueden determinar que ella lo sea sólo en casos determinados, como por ejemplo que se efectúe con claras

[95] Ibíd.., artículo 3º.

intenciones deshonestas o en relación a un sistema computacional interconectado con otro sistema computacional.

2) La interferencia de datos. Bajo este título el artículo 4º de la Convención se refiere a la sanción de conductas realizadas intencionalmente que produzcan el daño, eliminación deterioro o supresión de datos de un computador sin tener derecho para hacerlo. La norma además faculta a los Estados para requerir que estas conductas, para ser sancionables, produzcan un serio daño en el sistema afectado.

3) Interferencia de sistemas. En este caso la conducta sancionada es aquella realizada intencional e ilegítimamente con el objeto de interferir seriamente un sistema informático, ya sea transmitiendo, dañando, borrando, deteriorando, alterando o suprimiendo los datos del ordenador

4) El uso indebido de dispositivos. El artículo 6 establece como delito separado e independiente la comisión intencional de actos específicos ilegales respecto de ciertos dispositivos o datos de acceso con el objetivo de cometer alguno de los ilícitos descritos anteriormente contra la confidencialidad, la integridad y la

disponibilidad de sistemas de ordenador o datos. Como la comisión de estas ofensas a menudo requiere la posesión de medios de acceso ("hacker's tools") u otras herramientas, hay un incentivo fuerte para adquirirlos con objetivos criminales que entonces pueden conducir a la creación de una especie de mercado negro en su producción y distribución. Para combatir tales peligros con mayor eficacia, el derecho penal debería prohibir determinados actos potencialmente peligrosos en la fuente, antes de que sean cometidos los delitos señalados en los a Artículos 2 – 5 de la Convención.

El párrafo 1 (a) criminaliza la producción, venta, obtención para el uso, importación, distribución u otra forma de hacer asequible un dispositivo, incluidos programas de ordenador, diseñado o adaptado principalmente para el objetivo de cometer cualquiera de las ofensas establecidas en Artículos 2-5 de la Convención. La "distribución" se refiere al acto positivo de expedir datos a otros, mientras que el "hacer asequible" se refiere a los dispositivos en línea que se colocan para el empleo de otros. Este término también tiene la intención de cubrir la creación o la compilación

de hiperenlaces para facilitar el acceso a tales dispositivos. La inclusión de "programas de ordenador" se refiere a los programas que por ejemplo son diseñados para cambiar o hasta destruir datos o interferir con la operación de sistemas, como programas de virus, o programas diseñados o adaptados para obtener acceso a sistemas informáticos.

Respecto de este punto, según se señala en el reporte explicativo de la Convención[96], los redactores discutieron en detalle si los dispositivos deberían ser restringidos a los que son diseñados exclusiva o expresamente para cometer actos delictivos, excluyendo por tanto los dispositivos que tienen un uso dual. Sin embargo, esta última opción se consideraba altamente restrictiva, puesto que dificultaría en demasía la prueba de los actos sancionados, haciendo la disposición prácticamente inaplicable o de rara aplicación. Por otra parte, la alternativa de incluir todos los dispositivos, sin exclusión alguna, traía aparejado el problema de que de esa manera también se sancionaría a productos

[96] Convention on Cibercrime, Explanatory Report, de 8 de noviembre del 2001, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

legítimamente creados y distribuidos, razón por la que ella también fue finalmente rechazada. Quienes redactaron la Convención optaron por incluir un elemento volitivo necesario para configurar el ilícito, cual es la intención de cometer un acto ilegal en contra del sistema informático en cuestión, llegándose además al acuerdo de que los alcances de la disposición sólo se restringen a dispositivos que objetivamente son diseñados, o adaptados principalmente, para la comisión de los delitos[97].

El párrafo 1.a también criminaliza producción, venta, obtención para el uso, importación, distribución u otra forma de hacer asequible una contraseña de ordenador, códigos de acceso u otros datos similares que permiten el ingreso a todo o parte de un sistema informático..

La letra b) del párrafo 1º del artículo 6 sanciona asimismo la mera posesión de cualquiera de los elementos señalados en la letra a) de la disposición en comento, ella siempre y cuando sea con la intención de cometer cualquiera de los ilícitos señalados en los

[97] Ibíd..

artículo 2 a 5 de la Convención. A este respecto, dicho instrumento faculta a la Partes para que puedan determinar que para ser sancionable dicha tenencia es necesario poseer una determinada cantidad de elementos de los antes enumerados.

Cabe destacar que el párrafo 2º del artículo 6º señala que para ser sancionables las conductas antes descritas es menester que ellas sean realizadas con la intención de efectuar un acto ilícito, ello para evitar que se criminalice la producción, venta, puesta a disposición, etc., de dispositivos creados legítimamente, por ejemplo, para ser usados en contraataques a atentados remotos de un sistema informático.

5) Delitos relacionados con el uso de un ordenador. Los artículos 7 y 8 de la Convención contienen normas destinadas a tratar el uso de sistemas informáticos para la comisión de algunos delitos tradicionales que se facilitan por el uso de herramientas informáticas.

Como se señala en el Reporte Explicativo de la Convención, la mayor parte de Estados ya han penalizado estos delitos ordinarios, y sus leyes pueden o no ser lo suficientemente amplias

para extenderse a situaciones que implican redes computacionales (por ejemplo, las leyes existentes sobre pornografía infantil de algunos Estados pueden no extenderse a imágenes electrónicas). Por lo tanto, en el curso de la implementación de dichas disposiciones los Estados Parte deben examinar su legislación vigente respectiva con el objeto de determinar si ella se aplica o no a situaciones en que se ven implicados sistemas de ordenador o redes. Si la tipificación existente ya cubre estas conductas, no es menester que ella sea enmendada o que se dicten nuevas leyes para reglamentar estos casos.

Las conductas que en particular son abordadas por esta parte de la Convención se refiere a la falsificación y el fraude realizados por medio de sistemas informáticos. El hecho de que se hayan agregado estos ilícitos en particular, es porque la comisión que elaboró el borrador de la Convención llegó a la convicción de que las diferentes legislaciones no cubren siempre de manera adecuada el hecho de que estos ya tradicionales ilícitos se cometan mediante el uso de sistemas informáticos.

No cabe duda que la adopción de esta Convención sobre el Cibercrimen, que se encuentra abierta a la suscripción por parte de cualquier Estado que se sienta atraído por participar en ella, es un esfuerzo interesante por lograr armonizar las diferentes legislaciones en la lucha contra los delitos informáticos, sin embargo, ella a presentado numerosos y comprensibles reparos por parte de diversas organizaciones dedicadas a la lucha por los llamados "ciberderechos", por cuanto se considera que ella atenta en muchos casos en contra de derechos inalienables de las personas, especialmente la libertad, la intimidad, etc.

Algunos de los puntos que a su respecto más se han criticado son:

1) Las medidas que requieren que los proveedores de accesos y servicios en Internet tengan que mantener registros de las actividades de sus clientes (artículos 17, 18, 24, 25). Por cuanto se considera que dichas medidas suponen un riesgo significativo en la privacidad y otros derechos humanos de los usuarios de Internet, y son contrarios a principios bien establecidos de la protección de datos, como la directiva sobre protección de datos de la Unión Europea.

2) La concepción de "dispositivos ilegales" establecida en el artículo 6. A este respecto se señala que el concepto no tiene la suficiente especificidad como para asegurar que no se convertirá en un comodín para investigar a cualquier individuo que tenga actividades relacionadas con la informática completamente legales. Además, a juicio de algunos expertos, esta medida también provocaría una disminución en el desarrollo de nuevas herramientas de seguridad y ofrecería al gobierno el rol erróneo de dirigir la innovación científica.

3) Asimismo, también se critica la excesiva extensión de los crímenes relacionados con la propiedad intelectual según se dispone en el artículo 10. A juicio de quienes plantean esta opinión, está lejos de haber sido establecido que las medidas penales sean un remedio apropiado para la violación del copyright, ni que los tratados referidos impongan tales requisitos. Una convención internacional no debería establecer nuevas medidas penales en un área en la que la ley nacional todavía está por definir.

4) También se considera clave que se acuerden procedimientos claros para llevar a cabo investigaciones internacionales y que ninguna agencia para la protección del orden público pueda actuar en nombre de otra nación sin que existan unos procedimientos de investigación claros dentro de su propia jurisdicción. Diferentes países tienen procedimientos diferentes, eso está claro, y ahora se tendría la oportunidad de armonizar las legislaciones pero ello a condición de se asegure un alto nivel de consistencia cuando se consideran las protecciones de los derechos individuales.

5) Se piensa que las medidas sobre el crimen recogidas en los artículos 9 y 11 podrían conducir a un efecto paralizador del libre flujo de información e ideas. Imponer responsabilidad jurídica a los proveedores de Internet por los contenidos de una tercera persona supone una responsabilidad nada razonable a los que ofrecen servicios telemáticos y sin duda animará a la monitorización injustificada de las comunicaciones privadas.

6) El artículo 14, que establece los requisitos para el registro y aprehensión de datos informáticos almacenados, no dispondría de

protecciones procedimentales para salvaguardar los derechos de los individuos y asegurar que los procesos legales se desarrollan de la forma correcta. En particular, se señala que no hay ningún esfuerzo para asegurarse de que hay una revisión judicial independiente que asegure el respeto por las libertades básicas antes de que se lleve a cabo un registro ordenado por el Estado. Tales registros constituirían una "interferencia arbitaria" dentro de la normativa legal internacional.

7) Los expertos en privacidad han manifestado su oposición a esta propuesta. Uno de ellos advirtió de que los esfuerzos para desarrollar una convención internacional sobre "ciber-crimen" podrían conducir a "restricciones fundamentales en privacidad, anonimato y cifrado".

8) Los agentes encargados de la protección de datos han manifestado su oposición a esta propuesta. El Grupo Internacional sobre Protección de Datos en las Telecomunicaciones ha criticado intentos anteriores para mantener el tráfico de datos y recomendó las mejoras en la seguridad en lugar de crear nuevas leyes contra el crimen.

9) Los expertos técnicos han manifestado su oposición a esta propuesta aduciendo que el tratado propuesto podría acabar criminalizando inadvertidamente técnicas y software que se usa de forma común para hacer que los ordenadores sean resistentes a los ataques y que el tratado propuesto tendría un impacto adverso entre los encargados de seguridad, investigadores y profesores.

10) Quienes se muestran partidarios de esta postura creen que cualquier propuesta para crear una nueva autoridad con capacidad investigadora y legal debería incluir un análisis cuidadoso de los artículos 8 y 10 de la Convención Europea de Derechos Humanos y la jurisprudencia relacionada del Tribunal Europeo de Derechos Humanos. Además, la Declaración Universal de los Derechos Humanos habla directamente de las obligaciones del gobierno de proteger la privacidad de la comunicación y preservar la libertad de expresión en los nuevos medios. El artículo 12 establece que "Nadie será sujeto a una interferencia arbitraria en su privacidad, familia, hogar o correspondencia". El artículo 19 también establece que "todo el mundo tiene derecho a la libertad de opinión y expresión; este

derecho incluye el derecho a defender las propias opiniones sin interferencias y a buscar, recibir e impartir información e ideas a través de cualquier medio sin importar las fronteras".

Como señala EDUARDO FEBBRO, “Muchos especialistas y defensores de las libertades públicas ponen en tela de juicio la utilidad de una convención semejante, tanto más cuanto que ésta legaliza las prácticas más oscuras de la policía permitiéndole acceder sin rendir cuentas a nadie a los datos privados de los individuos. 22 asociaciones europeas, norteamericanas, japonesas, australianas y canadienses agrupadas en el seno de la GILC (Global Internet Liberty Compaign) denuncian los "vicios de una convención que va a hacer de cada ciudadano un criminal en potencia por el mero hecho de utilizar su correo electrónico". Paradójicamente, la convención deja fuera de su alcance la represión de uno de los cibercrímenes más corrientes en Internet, es decir el racismo. La represión de la propaganda racista y xenófoba apenas figura en un protocolo adicional del tratado y los Estados firmantes no están obligados a suscribir el párrafo. El Consejo de Europa reconoce el "inmenso desafío planteado por el tratado en materia de protección de los datos e informaciones privadas", al mismo tiempo que pone de relieve la necesidad urgente de transformar "el Far

West electrónico" en un ámbito "más seguro y frecuentable". Sin embargo, la batería de métodos existentes y las obligaciones que se desprenden de la convención parecen dibujar un futuro carcelario a la libertad de navegación en la red. El documento no sólo implica a los usuarios comunes y corrientes sino también a las empresas que venden el acceso a Internet. En ellas recae la responsabilidad del contenido de la difusión, lo que las convierte prácticamente en organismos parapoliciales privados. En ese contexto, los industriales de las nuevas tecnologías impugnan el hecho de que "imponer la responsabilidad de los intermediarios técnicos a propósito del contenido privado de los usuarios significa una carga enorme para las empresas, al tiempo que alienta el control injustificado de las comunicaciones privadas".

"Los últimos escándalos ligados al control de las comunicaciones en la red demuestran que el Far West está más bien del lado de las autoridades que del de los usuarios. Empresas como Microsoft, AOL o servicios policiales como el FBI ya han llevado a la práctica de manera más o menos evidente lo que la convención sobre la cibercriminalidad preten delegalizar. El año pasado, el FBI obligó a las compañías que venden el acceso a Internet a instalar en sus sistemas el programa "Carnívoro". Este agente informático indiscreto le permitió a la policía federal norteamericana espiar

las actividades en línea de cualquier usuario. El escándalo fue tan grande que el FBI tuvo que modificar su agente digital y rendir cuentas a la Cámara de Representantes. Carnívoro cambió de nombre, hoy se llama DCS1000 y sigue operando en condiciones siempre sospechosas. Más cínico es el método al que recurren Microsoft o AOL. Ambos gigantes de la informática idearon una suerte de pasarela de identificación destinada a automatizar los intercambios de datos con sus clientes. Uno se llama Magic Carpet, el otro Passport de Microsoft. En ambos casos, se trata de una suerte de "carpeta digital personalizada" con todos los datos, usos y costumbres de los clientes. Desde el sector privado, Microsoft y AOL detentan así una suma de informaciones confidenciales inestimables para los servicios de policía. Ligadas unas a otras y amparadas bajo leyes nacionales y una convención internacional, estas prácticas van estrechando cada vez más el espacio "infinito" de la red. Las asociaciones europeas de defensa de las libertades individuales ponen el grito en cielo ante la acumulación de candados y sistemas de control de la red"[98].

[98] FEBBRO, EDUARDO, El estado Policial Digital, http://www.rebelion.org/ddhh/digital080901.htm

2.- Hacking y cracking ante la ley chilena

2.1.- La ley 19.233

En nuestro país es la ley Nº 19.233 de mayo de 1993 la que se encarga de regular el tratamiento de los llamados delitos informáticos.

Dicha disposición tuvo su origen en una moción presentada ante la Cámara por el H. Diputado José Antonio Viera-Gallo, quien justificó su iniciativa de la siguiente manera:

"El vertiginoso desarrollo de las tecnologías de la información ha convertido a ésta en uno de los más preciados recursos. Ya no existe organización social compleja que pueda prescindir de la utilización de sistemas automatizados de tratamiento de la información, mediante computadores o redes de computadores, a fin de respaldar sus procesos de adopción de decisiones. Así se alcanza una mayor eficiencia.

"Nadie discute en la actualidad los grandes beneficios que la introducción de las referidas tecnologías ha producido, en términos de un mejor aprovechamiento de energías y recursos. Sin embargo la creciente importancia que ha adquirido la informática ha hecho patente la vulnerabilidad de las sociedades y de las organizaciones que las utilizan.

Son muchos los abusos que recurriendo a los avances de la ciencia de la información pueden cometerse. No cuesta gran esfuerzo imaginar el daño que puede causarse a enormes cantidades de personas, si la información contenida en un banco de datos, por ejemplo una AFP, fuera distorsionada, adulterada o destruida por la acción de un operador malintencionado o que busque algún tipo de enriquecimiento ilícito para sí o terceros. Tampoco resulta difícil suponer los devastadores efectos que tendría la interferencia de la transmisión de los datos con que debe alimentarse un sistema automatizado de información, o lo que significaría la revelación de ls datos que contenga, fuera de los casos en que tal acción estuviera permitida o expresamente autorizada por la ley. De ahí que la doctrina penal contemporánea emplee la expresión 'delito masivo' para referirse a los atentados contra la información acumulada en archivos computacionales o en bancos de datos, al tener en cuenta la gran cantidad de personas que pueden ser afectados por ellos.

"El proyecto de ley que presento a la consideración de la H. Cámara, tiene por finalidad proteger este nuevo bien jurídico que ha surgido con el uso de las modernas tecnologías computacionales: la calidad, pureza e idoneidad de la información en cuanto tal contenida en un sistema

automatizado de tratamiento de la misma y de los productos que de su operación se obtengan. Aquella, por el actual desarrollo tecnológico de la sociedad, merece ser protegida mediante la creación de figuras delictivas nuevas, que pongan de relieve su importancia. Nos hacemos eco de la tendencia existente en el derecho comparado contemporáneo y de las recomendaciones de organismos internacionales especializados en el tema. La protección de un sistema de información automatizado se realiza mediante la creación de figuras penales especiales, que evitan la necesidad de hacer interpretaciones extensivas de las tradicionales normas penales, para incluir conductas indebidas en contra de los sistemas automatizados de tratamiento de la información, tanto en lo referente al soporte lógico o programas de funcionamiento como en lo relativo a los datos que manejan. Es el camino que han seguido países como Estados Unidos de Norteamérica, Francia, Alemania, Austria, Suiza, entre otros. A la misma conclusión han llegado los escasos estudios realizados por juristas nacionales. Estos, después de un exhaustivo análisis de los tipos tradicionales, tales como el hurto, la apropiación indebida, la estafa los delitos de daño, han constatado que la protección de la información y de los soportes lógicos de los sistemas automatizados no se logra adecuadamente.

Sobre el particular cabe señalar que la necesidad de crear la figura del delito informático ha estado presente en nuestro país desde algún tiempo. Prueba de ello es la existencia de al menos dos anteproyectos de ley que lo establecían como parte de un conjunto de normas destinadas a regular la actividad informática. Sin embargo, precisamente por haber sido incluido en una normativa muy ambiciosa y compleja no logró traducirse en ley"[99].

"Como bien señaló en la presentación de su moción el Diputado VIERA-GALLO, el establecimiento de una ley que viniera a regular la novedosa, pero de creciente importancia, esfera de los delitos informáticos era un asunto de vital en el ámbito nacional, puesto que a partir de los años 80 se venía desarrollando en todo el mundo una verdadera revolución en el uso de los sistemas automatizados de información y era menester que dicho ámbito contara en nuestro país con las herramientas de protección adecuadas que garantizaran los derechos de los usuarios, fueren ellos empresas, organismos públicos o personas naturales.

---

[99] VIERA-GALLO, JOSÉ ANTONIO, Citado por RAPP ORTIGA, RAINER, Ob. Cit. Págs. 390-393.

2.2.- Críticas a la ley 19.233

Hora bien, aunque Chile fue pionero en la regulación de los delitos informáticos dentro de Latinoamérica, siendo el primer país en adoptar una ley especialmente creada al efecto, dicho cuerpo normativo no ha estado exento de variadas críticas provenientes de los más diversos sectores. Entre ellas destacan:

1) Se le critica a la ley 19.223 el que confunda entre los delitos informáticos propiamente tales y los llamados delitos computacionales. Ya en la primera parte de este trabajo vimos que es habitual que tanto en las legislaciones como en la doctrina se confundan aquellos delitos que efectivamente son informáticos, es decir, aquellos que tienen a la información como bien jurídico protegido y principal objeto del acto ilícito, con aquellos delitos que son de carácter tradicional, ya regulados por la legislación penal, y en que lo informático o los dispositivos computacionales se ven involucrados ya sea de manera tangencial o como medio para cometer dichos ilícitos. Esta crítica surge de la redacción del artículo 1º de la ley, en el cual se señala que "El que maliciosamente destruya o inutilice un sistema de tratamiento

de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento sufrirá la pena de presidio menor en su grado medio a máximo". Del análisis de esta norma se desprende que serán objeto de la sanción quienes dañen o inutilicen un aparato computacional y sus componentes, partes o piezas, es decir, los elementos de hardware, hechos todos que se encuentran ya consagrados en el código penal, ya sea mediante los delitos de daños, apropiación indebida, hurto, etc. En estos caso, no es la información en sí la que se ve amenazada sino determinados componentes físicos que no requieren, per se, una legislación especial que se les aplique. Cuestión distinta es si del daño o inutilización de las piezas de hardware sobreviene un atentado en contra de la información contenida en estos, caso en que sí es menester aplicar la normativa especial sobre delitos informáticos, pero no lo sería, por ejemplo, si se inutilizare o destruyere un computador nuevo, que no contenga en sí información alguna, situación en la que, erróneamente a nuestro juicio, el autor podría ser perseguido en virtud de esta ley sobre delitos informáticos.

Como señala SERGIO VALENZUELA GUZMÁN, “el sabotaje informático del artículo 1°, que se encuentra concebido como "el que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento,.....", resulta del todo prescindible. ¿Por qué esto? Debido a que la destrucción del soporte físico del tratamiento de la información, dicho en forma simple, el aparato computacional o hardware, ya es objeto de protección por la vía de delitos ya conocidos en nuestra legislación, como el robo, el hurto, la apropiación indebida, o los daños, sin que sea necesario construir tipos penales anexos para lo que ya se encontraba suficientemente protegido. Lo anterior ha sido señal de un problema consustancial a nuestra legislación, cuál es la frondosidad legislativa producto de una determinada coyuntura generalmente de origen político, y que termina legislando sobre la base de impulsos de lo que en determinado momento se estima como necesario, o supuestamente necesario, sin percatarse que el problema ya se encontraba resuelto. En este sentido, la ley de violencia intrafamiliar es un intento de

sancionar lo que ya previamente se encontraba establecido en nuestra legislación como los delitos de lesiones, injurias, o violación, con el agravante que esta "solución" legislativa ha saturado los tribunales con presentaciones que mayormente necesitarían un asistente social que un juez de letras. Asimismo, la ley de violencia en los estadios, gatillada por la polémica en torno a las denominadas "barras bravas", y de escasísima aplicación en los tribunales, es una reiteración de delitos como daños, maltrato de obra a Carabineros, incendio, u otros. Frente a lo anterior, sólo resta considerar como propiamente un delito de sabotaje informático y un aporte, la variante del artículo 3°, que lo configura como "el que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de la información, ...", que en definitiva es la protección al soporte lógico del sistema, es decir, lo que se denomina el software, y que verdaderamente ha requerido un tratamiento punitivo

diferenciado, ya que su intangibilidad determina atentados en su contra no previstos usualmente por nuestra legislación"[100].

2) Asimismo se critica por algunos autores que el tratamiento de los delitos informáticos se realice en una ley especial y no al interior del Código Penal. Sobre el particular CRISTIÁN MENESES DÍAZ señala que "El autor Rodolfo Herrera Bravo, formula como crítica a la ley N° 19.223 su ubicación fuera del Código Penal, lo que en su concepto constituye una desafortunada técnica legislativa. Al respecto, debemos recordar que el proceso de codificación del derecho fue un fenómeno iniciado en el siglo XIX, fundamentalmente en los países de Europa. Desde el Viejo Continente este fenómeno pasó a los países americanos, los que en la medida que obtenían su independencia comenzaron a realizar la denominada codificación del derecho nacional. Es consecuencia de este proceso, que en el año 1874 Chile dicta el Código Penal, formando un cuerpo de leyes metódico y sistemático. La dictación de leyes aisladas, necesariamente

[100] VALENZUELA GUZMÁN, SERGIO, Problemáticas de la Ley sobre Delito Informático, http://www.abogadosdetalca.cl/columna_delito_infor.htm

desvirtúan nuestra tradición legislativa. Al respecto, creo oportuno fomentar la realización una reforma al derecho penal sustantivo, que tenga como uno de sus pilares la existencia de un Código Penal como único cuerpo normativo que regule esta materia. En este mismo sentido, debo señalar que en el derecho penal español estas figuras delictivas han sido incorporadas en su Código Penal (artículo 248° que trata de la estafa informática; artículo 264° que regula el delito de daño informático o sabotaje y el artículo 278° que trata el espionaje informático)"[101].

3) Finalmente, también se le critica a la ley el que ella sólo se aboque al tratamientos de dos categorías de ilícitos: el sabotaje y el espionaje informático, dejando fuera otros importantes delitos como el fraude informático.

[101] MENESES DÍAZ, CRISTIAN ANDRES, Delitos Informáticos y Nuevas Formas de Resolución del Conflicto Penal Chileno, http://www.delitosinformaticos.com/delitos/penalchileno.shtml

2.3.- El cracking y la ley chilena

Es claro que la ley 19.223 se dedica en su articulado a sancionar al menos dos conductas consideradas habitualmente como propias de crackers: el sabotaje informático y el espionaje informático.

Respecto del sabotaje informático, el que en la legislación nacional ha sido definido como: "toda conducta típica antijurídica y culpable que atenta contra la integridad de un sistema automatizado de tratamiento de información o de sus partes componentes, su funcionamiento o de los datos contenidos en él"[102], es tratado por los artículos 1º y 3 de la ley.

El artículo 1º sanciona al que "maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento". Sobre este particular ya nos hemos referido anteriormente, al señalar que en este caso el legislador incurre en un error habitual en la materia, penalizando el atentado en contra de los elementos físicos del sistema, cuestión que ya se encontraba cubierta por la legislación tradicional del Código Penal, y que por tanto no requería un tratamiento especial en esta ley. A nuestro juicio, dichos atentados únicamente cobran relevancia para el derecho penal del

riesgo informático para el caso de que producto de la destrucción o daño de una unidad computacional se siga el consiguiente daño a la información contenida en ella, cuestión que contempla el inciso 2º de este artículo 1º, pero sólo como una causal para agravar la pena aplicable, puesto que en este caso se deberá aplicar el grado máximo de penalización que señala el inciso 1º del artículo en cuestión, es decir, presidio mayor en su grado máximo.

En todo caso, cabe señalar que la norma en cuestión no es del todo superflua, como ha señalado un autor, puesto que en ella también se contempla la protección al elemento lógico del sistema, el software, el cual no tenía protección especial en la legislación nacional hasta la dictación de esta ley. Como señalan HUERTA Y LIBANO, "Respecto del elemento lógico (software) éste, por su naturaleza jurídica, escapa a la esfera de protección penal común, precisando una tutela especial cuando las acciones punibles son realizadas mediante la ejecución de medios de tecnología computacional, con resultado típico destrucción o inutilización"[103].

---

[102] HUERTA MIRANDA, MARCELO Y LIBANO MANSSUR, CLAUDIO, Ob. Cit., Pág. 286.
[103] Ibíd.., Pág. 288.

Respecto de las conductas específicamente punibles, la norma es clara al señalar que lo será el destruir o el inutilizar un sistema de tratamiento de información, y el impedir, obstaculizar o modificar su funcionamiento.

Por su parte el artículo 3º de la ley, también destinado a criminalizar el sabotaje informático, sanciona al que "maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de la información".

Acá el bien jurídico protegido es específicamente la información, por lo que en este caso la ley ha estado acertada al incluir este ilícito dentro de los delitos informáticos.

Cabe agregar que respecto de ambas conductas la ley exige la existencia de una acción maliciosa, es decir, se requiere que cualquiera de las conductas antes señaladas se efectúe en forma dolosa, y en particular en este caso se requiere la existencia de un dolo directo, es decir, el individuo no sólo debe realizar el acto voluntaria y conscientemente, sino que además

debe estar animado por el propósito preciso de obtener la producción del hecho jurídicamente reprobable inserto en dicha conducta[104].

Respecto de los delitos de Espionaje Informático, estos se encuentran contemplados por los artículo 2º y 4º de la ley, siendo definidos en la doctrina nacional como "toda conducta típica, antijurídica y culpable que tiene por finalidad la violación de la reserva u obligación de secreto de la información contenida en un sistema de tratamiento de la información"[105].

En cuanto a las conductas penalizadas en este ámbito por la ley, podemos señalar que por un lado es el interceptar, interferir o acceder a un sistema de tratamiento de la información con el ánimo de apoderarse, usar o conocer indebidamente la información contenida en el mismo[106].

Por otro lado la ley también sanciona "al que maliciosamente revele o difunda los datos contenidos en un sistema de información"[107], contemplándose una pena agravada para el caso de quien incurre en estas conductas sea el responsable de dicho sistema de información.

---

[104] Ibíd.., Pág. 295.
[105] Ibíd.., Pág. 296
[106] Ley 19.223, artículo 2º.
[107] Ley 19.223, artículo 4º

Finalmente, podemos señalar que en nuestra legislación la piratería de software, una conducta típicamente atribuida a los hackers, no tiene una sanción penal expresa, puesto que si bien en cierta medida es regulada por la ley 17.336 sobre Propiedad Intelectual, su tratamiento es algo difuso, ya que la única referencia penal real se encuentra en la letra b) del artículo 80 el cual sanciona a los que en contravención con las disposiciones de dicha ley o de los derechos que ella protege "intervengan, con ánimo de lucro, en la reproducción, distribución al público o introducción al país, y los que adquieran o tengan con fines de venta: fonogramas, videogramas, discos fonográficos, cassettes, videocasetes, filmes o películas cinematográficas, o programas computacionales". Sin embargo en dicha disposición no se describen las conductas propias que configurarían el delito de piratería de software, además que se exige la existencia de un "animo de lucro", que, como vimos, generalmente no existe en este tipo de actividades realizadas por los crackers a través de Internet, por lo que en este aspecto el derecho carecería de sanción para estas conductas.

2.4.- El hacking en la ley chilena

A diferencia de lo que ocurre con las conductas de cracking, las que se encuentran claramente sancionadas por la ley 19.223, al menos en sus manifestaciones de sabotaje y espionaje informático, tratándose del hacking no existe en la doctrina nacional unanimidad respecto a considerar si éste se encuentra o no contemplado por dicha normativa.

Como señala CRISTIAN MENESES, en nuestra doctrina existe prácticamente consenso en señalar que el hacking directo o mero intrusismo informático carecería de consagración expresa en la legislación nacional. En dicho sentido se han expresado los autores HUERTA Y LIBANO, para quienes la ley 19.223 no tipifica el delito de hacking en cuanto acceso indebido. Para ellos "la ley, sólo en su artículo 2º se refiere al acceso a secas. Podría presentarse confusión y estimarse que se trata de cualquier acceso, autorizado o indebido. Sin embargo, al utilizarse, en el mismo artículo, la expresión indebidamente, se entrega cierta certeza de que tal acceso debe ser necesariamente indebido. Por lo demás, así se desprende de las actas de discusión del proyecto.

"Debido a que el legislador mantuvo en la atipicidad el delito de hacking, se produce que en Chile es impune la conducta del hacker que por

pruebas de carácter intelectual o mera diversión accede indebidamente a los sistemas, transgrediendo las medidas de seguridad.

"Asimismo, no constituye delito el acceso indebido realizado por un hacker indirecto, con el objeto de cometer sabotajes de datos.

"El hacking sólo se consideró a propósito del espionaje. Sin embargo tampoco es sancionable debido a que el acceso indebido es parte de los elementos objetivos del tipo del art. 2º"[108].

No obstante que la opinión mayoritaria en nuestra doctrina se incline a favor de la postura que considera no incriminable el hacking dentro de nuestra legislación, SERGIO VALENZUELA GUZMAN sostiene una opinión contraria, señalando al respecto:

"En su edición del día domingo 26 de agosto del presente, el diario "El Mercurio", en la primera página de su cuerpo C (5), destacaba que había sido detenido por la Brigada del Ciber Crimen de la Policía de Investigaciones un "hacker" o pirata informático de sólo 15 años de edad, agregando que era el primer caso de un delito informático cometido por una persona de tan corta edad en nuestro país. La conducta del pirata

---

[108] HUERTA MIRANDA, MARCELO Y LIBANO MANSSUR, CLAUDIO, Ob. Cit., Pág. 302.

informático habría sido escanear los puertos del servidor de la empresa Meganet S.A., mediante un computador personal que tenía en su propia casa, para tomar control del mismo y administrarlo remotamente. En su intento de eliminar indicios de su acceso, el menor se deshizo de varias carpetas, lo que en definitiva redundó en un funcionamento defectuoso del servidor intervenido e interrupciones por más de 48 horas del servicio entregado por la empresa. De la lectura de la información podemos adelantar dos conclusiones, primero, que el acceso indebido a un sistema computacional se ha convertido en un desafío seductor para un número cada vez mayor de usuarios computacionales, y lo que es más sorprendente, cada vez más jóvenes, que sin perjuicio de esto, cuentan con los conocimientos o la perseverancia para lograr su objetivo. Segundo, que el denominado "hacker", en apariencia, no busca un objetivo de destrucción o espionaje, sino que de reto intelectual o mera diversión, esto último denominado "joy riding". En el caso relatado, el menor sólo buscaba controlar remotamente el servidor, pero en su intento terminó por obstaculizar e interrumpir el funcionamiento de la empresa afectada, al deshacer una serie de carpetas, lo que se encuentra perfectamente configurado como el delito de sabotaje informático en el artículo 3° de la Ley analizada, que penaliza al que altere,

dañe o destruya los datos contenidos en un sistema de tratamiento de la información, en la especie, las carpetas borradas. ¿Pero si no hubieren sido borradas las carpetas, y la actividad del pirata informático hubiera sido el mero control a distancia del servidor intervenido sin daño alguno al soporte lógico, es decir, tan sólo el acceso indebido? Esta actividad, según algunos autores, restaría impune, conforme a los tipos penales de la Ley, lo que incluso se desprendería de las actas de discusión parlamentaria del proyecto, toda vez que el artículo 2° se gobierna sobre la base que el acceso sea con el ánimo de apoderarse, usar, o conocer indebidamente la información, lo que rigidiza el tipo penal y le agrega elementos subjetivos que implican algo más que el mero acceso. Discordamos de dicho planteamiento y postulamos que el artículo 2° efectivamente sanciona el "hacking" concebido como el mero acceso ilegítimo a un sistema de información computacional. Conforme al texto legal, la tipificación penal se desprende del giro "conocer" presente en la redacción legislativa, y su connotación ilegítima el agregado "indebidamente", lo que nos conduce a la polémica sobre cuál es entonces el acceso debido o legítimo. Y postulamos que tal delito se encuentra tipificado en nuestra legislación, no sólo por la redacción legal que así lo demuestra, sino que por su evidente necesidad,

por muy romántica y audaz que parezca la actividad del hacker, ya que en apariencia pareciera que no se afecta ningún bien jurídico, toda vez que la actividad de éste sería meramente exploratoria y de divertimento o reto intelectual. El pensamiento anterior no ha reparado que existe una esfera de intimidad de cierta información, ya que no es lo mismo un recetario de cocina internacional, que la base de datos de una tienda por departamentos, o el servidor del Ministerio de Defensa. ¿Pero, cuál sería el problema que se acceda a cualquiera de estos soportes lógicos si no será con fines de divulgación, daño o lucro, salvo la mera visualización, y por muy importantes que puedan parecer? El peligro es el problema potencial que se produce si se transforma en pensamiento común en una determinada sociedad que no existe una esfera de intimidad y privacidad que debe resguardarse. En este sentido, debe considerarse que la legislación penal intenta resguardar determinados bienes jurídicos por la vía de imponer sanciones penales a su efectivo daño o puesta en peligro, con el objeto de crear conciencia sobre su importancia para el desenvolvimiento de una agrupación humana. De consiguiente, si no se respetara y protegiera la vida, la propiedad, el honor, la libertad sexual, etc., por medio de los pertinentes delitos de homicidio, robo, hurto, injurias, por nombrar algunos, la

convivencia humana sería extraordinariamente difícil. ¿Y la intimidad o privacidad de meros datos? En el actual desarrollo de nuestra legislación no cabe duda que la vida privada e incluso pública de las personas se encuentra protegida con el correspondiente tipo penal, todo ello por expreso mandato constitucional. Así, el artículo 161-A del Código Penal, de reciente data, sanciona "al que, en recintos particulares o lugares que no sean de libre acceso al público, sin autorización del afectado y por cualquier medio, capte, intercepte, grabe o reproduzca conversaciones de carácter privado; sustraiga, fotografíe, fotocopie o reproduzca documentos o instrumentos de carácter privado; o capte, grabe, filme o fotografíe imágenes o hechos de carácter privado que se produzcan, realicen, ocurran o existan en recintos particulares o lugares que no sean de libre acceso al público." Asimismo, el inciso segundo de este artículo contempla la difusión de estas conversaciones, comunicaciones, imágenes o hechos, aunque inexplicablemente con la misma pena, ya que el disvalor es superior. En todo caso, al tenor de este artículo, podemos concluir que en nuestra legislación se sanciona el mero acceso a datos privados, siendo necesario tan sólo dilucidar que debe entenderse por "privado". Sin ánimo de extendernos sobre el particular, ya que se sustraería al propósito de este

artículo, diremos que privado es todo lo que explícita o implicitamente se quiere sustraer al conocimiento público, y para efectos de esta sustracción se tiene un título que lo justifique, ejemplo, es legítimo que cualquier persona sustraiga del dominio público el conocimiento de sus enfermedades, y se encuentra en su pleno derecho para tal pretensión, ya que forman parte de su integridad personal, pero, no contaría con tal derecho si la enfermedad en cuestión pusiera en peligro la salud individual y/o colectiva de terceros, como sería el caso de una enfermedad infecciosa, venérea o el Síndrome de Inmunodeficiencia Adquirida (SIDA), en que necesariamente habrían interesados en conocer tal realidad, y se encontrarían plenamente justificados, ejemplo, una eventual pareja sexual o un establecimiento hospitalario. Sentada la premisa que en nuestra legislación se protege la privacidad, sin mayor pesquisa de los propósitos del infractor, que no sea su actuar injustificado, es posible concluir que el delito de hacking se encuentra penado con cargo al artículo 2° de la Ley N° 19.223, aunque sea esta exploración con fines intelectuales o de diversión, en tanto se trate de datos o programas computacionales privados, para lo cuál el intérprete deberá acudir a signos explícitos o implícitos de que la

información que se trate no es de acceso público, como si para acceder a ella se requiere una clave"[109].

Ahora bien, no obstante el acuerdo que pueda existir en torno a la primera interpretación dada para el artículo 2º de la ley, nosotros nos sentimos más inclinados por acoger la tesis presentada por VALENZUELA GUZMAN, aunque realizando algunas consideraciones a su respecto.

Coincidimos con los autores HUERTA Y LIBANO en el hecho de que la norma es clara al establecer el requisito de que el acceso debe ser indebido para caer bajo la órbita de los dispuesto por el artículo 2º, es decir, queda fuera todo tipo de acceso legítimo que se haga a un sistema, como el que efectúa alguien contratado para probar los mecanismos de seguridad instalados, o el administrador de una red o el encargado de mantener, por ejemplo un sitio web. Sobre esto no hay discusión alguna. Sin embargo, creemos que dichos autores no profundizan lo suficiente sobre qué debe entenderse por un "acceso indebido", o más bien no realizan una correcta interpretación de la frase.

---

[109] VALENZUELA GUZMAN, SERGIO, Ob. Cit.

Estos autores al analizar el tipo penal señalan que éste debe separarse en dos términos: Acceso, el cual definen, de acuerdo con el diccionario de la Real Academia Española de la Lengua, como la entrada o paso a un lugar; e indebido: adverbio que a su juicio entrega la idea de ilicitud, injusticia, carencia de equidad, no autorizado.

Hasta aquí todo bien.

Más adelante los autores dicen: "Estimamos, por lo tanto, que el acceso indebido a la información consiste en las pericias tendientes a introducirse en un sistema de tratamiento de la información, burlando todas las medidas de seguridad y resguardo programadas en su entrada, con el fin de allegarse a la información reservada contenida en el sistema, recabarla y eventualmente utilizarla en beneficio o en perjuicio de terceros"[110].

Más adelante agregan, "desde esta perspectiva, el acceso indebido implica una violación de los passwords del sistema, la cual puede haberse producido de manera premeditada por su autor, o bien accidentalmente, es decir, la vulneración de las medidas de seguridad no estaban en el ánimo del

[110] HUERTA MIRANDA, MARCELO Y LIBANO MANSSUR, CLAUDIO, Ob. Cit., Pág. 301

delincuente, sin embargo, una vez en el sistema, el agente se apodera, conoce o utiliza la información confidencial a que no tenía derecho"[111].

Todo lo dicho hasta el momento por HUERTA Y LIBANO nos parece del todo correcto y ajustado a lo que debería ser una interpretación del artículo 2º de la ley, sin embargo no comprendemos por qué más adelante, como antes señalamos, los autores llegan a la conclusión de que dentro de dicho tipo no cabe la conducta de hacking directo, cuando ellos mismos al definir esta conducta lo hacen diciendo que "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"[112].

Creemos que existe una notoria contradicción entre lo dicho en una y otra parte. Es claro que la ley sanciona **todo** acceso realizado en forma indebida a un sistema, es decir, todo ingreso al mismo que se hace de

---

[111] Ibíd..
[112] Ibíd.., Pág 170.

manera ilegítima, sin autorización, y es un hecho que entrar a un sistema informático sin el permiso de su dueño o encargado, aunque sólo sea para fisgonear un poco o comprobar una cierta capacidad intelectual, no excluye el que dicho acceso sea del todo ilegítimo.

Además la ley tampoco señala en parte alguna que el acceso indebido tenga que ser realizado con la intención directa de provocar un daño, de hecho la descripción de la conducta habla de que el acceso puede ser únicamente para "conocer" indebidamente la información contenida en el sistema, para lo cual basta con el mero acceso.

Pensamos que la interpretación anterior no debería presentar ninguna duda a su respecto tratándose de sistemas protegidos por sistemas de passwords o mediante el uso de softwares especializados en impedir el acceso a un sistema a extraños, como sería el uso de un firewall, puesto que si la persona protege por contraseña un sistema o instala un firewall es obviamente porque no desea que nadie ajeno acceda a dicho sistema. La duda puede surgir respecto de aquellos sistemas que no cuentan con ningún sistema de seguridad al efecto, y en el que el ingreso es simple, sin necesidad de violar ningún mecanismo de seguridad para hacerlo.

Sin embargo, nosotros estamos por pronunciarnos a favor de que en este caso también se estaría produciendo un acceso indebido, puesto que el no colocar un sistema de seguridad en modo alguno significa que se le garantice el acceso a cualquier persona a nuestro sistema. Concluir algo diferente es como pensar que por el sólo hecho de que un día se nos quedara la puerta de nuestra casa sin llave ello faculta a cualquiera que vaya pasando para ingresar a ésta y "curiosear" por entre nuestras pertenencias.

En todo caso, estamos dispuestos a conceder que en los casos en que no se ha establecido un sistema especial de seguridad el considerar que el ingreso sea o no indebido es un asunto de prueba que le tocará al juez calificar, pero ello sólo en estos casos, pues respecto del resto creemos que el asunto es claro, debiendo ser sancionado quien haga ingreso a un sistema de manera indebida, aunque solo sea por motivos intelectuales o de mera diversión.

Lo que si lamentamos, es que de acogerse esta tesis el hacking blanco, directo o mero intrusismo informático sería sancionado con la misma pena que quien ingresa a un sistema con fines de realizar espionaje informático.

El simple hacking es con todo un conducta mucho menos dañina que las otras que se describen en el artículo 2º de la ley, y por tanto también sería menester que tuviese un tratamiento especial, como se hace en las legislaciones italiana y alemana, señalándose a su respecto una penalidad menor. Pero ello dentro del ámbito exclusivo del derecho penal, puesto que no compartimos aquellas posiciones doctrinarias que creen que el hacking debe obtener su sanción desde la órbita administrativa, puesto que en este caso claramente estamos en presencia de un delito, que pese a ser de menor gravedad no por ello deja de ser nocivo. Ello principalmente si observamos a esta conducta desde el punto de vista del Derecho Penal del Riesgo Informático, por cuanto aún cuando el hacking en sí puede no traer consecuencias directas para el sujeto pasivo objeto del delito, crea no sólo un temor al uso de las redes informáticas que debe ser evitado ya que es esencial para el desarrollo del sistema el que los usuarios se sientan seguros al utilizarlo, sino porque además nada puede garantizar que el hecho de ingresar a un sitio no pueda transformarse en el futuro en otro delito de mayor gravedad y en este caso es función del derecho el precaver que ello no suceda.

VI. A modo de conclusión

Al finalizar este trabajo no nos cabe llegar a otra conclusión que el manifestar que tanto la problemática de los delitos informáticos como de la regulación jurídica de Internet es sin duda un tema complejo, con lo cual en modo alguno creemos estar diciendo algo "novedoso" sino que con ello nos hacemos parte de la ya amplia doctrina que existe al respecto y que se inclina en el mismo sentido.

Al comenzar nuestra investigación, como habitualmente ocurre, partimos desde determinadas ideas preconcebidas en base a las cuales considerábamos al hacking y al cracking como dos formas más de delincuencia cibernética y que, por tanto debían ser perseguidas y sancionadas. Sin embargo, con el curso de nuestro trabajo fuimos descubriendo un sinnúmero de aristas que el tema en sí plantea y lo cual nos ha llevado a meditar mucho más detenidamente el asunto.

En las páginas precedentes hemos abordado tanto la problemática general en torno a los delitos informáticos, así como algunas de las particularidades que estos adquieren en el ámbito propio de Internet y la consagración legal que respecto de dichos ilícitos se ha ido elaborando.

Quizá en muchos de estos puntos no hayamos dicho nada nuevo que sea un real aporte a la técnica jurídica, no obstante ello, creemos que el principal aporte que puede encontrarse a nuestro trabajo haya sido el que a través de él hemos pretendido realizar un real esfuerzo por estudiar y explicar el fenómenos del hacking y el cracking, particularmente del primero, el cual nos ha asombrado por lo que de revolucionario y novedoso tiene, principalmente su filosofía e ideario.

Una cuestión que hemos lamentado de la mayoría de la literatura jurídica abocada al tratamiento de estos temas que hemos tenido oportunidad de consultar, sea el que en muchos de los casos los autores se limitan a regresar a lugares comunes, describiendo conductas sin en verdad denotar una real comprensión de ellas. El fenómeno del hacking y el cracking más allá de las connotaciones especiales que puedan tener para el derecho penal, en cuanto afectan a variados bienes jurídicos que el derecho debe proteger, son fenómenos sociales que es menester estudiar y comprender antes de hacer caer sobre ellos el máximo rigor de la ley. Para esto no basta con únicamente recurrir a las herramientas propias que el derecho nos da, ya que ellas hasta ahora se han presentado como

insuficientes, tanto para explicar el fenómeno como para regularlo y poner atajo a los delitos que de él se derivan.

Es una cuestión generalizada el que entre las personas no habituadas a la nueva realidad virtual se condene duramente el accionar de hackers y crackers, empero muchas veces dicho rechazo puede nacer de la mera ignorancia o desconocimiento. Si los operadores jurídicos, sean ellos jueces, abogados o investigadores, quieren en verdad comprender estos fenómenos es menester que no se contenten con leer un poco de literatura especializada en el tema, sino que es imprescindible el escuchar los que otras ramas de las ciencias tienen que decir sobre la materia y, por sobre todo, es necesario el adentrarse en el submundo del *underground* digital, para saber cuales son los planteamientos que desde ese sector se hacen, sus requerimientos, demandas y críticas a la realidad en que se encuentran inmersos, principalmente a la realidad no virtual. Solo así será posible que en el futuro el derecho logre adecuarse a la nueva realidad que lo enfrenta y cuestiona.

Creemos que no basta con pretender hacer uso de los conceptos tradicionales que se manejan en el derecho, para hacer frente al fenómeno virtual. Pensar que basta con adecuar los tipos penales ya existentes para lograr regular el entorno informático es no comprender en sus bases el

asunto planteado. Es menester adecuar la técnica legislativa a la nueva realidad, puesto que es mucho más difícil o ilusorio pretender que ésta se adecue a aquel. Para esto es menester un esfuerzo coordinado y multidisciplinario que involucre no sólo a jueces o abogados, sino también a técnicos informáticos, sociólogos y fundamentalmente a los usuarios de Internet, puesto que son precisamente estos últimos los que se verán más afectados con cualquier medida que se tome.

En el curso de nuestra investigación tuvimos la oportunidad de tomar contacto con una cantidad importantísima de gente que hace uso de herramientas que en el mundo normal son tradicionalmente consideradas como reprobables y que, por tanto, son consideradas ilícitas. De hecho nosotros mismos tuvimos la oportunidad de comprobar en la práctica el uso de dichos instrumentos. El problema con ello, es que no se puede pretender que el derecho al sancionar todas estas conductas sea lo suficientemente efectivo en su aplicación, pues se podría llegar al purismo estéril de creer que se deben sancionar todas las actividades consideradas "ilícitas" en el mundo no virtual, con lo que tendríamos entonces que sancionar o intentar meter a las cárceles a quizá el 90 o 100% de los usuarios de Internet, quienes en una u otra oportunidad han cometido alguna actividad

considerada como delictiva, cuestión que es imposible. Además en muchas ocasiones actividades que en la vida real pueden ser consideradas ilícitas en el mundo virtual son fundamentales para el desarrollo de la red, como por ejemplo ocurre con las conductas de hacking cuando ellas logran desentrañar problemas de seguridad que poseen los sistemas advirtiendo de ellos y así logrando que dichos errores sean modificados.

Si el derecho no se hace cargo de la particular realidad de Internet, y se conforma con ir dictando normas que no son capaces de responder a las particularidades de este entorno corre el riesgo de transformarse en letra muerta, como efectivamente sucede con muchas de las leyes que se han dictado sobre la materia en el mundo.

Además, al momento de intentar controlar Internet también se deben tener muy en consideración los derechos esenciales de los seres humanos, puesto que con el objeto de regular el ciberespacio no se puede pasar a llevar principios y reglas que a la humanidad le han tomado siglos ir acrisolando, como la libertad, el derecho a la intimidad, etc.

En lo que respecta a nuestro país, y como hemos constatado anteriormente, es un hecho que el tema de los delitos informáticos aún no ha sido abordado en la dimensión que realmente requiere. Tanto la doctrina,

que le ha dedicado muy pocas líneas a su tratamiento, como la normativa positiva carecen de un estudio y tratamiento sistemático y acabado que permita hacer frente a un fenómeno que en el mundo cobra cada día más relevancia, y del que nuestro país no está ni estará ajeno en el futuro.

Por de pronto, creemos que es menester que se tomen medidas por parte de las autoridades para combatir con fuerza al verdadero cibercrimen, antes de que se transforme en un área más en que los delincuentes actúen impunemente.

En el ámbito internacional pensamos que es importante que Chile participe y promueva activamente acuerdos que permitan enfrentar de forma global a aquellos delitos que se cometen, principalmente, a través de Internet, por cuanto ha quedado demostrado, en los hechos, que es imposible para las naciones, aisladamente, perseguir y sancionar a los cibercriminales, puesto que su accionar, en la mayoría de los casos, trasciende todas las fronteras e involucra a más de una legislación. Es por ello que pensamos que nuestro país debería suscribir la Convención Internacional contra el Cibercrimen, por cuanto es aquel uno de los primeros esfuerzos serios de la comunidad internacional por salirle al paso a los ciberdelincuentes actuando de manera coordinada.

En el ámbito interno, creemos que se hace urgente una reforma a la Ley 19.233, por cuanto ella hasta ahora ha tenido una reducida aplicación práctica y esto, no porque los delitos informáticos no se cometan, sino porque la norma misma es deficiente, como ya señalamos anteriormente, puesto que no contempla todas las formas de comisión posibles de manera clara, como ocurre, por ejemplo, con el delito de hacking o mero acceso no autorizado, el que no se encuentra tipificado de manera expresa como conducta punible. A nuestro parecer, dicha reforma debiera contemplar la descripción típica de los delitos cometidos a través de internet y de los demás delitos informáticos , mediante la inserción de un nuevo párrafo en nuestro Código Penal, denominado **"Delitos contra la Información Digitalizada"**, puesto que tal técnica podría tener además, un efecto sicológico sobre los jueces, que siempre parecen inclinarse a la aplicación de los delitos contra los bienes jurídicos tradicionales contemplados en dicho cuerpo legal. En el mismo sentido, no nos parece adecuado que estos delitos sean sancionados mediante la técnica de considerarlos como "agravantes" de los delitos contra los bienes jurídicos tradicionales, en cuanto se afectan dichos bienes utilizando los sistemas informáticos, ya sea a través de Internet o no.

Se suma a los anteriores inconvenientes, el hecho de que la mayoría de los jueces, quienes tienen a cargo conocer de los casos de delitos informáticos que lleguen a sus manos, investigarlos y, en definitiva, juzgarlos, carecen de los conocimientos necesarios sobre la materia, lo cual hace que, de los pocos casos que se denuncian, en la mayoría de ellos se sobresea la causa por falta de pruebas o se le apliquen otras normas de derecho penal tradicional, y no las que contempla la ley 19.233, asimilándose los casos a delitos contra la propiedad, la intimidad, etc., no juzgándose ellos como delitos informáticos.

De hecho, cabe destacar que de los años que lleva en vigencia la actual ley, ella no fue aplicada por primera vez sino hasta 1999, sin que conozcamos otros casos, ocasión en que la jueza del 16º juzgado del crimen de Santiago condenó a 541 días de presidio a un ex-funcionario del departamento de informática del Servicio de Impuestos Internos por provocar intencionalmente caídas al sistema computacional.[113]

En lo que respecta al tema específico de que hemos tratado en estas páginas, pensamos que se debería incorporar en una nueva legislación la

---

[113] LOPEZ, MACARENA, Ley 19.233 y su Aplicación en los Tribunales. http://www.derecho.udp.cl/e/libro/24.LOPEZ.pdf

consagración específica de los delitos de hacking y cracking en sus diversas manifestaciones. Para ello, es menester que una nueva norma adelante la barrera de protección, señalando, respecto del hacking, que el mero acceso o intrusismo en un sistema informático de manera no autorizada es constitutivo de delito, aún cuando en los hechos no se produzca daño alguno, puesto que pensar que el mero acceso a nuestro computador no constituye una actividad ilícita es lo mismo que decir que cualquier persona puede ingresar a nuestro hogar y registrar nuestras cosas sólo porque la puerta o la ventana se encontraban abiertas. Además respecto del cracking se debería incluir otras conductas además del sabotaje o el fraude informático, como por ejemplo el acceso a sistemas comerciales protegidos mediante claves, como sería una página Web con contenido de pago, en cuanto si bien en este caso no se produce un daño directo si se está usufructuando de un servicio sin pagar correspondientemente por él. Otras figuras que se deberían contemplar son todas aquellas que dicen relación con los atentados a la propiedad intelectual cometidos por medios informáticos, los cuales también carecen de una real sanción en la Ley sobre Propiedad Intelectual, y deberían ser objeto de un estudio pormenorizado en una nueva ley sobre delitos informáticos.

Además, la prueba en estos delitos es muy difícil, así como loo es también determinar al autor, lo que podría verse facilitado en parte por la implantación del sistema probatorio contemplado en la reforma procesal penal que se lleva a efecto en el país, de gran libertad y sin ponderación legal de ella.

Es urgente que en el futuro inmediato, en Chile se reconsidere el tratamiento de la problemática informática, creando normas adecuadas, dentro del ámbito del Derecho Penal y como parte integrante del Código del ramo, con el objeto de salvaguardar los intereses tanto de los individuos como de las instituciones . Para ello es necesario proceder con urgencia a la capacitación de los jueces con competencia criminal. Asimismo, en caso de crearse la nueva normativa, es indispensable que en su elaboración sean consultados os especialistas en la materia, que conozcan los fenómenos hacker y cracker, cómo estos funcionan y cómo neutralizarlos. Estos especialistas son ellos mismos y ese es el mismo camino que han seguido las empresas, las que contratan a ex – hackers para que cautelen la seguridad de sus redes y detecten sus falencias.

Es de esperar que el anterior trabajo pueda ser un aporte más en esta actividad que es necesario llevar adelante para comprender y conocer mejor

lo que sucede en Internet y el mundo informático, para de esta manera regularlo en forma adecuada. Si es así podemos darnos por satisfechos de todo el tiempo invertido en navegar por la red en busca de información adecuada y en intentar entregar a través de nuestra memoria de prueba un trabajo que sea útil a alguien más que a nosotros mismos.

- F I N -

VII. Bibliografía

1.- Bibliografía y documentos electrónicos citados en el trabajo

1. CARRION, HUGO DANIEL, Presupuestos para la Incriminación del Hacking. Obtenido desde el sitio web "Delitos Informáticos", http://www.delitosinformáticos.com.

2. COMITÉ DE MINISTROS DEL CONSEJO DE EUROPA, Convention on Cibercrime, Explanatory Report adoptado en noviembre 8 del 2001. (La traducción es nuestra). http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

3. Convention on Cibercrime, Explanatory Report, de 8 de noviembre del 2001, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

4. CONVENCIÓN CONTRA EL CIBERCRIMEN

5. DAVARRA RODRÍGUEZ, MIGUEL ANGEL, Citado por RAPP ORTEGA, RAINER, El Delito Informático en Chile y en el Derecho Comparado. Memoria de Prueba, Facultad de Derecho Universidad de Chile, 2001.

6. DELIO, MICHELLE, Da Vinci, El Primer Hacker de la Historia,

http://buscar2.terra.com/wired/cultura/03/01/29/cul_62114.html

7. El Problema Legal de Combatir el Crimen Cibernético, http://www.ciudadfutura.com/internet/cibercrimen13.htm.

8. FEBBRO, EDUARDO, El estado Policial Digital, http://www.rebelion.org/ddhh/digital080901.htm

9. Franklin Sandoval, "Internet el arte de romper paradigmas". Disponible en Monografias.com (http://www.monografias.com)

10.FISHER, KING, La Conciencia de un Cracker, http://www.df.lth.se/~triad/triad/3words/Consesp.html

11.HERNÁNDEZ, CLAUDIO, "Hackers, Los Piratas del Chip y de Internet", libro electrónico gratuito disponible en http://.perso.wanadoo.es/snickers

12.HUERTA MIRANDA, MARCELO Y LIBANO MANSSUR, CLAUDIO, Delitos Informáticos. Segunda Edición Complementada y Actualizada a 1998. Editorial Jurídica Conosur Ltda.., Santiago, Chile, 1998.

13.KING FICHER, La Conciencia de un Cracker, traducción de Katia Coen, http://www.df.lth.se/~triad/triad/3words/Consesp.html

14.Ley 19.223

15.LEVY, STEVEN, Hackers: Heroes of the Computer Revolution, edición digital obtenida desde el canal #bookz en el IRC en la red Undernet.

16.LEVY, STEVEN, Página Personal, http://www.echonyc.com/~steven/

17.LOPEZ MORENO, JUAN, Comunicación, La World Wide Web como Vehículo de Delincuencia: Supuestos Frecuentes. En "Internet y Derecho Penal", Varios Autores. Escuela Judicial, Consejo del Poder Judicial, Madrid, España, 2001.

18.MENESES DÍAZ, CRISTIAN ANDRES, Delitos Informáticos y Nuevas Formas de Resolución del Conflicto Penal Chileno, http://www.delitosinformaticos.com/delitos/penalchileno.shtml

19.MENTOR,Manifiesto Hacker, http://www.sindominio.net/biblioweb/telematica/mentor.htm

20.MORON LERMA, ESTHER, Internet y Derecho Penal: «Hacking» y otras Conductas Ilícitas en la Red. Editorial Aranzadi, 1999, Pamplona, España.

21.RAYMOND, ERIC S, The Jargon File 4.3.3, http://www.catb.org/~esr/jargon/

22.RAYMOND, ERIC S., How to Become a Hacker, http://www.catb.org/~esr/faqs/hacker-howto.html

23.RAYMOND, ERIC S, La Catedral y el Bazar, texto en formato digital obtenido en su versión en español en el canal #biblioteca del IRC en la red Undernet.

24.ROVIRA DEL CANTO, ENRIQUE, Delincuencia Informática y Fraudes Informáticos. En Estudios de Derecho Penal dirigidos por Carlos María Romeo Casabona, Editorial Colmenares, España, 2002.

25.STERLING, BRUCE, "The Hacker Crackdown", traducción hecha por el equipo de Kriptópolis, http://www.kriptopolis.com.

26.TÉLLEZ VALDES, JULIO, Derecho Informático, Universidad Autónoma de México, México, 1987.

27.TERRA.COM,Cibercultura,http://www.terra.com/informatica/que-es/cracker.cfm

28.VALENZUELA GUZMÁN, SERGIO, Problemáticas de la Ley sobre Delito Informático, http://www.abogadosdetalca.cl/columna_delito_infor.htm

29.VIEGA RODRÍGUEZ, MARÍA JOSÉ, Delitos Informáticos, Revista Electrónica de Derecho Informático, Nº 9, http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107138.

30.VIERA-GALLO, JOSÉ ANTONIO, moción con el que se inició el proyecto de ley que regulaba los delitos informáticos en Chile. Citado por RAPP ORTIGA, RAINER, Ob. Cit. Págs. 390-393.

31.WILLIAMS, PHIL, Crimen Organizado y Crimen Cibernetico: Sinergias Tendencias y Respuestas. http://usinfo.state.gov/journals/itgic/0801/ijgs/gj-7.htm

2.- Documentos consultados en la investigación, pero no citados.

1. Ahumada Zúñiga, Amador. "La ley chilena de delito informático". http://www.ubik.to/vr/vr12/chile.htm

2. A.I.H, http://www.infohackers.com/.

3. Charchi, "Hackers y Crackers. [021.txt]", http://www6.gratisweb.com/disidents/ascii/ezine/hyc.html.

4. "Conceptos de delitos informaticos". http://tiny.uasnet.mx/prof/cln/der/silvia/define.htm

5. "Concreción del hacking". http://hucker-mid.galeon.com/hacking/diferencias.htm

6. Damicita, "¿Como Son Los Hackers En Realidad?", http://www6.gratisweb.com/disidents/ascii/ezine/qshackers.html.

7. "Definiciones de Delito Informatico". http://www.angelfire.com/la/LegislaDir/Defin.html.

8. "Delitos Informaticos". http://personales.ciudad.com.ar/roble/delitosinf.htm.

9. "Delitos Informaticos". http://www.angelfire.com/la/LegislaDir/.

10.“Delitos informáticos: Qué son y cómo se previenen”. http://www.estarinformado.com.ar/pag%20tecnologia/TECNOLOGIA-2.htm

11.“Delitos Informaticos reconocidos por ONU”. http://www.apc.org/espanol/rights/lac/cdocs.shtml?x=8325

12.Figueroa Alcantara, Hugo. “Ciberespacio y ética hacker”. http://hfigueroabsociol.tripod.com/hacker.htm.

13. Gonzalez Ruz, Juan Jose. “protección penal de sistemas, elementos, datos, documentos y programas informáticos. http://criminet.ugr.es/recpc/recpc_01-14.html

14.“Hacker – Crackers”, http://www.lasalle.edu.co/csi_cursos/informatica/termino/hackers_y_Crackers.htm.

15.“La Etica del Hacker”, http://leo.worldonline.es/jerzegor/textos/hacker_ethic.es.html.

16.Libano Manssur, Claudio. “Los Delitos de Hacking en sus Diversas Manifestaciones”, http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107511.

17.LOPEZ, MACARENA, Ley 19.233 y su Aplicación en los Tribunales. http://www.derecho.udp.cl/e/libro/24.LOPEZ.pdf

18.Machado, Jorge. "Hackers, crackers, piratas, prehackers y delincuentes informaticos". http://www.perantivirus.com/sosvirus/general/hackers.htm

19.MAGLIONA M., CLAUDIO Y LOPEZ, MACARENA. "Delincuencia y Fraude Informático, Derecho Comparado y Ley N°19.233. EDITORIAL Jurídica de Chile, 1999.

20."Manifiesto Hacker", http://www.vda.com.ve/gil/lared/manhac.htm.

21. Medina Jara, Rodrigo. "Chile: Los delitos informáticos en la legislación chilena". http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=142623

22.Melisa Tuya, "De hackers, crackers y demás familia", http://www.baquia.com/com/20010125/art00016.html.

23."Que es y que no es un hacker", http://www.geocities.com/delincuentes_digitales/anteced.htm.

24.“Que es un Hacker?”. http://www.starchat1.cl/informatica/hacker.htm.

25.“¿Qué puede entenderse por deliro informatico?”. http://www.mir.es/policia/bit/legisla.htm.

26.Raymond, Eric S. “Cultivando la Noosfera”. http://sindominio.net/biblioweb/telematica/noosfera.html.

27.Raymond, Eric Steven, “Como convertirse en hacker”, http://sindominio.net/biblioweb/telematica/hacker-como.html.

28.Saez Capel, Jose. “Argentina: El proyecto de Convención del Consejo de Europa para reprimir el ciberdelito y los peligros que entrañará ...”, http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=119697

29.Sanchez Noriega. J.L. “la ética del hacker y el espíritu de la era de la información”. http://www.elciervo.es/elciervo/libros/libros_2002_10/etica.html.

30.“Seguridad Informática: Hackers.” http://www.monografias.com/trabajos/hackers/hackers.shtml.

31.“Tipos de delitos informaticos”. http://tiny.uasnet.mx/prof/cln/der/silvia/tipos.htm.

32.“Tras la pista de un hacker”. http://mouse.tercera.cl/antes/Nro.116-1998.29.01/Nro.116B.html.

33.Varios autores. “delitos y tecnología de la información. http://delitosinformaticos.com/delitos/delitosinformaticos2.shtml.

34. Vila Lozano, Jorge. “delito informático y tecno-era”. http://www.google.cl/search?q=cache:v2xm0LYbIpwC:www.fiscalia.org/doctdocu/doct/delinftecnoera.pdf+delito+informatico+internet&hl=es&lr=lang_es&ie=UTF-8.

35. Villalba Diaz, Federico. Argentina: Los delitos y contravenciones informáticas. “Los Hackers y el Código Contravencional de la Ciudad de Buenos A. http://v2.vlex.com/global/redi/detalle_doctrina_redi.asp?articulo=107546