



UNIVERSIDAD DE CHILE

Facultad de Derecho

Departamento de Ciencias Penales y Criminología

TRATAMIENTO PENAL A LA INTERVENCIÓN
INDISCRIMINADA DE LAS TELECOMUNICACIONES
PERSONALES VÍA INTERNET DE LOS CIUDADANOS
CHILENOS, POR AGENTES DE ESTADO EXTRANJEROS.

*Memoria de pregrado para optar al grado de licenciado en
ciencias jurídicas.*

INTEGRANTES:

Jorge Aníbal Aranda Ortega

Manuel Alejandro Ramírez González

PROFESOR GUÍA:

Myrna Villegas Díaz

Santiago, Chile
2008

Facultad de Derecho

Departamento de Ciencias Penales y Criminología

TRATAMIENTO PENAL A LA INTERVENCIÓN INDISCRIMINADA DE LAS
TELECOMUNICACIONES PERSONALES VÍA INTERNET DE LOS
CIUDADANOS CHILENOS, POR AGENTES DE ESTADO EXTRANJEROS.

INTEGRANTES:

Jorge Aníbal Aranda Ortega

Manuel Alejandro Ramírez González

PROFESOR GUÍA:

Myrna Villegas Díaz.

Calificación final: 6.8

Santiago, Chile
2008

*A nuestras familias,
compañeros,
y amigos.*

AGRADECIMIENTO

A quienes con su estímulo nos ayudaron para que esta publicación fuera posible: familiares, compañeros, profesores y amigos.

RESUMEN

La intervención en las telecomunicaciones vía correo electrónico realizada por agencias de inteligencia extranjeras, importa la verificación de vulneraciones al Derecho a la vida privada y a la inviolabilidad en la comunicaciones privadas, consagrado en el artículo 19 N° 4 y 5° de la Constitución Política de la República de Chile y en los tratados sobre Derechos Humanos vigentes hoy en Chile. Junto a ello, esta violación normativa conlleva la verificación de figuras típicas como la del artículo 161 – A del Código Penal chileno. Esta tipo de intervención se encuentra en auge gracias a la llamada “guerra contra el terrorismo”, y encuentra su justificación legal en los Estados Unidos en la U.S.A. Patriot Act.

La presente investigación indaga las posibilidades de persecución penal para estos delitos, y de las medidas que pueden adoptar los ciudadanos chilenos al conocer que sus telecomunicaciones son intervenidas. Para tal efecto, se exponen los antecedentes fácticos afines al problema; luego se analizarán las legislaciones atingentes; igualmente, se estudian los criterios de legitimidad para intervenir las telecomunicaciones; y, finalmente las posibilidades de aplicación de las leyes.

Lamentablemente, encontramos que ninguno de los mecanismos legales nacionales vigentes resulta idóneo para perseguir penalmente las vulneraciones descritas, ni tampoco para proteger los Derechos Fundamentales y Humanos conculcados. De este modo, ciertas medidas político-criminales preventivas, tales como la anonimización y la encriptación de mensajes de correo electrónico, resultan ser la forma más accesible de proteger estos Derechos.

TABLA DE CONTENIDOS

| | |
|--|----|
| Introducción | 9 |
| 1. Capítulo I Descripción de los antecedentes fácticos del problema, y criterios de legitimidad del estado para vulnerar el derecho a la vida privada | 14 |
| 1.1. Internet y el correo electrónico | 14 |
| 1.1.1. ¿Qué es la Internet? historia y funcionamiento elemental. | 15 |
| 1.1.2. Concepto, características, e intervinientes de la red Internet..... | 20 |
| 1.1.2.1. Concepto..... | 20 |
| 1.1.2.2. Características y problemática fundamental para este estudio..... | 22 |
| 1.1.2.3. ¿Quiénes intervienen en Internet? | 24 |
| 1.1.3. Protocolos de Internet y el correo electrónico | 24 |
| 1.1.3.1. Protocolo TCP/IP. | 25 |
| 1.1.3.2. El servicio de correo electrónico y los protocolos SMTP, POP3, IMAC. | 26 |
| 1.1.4. La seguridad en las telecomunicaciones vía correo electrónico en Internet. | 29 |
| 1.1.5. Intervención en las telecomunicaciones y violación normativa. | 33 |
| 1.2. El derecho a la vida privada e intimidad: concepto y conflictividad..... | 34 |
| 1.2.1. Aproximación doctrinal a un concepto. | 36 |
| 1.2.2. Regulación positiva en Chile..... | 38 |
| 1.2.3. El derecho al secreto de las comunicaciones. | 41 |
| 1.2.4. Vulneración de derechos fundamentales entre privados, y vulneración de éstos por parte del Estado. | 44 |
| 1.3. Criterios de legitimidad de la intervención de los Estados, tendencias penales y sociales. | 47 |
| 1.3.1. Criterios de legitimidad del poder político. Los derechos humanos. | 47 |
| 1.3.2. La intervención mínima del derecho penal..... | 57 |
| 1.3.3. La crisis y restauración del Estado de bienestar, de la legitimidad democrática y la Globalización económica. | 61 |
| 1.3.4. Legitimidad de la intervención del Estado en el ámbito de las telecomunicaciones personales vía Internet. Presupuestos fácticos, estabilidad política, los derechos humanos y la seguridad nacional | 68 |
| 2. Capítulo II Descripción y análisis de las instituciones jurídicas procesales y penales asociadas..... | 72 |
| 2.1. La sociedad informatizada: desafío y riesgo | 72 |
| 2.2. Configuración de las conductas punibles (penalmente relevantes), como delitos informáticos..... | 78 |
| 2.2.1. Principio de legalidad o reserva. | 79 |
| 2.2.2. La responsabilidad penal individual y algunas observaciones acerca de la participación. | 81 |

| | |
|--|-----|
| 2.2.3. La criminalidad informática. | 82 |
| 2.2.3.1. Delitos informáticos..... | 82 |
| 2.2.3.1.1. “Delito Informático”..... | 83 |
| 2.2.3.1.1.1. Definiciones doctrinales. | 83 |
| 2.2.3.1.1.2. Definiciones institucionales. | 85 |
| 2.2.3.1.1.3. Definiciones legales. | 86 |
| 2.2.3.1.2. “Delitos Informáticos”. | 87 |
| 2.2.3.1.3. Nuestra postura..... | 92 |
| 2.2.3.1.2. Clasificación de las conductas que componen los delitos informáticos. | 94 |
| 2.3. La aplicación de la ley penal en el espacio..... | 100 |
| 2.3.1. Los principios sobre validez espacial de la ley penal chilena..... | 102 |
| 2.3.1.1. Principio básico: el principio de territorialidad. | 102 |
| 2.3.1.2. Excepciones a la territorialidad de la ley penal. | 106 |
| 2.3.1.2.1. Aplicación del principio de personalidad o nacionalidad. | 107 |
| 2.3.1.2.2. Aplicación del principio real o de defensa. | 109 |
| 2.3.1.2.3. Aplicación del principio de universalidad..... | 110 |
| 2.4. Valor en Chile de las leyes penales extranjeras. | 111 |
| 2.5. La Extradición. | 113 |
| 2.5.1. Concepto..... | 113 |
| 2.5.2. Fuentes normativas de la extradición. | 114 |
| 2.5.3. Condiciones en que procede la extradición. | 114 |
| 2.5.4. Efectos de la extradición. | 116 |
| 2.6. Aspectos procesales y penales relativos a la intervención en las telecomunicaciones..... | 116 |
| 2.6.1. El proceso penal, su caracterización, y los principios que lo rigen. | 118 |
| 2.6.1.1. Concepto de proceso penal y sus finalidades..... | 118 |
| 2.6.1.2. Caracterización de los procesos penales..... | 120 |
| 2.6.1.3. Sobre los principios procesales penales en general. | 124 |
| 2.6.1.4. Principios procesales penales en Chile..... | 126 |
| 2.6.1.5. Principios procesales penales que se podrían considerar comunes.. | 130 |
| 3. Capítulo III La ilegalidad de la intervención en las telecomunicaciones por parte de agentes de estado extranjero..... | 133 |
| 3.1. Palabras preliminares. | 133 |
| 3.2. Aplicación al problema de la ley penal en el espacio..... | 135 |
| 3.2.1. Primera hipótesis de solución: principio de jurisdicción universal. | 142 |
| 3.3. Sobre la problemática territorial de Internet en disonancia con el principio de territorialidad del Derecho penal..... | 149 |
| 3.3.1. El carácter transfronterizo de la red como elemento determinante de la problemática en cuestión. | 150 |
| 3.3.2. La Criptografía como una medida político-criminal de carácter preventivo frente a la intervención en las telecomunicaciones vía correo electrónico.. | 153 |

| | |
|--|-----|
| 3.4. Reflexiones sobre la ilegalidad de la Intervención en las telecomunicaciones..... | 158 |
| 4. Capítulo IV. Alternativas de persecución penal nacionales e internacionales | 162 |
| 4.1. Palabras preliminares. | 162 |
| 4.2. Los tipos de la legislación chilena..... | 163 |
| 4.2.1. Generalidades..... | 163 |
| 4.2.2. Párrafo 5 título III, libro II del Código Penal: el artículo 161-A del Código Penal. | 167 |
| 4.2.3. La Ley nº 19.223. | 172 |
| 4.2.4. La Constitución: el recurso de protección. | 179 |
| 4.3. Posibilidades de persecución penal conforme al Código Procesal penal. | 182 |
| 4.3.1. Archivo provisional y principio de oportunidad. | 182 |
| 4.3.2. Formalización de la investigación e improcedencia de la extradición. ... | 184 |
| 4.3.3. Improcedencia de la solicitud de extradición..... | 185 |
| 4.3.4. Las dificultades probatorias. | 186 |
| 4.4. La justicia internacional..... | 189 |
| 4.4.1. Preámbulo..... | 189 |
| 4.4.2. La Convención americana sobre Derechos Humanos y la Corte Interamericana de Derechos Humanos..... | 189 |
| 4.4.3. Hacia una jurisdicción internacional para el tratamiento de estos delitos. Análisis crítico del Convenio sobre Cibercriminalidad y el Tribunal Penal Internacional..... | 195 |
| 4.5. Procedencia de una Acción de Protección en resguardo del Derecho a la Vida Privada, y a la Inviolabilidad de la Correspondencia..... | 204 |
| Conclusiones | 208 |
| Bibliografía..... | 215 |

INTRODUCCIÓN

Nadie podría hoy en día la negar importancia de la red Internet en el desarrollo del tráfico diario, se ha convertido en algo tan cotidiano e imprescindible de manera tan repentina, que poco o nada podemos hacer para negarnos a sus beneficios y virtudes. De modo tal, las telecomunicaciones se han agilizado como nunca antes hemos visto; los correos electrónicos se han convertido en un popular medio de comunicación, económico, y sumamente efectivo.

Estas virtudes no sólo han beneficiado directamente a las personas ordinarias, sino que han tornado, sin ningún misterio, aún más vertiginoso el ritmo de los negocios en el mundo actual. El tráfico económico en todas sus escalas se ha agilizado con la presencia de la red, desde la página de subastas personales, hasta el cierre de millonarios negocios, o incluso con la sustanciación de arbitrajes comerciales en línea.

Todas estas maravillas no deben encandilarnos, pues ya con casi quince años de Internet abierta y civil, hemos comprobado de manera cotidiana que la red acarrea dificultades y peligros que normalmente nos pueden afectar, o nos afectan sin que nos demos cuenta. Por ejemplo, la proliferación de actividades detestables como la pornografía infantil, el tráfico ilegal de armas, la violación de bases de datos sensibles, entre otras cosas, nos hacen mirar con recelo estos proceso de modernización.

En este sentido, nuestra labor como estudiantes de la carrera de Derecho no puede ser ajena a estos problemas tan cotidianos como novedosos, por lo que nos avocamos a estudiar en este trabajo, como lo adelanta su

extenso nombre, el problema de la intervención en las telecomunicaciones por parte de agentes de estado extranjeros.

Nuestra cavilación inicial fue preguntarnos por qué agentes ajenos a nuestras realidades y problemas pueden vulnerar un derecho latamente consagrado en las constituciones occidentales de los pueblos que aspiran a ser civilizados, tal como es la vida privada y su correlato en la inviolabilidad de las telecomunicaciones. Nuestra postura es crítica de tal situación, y en esta entrega nos propusimos indagar al respecto y abrirnos camino en un campo poco desarrollado en las líneas de investigación habituales de los alumnos de nuestra escuela, pues buscamos cultivar alguna novedad en la discusión legal al respecto, siquiera modesta.

Particularmente, como nadie antes ha alegado un supuesto de intervención ilícita en las telecomunicaciones personales vía Internet y no existe jurisprudencia directamente alusiva en Chile al concreto respecto, nos sinceramos al advertir que en comienzo no detentábamos una hipótesis clara de trabajo. Por tal motivo, más bien nos propusimos abrir un camino y determinar si en Chile es posible custodiar tales derechos en sede penal, y en base a las intuiciones pensamos que en Chile existen tales mecanismos jurídicos de defensa, pero que serían inefectivos para los propósitos mencionados. Las razones de esa ineficiencia radicarían en la insuficiencia de competencia de los tribunales nacionales, como también en problemas probatorios alusivos a la emergente informática forense. También supusimos que existen a su vez razones políticas que entraban la eficacia de los procedimientos tutelares existentes; esto en directa relación con un nuevo escenario político mundial en torno a la llamada “guerra al terrorismo”, lo que unido a la universalización de las telecomunicaciones vía Internet, ha desembocado en amplias atribuciones para la intervención indiscriminada en

las comunicaciones privadas electrónicas de los ciudadanos por parte de las agencias de inteligencia estatales, en pos de la seguridad nacional.

Así, cabe mencionar que esta entrega es de carácter fundamentalmente dogmático-jurídico, de forma tal que por razones obvias nos centraremos en materias penales y procesales. Sin embargo, las exposiciones dogmáticas van precedidas de antecedentes fácticos relativos a la proliferación de la telemática y de la informática, necesarios para nuestra demostración, por lo que el estudio de tales antecedentes, que escapa a la dogmática pura, hace necesario averiguar datos y circunstancias más allá del derecho positivo. En continuación de lo anterior, también es relevante mencionar que nuestra opción metodológica será la utilización del método deductivo, es decir, abordando las aristas más generales del problema, para ir adentrándonos en lo más específico.

Dentro de los objetivos que nos planteamos en esta memoria constan los de describir los principales problemas penales y procesales, en la protección del derecho a la vida privada informática de los ciudadanos ligado a las comunicaciones personales vía Internet, frente a la intervención indiscriminada de agencias de inteligencia extranjeras estatales. Del mismo modo pretendemos evidenciar la antedicha ineficacia procesal intuida y plantear algunas hipótesis de solución.

Así mismo, para lograr tal evidencia, pesquisamos información preferentemente doctrinal y legal para describir los mecanismos procesales existentes nacionales de protección al derecho a la vida privada en las telecomunicaciones personales vía Internet, y al mismo tiempo, evaluar prospectivamente lo urgente que es el mejoramiento de los mecanismos de protección procesales nacionales de dicho derecho frente a la intervención arbitraria de agencias de inteligencia extranjeras. Del mismo modo, y concatenado con lo anterior, nos proponemos reafirmar lo relevante que es la

consagración efectiva del derecho a la vida privada de los ciudadanos en un Estado de Derecho liberal o social democrático.

En el camino nos encontramos no con pocas dificultades, sin embargo, la mayor de ellas fue la carencia de bibliografía en ciertos temas acotados, en especial en temas de derecho informático relacionado con derecho penal, y en relación a temas de informática forense. El resto de las adversidades responden a lo normalmente esperable, es decir, lo que cualquier estudiante debiera enfrentar en una investigación monográfica.

Así, nuestra monografía está estructurada en cuatro capítulos. En el primer capítulo pasaremos revista a los antecedentes fácticos del problema de la intervención de las telecomunicaciones tales como la proliferación de la Internet y del correo electrónico, su historia y funcionamiento, sus características y desventajas; también en el abordaremos los derechos a la vida privada y a la inviolabilidad de las comunicaciones, y examinaremos los criterios de legitimidad que detenta el estado para, eventualmente, vulnerar estos derechos. En el segundo capítulo, realizaremos una descripción de las instituciones jurídicas penales y procesales relativas a estas intervenciones, tales como la aplicación de la ley penal en el espacio, los principios de nacionalidad y de universalidad, la extradición, y los principios procesal penales aceptados comúnmente por los Estados occidentales. En la tercera parte de la memoria explicaremos la ilegalidad de la intervención masiva de los correos electrónicos por parte de otros agentes de Estado, basados en nuestra crítica y negación del principio de universalidad impulsado unilateralmente por un país, este caso, los Estados Unidos; también avanzamos en soluciones de medidas político-criminales de carácter preventivo, basadas en métodos criptográficos como una defensa fáctica, y no jurídica, de la inviolabilidad de las telecomunicaciones. Finalmente, revisamos las posibilidades que nos surte nuestro ordenamiento jurídico para poder reclamar, en sede penal, la

vulneración de los derechos conculcados, por lo que en esta sección pasamos revista a los tipos penales pertinentes, a la eventual sustanciación de un proceso penal en Chile, a una posible reclamación en sede internacional ante la Comisión y Corte Interamericana de Derechos Humanos y también revisamos aspectos relevantes de la Convención del Cibercrimen; también se explorará, como última posibilidad, la interposición de una acción de protección constitucional. Todas estas vías de actuación no dan una solución o una posibilidad de reclamación útil, por lo que en las conclusiones finales intentaremos delinear el problema al que nos enfrentamos realmente, y comparar nuestros resultados con nuestro punto de partida.

CAPÍTULO I
DESCRIPCIÓN DE LOS ANTECEDENTES FÁCTICOS DEL PROBLEMA, Y
CRITERIOS DE LEGITIMIDAD DEL ESTADO PARA VULNERAR EL
DERECHO A LA VIDA PRIVADA.

1.1. Internet y el correo electrónico.

En el presente apartado, nos esforzaremos por explicar de la manera más propedéutica y sucinta el sustrato fáctico de nuestra investigación: La red Internet y los métodos de telecomunicación que puede propiciar, especialmente, el correo electrónico.

Para tales efectos, nos centraremos en la historia de esta red para explicar su funcionamiento básico, y luego su concepto, características, y sujetos intervinientes. Más tarde chequearemos el concepto de protocolo, y su utilidad en esta maquinaria informática, poniendo hincapié en aquellos protocolos capitales para efectos de nuestra investigación, que permiten el correo electrónico. Para terminar, explicaremos algunos elementos de seguridad informática, y para finalizar, trazaremos algunas perspectivas de las violaciones normativas que podría acarrear la violación de estos mecanismos de seguridad.

Cabe aclarar que la explicación dada no está desarrollada por informáticos aficionados sino por estudiantes de derecho, por lo que en muchos casos se puede pecar de extremo simplismo. A cambio de ello, se ha tratado de dar la explicación más sencilla a cada cuestión, de modo que sea aprehensible algo que al sujeto relacionado con las humanidades y con el derecho resultare difícil de aprehender, y porque no decirlo, muchas veces ingrato.

1.1.1. ¿Qué es la Internet? Historia y funcionamiento elemental.

Algo que se ha tornado tan cotidiano y habitual, tanto en el trabajo como en el ocio, es el uso de esta red para el desenvolvimiento de los más amplios propósitos de nuestras vidas, tales como enviar una carta para saludar a un amigo, concretar un negocio multimillonario, jugar a las damas chinas contra un oponente italiano, o simplemente informarnos de los sucesos hodiernos en una página de prensa. Todas esas acciones se realizaron vía Internet... Sin embargo, poco tiempo dejamos para responder a la pregunta: ¿Y cómo es que mi computador lo hace? Este subapartado pretende responder esa interrogante en base a la historia de la red Internet, pues cada vez que se resuelve un problema en la evolución histórica de la red se explica un fundamento de su funcionamiento que perdura hasta hoy.

Lo cierto es que para comprender que es la Internet, debemos remontarnos a la guerra fría, pues en cierta medida esas circunstancias determinaron en buena parte sus características.

Corría el año 1965, cuando una agencia gubernamental estadounidense llamada DARPA trabajaba en un sistema de manejo de información táctica y estratégica que permitiera a una conjunto de centrales militares enviar y recibir información en caso de un ataque nuclear del bloque comunista. Sin embargo, si existía a esa fecha el teléfono y el telégrafo como medios de telecomunicación eficientes... ¿Por qué desarrollar un nuevo sistema?

La respuesta es sencilla: esos sistemas de telecomunicación son centralizados, es decir, en una o en muy pocas instalaciones concentran todo su potencial de despliegue. De este modo, atacando a dichas centrales, se

podía poner en jaque a todo un sistema de telecomunicación, y con ello, ralentizar, o tornar nula, cualquier toma de decisión de defensa por falta de información relevante.

De esta forma, el cometido de DARPA era tan ambicioso como novedoso: debía crear una red de información y telecomunicaciones descentralizada, de modo que la pérdida de uno de sus nodos (o “centrales”) no conllevara la caída de todo un sistema, y junto a ello, permitiera tomar decisiones defensivas acertadas con celeridad, pudiendo concretar así una “...iniciativa de defensa en la guerra fría”¹.

Según afirma REUSSER, los principios de funcionamiento de esta red fueron enunciados por Leonard Kleinrock, en el marco de investigaciones desarrolladas en el Instituto Tecnológico de Massachussets.²

Así, en 1969 DARPA logró crear la llamada DARPANet, que sería una verdadera proto-internet, que funcionaba bajo el mismo principio elemental con que funciona la red Internet hoy día: la información que contiene un ordenador y que se envía a otro se divide en pequeños fragmentos o paquetes, los cuales son enviados a otro ordenador distante. Cada fragmento puede tomar un rumbo distinto, pudiendo cada uno de ellos trazar un derrotero diferente al de los otros paquetes para llegar al ordenador de destino. Esa posibilidad de rutas distintas es posible gracias a tres presupuestos: 1 – Que la red tiene varios nodos o “centrales” retransmisoras interconectadas, y no una o pocas centrales neurálgicas. 2 – Que todos esos nodos están interconectados entre sí, ya fuere

¹ ADAME MARTÍNEZ, MIGUEL ANGEL. 1998. Derecho en Internet. Sevilla, España, Edit. Mergablum. 15p.

² REUSSER, CARLOS. 2003. Internet, Conceptos Generales. Santiago, Chile, Centro de Estudios de Derecho Informático, Universidad de Chile. 2p.

directamente o indirectamente, de modo que todos los nodos tendrían acceso a todos los otros nodos. 3 – Que los paquetes enviados lleguen a su destino, y puedan ser reordenados como quién junta distintas piezas de un rompecabezas, creando un todo dotado de sentido e inteligibilidad.

Ese tercer presupuesto es quizá el más complejo de ese entonces, dado que la creación de nodos y su interconexión dependen de un soporte físico posible, la transmisión y reagrupación de paquetes tenía que sortear algunos problemas tales como: ¿Qué hacer si llegan paquetes defectuosos o repetidos, o faltan paquetes? Es decir, y siguiendo el ejemplo del rompecabezas, tengo piezas incompletas o mal impresas, o me sobran algunas porque están repetidas, o lisa y llanamente me faltan. Por otro lado. ¿Qué hacer si las configuraciones inmateriales básicas, o sistemas operativos, de los dos ordenadores que intentan compartir información, son distintos? Para explicarlo de modo didáctico, sería como tratar de comunicar a dos personas que hablan idiomas diferentes, como a un chino y a un peruano.

Esas soluciones fueron dadas por los protocolos, que serían “...un lenguaje de reglas y signos que rigen el intercambio de información entre ordenadores...”³. Protocolo sería una verdadera especie de “lengua franca” entre los ordenadores, tal como otrora fue el latín en la edad media. La idea es que estos protocolos sean comunes a todos los usuarios de Internet. Este concepto será más ahondado después, pero de momento esta caracterización nos sirve.

Ya determinado este funcionamiento básico, la red comenzó a crecer en tamaño y a incorporar más nodos. Así, en 1972 cambió su nombre a ARPANet,

³ REUSSER. Op. Cit. 13p.

y ya contaba con 40 nodos. En 1979 se cambia su otra vez nombre al que sería su definitivo: Internet, acrónimo de la voz inglesa *Interconnected Networks*, que en español sería como Redes Interconectadas.

Con el tiempo, las investigaciones lograron cosas hace una década eran impensadas, como poder enviar mensajes de texto a manera de correo (correo electrónico), o intercambiar información digitalizada en archivos (transmisión de archivos). Así, las instituciones civiles académicas se comenzaron a interesar en este proyecto dada las proyecciones que prometía. De tal modo, la *National Science Foundation* (NSF), de Estados Unidos, colaboró conectando a los ordenadores de algunas universidades a la floreciente red.

Luego de reemplazar en 1981 el protocolo más antiguo NCP por el TCP/IP (que básicamente es el protocolo encargado de solucionar el problema enunciado de transmisión y ordenamiento de paquetes) agilizando la interconexión, el acceso de la empresa privada a la red, en 1985, para explotar su potencial económico desata un hito que determina una constante y explosiva expansión en de la red, pues se utiliza hasta hoy su potencial en la realización de negocios a distancia. Ahora su finalidad militar se he relevada, pero no abandonada.

Sin embargo, la Internet detentaba muchos problemas hoy resueltos, los cuales se fueron superando sucesivamente hasta 1994. Estos guardan principalmente relación con el acceso a los distintos ordenadores conectados a la red (los cuales son millones), y con el acceso restringido que oponía el gobierno de Estados Unidos, dado que nunca, hasta la década de los noventa del siglo pasado, aspiró a abandonar su finalidad militar ya enunciada.

Sobre el problema de acceso a los distintos ordenadores, originariamente para acceder a la información de otro ordenador, a cada uno de ellos se le designa un número IP (*Internet Protocol*), que es una sucesión de cuatro cifras numéricas que llegan hasta al 255, separadas por puntos. Así, para tener acceso se debía marcar el número IP como quién hoy marcaría un número de teléfono para llamar a un amigo.

Esto dificultaba considerablemente el acceso a la información, por que se debía tener, antes de acceder a la red, una verdadera guía de números IP, como podría ser hoy la guía de teléfonos. Además, para acceder de un ordenador a otro, se debía marcar otra vez otro número, y volver a reutilizar otro derrotero telemático, lo que se traducía en una inversión considerable de tiempo.

Para solucionar este problema se creó un protocolo llamado *Hyper Text Transfer Protocol* (HTTP) a comienzos de los noventa, que básicamente permite una asociación entre dos ordenadores, reuniendo en una conexión dos o más números IP de manera rápida. Para ello, se creó además la idea de “dirección en Internet” en el concepto dirección URL (*Uniform Resource Locator*), junto al programa *Domain Name Service* (DNS). La idea es simple: a cada número IP se le designa un nombre alfanumérico que sería la dirección de Internet (Ej. www.uchile.cl), luego, el programa DNS se encarga de asociar el nombre al número IP, y posteriormente, ya asociado, el protocolo HTTP se ocupa de establecer la conexión entre los dos ordenadores, y luego de establecida, deja de operar, tal como lo haría una máquina automática que marca números de teléfono.

El programa DNS es tan complejo de operar, que sólo nodos considerables, o servidores, pueden ofrecerlo. Este programa no está dentro de cada ordenador que se conecta a Internet.

Creados este programa y este protocolo, se puede decir que nace la Gran Red Mundial (*World Wide Web*), que permite la navegación rápida a cualquier lugar del mundo sin tener que contar con una gran guía de números IP.

Para facilitar aún más las cosas, para aquellos que carecen de grandes conocimientos de informática y de telemática, se crearon interfaces más amables, basadas en representaciones gráficas de la información contenida en los distintos ordenadores, de una manera muy similar a como se representaría en un diario mural escolar. También se crearon programas que facilitan el acceso a esas distintas representaciones, sin necesidad de digitar complejas fórmulas. El primer concepto enunciado es el de página web, y el segundo es el de navegador. El primer navegador se llamaba *Mosaic*, y se terminó de crear en 1993.

Pero pese a todo lo anterior, aún el gobierno estadounidense no autorizaba el acceso universal a la red Internet, pero ya caído el muro de Berlín y desaparecido el gran temor de una guerra nuclear, se liberalizó el acceso en 1994.

Ya hacia 1995, el crecimiento de la red es impresionante, y de una u otra forma es lo que conocemos hoy cada vez que accedemos a ella.

1.1.2. Concepto, características, e intervinientes de la red Internet.

1.1.2.1. Concepto.

Luego de lo ya expuesto, podemos dar una definición de Internet ideada por ADAME MARTÍNEZ, por considerarla pedagógica y sencilla, explicitando primero el concepto general de red, y luego el de Internet: “Una red es un conjunto de ordenadores que se conectan entre sí gracias a que comparten un mismo lenguaje (llamado protocolo). Las redes de comunicación entre ordenadores pueden ser de varios tamaños, según el número de ordenadores que incluyan conectados... “Internet es una red que conecta al menos varias centenas de miles de ordenadores que hablan un mismo idioma, que es el protocolo *TCP/IP*, acrónimo de *Transmission Control Protocol/Internet Protocol*)...”⁴ También, podemos agregar que a Internet se le caracteriza como la llamada “red de redes”, dada su extensión mundial.

Internet, asimismo, reconoce tres niveles de operación⁵, siendo estos:

- 1 - El medio físico, que es el soporte tangible de la red, tal como son los cables y los ordenadores.
- 2 – Los protocolos generales, que serían un lenguaje común a todas las máquinas, que sirven para realizar las operaciones capitales de Internet, tal como el protocolo TCP/IP.
- 3 – Los protocolos especiales, que sería aquellos que siendo también un lenguaje común a todos los ordenadores, propician funciones específicas y accesorias, tal como el protocolo SMTP, que habilita el correo electrónico.

Ya conocido su concepto, el cual ya podía ser deducido de su historia y funcionamiento, otra interrogante nos queda en el tintero... Ya sabemos qué es

⁴ ADAME MARTÍNEZ. Op. Cit. 15p.

⁵ Esta diferenciación es propuesta por FERNÁNDEZ ALLER, CELIA y SUÁREZ SÁNCHEZ DE LEÓN, JOAQUÍN MARÍA. 1999. *Informática para Abogados*. Madrid, España, Ediciones Anaya Multimedia S.A. 115p.

la red, pero no sabemos cómo es ella. La gran extensión de Internet inevitablemente nos lleva a preguntarnos aspectos tales como... ¿Hay un controlador de Internet? ¿Puede alguien comprar toda la red? ¿Quién administra todo esto? ¿Puede desaparecer de la noche a la mañana? Etcétera.

Responder preguntas de esa índole es el menester del sub-apartado siguiente.

1.1.2.2. Características y problemática fundamental para éste estudio.

Para responder a las preguntas enunciadas, debemos considerar las características de Internet. Para tales efectos seguiremos la clasificación utilizada por MOYA GARCÍA⁶.

1- Globalizada, dado que abarca ordenadores en todo el mundo. Así, es posible acceder a información de cualquier lugar del planeta que se encuentre conectado. De ahí que Internet sea indispensable para acuñar el bullado término de “aldea global”, pues, literalmente, todos los participantes de la red están interconectados, es decir, la humanidad completa.

2- Descentralizada, pues no hay un organismo o estado nacional que determine unilateralmente el crecimiento de Internet. Sin embargo, hay organismo que coadyuvan a su estabilidad y desarrollo. Estos son principalmente la ISOC (*Internet Society*) que vela por mantener disponibilidades universales y estudiar las

⁶ MOYA GARCÍA, RODRIGO. 2003. Libertad de expresión en la red Internet. Revista Chilena de Derecho Informático, Facultad de Derecho, Universidad de Chile, Santiago, Chile (2): 89-108. Pese a ello, ADAME MARTÍNEZ, Op. cit. 18p. desarrolla otra caracterización, basada en la pluralidad, dinamismo, e internacionalidad. Sin embargo, preferimos aquél dado que permite denotar mejor los conflictos que se suscitan en la red.

virtudes y limitaciones de la red; y la ICANN (*Internet Corporation for Assigned Names and Numbers*) que se ocupa de la organización y asignación de los nombres de dominio de Internet, es decir, de los códigos alfanuméricos asociados a los números IP, y finalmente la IRTF (*Internet Engineering Task Force*), ocupada de la implementación y creación de nuevos parámetros y estándares en la red.

3- Abierta, dado que cualquiera que tenga un ordenador adaptado con un módem y con acceso a la conexión puede integrarse a Internet.

4- Gran capacidad y almacenamiento, debido al gran y creciente potencial de los servidores. Cada día, conforme al crecimiento de la red, es posible almacenar más y más información, y acceder a ella.

5 - Interactiva, en el sentido que todos pueden aportar contenidos o emitir opiniones y recibir réplicas. Por ende, de una u otra manera, la red se construye conforme a las preferencias de los usuarios.

6 – Controlada por los Usuarios, relacionado con lo anterior, los mismos usuarios construyen los contenidos de la red. Por ejemplo, se realizan votaciones para designar al artista de la semana en una página destinada a la música rock.

Como corolario de lo anterior, y para efectos de nuestra investigación, es útil tener presente que el hecho de que la red Internet sea abierta, acarrea el problema de que todo contenido o información que sea privada pueda ser violada, y por tanto, habría una vulneración al derecho fundamental a la vida privada. Este punto será desarrollado después, pero es conveniente enunciarlo desde ya, dado que es un tema importante dentro de la investigación.

1.1.2.3. ¿Quiénes intervienen en Internet?

Según MATURANA MIQUEL⁷, podemos reconocer en la red Internet los siguientes sujetos intervinientes:

1 – Proveedor de Servicio de Internet, que es quién provee de un requisito necesario para acceder a la red. Estos a su vez pueden subclasificarse en tres tipos: Proveedores de Acceso a Internet que entregan un servicio de acceso a la red, como una compañía telefónica; Proveedores de Enlace, que entregan la posibilidad de interconectar ordenadores remotos mediante un enlace físico; y Proveedores de Alojamiento, que otorgan espacio continuo y permanente para almacenar datos.

2 – Proveedores de Contenidos: son quienes aportan información y opiniones a la red. Eventualmente todos podríamos ser proveedores de contenidos. Por ejemplo, al escribir una carta a un diario de publicación virtual ya estamos aportando contenidos a la red.

3 – Los Usuarios: son quienes navegan por la red, y toman conocimiento de los contenidos que en ella se encuentran. Por ejemplo, quién lee un diario de publicación virtual desde su computador conectado a Internet.

1.1.3. Protocolos de Internet y el correo electrónico

Dadas la características de la red, y como bien pudimos caracterizar antes, para que la red funcione son necesarios los llamados protocolos, que vendrían a ser, en términos simples, un idioma común que tienen todos los computadores. Esto es necesario dada la diversidad de sistemas operativos que pueden tener los ordenadores a lo largo del planeta, vale decir, sus

⁷ MATURANA MIQUEL, CRISTIÁN. 2002. Responsabilidad de los proveedores de acceso y de contenido en Internet. Revista Chilena de Derecho Informático Facultad de Derecho, Universidad de Chile, Santiago, Chile (1): 17-30.

configuraciones inmateriales son distintas e incompatibles entre sí. Si seguimos el ejemplo anterior, quizá un chino y un peruano puedan entenderse si ambos saben algo de inglés.

Para nuestros propósitos, nos interesa estudiar los protocolos TCP/IP, SMTP, IMAP y POP3, que son los principales responsables del funcionamiento del servicio de correo electrónico.

1.1.3.1. Protocolo TCP/IP.

Si bien son protocolos diversos, ambos deben operar juntos al ser sus labores complementarias, y pertenecen al segundo nivel de operación de Internet. Así, explicaremos primero el IP, y luego el TCP, para finalmente denotar su evidente confluencia.

1- IP, *Internet Protocol*: Como estudiamos en el anexo de historia y funcionamiento de Internet, uno de los presupuestos de Internet era la división de los datos en pequeños paquetes que puedan viajar por la red. El protocolo encargado de dicha operación es éste. Así, en un ordenador emisor de información, divide, empaqueta y envía. Sin embargo, vimos que pueden llegar paquetes de más, de menos, o paquetes defectuosos. El IP no se preocupa de este problema, sino que sólo envía datos.

2- TCP, *Transfer Control Protocol*: ¿Qué sucede si los paquetes llegan defectuosos, no llegan o llegan repetidos? Este protocolo se ocupa de tal problema. Para decirlo de la manera más propedéutica posible, es un verdadero administrador de la transferencia de información. Así, cuando al receptor tiene problemas con los paquetes, este protocolo se encarga de replicar automáticamente al emisor para que los paquetes sean reemitidos, de modo de recolectar

todas las partes íntegramente. Empero, este protocolo no genera paquetes, sino que sólo administra y ordena.

Como podemos advertir la complementariedad entre ambos protocolos es necesaria, dado que lo que el protocolo IP genera, el TCP lo ordena. De otra manera, Internet no tendría sentido, siendo este protocolo la base de toda la red.

1.1.3.2. El servicio de correo electrónico y los protocolos SMTP, POP3, IMAC.

Antes de adentrarnos en lo que corresponde a la explicación de estos protocolos, es conveniente que expliquemos primero que es un correo electrónico.

Un correo electrónico, en una definición muy clara y sencilla, es "...el servicio básico y más popular a la vez, de los que se ofrecen en Internet. Se trata del intercambio a través de la red de información escrita mediante un ordenador... Una de las utilidades más extendidas del correo electrónico es la posibilidad de adjuntar un archivo de texto, imagen o sonido..."⁸. De una u otra manera, todos quienes hemos tenido acceso a Internet hemos tenido acceso a un correo electrónico.

El funcionamiento es sencillo: dentro de un servidor de correo se almacenan los datos enviados. A ese servidor se ingresa previa suscripción, que normalmente es gratuita, y para ingresar se detenta una contraseña, por lo que el correo supone ser confidencial. Así, dentro del almacenamiento del servidor se guardan los mensajes, los cuales, una vez habiendo ingresado con

⁸ FERNÁNDEZ ALLER y SUÁREZ SÁNCHEZ DE LEÓN. Op. Cit. 149p.

la contraseña, se pueden leer, como si fuera una casilla del correo analógico, es decir, el de tinta y papel.

Para tal efecto, se han creado interfaces amistosas que ordenan los correos y facilitan considerablemente la utilización de esta herramienta.

De perogrullo está decir que la popularidad de este servicio radica en que sirve para contactar a gente que se encuentra muy lejos a muy bajo costo. También sirve para concretar negocios a distancia con costos de transacción más bajos que el fax o el teléfono.

Ahora bien, entendiendo el que es el correo, podemos entrar a comprender los protocolos subyacentes a este servicio, perteneciente al tercer nivel operacional de Internet.

De tal forma, el protocolo SMTP (*Simple Mail Transfer Protocol*) opera bajo el mismo principio del TCP/IP, pero de manera más específica. Esto es, entre el emisor y el receptor existen una serie de comandos alternados que posibilitan el envío del mensaje. Siempre el primero en abrir la comunicación es el emisor con un comando llamado HELO, y luego, se van verificando una serie de comandos entre emisor y receptor, como si fuera un “diálogo alternado” de una obra de teatro muy bien aprendida. Si fallare uno de los pasos, saldrá un error que será notificado en la cuenta de correo como un correo devuelto. Por ejemplo, cuando se envía un correo a una dirección errónea, falla un “parlamento” de este “diálogo alternado”, el cual consiste en que ante un determinado comando, el emisor debe entregar una casilla de correo válida y vigente como destinatario.

¿Por qué no hacemos este paso a paso cuando enviamos un correo? Básicamente, porque la interfaz del correo hace esta “obra de teatro” por nosotros, y sólo nos avisa cuando algo que nosotros ingresamos está mal, o cuando el receptor está impedido de recibir.

Uno de los grandes problemas de este protocolo es que no es capaz de discriminar entre emisores cuando puede recibir un correo, esto es, que en el fondo siempre está abierto a cualquiera que quiera escribir. Esto ha devenido en el llamado “correo basura”, que consiste en que, generalmente por motivos publicitarios, se envían correos en serie a muchas direcciones extraídas de una base de datos. Estos correos suelen ser muchos y atochan el almacenamiento de un servidor, o por defecto, hacen más complicado revisar la casilla.

En segundo lugar, junto al protocolo SMTP, operan en el funcionamiento del correo electrónico los protocolos IMAP (*Internet Message Access Protocol*) y POP3 (*Post Office Protocol 3*), que permiten tener acceso a los correos electrónicos almacenados en un servidor remoto, es decir, que se encuentra en otra locación geográfica distinta a la del usuario que accede a éste. La principal diferencia entre el protocolo POP3 y el IMAP es que el primero permite descargar todos los correos y operar así con una conexión intermitente, no así el IMAP que requiere de una conexión continua.

Normalmente los correos electrónicos que usan la mayoría de los ciudadanos son los ofrecidos por empresas que entregan gratuitamente una cuenta de correo electrónico, tales como el Gmail, o el Yahoo mail. En estos casos, existe un servidor que almacena y administra todos los correos, y por ende, puede tener acceso a todos ellos eventualmente.

1.1.4. La seguridad en las telecomunicaciones vía correo electrónico en Internet.

El tráfico cotidiano vía Internet en general, y vía correo electrónico en especial, presupone situaciones en las cuales la información que circula por la red debe ser reservada sólo a quienes son el emisor y el destinatario de lo comunicado, es decir, se generan hipótesis de protección del derecho a la vida privada en la red Internet.

Un problema de que la red Internet sea abierta, como enunciamos anteriormente, es que la información circulante puede quedar expuesta ante cualquiera que tenga acceso a ella, ya fuere con o sin consentimiento de quienes comparten dicha información.

Para que la privacidad pueda tener asidero en la red, se deben cumplir ciertos requisitos necesarios⁹, que son:

- 1- Autenticidad y Autenticación: esto consiste en que tanto el remitente como el receptor deben estar determinados e identificados de manera recíproca, de modo que no queden dudas acerca de que el mensaje ha llegado a quién estaba destinado y sobre la identidad de quién lo escribe.
- 2- Integridad: según esta idea, el mensaje debe llegar en las mismas condiciones que fue redactado, sin ser adulterado, editado, o trastocado.
- 3- Confidencialidad: El mensaje no puede ser expuesto a otras personas ajenas al receptor y al emisor. En este requisito es donde el derecho a la vida privada se hace más plausible.
- 4- Repudiación o Rechazo: Es la hipótesis de que una de las partes se niegue a participar del acto comunicativo, rechazando el mensaje sin conocer su contenido.

⁹ REUSSER. Op. Cit. 19p.

Estos cuatro requerimientos fundamentales son necesarios para el éxito en la confidencialidad de un mensaje.

Empero, la pregunta ahora es: ¿Cómo se puede lograr esta confidencialidad cumpliendo los cuatro requisitos? La respuesta es mediante procedimiento de criptografía, que se configura como una verdadera medida político-criminal de prevención, que otorga seguridad por medios técnicos.

La criptografía puede ser definida como "...la técnica de transformar un mensaje inteligible, denominado texto en claro, en otro que sólo puedan entender las personas autorizadas a ello, que llamaremos criptograma o texto cifrado. El método o sistema empleado para cifrar el texto en claro se denomina algoritmo de encriptación... La Criptografía es una rama de las Matemáticas, que se complementa con el Criptoanálisis, que es la técnica de descifrar textos cifrados sin tener autorización para ellos, es decir, realizar una especie de Criptografía inversa. Ambas técnicas forman la ciencia llamada Criptología."¹⁰

Otra definición posible es "...la ciencia que estudia la escritura secreta, la forma de ocultar el significado de la información, basándose principalmente en mantener la privacidad de las comunicaciones entre dos personas alterando el mensaje original, de modo que sea incomprensible a toda persona que no sea el destinatario, y que proporcione la necesaria autenticación, esto es la firma del mensaje para que un mensaje para que un tercero no pueda hacerse pasar por el emisor..."¹¹

¹⁰ DÍAZ LEVANO, CAROLINA, y PERAZA DARVE, MARÍA LAURA. 2005. La Criptografía: "Una guerra de Piratas y Corsarios". [en línea] Revista de Derecho Informático Alfa-Redi (82). <<http://www.alfa-redi.org>> [consulta: 15 enero 2007].

¹¹ GONZÁLEZ NAVARRO, BLAS ALBERTO. 2001. Criptología y libertades públicas. En: LOPEZ ORTEGA, JUAN JOSÉ (Compilador). Internet y Derecho Penal. Madrid, España Cuadernos de Derecho Judicial, Consejo General del Poder Judicial. pp. 147-237. 152p.

En nuestras palabras, y de manera más sencilla, la criptografía es una disciplina cuya finalidad es la ocultación del contenido de mensajes, de manera de preservar oculto su contenido de quienes son ajenos a él. La ocultación se hace mediante una clave, que no es otra cosa que el método escribir y entender el mensaje oculto.

En la criptografía, es posible encontrar dos clases de claves: las simétricas y las asimétricas. La clave simétrica consiste en aquella que es igual para el emisor como para el receptor. Por ejemplo, si a cada letra del abecedario le designamos un número tal como $A=1$, $B=2$, $C=3$, y así sucesivamente. Luego, encontramos escrito 13-1-13-1. Como receptores, debemos usar la misma clave que usó el emisor para redactar el mensaje, que sería reemplazar cada letra del abecedario por un número. Así, el mensaje oculto es “Mamá”.

La clave simétrica posee una seria desventaja: cada vez que enviamos un mensaje y nuestro receptor no conoce la clave, debemos señalar la clave en ese mensaje o en otro. De éste modo, nos arriesgamos a que el mensaje sea descifrado.

En cambio, la clave asimétrica no tiene ese problema porque funciona de una manera más efectiva pero más compleja: se requiere la existencia de una clave de conocimiento común, o “clave pública”, y de otra de conocimiento exclusiva del usuario o “clave privada”. Cada persona tiene así dos claves (una pública que todos conocen, y una privada que sólo conoce el usuario), siendo cada clave necesaria para descifrar un mensaje cerrado con la otra clave. Es decir, si Pedro encripta un mensaje con la “clave pública” de Juan, ese mensaje sólo se podrá abrir con la “clave privada” de Juan, que obviamente sólo Juan conoce porque, valga la redundancia, es privada. A la inversa, si Pedro encripta

su mensaje con propia su “clave privada”, Juan sólo podrá abrir el mensaje con la “clave pública” de Pedro.

En este último caso, en realidad, todos podrían abrir el mensaje de Pedro porque su “clave pública” es conocida por todos, lo que en rigor no sería un método de ocultación de información, sino un método de autenticación.

En fin, y siguiendo con el ejemplo, si Pedro encripta su mensaje con su propia “clave privada” y al mismo tiempo con la “clave pública” de Juan, Juan deberá usar dos claves: su propia “clave privada” y la “clave pública” de Pedro. De este modo, Juan tendrá la certeza de que el mensaje proviene de Pedro (autenticidad), y que sólo él leerá el mensaje (privacidad). Además, si lo desea, puede repudiar el mensaje (rechazo).

Sin embargo... ¿Cómo se puede verificar si el mensaje es íntegro? Para ello, cuando se encripta el mensaje, suele haber un mecanismo que lo copia y lo envía con un “duplicado” oculto dentro del mismo mensaje. Así, en caso de disconformidad con el original, esto se hará patente (integridad).

Hoy en día, el sistema de encriptación más efectivo es el método PKI (*Public Key Infrastructure*), que funciona bajo este supuesto. Esto, acompañado de un sistema de firma electrónica (que sería equivalente a encriptar con la clave privada en el ejemplo anterior), son efectivos para preservar la información de intromisiones indeseadas, verificando la identidad de los en el proceso de comunicación.

De este modo, un sistema de clave asimétrica puede poseer las cuatro características necesarias para que un sistema de comunicación sea privado.

1.1.5. Intervención en las telecomunicaciones y violación normativa.

Lamentablemente, no todo sistema es indefectible. Es posible que los mecanismos de seguridad detenten fallos que los hagan vulnerables, y por lo tanto, se vea vulnerado el derecho fundamental a una vida privada.

Estas fallas pueden devenir de la impericia del propio usuario, o pueden ser provocadas por sujetos expertos que busquen conocer información ajena. Estos sujetos, conocidos como “*hackers*”, son conocedores de lenguajes de programación y buscan acceder a información privada mediante elucubraciones informáticas.

Estos “*hackers*” no son la única amenaza que enfrenta la preservación de este derecho en la red Internet. También hay programas de inteligencia creados por países desarrollados, que se ocupan del análisis de correos electrónicos. Estas intromisiones las realizan so pretexto de custodiar la seguridad nacional, y de proteger a los ciudadanos del terrorismo.

La más famosa de estas redes es la red ECHELON, y el programa registrador de correo más potente del que se tiene conocimiento es el *Carnivore* del FBI, ambos pertenecientes al aparato de seguridad de los Estados Unidos.

Sobre ECHELON es posible aseverar que hace algunos años salió a la luz pública, pero aún sin tener certeza fehaciente de su verdadero alcance y potencialidades. Duncan CAMPBELL reveló la existencia de esta red en 1999¹²; él asevera que la red pende de una alianza estratégica entre los Estados

¹² El Parlamento Europeo en el año 1999, ante estas noticias, constituyó una comisión investigadora para ahondar los escasos conocimientos que se tiene de esta red, dirigida por el eurodiputado Gerhard Schmid. Ver: PARLAMENTO EUROPEO investiga. 2004. [en línea] News Room del Parlamento Europeo. 2 de abril 2004. <<http://www.europarl.europa.eu/highlights/es/108.html>> [consulta: 6 enero 2007].

Unidos, Reino Unido, Nueva Zelanda y Australia llamada UKUSA, constituida en 1948 para interceptar comunicaciones en los albores de la guerra fría para vigilar al bloque comunista. Esta alianza creó la red ECHELON para interceptar información táctica y estratégica relevante. Sin embargo, actualmente se estima que espía a corporaciones transnacionales y a sujetos sospechosos de terrorismo.¹³

Del mismo modo, la comisión investigadora que constituyó el Parlamento Europeo llevó a cabo un trabajo al respecto, y logró determinar la existencia indudable de dicha red en el 2001.¹⁴

Con todo, en este afán, no sólo se registran correos de ciudadanos estadounidenses, sino que todos los que transiten por un servidor de dicho país, lo que significa que a la postre cualquiera de nosotros podría ser vigilado sin que nunca lo sospechare.

Lo anterior se ve amplificado con el supuesto de que en los Estados Unidos, bajo la administración George W. Bush se ha propiciado la dictación de la llamada *U.S.A. Patriot Act*, que permite estas intervenciones¹⁵ en desmedro de otros derechos fundamentales, como el de la vida privada.

1.2. El derecho a la vida privada e intimidad: concepto y conflictividad.

¹³ CAMPBELL, DUNCAN. 2001. Silencio, se espía. [en línea] El Correo de la UNESCO, marzo, 2001. <http://www.unesco.org/courier/2001_03/sp/doss10.htm> [consulta: 6 de enero del 2007].

¹⁴ GONZÁLEZ, JUAN CARLOS. 2001. UNA COMISIÓN DE LA EUROCÁMARA confirma la existencia de ECHELON. [en línea] El Mundo, España, jueves 8 de Marzo, 2001. <<http://www.elmundo.es/navegante/2001/03/08/seguridad/984041457.html>> [consulta: 6 enero 2007].

¹⁵ En lo sucesivo, cuando señalemos una intervención en las telecomunicaciones “a secas”, queremos referirnos a intervenciones tanto discriminadas como indiscriminadas. En cambio, cuando nos referimos a intervenciones masivas, hacemos alusión sólo a aquellas indiscriminadas y que pueden afectar eventualmente a cual sujeto.

Pero, en estricto rigor... ¿Qué es la vida privada? ¿Cual es su entidad como derecho fundamental? ¿Es de índole universal o es sólo local a nuestro sistema jurídico de raigambre continental? Sólo respondiendo estas interrogantes, y conceptualizando al derecho a la vida privada, podremos ponernos en el escenario adecuado para comprender si la intervención está o no justificada en un Estado de derecho moderno y democrático.

Como vimos anteriormente, la red Internet permite la intromisión de extraños a lo que queda reservado a nuestra vida privada, dada la característica de abierta de la red.

Sin embargo, conceptualizar la vida privada, en sede doctrinal, como un derecho fundamental es un tema de suyo enrevesado. Esta dificultad está determinada por la confluencia de definiciones de vida privada e intimidad que tienden a identificarse, por una supuesta equivocidad de ambos términos. Parte de ello será desarrollado a continuación.

Pese a lo anterior, el derecho a la vida privada está consagrado en la legislación positiva¹⁶, tanto a nivel constitucional como legal, lo que disipa dudas sobre lo etérea que pudiere resultar su configuración. De tal modo,

¹⁶ Para efectos de toda esta monografía, debemos comprender básicamente que los Derechos Fundamentales son aquellos que están positivizados una Constitución y no son meramente programáticos. En cambio, los Derechos Humanos son primordialmente aspiracionales, y por ello no necesariamente reconocidos en una Constitución; éstos generalmente están reconocidos en tratados internacionales, cuya aplicación concreta es muchas veces insatisfactoria. Pese a ello, en el caso del Derecho a la vida privada y a la inviolabilidad de la correspondencia ocurre una coincidencia entre estas categorías, por lo que a lo largo de la presente monografía se les tratará indistintamente de Derechos Humanos y de Derechos Fundamentales, sabiendo que pueden ocupar ambas etiquetas simultáneamente. Para mayor abundamiento: PECES-BARBA. G. 1999. Curso de Derechos Fundamentales. Teoría General. Madrid, España, Universidad Carlos III, Boletín Oficial del Estado de Madrid. 21p y siguientes.

haremos referencia a la consagración positiva del derecho a la vida privada en el ordenamiento jurídico chileno.

Sin embargo, tenemos que enfrentar otro problema aún más debatido: La colisión de la vida privada con otros derechos fundamentales. ¿Es posible la colisión? Para tal efecto haremos una breve referencia a la discusión y continuando con un tópico similar, realizaremos una distinción entre colisión de derechos e intervención del Estado en la vida de los ciudadanos, considerando que la limitación a la intervención del Estado reconoce un límite en los derechos fundamentales en general.

1.2.1. Aproximación doctrinal a un concepto.

Frecuentemente, usamos los conceptos de vida privada e intimidad sin distinguir el uno del otro, lo que nos lleva a equivocaciones¹⁷.

En primer lugar, es debido aclarar que estos conceptos son muy difíciles de determinar por dos razones: la primera es la fecunda similitud entre ambos, lo que lleva a confusiones y usos indistintos de uno y otro; la segunda, y que es más definitoria, es su relatividad social y temporal, lo que los hace variar conforme a las circunstancias¹⁸. En especial, esta última consideración es la que hace que estos conceptos sean difíciles de definir, y más aún, es aquella realidad la que determina su relatividad temporal y espacial.

¹⁷ El desarrollo y alguna consecuencias de esta equivocidad las representa BARROSO, PORFIRIO y LOPÉZ TALAVERA, MARÍA DEL MAR. 1998. La Libertad de Expresión y sus Limitaciones constitucionales, Madrid, España, Editorial Fragua. 99p y siguientes. Para estos autores, la necesaria distinción entre ambos términos es para determinar las limitaciones de la intimidad y de la vida privada.

¹⁸ BARROSO y LOPÉZ TALAVERA. Op. Cit. 106p.

Ya atendidas estas circunstancias, BARROSO y LOPÉZ TALAVERA, estiman que es posible de ellos extraer al menos denominadores comunes para una aproximación en un sentido elemental: la intimidad humana sería una realidad reservada para los demás, que se manifiesta en un ámbito íntimo y personal de nuestras vidas y pensamientos, como podrían ser nuestros sentimientos no exteriorizados respecto de otra persona; en cambio, la vida privada es un aspecto de nuestra vida privada sometido igualmente a reserva, pero respecto de nuestro quehacer cotidiano y de cosas que exteriorizamos, pero que simplemente queremos que todos los demás no lo sepan, como podría ser la vida en familia, con los amigos, o nuestras relaciones amorosas, etc.

A nuestro parecer, un criterio determinante para diferenciar los conceptos, sería asumir la intimidad como una no exteriorización, hacia los demás, de nuestros pensamientos y emociones, la vida privada a una exteriorización acotada y selectiva de nuestras emociones y pensamientos, y finalmente, la vida pública a una exteriorización indiscriminada.

En relación a la aparición de nuevas tecnología, DEL PIAZZO establece una doble faz del derecho a la intimidad y a la vida privada. En primer lugar, dice que hay una faz pasiva, según la cual nadie puede entrometerse en la privacidad de una persona, lo que en la doctrina norteamericana se comprende como “el derecho a ser dejado en paz” (*right to be alone*). Sin embargo, las llamadas tecnologías de la información de las telecomunicaciones, y en especial la red Internet, reafirman una faz activa del derecho a la vida privada ya sea a la intimidad, donde se tiene control sobre mi información y sobre quién está legítimamente autorizado para detentarla, actualizarla, y utilizarla.¹⁹

¹⁹ DEL PIAZZO, CARLOS. 2006. Los Derechos Humanos ante las Nuevas Tecnologías. [en línea]. Revista de Derecho Informático Alfa-Redi. (48) <<http://www.alfa-redi.org/>> [consulta: 5 diciembre 2006].

Esta faz pasiva surge, y toma relevancia en la actualidad, a propósito de la acción de *Hábeas Data*, mediante la cual se puede pedir a quién detenta información, sin consentimiento del dueño de ella, a borrarla de sus bases de datos.

1.2.2. Regulación positiva en Chile.

En los tratados internacionales, de entre los que se incorporan a nuestro ordenamiento jurídico a través del artículo 5º de la Constitución Política²⁰, estos derechos reconocen protección, partiendo por la Declaración Universal de Derechos Humanos²¹, que en su artículo 12 establece que “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación...” Esta disposición, curiosamente, no se refiere a la intimidad.

También hace referencia a este derecho el Pacto Internacional de Derechos Civiles y Políticos de 1966²², que en su artículo 17 prácticamente reitera el artículo 12 de la Declaración Universal de Derechos Humanos, pero el requisitos de las injerencias las amplía a “...arbitrarias o ilegales...”. Igualmente, no reconoce el concepto de intimidad.

²⁰ CHILE. 1980. Constitución Política de la República. 24 octubre 1980. [en línea] <www.bcn.cl> [consulta: 22 enero 2007]. En adelante, cada vez que se menciona la Constitución, se entenderá que nos referimos a la Constitución de Chile.

²¹ CHILE. 1948. Declaración Universal de Derechos Humanos. 10 diciembre 1948. [en línea] <<http://www.ddhh.gov.cl/>> [consulta: 22 enero 2007].

²² CHILE. 1989. Pacto de Derechos Civiles y Políticos. 29 abril 1989. [en línea] <www.bcn.cl> [consulta: 22 enero 2007].

La misma idea de reiteración se aprecia en el artículo 11 de la Convención Interamericana sobre Derechos Humanos de 1969²³, donde se agrega un primer inciso de “...derecho al respeto de su honra y al reconocimiento de su dignidad...”. Los incisos segundo y tercero reiteran lo que dice el Pacto de Derechos Civiles y Políticos de 1966.

En la Constitución Política Chilena, el artículo 19 n° 4° reconoce el derecho de “El respeto y protección de la vida privada y pública y a la honra de la persona y su familia”. Esta protección es completada por el artículo 19 n° 5°: “La inviolabilidad el hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas señalados por la ley.”

En fin, la regla general es que no se puede intervenir la vida privada y dañar la honra de las personas. No se protege la intimidad expresamente. Se establece el principio de legalidad para intervenir las comunicaciones y el hogar.

Cabe recordar que estos derechos se encuentran amparados por la acción de protección del artículo 20°. Al consagrar esto, podría suscitarse una hipótesis de colisión de derechos respecto del artículo 19 n° 12, dándonos las primeras luces de lo que sería el conflicto de derechos.

A nivel legal, las limitaciones estarían dadas por las hipótesis de responsabilidad civil extracontractual del Código Civil²⁴, en su título XXXV del

²³ CHILE. Convención americana sobre Derechos Humanos, denominada “Pacto de San José de Costa Rica” .1969. Presidente de la República, PATRICIO AYLWIN AZOCAR. 5 enero 1991. [en línea] < www.bcn.cl > [consulta: 23 enero 2007].

²⁴ CHILE. Ministerio de Justicia. 1855. Código Civil. 22 noviembre 1855. [en línea] <www.bcn.cl> [consulta: 22 enero 2007]. En lo sucesivo que se refiera al Código Civil a secas se tratará del chileno.

libro IV, y eventualmente por las hipótesis de responsabilidad penal de los artículos 412 al 431 del Código Penal²⁵.

Especial atención merece el artículo 161 A de nuestro Código Penal, que establece un tipo a quién intervenga comunicaciones de carácter privado. Esta hipótesis de persecución penal reconoce una excepción: los artículos 222 y 223 del Código Procesal Penal²⁶, donde se puede autorizar la interceptación de comunicaciones telefónicas para efectos de la etapa de investigación.

El panorama respecto de la ley 19.722 sobre libertades de opinión e información y ejercicio del periodismo, es tal, que en el título IV se establece un derecho de rectificación y de aclaración, donde alguien aludido a una información de manera errónea e imprecisa tiene derecho a que el medio de comunicación remedie el error sin costo, estableciendo un procedimiento muy particular, existiendo un plazo de prescripción de 20 días desde que se pudo conocer la información por parte del ofendido.

En caso de no realizarse la enmienda, el director y el propietario o concesionario del medio de comunicación social serán solidariamente obligados a pagar una multa de 12 a 100 U.T.M.

Respecto de los delitos de injuria y calumnia, se establece una regulación especial en ésta ley, siendo importante el artículo 30, que establece que quién cause injuria por un medio de comunicación social, no se le admitirá prueba de verdad acerca de sus expresiones, salvo que la imputación se

²⁵ CHILE. Ministerio de Justicia. 1874. Código Penal. 12 noviembre de 1874. [en línea] <www.bcn.cl> [consulta: 22 enero 2007]. En lo sucesivo que se refiera al Código penal a secas se tratará del chileno.

²⁶ CHILE. Ministerio de Justicia. 2000. Ley nº 19.696: Código Procesal Penal. 12 octubre 2000. [en línea] <www.bcn.cl> [consulta: 22 enero 2007]. En adelante cuando nos refiramos al Código Procesal Penal, aludiremos al chileno.

hubiere hecho con un interés público real. Para determinar que es el interés público, el mismo artículo, a continuación, señala una lista taxativa de hipótesis, que son: hechos referente al desempeño de funciones públicas; hechos realizados en el ejercicio de una profesión u oficio cuyo conocimiento sea de interés público; actividades de libre acceso público; cuando lo difundido hubiere sido con consentimiento del interesado; cuando haya archivos o registros públicos; hechos consistentes en la comisión o participación de un delito. Finalmente, la ley define que es la esfera privada, y establece que son los “hechos relativos a su vida sexual, conyugal, familiar o doméstica, salvo que fueren constitutivas de delito”.

En suma, la ley delinea lo que puede ser o no la esfera privada, resguardando la veracidad de lo expresado, y la intimidad y honra.

Sin embargo, por lo menos la Constitución chilena y los tratados internacionales revisados no establecen una delimitación clara entre el derecho a la intimidad y a la vida privada. Es más, sólo hablan del derecho a la vida privada.

Entonces, para efectos de esta investigación, nos centraremos principalmente en el derecho a la vida privada, en el entendido que es una exteriorización discriminada a ciertas personas de nuestros pensamientos y emociones, como pretendimos definir en el apartado anterior, en sede doctrinal. Así, la violación de la correspondencia electrónica sería una violación del derecho a la vida privada.

1.2.3. El derecho al secreto de las comunicaciones.

La doctrina extranjera reconoce el presente derecho como una de las manifestaciones concretas del derecho a la vida privada. Así lo conviene

MONTAÑÉS PARDO²⁷⁻²⁸, que realizando un análisis de la jurisprudencia española y europea²⁹ señala: “el secreto de las comunicaciones constituye una garantía del derecho a la vida privada y, en especial, a la intimidad personal que constituye su núcleo esencial.... Ello es así porque el derecho a la intimidad personal y familiar guarda un estrecho parentesco, por ser una de sus manifestaciones fenoménicas (con) el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, cuya interceptación por tanto significa una grave injerencia en aquél.”

Por otro lado, concordamos con dicho autor con que tal derecho se concretiza en una doble dimensión³⁰; primero comprende la libertad de comunicación, es decir el derecho de poder comunicarse con cualquier otro sin interrupción o suspensión alguna. Segundo incluye el secreto del mensaje, de carácter negativo, entendido como el derecho a que terceros no conozcan el contenido de la comunicación.

Del mismo modo, entre sus características destaca su configuración como una garantía formal³¹, o sea se protege la reserva o privacidad de la comunicación, sea cual sea el contenido de la misma. En mayor profundidad, se trata acerca de la intrascendencia del contenido de ella y que no se exteriorice

²⁷ MONTAÑÉS PARDO, Miguel Ángel. 1999. La intervención de las comunicaciones. Doctrina jurisprudencial. España, Editorial Aranzadi. 22p.

²⁸ Así también lo señala RODRÍGUEZ RUIZ, B. 1998. El secreto de las comunicaciones: tecnología e intimidad. Monografía. Madrid, España, Editorial McGraw-Hill; VIGOROUX, A. 2002. Del Deber de Retención de los Datos de Tráfico relativos a las Comunicaciones Electrónicas. [en línea] Revista de Derecho Informático (49). <www.alfa-redi.org/> [consulta: 13 enero 2007]. BELDA PÉREZ- PEDRERO, Enrique. 1998. El Derecho al secreto de las comunicaciones. [en línea] Parlamento y Constitución. Anuario (2). <www.dialnet.unirioja.es/servlet/articulo?codigo=197133> [consulta: 13 enero 2007]. pp. 169-194.

²⁹ MONTAÑÉS PARDO. Op.cit. 22p. Alude a jurisprudencia del Tribunal Constitucional español (STC. 114/1984, STC. 85/1994, STC. 34/1996, STC. 54/1996 y STC 123/1997) y del Tribunal Europeo de Derechos Humanos (TEDH. 1978 caso *Klass* y TEDH 1984. caso *Malone*).

³⁰ MONTAÑÉS PARDO. Op. cit. 23p.

³¹ Ídem.

ningún dato que afecte la vida privada de quienes se comunican no obsta a su protección bajo el derecho en comento. En definitiva se protege la opacidad de la propia comunicación, no de su contenido.

Paralelamente y, como consecuencia de ello, el secreto de las comunicaciones no afecta a los partícipes de la comunicación, sino sólo a los terceros ajenos a ella. Los partícipes, el autor señala: “podrán quedar afectados directamente, en su caso, por el respeto de la vida privada e intimidad de su interlocutor, lo que dependerá del contenido de la comunicación”.³²

El autor prosigue especificando lo que, a su parecer, la Constitución española, en su artículo 18.3: “3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.”³³, reconoce como objeto de protección del derecho al secreto de las comunicaciones. Se refiere al término “comunicaciones”, ella enumera las más habituales, en especial de las postales, telegráficas y telefónicas, “pero no se ha restringido la protección a ninguna de las formas posibles, comprendiendo por ello tanto las presentes (correo, teléfono, videoteléfono, fax, etc.) como las que puedan desarrollarse en el futuro.”³⁴ Criterio que, en su opinión, ha compartido el Tribunal Europeo de Derechos Humanos al analizar el alcance y extensión del artículo 8º del Convenio, incluyendo dentro de la garantía del mismo a todo tipo de de medios que permitan una comunicación privada.

Por último, en lo que respecta a nuestro país, es necesario reflexionar acerca del reconocimiento o no, en nuestro ordenamiento jurídico, del derecho al secreto de las comunicaciones.

³² Ídem.

³³ ESPAÑA. 1978. Constitución Española. Artículo 18.3. [en línea] <www.congreso.es/funciones/constitucion/indice.htm> [consulta: 22 enero 2007].

³⁴ MONTANÉS PARDO. Op. cit. 24p.

De lo que se desprende de nuestra Constitución el artículo 19 n° 5 asegura a todas las personas: “la inviolabilidad del hogar y de toda forma de comunicación privada” y luego señala la existencia de limitaciones legales para este derecho. A su vez el artículo 5° prescribe en su inciso segundo: “El ejercicio de la soberanía reconoce como limitación el respeto a los derechos esenciales que emanan de la naturaleza humana. Es deber de los órganos del Estado respetar y promover tales derechos, garantizados por esta Constitución, así como por los tratados internacionales ratificados por Chile y que se encuentren vigentes”. Esta última afirmación nos interesa, principalmente, puesto que aunque se pudiera impugnar el reconocimiento del derecho por los términos utilizados en nuestra carta fundamental, tal indicación amplía el espectro de los derechos fundamentales constitucionalmente reconocidos a los de los tratados internacionales vigentes, ratificados por Chile. El autor español BELDA PÉREZ- PEDRERO³⁵, por su lado, asevera: “El secreto de las comunicaciones es un derecho universalmente aceptado y su consideración por parte de los órganos encargados de la aplicación de los convenios sobre derechos y libertades, nos ha de servir para explicar las dudas que acerca de su contenido surjan en nuestro país...”.

En suma sin entrar a la discusión terminológica de nuestra Constitución, o acerca del espíritu de la ley, o cualquier otra vía interpretativa, se reconoce la incorporación a nuestro ordenamiento jurídico del derecho al secreto de las comunicaciones, vía el contenido de los tratados internacionales vigentes, ratificados por Chile.

1.2.4. Vulneración de derechos fundamentales entre privados, y vulneración de éstos por parte del Estado.

³⁵BELDA PÉREZ-PEDRERO. Op. cit. 172p

¿Qué sucede en los casos que el Estado vulnera un derecho fundamental en el ejercicio de su autoridad? ¿Quién detenta la competencia de ese conflicto? ¿Qué sucede en general con las colisiones de derechos? ¿Puede una persona violentar un derecho fundamental de otra, amparado y autorizado por el Estado, porque está ejerciendo otro derecho fundamental? Es un conjunto de interrogantes cuyo trasfondo genera la presente discusión.

Así, siguiendo a ALDUNATE³⁶, existen y conviven diversas teorías respecto a este punto, dentro del tópico llamado “conflicto de derechos fundamentales”, pudiendo clasificarlas en dos grupos: las que niegan la colisión y las que la aceptan.

Para efectos de esta investigación, no es trascendental explicitarlas todas, sino simplemente enunciar la discusión al respecto.

En fin, volviendo al mencionado autor, es discutido en la doctrina si los derechos realmente colisionan. La opinión de ALDUNATE es que si lo hacen, pero en sede de tribunales ordinarios donde se adjudican derechos en la práctica, no ocurre.

Otra tesis, defendida en Chile por GARCÍA-HUIDOBRO³⁷, asevera que no hay colisión porque hay una distorsión en la modernidad y posmodernidad del concepto de derecho, según el cual se detenta el ejercicio de una prerrogativa o de una prestación por parte del Estado (o su aseguramiento), y no de una carga (algo que se hace en beneficio ajeno). El concepto premoderno

³⁶ ALDUNATE, EDUARDO. 2005. La Colisión de Derechos Fundamentales. Revista Derecho y Humanidades (11). Santiago, Chile, Facultad de Derecho, Universidad de Chile: 69-78.

³⁷ GARCÍA-HUIDOBRO, JOAQUÍN. 2005. Conflicto de Derechos. Revista Derecho y Humanidades (11). Santiago, Chile, Facultad de Derecho, Universidad de Chile: pp. 61-68.

dentro del derecho reconocía la carga y la prerrogativa, porque tendía a un orden de las cosas en relación a lo que es justo. Esa noción de justicia no radica en una sistemática en la resolución de conflictos humanos, como en el ideal de la ilustración, sino en una problemática casuista de adjudicación de derechos en la acepción de carga y prerrogativa simultánea.

También hay quienes que simplemente creen que un derecho sede a favor de otro, dando justificaciones circunstanciales.³⁸

En fin, esta discusión se desarrolla en el marco de la posible vulneración de derechos fundamentales de una persona a favor de otra. Sin embargo... ¿Qué sucede si esa vulneración es realizada por el Estado? ¿Se supone que un Derecho Fundamental obligatoriamente debe ceder a favor del interés de todos nosotros como nación?

A nuestro parecer, y con independencia de las tesis referentes a la colisión de derechos, el Estado no es un “sujeto de derechos” como en los casos que presupone el apartado anterior, sino que es quién está obligado a preservarlos. Dicha labor es la que determina su cometido fundamental. Dicho en otras palabras, la razón del Estado son los Derechos Fundamentales, y no la seguridad nacional u otros criterios que finalmente tienden a la vulneración de esos derechos.

De tal modo. ¿Qué determina al Estado para, eventualmente, vulnerar Derechos Fundamentales? En nuestro caso especial. ¿Qué justifica la

³⁸ Este es el caso de BARROSO y LÓPEZ TALAVERA. Op. cit. 128p y siguientes. Una postura que critica esta tendencia de la jurisprudencia portorriqueña es desarrollada por ALVÁREZ GONZÁLEZ, JOSÉ JULIÁN. 2005. Colisión entre los Derechos Fundamentales a la libre expresión y a la intimidad y dignidad humana en los Estados Unidos y Puerto Rico. Revista Derecho y Humanidades (11). Santiago, Chile., Facultad de Derecho, Universidad de Chile: 79-95.

intromisión del Estado en la correspondencia electrónica vía Internet? Para tales efectos, deberemos examinar los criterios de legitimidad del Estado para actuar en tales casos.

En fin, más allá de sí existe una colisión o conflicto de derechos, el tema que nos preocupa es otro muy parecido: ¿Qué sucede si el Estado en el ejercicio de su autoridad afecta un Derecho Fundamental?

1.3. Criterios de legitimidad de la intervención de los Estados, tendencias penales y sociales.

1.3.1. Criterios de legitimidad del poder político. Los derechos humanos.

Los Estados en el ejercicio del poder, deben necesariamente respaldarse en criterios de legitimidad, que son sustento material ineludible para su actuar frente a los ciudadanos, atendida la teoría de representatividad que encierra el Contrato Social, uno de los pilares dogmáticos de los Estados de gran parte de occidente, erigido por Rousseau hace ya dos largos siglos. Especialmente con el Derecho Penal, la herramienta más poderosa de que disponen, en cuanto ejercicio de la función punitiva y, lo que es más relevante, elemento legítimo de vulneración de los derechos de los individuos.

Siguiendo los razonamientos de VILLEGAS y LAVÍN³⁹. “Todo Poder advierte la necesidad de obtener su autojustificación, esto es lo que llamamos

³⁹ VILLEGAS DÍAZ, M. y LAVÍN ESPINOZA, M. 2005. Terrorismo e intervención penal en la red Internet .Uso de las tecnologías de la información y las comunicaciones en la represión penal del terrorismo. [en línea] Departamento de Investigación, Universidad Arcis. <<http://derecho.universidadarcis.cl/index.php?option=content&task=view&id=8&Itemid=45>> [consulta: 17 enero 2007]. 21p.

legitimación. MAX WEBER⁴⁰ indicó las condiciones de legitimidad del poder social:

- a) Que el ordenamiento jurídico se estatuyera positivamente,
- b) Que los sujetos de derecho creyeran en su legalidad, esto es, en la corrección formal de los procedimientos de creación y aplicación en el derecho. Desde esta óptica, la creencia en la legitimidad se reduciría a creencia en la legalidad.

No obstante, no es posible afirmar que al ser el Estado el creador de las normas de acuerdo a un sistema de reglas racionales sancionadas, entonces *per se* se legitime. Un procedimiento, como tal, no puede producir legitimación. Más bien, la sanción misma necesita ser legitimada. WINCKELMANN,⁴¹ sostiene que la creencia en la legalidad no se legitima por sí sola, sino que es preciso un consenso racional respecto de los valores, pues ellos son los principios fundadores de la sanción normativa.

La creencia en la legalidad se deriva, entonces, de una previa creencia en la legitimidad. El poder estatal no puede apoyarse en la legalidad y el monopolio que ostenta en la producción del ordenamiento jurídico, sobre la base de su *ius puniendi*, sin antes estar legitimado. En este sentido HABERMAS señala: “El procedimiento inobjetable de sanción de una norma, el hecho de que un proceso se ajuste a la formalidad jurídica, únicamente garantiza que las instancias previstas dentro de un sistema político,

⁴⁰ WEBER, M. *Wirtschaft und Gessellschaft*. En: Economía y sociedad. Volumen I. Traducción de Imaz, E., Medina Echavarría, J., García Maníes, E., Roura Parella, J. y Ferrater Mora, J. 1956. 2ª ed. México, Editorial F.C.E. pp. 160 y siguientes. Cit por VILLEGAS DÍAZ y LAVÍN ESPINOZA. Op.cit.21p.

⁴¹ WINCKELMANN, J. 1952. *Legitimität und legalität in Max Weber Herrschaftssoziologie*. Tubinga. pp. 75 y siguientes. Cit. por HABERMAS, J. 1986. Problemas de legitimación en el capitalismo tardío. Buenos Aires, Argentina, Edit. Amorrurtu. 122p. Cit. por VILLEGAS DÍAZ y LAVÍN ESPINOZA. Op.cit. 21p.

competentes y acatadas como tales, son responsables por el Derecho vigente. Pero esas instancias son parte de un sistema de poder que tiene que estar legitimado en total si es que la legalidad pura ha de considerarse signo de legitimidad”⁴².”

La historia de la humanidad no ha transcurrido en vano, el Antiguo Régimen fue sucedido por Estados Naciones de corte liberal y socialista, en las dos vertientes más relevantes, que apoyados en la Ilustración, lograron importantes conquistas políticas y jurídicas, que cuentan como elemento primordial, el Derecho Constitucional que consagró garantías y derechos individuales, en condiciones de igualdad entre los ciudadanos, al menos en el papel. Tales con el correr del siglo pasado y en el periodo de post-guerras, se fueron profundizando, masificando y multiplicando, finalmente y como gran hito, cristalizaron a nivel mundial, respaldados en el Derecho Internacional. Con la Organización de Naciones Unidas, su sustento jurídico y estructural.

En suma, tales derechos que han significado el gran triunfo del liberalismo, y en consecuencia de los individuos en la protección frente a sus pares y principalmente contra el Estado, quien, como lo demuestra la historia largamente, es el principal agente conculcador de los derechos individuales, tanto de manera legítima como ilegítima.

El ámbito del derecho penal, es uno de los frentes principales en que hasta la actualidad se libra cotidianamente esta lucha. La Doctrina Penal obviamente no ha sido pacífica en la materia y se ha preocupado concienzudamente de brindar un apoyo desde las más variadas perspectivas, acerca de los criterios de legitimidad del poder político. Aspecto que aborda con total propiedad, pues, legitimar el ejercicio de tal poder no es sino legitimar su

⁴² HABERMAS. Op cit.122p. Cit. por VILLEGAS DÍAZ y LAVÍN ESPINOZA. Op.cit. 21p.

propia existencia, en el contexto del desarrollo de las corrientes modernas de pensamiento.

Dentro de la maraña, que desde siempre han sido las discusiones dogmáticas penales, que rara vez alcanzan un consenso duradero y unívoco, es necesario en el desarrollo de la presente monografía adoptar una posición, que fundadamente cimiente los criterios de legitimación del ejercicio del poder político por parte del Estado.

Por su parte FERRAJOLI⁴³, aborda la problemática en su obra, de la cual extraemos sus postulados más valiosos, para efectos de nuestra investigación. Para él: “El fin del derecho penal..., consiste entonces en impedir la razón construida, o sea la minimización de la violencia en la sociedad. Es razón construida el delito. Es razón construida la venganza. En ambos casos se verifica un conflicto violento resuelto por la fuerza...La ley penal está dirigida a minimizar esta doble violencia....

Es claro que, entendido de esta manera, el fin del derecho penal no puede reducirse a la mera defensa social de los interesados constituidos contra la amenaza representada por los delitos. Dicho fin supone más bien la protección del mas débil contra el más fuerte, tanto del débil ofendido o amenazado por el delito, como del débil ofendido o amenazado por las venganzas; contra el más fuerte, que en el delito es el delincuente y en la venganza es la parte ofendida o los sujetos con ella solidarios. Precisamente – monopolizando la fuerza, delimitando los presupuestos y las modalidades e impidiendo el ejercicio arbitrario por parte de los sujetos no autorizados – la prohibición y la amenaza de las penas protegen a los reos contra las venganzas

⁴³ FERRAJOLI, LUIGI. 1995. El Derecho Penal Mínimo. En: Prevención y Teoría de la Pena. Juan Bustos (director) Santiago, Chile, Ed. Jurídica Conosur Ltda.: pp. 39-40.

u otras reacciones más severas. En ambos aspectos la ley penal se justifica en cuanto ley del más débil, orientada hacia la tutela de sus derechos contra las violencias arbitrarias del más fuerte. De este modo los derechos fundamentales constituyen precisamente los parámetros que definen los ámbitos y los límites como bienes, los cuales no se justifica ofender ni con los delincuentes ni con las puniciones.

Un sistema penal -puede decirse- está justificado únicamente si la suma de las violencias -delitos, venganzas y puniciones arbitrarias- que él puede prevenir, es superior a las de las violencias constituidas por los delitos no prevenidos y por las penas por ello conminadas. Naturalmente, un cálculo de éste género es imposible. Se puede decir, no obstante, que la pena está justificada como mal menor -esto es, sólo si es menor, o sea menos aflictiva y menos arbitraria- respecto a otras reacciones no jurídicas y más en general, que el monopolio estatal de la potestad punitiva está tanto más justificado cuanto más bajos son los costos del derecho penal respecto de la anarquía punitiva.”

Del mismo modo FERRAJOLI⁴⁴, nos aporta acerca del concepto de garantismo y estado de derecho, que sirven de trasfondo al criterio legitimador de la potestad punitiva del Estado, ya aludido por él mismo. “Si aceptamos la oposición establecida por Hobbes y Kant entre poderes salvajes y estado de derecho, es claro que el garantismo –entendido en el sentido de estado constitucional de derecho, esto es aquél conjunto de vínculos y de reglas racionales impuestos a todos los poderes en tutela de los derechos de todos-

⁴⁴ FERRAJOLI, LUIGI. 2000. El garantismo y la filosofía del derecho. Colombia. Universidad Externado. pp. 132-142.

representa el único remedio para los poderes salvajes⁴⁵...garantismo y estado de derecho son paradigmas teóricos de carácter general que comportan una sistema de límites y vínculos para todos los poderes –no sólo para el poder judicial sino también para el legislativo y el ejecutivo, y no sólo para los poderes públicos sino también para los privados- en garantía de los derechos fundamentales de todos.”

Respecto a la característica garantista que debe guardar el sistema penal para la legitimación de la potestad punitiva del Estado, la doctrina nacional tampoco se ha mantenido indiferente. BUSTOS⁴⁶ señala: “Desde otra perspectiva, la de la persona y su libertad, cabe considerar al sistema penal como un sistema garantista. Un sistema penal como sistema de garantías es consecuencia de de una política criminal en un Estado social y democrático de derecho...El sistema penal en un orden democrático ha de partir de un presupuesto básico: la dicotomía ente la libertad y el poder. Desde esta perspectiva el sistema penal surge como un sistema de trincheras garantistas cuyo objetivo es la exclusión de la arbitrariedad.... Por eso los procesos de criminalización, esto es, los de creación y de aplicación de la norma penal, deben cumplir condiciones de validez democrática. No basta con la promulgación de normas formalmente válidas. Es necesario que en las leyes que formalizan los procesos de criminalización se precipiten principios materiales consustanciales al Estado social y democrático de derecho para que sean también materialmente válidas”.

⁴⁵ FERRAJOLI. “El garantismo...”, Op.cit. pp.126-131, distingue una serie de “poderes salvajes”, de cuatro tipos: poderes salvajes ilegales y extralegales; poderes salvajes privados y poderes salvajes públicos. Entrecruzando las dos distinciones se obtienen las cuatro categorías.

⁴⁶ BUSTOS RAMÍREZ, J.2005. La Política Criminal y el Derecho Penal. En: Lecciones de Derecho Penal. Parte primera. En: Obras Completas, volumen II, Lima, Perú, Edit. Aranzadi. pp. 509-510.

Dentro de esta lógica, y a su vez, adoptamos la idea de intervención mínima del Derecho Penal⁴⁷ y siguiendo, también a DÍAZ⁴⁸, concordamos con que los derechos humanos son el criterio de legitimidad del poder político. Estos constituyen el contenido concreto, histórico, de los grandes valores éticos y políticos que son la libertad, la igualdad, la justicia y la paz, entre otros.

Sin embargo el problema está, en que, junto a zonas comunes, cada hombre e ideología entiende a su modo esos valores, y por lo tanto esos derechos humanos. No obstante a pesar de la fundamental diversidad, en la actualidad resulta extraordinariamente difícil encontrar que alguien abierta y explícitamente se reconozca contrario a los derechos humanos, genéricamente considerados. En efecto hoy todos decimos, admitir y respetar los derechos del hombre. Sin embargo, pregonar un apego irrestricto a ellos, en los hechos, es ilusorio, basta con ejemplificar que en la ONU ningún país se atrevió a votar en contra ni de la Declaración Universal de derechos humanos de 1948 ni de los pactos internacionales de derechos económicos sociales y culturales por una parte y de derechos civiles y políticos, por otra, de 1966; lo cual no impide, sin embargo, que sólo una pequeña parte de los Estados, que votaron a favor de dichos pactos los hayan ratificado y mucho menos aplicado. A pesar de esto es pacífico concluir que ese respeto a los derechos humanos se convierte, aunque sólo sea en el plano teórico-ideológico, en el criterio legitimador del poder político. Ningún país en la actualidad se contenta con ser acusado de perseguidor y negador de los derechos humanos, al contrario intentan justificarse en base a ese criterio.

⁴⁷ BARATTA, ALESSANDRO. 1986. Requisitos Mínimos del respeto de los derechos humanos en la ley penal. Revista Nuevo Foro Penal (34), Bogotá, Colombia: 421-435.

⁴⁸ DIAZ ELIAS. 1976. Socialismo Democrático y Derechos Humanos. En: FERNANDO TORRES (Editor). Política y Derechos Humanos. Valencia, España. pp. 125-148.

Subsiste, no obstante, la duda acerca de la fundamental diversidad de interpretaciones acerca del contenido de los derechos humanos; Primero y fundamentalmente se debe respetar este pluralismo ideológico y la posibilidad de elegir, entre ellas, principalmente porque “son productos de las decisiones autónomas de la conciencia ética del hombre, que operan con un trasfondo en la interrelación dialéctica con esos factores reales y su sentido histórico. Luego porque elegir entre ellas, se trata de una decisión libre pero enraizada en esas condiciones sociales e históricas que crean la vida real del hombre”⁴⁹. Ambas, pluralismo y posibilidad de opción no forzada constituyen base esencial para toda concepción política.

A raíz de lo anterior, es que el problema evoluciona a qué derechos humanos deberán reconocerse y potenciarse para que el poder político aparezca legitimado suficientemente. La primera respuesta es el relativismo absoluto, para unos serán unos y para los restantes otros. Lo que equivale a decir que todo poder es legítimo o que ninguno lo es, en consecuencia una respuesta totalmente insatisfactoria. Tal resultado se vincularía irremediabilmente con las pretensiones legitimadores puramente formales, fundadas exclusivamente en la consagración normativa, perseguidas por autores como Karl Schmitt, que a mediados del siglo pasado dio sustento jurídico a los tristemente célebre movimientos fascistas. No olvidar jamás que el poder político del Estado no deber ser legitimado por criterios netamente formales, pues de esa manera cualquier barbarie puede ser legitimada, encubierta bajo procesos decisorios políticos, aparentemente democráticos. En efecto, todos los regímenes, ideologías o sistemas políticos, deben presentarse como los más justos en cada momento.

⁴⁹ DIAZ, E. Op.cit., 128p.

Nuevamente la pregunta muta entonces a quién debe establecer cuales han de ser de esos derechos y valores, aquí y ahora los mas justos. Existen tres posibles teóricas soluciones. Se dictan tales valores por una persona, dado su carácter excepcional, lo que configuraría una autocracia; los decide un grupo minoritario, una elite dirigente, que da pie a una aristocratismo; o se deja mayoritariamente al grupo social entero, una democracia. Concordamos con DIÁZ en su opción por esta última, con las prevenciones dadas acerca de la reglas de la mayoría. Constan en que la democracia sólo es verdadera y coherente cuando respeta al criterio individual y minoritario, porque también forman parte del todo social y a su vez “la complejidad del problema de las interrelaciones minoría-colectividad debe hoy seguir para evitar precipitadas recaídas en fáciles simplificaciones populistas”⁵⁰.

Por otro lado la regla de las mayorías debe cumplir con ciertos requisitos para constituir cauce de determinación de los derechos humanos. A decir, primero el respeto de la libertad crítica, con lo que supone de respeto al individuo y segundo el reconocimiento del derecho a una efectiva participación política de todos los ciudadanos. “Sin elecciones libres las mayorías no pueden probar que lo son. Sin libertad individual y sin libertad de las minorías, las mayorías no pueden probar que efectivamente son mayorías”⁵¹. Se erige a la libertad crítica en base fundamental para la democracia y los derechos humanos. Asociadas a ella están la libertad de expresión, de opinión, participación libre – a través de partidos políticos y el Parlamento- en la producción de la decisión política y, a su vez, seguridad en la efectiva protección jurídica de tales libertades y de las que sirven de base a ellas, como la libertad de reunión, de asociación política etc., que, siguiendo al autor,

⁵⁰ Ibid.131p.

⁵¹ Ibid. 133p.

constituyen la base de legitimidad del Estado. Sin libertad no hay ni igualdad, ni paz ni justicia alguna.

Continuando la secuencia lógica de DÍAZ, se debe ahora dar respuesta a una pregunta pragmática acerca de qué significa para el proletariado los derechos que se han considerado básicos y fundamentales, los derechos de libertad de crítica y de participación política, de qué les sirven aunque se les sean reconocidos legalmente, si carecen de los medios económicos y culturales necesarios para realmente decidir, en comparación con el de las clases burguesas dominantes⁵², que han impuesto sus términos económicos y culturales, pues gozan con los medios para realizarlo. Dicho de otro modo serían compatibles los Derechos Humanos, es decir, derechos de los hombres y no de sólo de la burguesía⁵³, con una sociedad donde están implantadas relaciones de producción de carácter capitalistas. A lo que se debe responder, que no basta con el reconocimiento de los derechos y su amparo legal, “no basta con un derecho igual, si se está tratando con individuos social y económicamente desiguales. Lo que el Derecho debe buscar es la igualdad real, salvando esas profundas desigualdades existentes”⁵⁴. El Derecho deberá ser igual en lo que se refiere a la libertad y seguridad, pero en lo restante será desigual para lograr la igualdad, o sea se establecerá a favor del más débil. Existe, en consecuencia, una interconexión ineludible entre libertad e igualdad.

⁵² Ibid. 138p: “lo que tradicionalmente – y con acento universalista – se han denominado como derechos innatos... no han sido por lo general derechos para la burguesía (por ella y para ella declarados); es decir derechos que han favorecido sobre todo a dicha clase social, minoritaria pero dominante”.

⁵³ Ibid. 141p. El autor distingue entre derechos fundamentales del hombre y de la burguesía. Los primeros son “son derechos humanos que aunque utilizados hasta ahora...en beneficio preferente o exclusivamente de la burguesía, pueden y deben ser derechos reivindicados y exigibles por todos los hombres” y los segundos “derechos propios de la burguesía..., que solo tienen sentido en un mundo escindido en clases y dominado por aquella.”, por ejemplo, la propiedad.

⁵⁴ Ibid. 136p.

Los obstáculos para una serán para la otra. Sin libertad no hay vía para la igualdad.

En consecuencia el criterio de las mayorías sólo será real cuando realmente las mayorías sean dominantes. Se impondrán los valores y los derechos humanos mayoritarios cuando la mayoría potencial (proletariado) sea a través de una praxis adecuada, la clase realmente dominante. En suma no basta con la democracia jurídico-política, esta debe ser además económica-social.

1.3.2. La intervención mínima del derecho penal

Como soslayamos anteriormente, adoptamos esta idea de función del Derecho Penal, que se encuentra lógicamente asociada con el criterio de legitimación de ejercicio del poder político del Estado fundado en los derechos humanos. Ciñéndonos a los postulados de BARATTA, tal como ya adelantamos, dicha idea de mínima intervención penal le da al concepto de los derechos humanos una doble función. Una negativa acerca de los límites de la intervención penal y una positiva concerniente a la definición del objeto posible pero no necesario de la tutela por medio del derecho penal.⁵⁵

Los principios que articulan la política de la mínima intervención penal, se orientan en una gran división, resultante de la adopción de un punto de vista interno y otro externo al sistema penal.

Principios intrasistemáticos, “indican los requisitos para la introducción y mantenimiento de figuras delictivas en la ley” y los extrasistemáticos “se refieren..., a criterios políticos y metodológicos para la descriminalización y para

⁵⁵ BARATTA, A., Op.cit., 421p.

una construcción alternativa la sistema penal de los conflictos y de los problemas sociales”.⁵⁶

Myrna VILLEGAS realiza una selección de aquellos principios más relevantes, que para nuestros efectos resulta de gran utilidad⁵⁷.

Desde un punto de vista intrasistémico, destaca, ellos parten por el carácter de última ratio que asiste al derecho penal, su carácter subsidiario y fragmentario, en que el Estado ha de intervenir penalmente frente a los ataques más graves de los bienes jurídicos considerados dignos de protección.

Primero se refiere al principio de legalidad, entendiéndolo como una exigencia de seguridad jurídica, es decir, la necesidad de conocimiento previo del delito, y garantía política de los ciudadanos de no poder ser sancionados con otras penas que las señaladas expresamente en la ley. Luego señala que contiene las siguientes garantías para el ciudadano: garantía criminal, la ley debe señalar la pena correspondiente al hecho, requiriendo de ley orgánica constitucional; garantía jurisdiccional, tanto la existencia del delito como la imposición de la pena deben ser determinadas por sentencia judicial, fruto de un proceso previo y legalmente establecido; garantía de ejecución, la ejecución de la pena debe sujetarse a una ley que la regule y la prohibición de la analogía contra reo. Prosigue declarando la necesidad de tipificación del hecho y la sanción, por una ley previa, para la protección del bien jurídico, hecho que debe ser reprochable al sujeto. Lo constituyen los siguientes principios: principio de irretroactividad (*lex praevia*); tipicidad o de taxatividad en las normas penales (*lex scripta et stricta*); lesividad o exclusiva protección de bienes jurídicos;

⁵⁶ Idem.

⁵⁷ VILLEGAS DIAZ, MYRNA. 2001. Terrorismo: Un problema de Estado, tratamiento jurídico en la legislación comparada. Especial referencia a los delitos de terrorismo en las legislaciones de Chile y España. Tesis de Doctor en Derecho. Salamanca, España, Área Penal, Departamento de Derecho Público, Universidad de Salamanca. Vol. 1, pp. 4-5.

principio de culpabilidad o de imputación personal, y junto a él, el principio de exigibilidad social del comportamiento alternativo; y el principio de la responsabilidad penal por el acto (derecho penal del hecho).

Por otro lado continúa, con el principio de racionalidad y proporcionalidad de las penas, que se desdobra en proporcionalidad abstracta y proporcionalidad concreta. El primero hace referencia a que sólo las violaciones a los derechos humanos fundamentales pueden ser objeto de sanción penal, y la pena deber ser proporcional al daño causado. Por el segundo, la pena debe adecuarse al costo social acarreado consigo, que con criterios criminológicos, debe considerar ante todo la incidencia negativa de la aplicación de ciertas penas sobre el sujeto y sobre la sociedad en general.⁵⁸

Asimismo, ha de respetarse el principio de humanidad, que prohíbe los tratos crueles, inhumanos y degradantes. También el principio de idoneidad, en que el legislador queda obligado a realizar un estudio preciso de los efectos socialmente útiles de la pena.⁵⁹ Y el principio resocializador, como fin de la pena o medida de seguridad.

Del mismo modo avanzando en la exposición, VILLEGAS DÍAZ, considera también el principio de representación popular, en cuya virtud se garantiza el proceso de formación de la ley penal, imponiendo la participación popular en la voluntad legislativa, a través de elecciones libres y secretas y la libertad de organización de partidos y movimientos políticos. Junto a ellos se debe respetar el principio de instrumentabilidad administrativa de la ley penal, para que ella pueda prescindir del carácter clasista y de la manera selectiva de funcionar propia del sistema punitivo y el principio de respeto a las autonomías

⁵⁸ BARATTA, A. Op.cit. pp. 424.-425.

⁵⁹ BARATTA, A. Op.cit. 424p.

culturales, continente de una concepción positiva del pluralismo cultural que considere la pertenencia de todos los grupos, culturalmente delimitados, en la realidad social incorporada el Estado⁶⁰.

Desde un punto de vista extrasistémico, VILLEGAS DÍAZ selecciona de entre ellos, aquellos que propenden a la descriminalización (principio de no intervención útil, principio de politización de los conflictos, principio de la conservación de garantías formales)⁶¹ y a aquellos de carácter metodológico de la construcción alternativa de los conflictos y problemas sociales, en que destaca el principio general de prevención, que trata de desplazar el control “reactivo”, es decir, de respuesta a expresiones individuales de los conflictos que se manifiestan en conductas desviadas, a formas de control “proactivo”, respuesta a las situaciones en las que los conflictos se producen⁶².

BARATTA, respecto lo último destaca que el derecho penal no está adecuado para dar respuesta eficaz a los derechos humanos, porque estructuralmente está limitado a una respuesta circunscrita a un caso concreto determinado. Se trata de una “respuesta a los síntomas y no a las causas”. El análisis sociológico es el que permite encontrar estas causas y así se tiende mas allá de una política criminal alternativa: “la política de justicia social, el respeto a los derechos humanos, la satisfacción de necesidades reales de los sujetos en una sociedad... son la verdadera alternativa democrática a la política criminal”⁶³.

⁶⁰ Más ampliamente. Ibid. 423p, 426p y 427p.

⁶¹ Ampliamente. Ibid. 432p y siguientes.

⁶² Ibid. 434p.

⁶³ Idem.

1.3.3. La crisis y restauración del Estado de bienestar, de la legitimidad democrática y la Globalización económica⁶⁴.

No obstante las conclusiones acerca de los derechos humanos como criterio de legitimidad de la intervención del Estado, no se puede ignorar la influencia relevante que ha ejercido el proceso de crisis del Estado de bienestar y la Globalización económica en dicho principio fundamental.

Desde una primera perspectiva, FERRAJOLI⁶⁵, nos ilustra a *grosso modo*: “El efecto más relevante del desarrollo del *Welfare state* sobre las formas institucionales de los estados de capitalismo avanzado ha sido, sin duda, la crisis del modelo liberal clásico del Estado de derecho...en la cual la acción del Estado estaba limitada a funciones esencialmente políticas (la defensa del orden público y la garantía del funcionamiento sin trabas del mercado)...La crisis concierne, en este sentido, a las dos principales funciones del *Welfare state* –el gobierno estatal de la economía y las prestaciones públicas de naturaleza social y asistencial- ...Las expectativas sociales correspondientes a las nuevas funciones –la subsistencia, el empleo, la vivienda, la instrucción, la asistencia sanitaria- son así introducidos y reconocidos por las Constituciones de este siglo como “derechos fundamentales”: lo así llamados derechos sociales a prestaciones positivas... que se colocan junto a los antiguos derechos individuales de libertad, concebidos, en cambio, como derechos a prestaciones negativas. Pero los nuevos derechos, bien o mal satisfechos por el Estado de bienestar según procedimientos de naturaleza prevalentemente política, permanecen, en lo que respecta a la forma jurídica, como simples proclamaciones de principio desprovistas de garantías efectivas...El resultado de esta convivencia entre el viejo Estado constitucional de derecho y el nuevo

⁶⁴ VILLEGAS, M. 2001. Op.cit., pp. 93-104.

⁶⁵ FERRAJOLI. El garantismo... Op. cit. pp. 65-91.

Estado social es una divergencia profunda entre las estructuras legales y las estructuras reales de la organización estatal...Legalidad, publicidad y control resultan, así, paradigmas obsoletos, reservados a zonas superficiales de la actividad del Estado, donde las nuevas y principales funciones del *Welfare state* tienden a desarrollarse en espacios de acción extralegal o de legalidad atenuada, privilegiando técnicas de poder normativamente atípicas, libres de vínculos y de estorbos garantistas, flexiblemente adaptables a los cambios coyunturales... ¿Cómo incide en las formas ya en crisis del Estado de derecho, la crisis, sobre la cual estamos discutiendo, del *Welfare state*?

Esta crisis –debida o no sólo a razones económicas, sino también al predominio de estrategias políticas explícitamente regresivas y antisociales- se manifiesta sobre todo en la reducción del gasto público destinado a las prestaciones sociales y asistenciales del Estado con respecto de la cantidad por el contrario creciente, de las demandas. Está claro que esta restricción...tiene el efecto de acentuar el carácter selectivo e inevitablemente discriminatorio de la satisfacción de las demandas....

La crisis de la legalidad general y abstracta como forma de trato igual y vínculo preordenado a la acción pública es, por descontado, le fenómeno más vistoso. La reducción de la legalidad democrática producto de la insuficiencia económica y política de una satisfacción de tipo igualitario – o cuanto menos imparcial- de las crecientes demandas sociales, es suplida por ese sucedáneo de legitimación representado por la satisfacción sólo de aquellas demandas provenientes de los grupos de presión más poderosos en el mercado político.

Por lo tanto, si el desarrollo del *Welfare state* ha correspondido a una crisis del Estado de derecho, la crisis del Estado de bienestar amenaza con producir su disolución....

Una primera respuesta posible es aquella sugerida por las estrategias neoliberales, que hoy encuentran sustento teórico en el renaciente neoliberalismo económico y en experimentaciones prácticas de muchos países, como Estados Unidos e Inglaterra. La propuesta teórica, de la cual en esta parte se ha hecho portavoz..., Niklas Luhmann, es la de la restauración de las viejas formas liberales del Estado constitucional de derecho y, correlativamente, de un retorno a la economía de mercado, de una reducción del intervencionismo estatal en la economía y sobre todo de una restricción de las prestaciones públicas de naturaleza social y asistencial.

Esta hipótesis tiene el grave defecto, al menos en sus formulaciones más radicales, de ser irrealista. Si es cierto que el *Welfare state* nació en el siglo XX como una respuesta a la crisis de inestabilidad del capitalismo y como remedio a la incapacidad de autorregulación del mercado, no se entiende qué autoriza a pensar que lo que hasta ayer era considerado no autónomo haya encontrado hoy una autosuficiencia que le permita, sin el auxilio externo del Estado, no incurrir en las mismas crisis....

Excluida, así, la perspectiva de un simple retorno al mercado y de una renuncia del sistema económico a las prestaciones de regulación y asistencia estatales, la propuesta del neoliberalismo se reduce, en sustancia, al proyecto de una refundación sólo parcial del Estado Liberal de derecho, como cobertura y sostén, simplemente, de la reducción de las funciones públicas de naturaleza social. Este proyecto tiene un carácter inevitablemente antidemocrático... Para bien o para mal, como también ha recordado Norberto Bobbio, Estado social y democracia son en suma inescindibles no sólo histórica sino también estructuralmente....

El objetivo, en suma, en la fase de crisis del derecho que atravesamos, es el de un garantismo de los derechos sociales casi completamente por fundar, y el de un garantismo de las libertades individuales en gran medida por restaurar.

Es evidente que una perspectiva garantista como la aquí delineada es diametralmente opuesta a aquella perseguida por las estrategias neoliberales. Las dificultades que se oponen a la misma son, sobre todo políticas; legalidad, controles y garantías chocan de hecho con la resistencia de los aparatos políticos y burocráticos, de los grupos de presión y de los centros de interés consolidados, cuyo poder subjetivo es tanto mayor cuando más amplias son la discrecionalidad y la anomia. Es por esto su presupuesto esencial es hoy una refundación democrática de la representación política y un reforzamiento de los institutos de la democracia...; esto es la democratización de los partidos, la articulación de nuevas formas de participación política, el desarrollo de espacios de libertad, de autodeterminación y de poderes directamente sociales a los cuales quede vinculada la representación.”

La Globalización económica, caracterizada como un nuevo embate del neoliberalismo para la destrucción de los cimientos del Estado de bienestar, ha generado cambios subvertidores del orden jurídico y económico-social, propio de los Estados- Nación, tal como nacieron y se desarrollaron desde finales del siglo XIX y durante todo el siglo XX. Constriñendo en su andar los derechos humanos, esenciales, como criterios legitimadores de ejercicio del poder político del Estado, y en especial de la función punitiva, que cumple el sistema penal.

Su origen se debe al “derrumbe de los países del Este”, que con la caída de la URSS ha facilitado el crecimiento del poderío económico y bélico de EEUU; la necesidad del capital monopólico de aumentar sus tasas de

ganancias y la idea de un mercado capitalista a nivel mundial. Unido a la crisis de legitimación de los sistemas democráticos que se han asociado al modelo de economía liberal de mercado, productor de un estancamiento social.

En su esencia, la globalización es un modelo económico, que creemos, en concordancia con la postura VILLEGAS DÍAZ, es contraria a los Estados nacionales y sus economías, exceptuando a los países ricos. No se trata de un “proceso de internacionalización de la economía y la producción”, porque ha sido diseñado para responder a las necesidades del capital monopólico, negando la división entre países ricos y pobres, y permitiendo legalmente la intervención de los primeros sobre los últimos.

En rigor, alberga una contradicción, insalvable, en nuestra opinión⁶⁶. Por un lado, se amplían los espacios económicos y sociales, y por el otro, se restringen los espacios políticos⁶⁷. Particularmente notorio ha sido en Latinoamérica⁶⁸. Se trata de una alteración en la organización interna del Estado, que modifica las instancias de poder, y las dispersa, al constituirse en espacios de decisión específicos e independientes del sistema político democrático, para que puedan facilitar la rapidez y vertiginosidad del proceso de desarrollo para la integración supranacional. Estos procesos afectan directamente al Estado nacional que en teoría mantiene la soberanía, pero se trata de una soberanía compartida. La globalización pretende crear un nuevo orden mundial, pero en las actuales condiciones no existe posibilidad alguna de la creación de un Estado Mundial capaz de ser gobernado y que se

⁶⁶ Concordamos con la opinión de DE VEGA, PEDRO. 1998. Mundialización y Derecho Constitucional, para una palingenesis de la realidad constitucional. En: Memorias del VI Congreso Iberoamericano de Derecho Constitucional: 15 al 17 de abril de 1998. Santa Fe de Bogotá, Colombia, Universidad Externado de Colombia. pp. 1509- 1510, en cuanto la integración supranacional no puede imponerse a costa de violentar la voluntad general del pueblo, manifestada en la soberanía popular.

⁶⁷ Idem.

⁶⁸ VILLEGAS, M., Op. cit. Ejemplo extraído, “El Tratado de Libre Comercio del Atlántico Norte, el Mercosur, el Pacto Andino, son manifestaciones recientes.” 95p.

corresponda con la realidad totalizadora de la globalización. Así el Estado sigue siendo el marco de referencia del sistema social, pero ahora ve su capacidad política disminuida, precisamente por el principio de soberanía compartida. Los grandes capitales financieros son los que intervienen y manejan las decisiones de los Estados, como un verdadero poder invisible.

La tensión entre la lógica económica de un mercado globalizado y la lógica de las valoraciones políticas que legitima y justifica la intervención estatal, determinan que la razón económica es la que actualmente dirige la historia.

Y esa ideología desarrollista, pretender erigirse obviando deliberadamente los problemas que acarrea el “crecimiento”. Mientras los países crecen en su producción, paralelamente se globalizan también sus consecuencias sociales y políticas: la falta de trabajo, la pobreza, la marginalidad, la violencia. Visto de otro modo se trata de un crecimiento que favorece tan sólo a una parte de la población, los que detentan el capital y pueden invertir.

En este contexto de globalización, consecuencia del afán desarrollista, los principios de soberanía y democracia (entendidos como voluntad del pueblo) resultan ser perjudicados.

La soberanía, pues globalización significa integración, de todas las partes en un todo⁶⁹, lo que implica el socavar las soberanías nacionales, y más allá de

⁶⁹ PIZZOLO CALOGERO. 1998. La relación constitución-globalización. Una visión desde el derecho constitucional americano. En: Memorias del VI Congreso Iberoamericano de Derecho Constitucional, 15 al 17 de Abril de 1998. Santa Fe de Bogotá, Colombia, Universidad de Externado de Colombia, pp. 1689-1716.

eso, la propia soberanía que encuentra en el pueblo mismo su propia justificación.

Del mismo modo, de acuerdo con VILLEGAS DÍAZ, se afecta el derecho de la autodeterminación de los pueblos, por cuanto no es la voluntad popular quien decide los destinos del país, sino el capitalismo financiero. Que al mismo tiempo, determina el sistema político al cual obedece el ordenamiento jurídico en su conjunto.

Por otro lado, la legitimidad del constitucionalismo comienza a zozobrar, ya que como base fundamental del sistema político, social y económico que impera en un país, comienza ser cuestionada en la medida en que no se adapta a este nuevo fenómeno. En otra vertiente, la Constitución deja de ser entendida, en los hechos, como un sistema regulador de garantías fundamentales y prima su faceta en cuanto derecho de estructuras y de organización estatal. Estamos en presencia de una judicialización de la política en la que los órganos judiciales y de control proliferan para resguardar una legitimidad democrática que se ha venido autodestruyendo en la forma de ejercicio real del poder.

Se hace necesario entonces rescatar el principio democrático y el sistema encuentre las bases mínimas de una legitimación. Principio que en presencia del nuevo modelo socioeconómico de desarrollo capitalista, se reduce a defender la soberanía popular y tender hacia una apertura real de los canales de participación. La democracia no es una mera declaración, sino que ha de encontrar su concreción en la voluntad general y soberana del pueblo.

Ante la inminencia de la progresiva ausencia de realidad constitucional creemos, en comunión con VILLEGAS DÍAZ, el deber de retornar a la idea de

Pacto Social y soberanía democrática elaborada por Rousseau⁷⁰, primer paso, necesario en el momento actual, para avanzar hacia un estadio superior que permita definitivamente lograr una unidad real del poder del pueblo.

1.3.4. Legitimidad de la intervención del Estado en el ámbito de las telecomunicaciones personales vía Internet. Presupuestos fácticos, estabilidad política, los derechos humanos y la seguridad nacional

En el contexto de la “Guerra al terrorismo” liderada por EEUU⁷¹, a partir de los tristemente célebres atentados de Nueva York y Washington del año 2001, se han generado consecuencias políticas y jurídico-penales a escala mundial, de profundidades insospechadas.

Una de las medidas de mayor alcance para las personas del orbe, ha sido la enorme extensión que ha alcanzado la *U.S.A. Patriot Act*, específicamente la firmada por George W. Bush, con fecha veintiséis de Octubre del año 2004. Tal normativa, entre muchas otras atribuciones entregadas al Estado, permite la intervención de las comunicaciones privadas (obviamente incluyendo los correos electrónicos), que pasen por territorio norteamericano. Situación no menor, ya que casi la totalidad de los proveedores de este servicio de Internet, mantienen sus servidores en territorio de EEUU.

⁷⁰ Se debe especificar que nos referimos a la versión del Iluminismo y no la de Gunther JAKOBS y su Derecho Penal del Enemigo, que desvirtúa el carácter del Pacto Social de Jacques ROUSSEAU.

⁷¹ La guerra contra el terrorismo, según nuestra opinión, responde a una motivación ideológica de promoción expansionista de los intereses geopolíticos y económicos de los Estados Unidos, siendo así una justificación de su actual comportamiento intervencionista. Esto propicia el expansionismo penal, el secretismo estatal, y el estado policial que se ha consolidado lentamente en los Estados Unidos, vulnerando Derechos Humanos y Derechos Fundamentales. Un ejemplo de esa intervención es la misma U.S.A. Patriot Act. De hecho, en la misma información del gobierno estadounidense se puede apreciar lo difuso que resulta este enemigo terrorista, y como se permite en pro de su persecución las antedichas restricciones. Véase: UNITED STATES OF AMERICA. What is the War on Terrorism? S.a. [en línea] <<http://www.whitehouse.gov/infocus/nationalsecurity/faq-what.html>> [consulta: 19 enero 2007].

Consecuencialmente la gran mayoría de las comunicaciones privadas vía Internet de todos los ciudadanos del Mundo, pueden potencialmente ser intervenidas por agentes de Estado extranjeros; con las consecuencias amenazadoras del derecho al secreto de las comunicaciones y las ulteriores consecuencias políticas y penales de ser incorporado en una lista de sospechosos de terrorismo.

Es cierto que la *U.S.A. Patriot Act* (en adelante USAPA), establece nuevos poderes no sólo para los organismos americanos que operan dentro del territorio de éste país, sino también para las agencias internacionales de inteligencia americanas que ya venían interviniendo de manera secreta las comunicaciones que se producían por Internet por ciudadanos no americanos. La USAPA aumenta esta vigilancia con menoscabo de los “*Checks and Balances*”, entre los poderes de EEUU, que permite al poder judicial controlar al ejecutivo. De hecho expande el uso de los instrumentos preexistente de intervención, de entre los cuales se cuenta el uso de aparatos o programas que permitan la interceptación de comunicaciones, como el *Carnivore* y la Red ECHELON.

EEUU, ha hecho uso de las facultades que confiere la FISA (*Foreign Intelligence Surveillance Act*), a las agencias de inteligencia como la NSA (*National Security Agency*). La primera permitía hacer uso de los mecanismos de intervención de las comunicaciones, dictando órdenes judiciales un tribunal “secreto” a petición del Fiscal General. Este sólo debía de argumentar que la persona objeto de la intervención era un agente extranjero. En el caso de las intervenciones de comunicaciones electrónicas, FISA permite la intervención durante un año sin orden judicial. Tras la aprobación de la USAPA, la cuestión

ha empeorado al ampliarse el ámbito de la aplicación de FISA a los ciudadanos y residentes de EEUU y a los que se comuniquen con ellos, principalmente.⁷²

La pregunta atingente nace espontáneamente, ¿cuáles son los fundamentos subyacentes para legitimar dicha intervención arbitraria?. Ciñéndonos al análisis de VILLEGAS⁷³, se alude a la preservación de la estabilidad de la democracia. Pues no es nuevo el hecho de que todo régimen de gobierno intente legitimar las actuaciones represivas del Estado hacia las manifestaciones de violencia.

La misma autora profundiza sobre el concepto de estabilidad en un sistema democrático, en el que el poder de actuación por parte de los aparatos del Estado, está subordinado y tiene como límites los derechos humanos⁷⁴, las garantías constitucionales y la rotativa en el gobierno. Sin embargo la USAPA y las atribuciones que confiere, se fundan en las ideas de seguridad y orden público, propia de los regímenes autoritarios y en general todo tipo de Estados no exclusivamente democráticos.

Sus postulados rememoran la Doctrina de Seguridad Nacional en el ámbito interno (seguridad interior del Estado y orden público) y a la Geopolítica en el ámbito externo (Seguridad exterior de Estado), utilizadas por las dictaduras militares. En ambas el enemigo se identifica con todo aquél cuyo objetivo sea la destrucción del sistema (DSN) o la Nación (Geopolítica).

De este modo, todos somos potencialmente enemigos, aún más, con la doctrina del Derecho Penal del enemigo, emparentada a las anteriores de algún

⁷² ESTADOS UNIDOS DE AMÉRICA. 2001 Patriot Act. Senado de los Estados Unidos. 24 octubre 2001. [en línea] Ciber P@is. <www.palomallaneza.com/ciber/usapa.htm>, [consulta: 3 julio 2006].

⁷³ VILLEGAS. Terrorismo: Un problema de Estado..., Op. cit. pp. 99-104.

⁷⁴ En concordancia con lo ya expuesta en el punto 1.3.1.

modo; que en la USAPA y parte de la doctrina a nivel mundial, encuentra su sustento legal y teórico, con cada vez mayor solidez. Es decir, debido a las circunstancias ya señaladas de los principales proveedores de servicio de correo electrónico, cualquiera de nosotros si levantaremos sospecha de cualquier manera, acerca de estar involucrados en actividades terroristas, seríamos intervenidos en nuestras comunicaciones privadas vía Internet, sin ni siquiera enterarnos y podríamos sufrir ulteriores consecuencias por poder ser incorporados a una lista de sospechosos de terrorismo. No habría que ser muy osado para que se desencadene esto, los sistemas de interceptación de comunicaciones privadas, buscan palabras claves, tales como “bomba” u “Osama Bin Laden”, que descontextualizadas no significan ninguna amenaza, pero podrían significar paradójicamente una amenaza para los individuos, por parte del Estado y sus agentes.

Sabido todo esto, no queda más que cuestionarse acerca de los medios, a través de los cuales, individuos nos pueden proteger de tales atropellos. El Derecho no puede mantenerse indiferente en la materia, y sin duda no lo está. En el área penal material y formal urge analizar las posibles repuestas a tal pregunta.

CAPÍTULO II

DESCRIPCIÓN Y ANÁLISIS DE LAS INSTITUCIONES JURÍDICAS PROCESALES Y PENALES ASOCIADAS (PARTE GENERAL)

“Las enfermedades, la miseria y la criminalidad son flagelos que han conmovido y siguen conmoviendo a la vida humana; contra el tercer flagelo, no se ha verificado ningún sustancial progreso. En efecto, el delito en sus más variadas formas sacude a todos los Estados, incluso los de mayor civilización.

¿Qué manifestaciones de delincuencia han aumentado? Las que se engendran dentro de todas las modernas invenciones, las cuales, si han logrado progresos en las artes y en las industrias, no es menos cierto que han dado origen también a numerosas formas de delincuencia.”

GIORGIO DEL VECCHIO.

2.1. La sociedad informatizada: desafío y riesgo

La informática⁷⁵ ha reducido las dimensiones del mundo actual a una “aldea global”, interconectadas con las llamadas “autopistas de la información”. Esta se ha convertido en un valor de mercado y la frase, ya clásica, “la información es poder” ha dejado de ser un mero eslogan para pasar a ser una realidad incuestionable.

Toda reorganización tecnológica lleva consigo una reorganización económica, política y social. Las posibilidades de almacenamiento, tratamiento y control de la información que ofrece la Informática la convierten con frecuencia en un instrumento de presión y control social que amenaza la libertad y en último termino la dignidad del individuo. Este sector se hace más

⁷⁵ Tecnicismo que viene de la conjunción de las palabras “información” y “automática”. Por lo tanto no es más que información automatizada.

evidente en el sector público, donde se concentra gran cantidad de la información⁷⁶. Deviene imprescindible regular estrictamente el uso de la informática “para evitar el peligro de la contaminación de las libertades, que es el contrapunto negativo que amenaza con invalidar los logros del proceso tecnológico”⁷⁷.

Uno de los grandes artífices de la configuración de esta “aldea global”, es Internet, que entre sus variadas funciones sirve de medio de comunicación de masas, el más rápido y efectivo jamás creado. ¿Quién iría a imaginar siglos atrás que a través del e-mail los ciudadanos de todos los países del orbe fueran capaces de comunicarse con sus pares desde las latitudes más lejanas con una velocidad e interactividad sorprendente? Sin embargo, como ya decíamos, todo avance tecnológico encierra un peligro inmanente, basta con recordar que ALFRED NOBEL, reparó con tristeza en la doble potencialidad que encierra cualquier invención, y no se equivocó, la dinamita (TNT) ha servido para la actividad del hombre en tiempos de paz y para su destrucción en tiempos de guerra.

Internet no escapa a esta lógica, “como todos los grandes proyectos que benefician a la humanidad, no debemos analizar su fin en sí, sino la ética de aquellos que lo manejan. Es importante tener presente que este invento en particular encierra en si mismo la posibilidad del control global sobre la población⁷⁸”. Dicho desde otra perspectiva, no es correcto afirmar que Internet y el correo electrónico, como una de sus principales herramientas, son

⁷⁶ FERREYROS SOTO, C. 1996. Aspectos metodológicos del delito informático. Mérida, España, ID UNED, pp. 407-412.

⁷⁷ Véase DAVARA RODRÍGUEZ, M. A. 2002. Manual de Derecho Informático, Pamplona, España, Editorial Aranzadi.

⁷⁸ LAGO, MARÍA. SOLEDAD. 2001. Sistemas mundiales de interceptación de las comunicaciones. En: Programa de actualización de Derecho Informático, Curso de posgrado de Régimen jurídico de los bancos de datos, Buenos Aires, Argentina, Universidad de Buenos Aires, Facultad de Derecho. 33p.

invenciones malignas, las tecnologías son siempre éticamente neutras, lo relevante es emitir un juicio de valor acerca de los fines de aquellos que de una u otra forma lo manejan, para, de este modo, crear la conciencia en la ciudadanía, de la necesidad de un control social, político y jurídico de un medio de comunicación rico en capacidades, pero a la vez fácilmente subvertible, en cuanto a sus usos, por la autoridad.

Los poderes públicos realizan, en ocasiones, intromisiones en la esfera privada y la dignidad personal que afectan directamente a la participación democrática del ciudadano, ya que la concentración de la información y su tratamiento en centros de poder favorece el abuso, por parte de éstos y hacen indispensable la protección del derecho a la vida privada del individuo frente al celo del Estado por defender “intereses generales”.

Si las sociedades capitalistas han sido calificadas como “sociedades del riesgo”⁷⁹, a ello ha contribuido indudablemente la informática, en la medida en que puede ser utilizada para fines ilícitos. Tal como lo advertíamos en el capítulo anterior, el FBI y la NSA, emplean constantemente instrumentos informáticos despreciando los derechos fundamentales, principalmente respecto la vida privada e incluso los intereses comerciales de personas naturales y jurídicas, para sí controlar el “libre mercado”.⁸⁰ En Europa se han verificado también atentados a la vida privada perpetrados por compañías privadas y agencias internacionales de información⁸¹. En Alemania tuvo buena acogida la idea de proponer a quienes abrieran cuentas bancarias el otorgamiento de su consentimiento para procesar en los ordenadores de las agencias privadas

⁷⁹ Sobre la denominada “sociedad del riesgo” véase PEREZ DEL VALLE, C. 1996. Sociedad del Riesgo y reforma penal, en Poder Judicial, 2ª y 3ª Época, Consejo General del Poder Judicial (43-44) pp. 61-84..

⁸⁰ Así lo denuncia COSTA, SILVIO. 2003. El sistema ECHELON de espionaje global o la ley del todo vale. [en línea] Rebelión. <<http://www.rebellion.org/cibercensura/costa210103.htm>> [consulta: 17 enero 2007].

⁸¹ Ídem.

todos los movimientos bancarios. En Estados Unidos reciben el nombre de “Credit Report” y obtienen y manejan datos sobre la solvencia, hábitos y modos de vida de las personas, en definitiva, informaciones personalísimas de los ciudadanos, de forma incontrolada, con escasa fiabilidad y precisión. En Chile no somos ajenos a esto, nuestro DICOM, aunque en menor grado, encierra el mismo potencial peligro.

Como se viene observando los ejemplos abundan en el sector público y privado, de los más diversos países, e incluso la violación de dichos derechos fundamentales encuentra soporte tecnológico en los sistemas internacionales de interceptación de comunicaciones ECHELON, y en programas de espionaje como el CARNIVORE.

La tecnología informática facilita la acumulación de datos personales y posibilita su transmisión, interrelación y manipulación por parte de sujetos, que actúan individualmente u organizados en grupos y redes. En las sociedades informatizadas el poder no reside, en el ejercicio de la fuerza física, sino en el uso de las informaciones, que permite influir y controlar la conducta de los ciudadanos, sin necesidad de recurrir a medios coactivos.

Para ilustrar el peligro que encierra esta concentración de informaciones y en definitiva de poder, hay que reparar que producto de la interrelación de diversos datos obtenidos casualmente en la red, proveídos bajo la creencia de estar en absoluta confidencialidad, a través de medios como el correo electrónico o el simple acceso a páginas *web*, por ejemplo, para suscribirse a su revista favorita, se van creando perfiles de personalidad, que pueden determinarnos como individuos con gran detalle. Las reflexiones de LAGO son escalofriantes: “Imagínense un sistema que le permitiera a alguien tener acceso a todos los datos que existen sobre nosotros, que tenga la posibilidad de

escuchar y grabar todas las conversaciones por teléfono, fax, correo electrónico, que rastree lo que hacemos en Internet, que, en definitiva, sepa todo lo que hacemos. Es inimaginable el poder que tendría esa “persona”, sobre nosotros, ahora piensen que el dueño de este sistema es uno o varios gobiernos”⁸². Se nos vienen a la mente obras de ciencia ficción como la película “Enemigo Público” o la novela “1984” de George Orwell. Sin embargo la ficción se ha convertido en realidad con la existencia de ECHELON, y CARNIVORE.

Ahora bien, el hecho que la informática represente una amenaza para la vida privada de las personas no debe asumirse resignadamente, como si se tratara de una realidad inmutable, sino que, por lo contrario, debe conducir a incrementar la tutela de la misma.

Es indudable que Internet y el correo electrónico, constituyen en la sociedad actual un medio eficaz para una mejor atención de los ciudadanos. Habrá que ponderar las ventajas y los inconvenientes que éstos presentan para potenciar las primeras y mitigar, en lo posible, los segundos, intentando evitar que la presunta bondad de los fines perseguidos lleve a usos abusivos de los medios informáticos.

Desde nuestro punto de vista, es necesaria la tutela penal ante las vulneraciones de la vida privada que se realizan mediante la informática, aunque existan otros medios de protección menos severos en el ordenamiento jurídico nacional y en el derecho extranjero. Para la situación fáctica que es de nuestro interés queda descartado de plano una tutela desde el Derecho Administrativo o Privado. Primero, se trata de dar un tratamiento jurídico a la intervención de las comunicaciones personales electrónicas ilícitas, cometidas por agentes de Estado extranjeros, no se puede esperar como una solución

⁸² LAGO, M. S. Op. cit., pp. 2-3.

viable y sostenida en el tiempo, desde una perspectiva política y jurídica, que el Estado extranjero aplique condenatoriamente su derecho administrativo a agentes que pertenecen a sus propio aparato, más aún, en el marco jurídico internacional imperante por la fuerza de las potencias mundiales, exacerbado por los hechos del once de Septiembre del 2001, que considera justificadas aquellas intervenciones ilegítimas. Segundo, tales intereses sociales de protección de la vida privada, son jurídicamente de tal entidad que se encuentran consagrados a nivel constitucional como derecho fundamental, en el artículo 19 nº 4 y 5 de nuestra Carta Fundamental, están directamente vinculados a la dignidad del individuo y son por ende merecedores de tutela penal. Además, como ha declarado HASSEMER, uno de los sectores que definen el nuevo Derecho Penal es el tratamiento informático de datos⁸³. Por último y por razones de estricta justicia el Derecho no se puede mantener indiferente a tales realidades, como mecanismo de control social que es, especialmente por tener el monopolio del *ius puniendi*, a través del Derecho Penal. Debe tutelar los intereses sociales más relevantes, eficazmente, adaptándose a esta nueva realidad y así proteger a los individuos frente a este acopio de información e intromisión en las comunicaciones electrónicas personales vía Internet, ilícitas, provenga de quien provenga.

Así pues, deviene necesaria la protección penal de los datos personales como límite a una utilización de la informática que pueda vulnerar la vida privada de los ciudadanos y coartar el ejercicio de sus derechos. Sin embargo, los avances de la sociedad tecnológica, específicamente, en cuanto de las telecomunicaciones han supuesto un nuevo reto para los juristas, que le han debido hacer frente ante la insuficiencia del Derecho Penal tradicional en éste ámbito.

⁸³ HASSEMER, W.1999. Perspectivas del derecho penal futuro: pp. 37-41; igualmente en Oportunidades para la privacidad frente a las nuevas necesidades de control y las tecnologías de la información En: Nueva Doctrina Penal. pp. 97-120.

Se evidencia la necesidad de elaboración de un Derecho Penal internacional, que partiendo de la armonización entre las diversas legislaciones, castigue la comisión de delitos burlando la legislación nacional, como sucede cuando se utilizan para cometer conductas delictivas servidores de Internet, radicados en un país donde la delincuencia informática deviene impune⁸⁴ o está de manera cuestionable jurídicamente justificada⁸⁵. Dado que uno de los rasgos característicos de Internet es el que para la ley penal de cualquier país es extraterritorial, una protección de datos eficaz no puede conseguirse únicamente a través de normas jurídicas estatales. En consecuencia a futuro, es necesaria la coordinación de los distintos ordenamientos jurídicos para la prevención y no tan solo la represión de tales conductas delictivas.

Para la obtención de dichos fines y como lo prometimos al concluir el capítulo anterior es necesario realizar un análisis acerca del tratamiento penal que dichas conductas ilícitas deben recibir, tanto desde una perspectiva sustantiva y adjetiva.

2.2. Configuración de las conductas punibles (penalmente relevantes), como delitos informáticos

Para el tratamiento penal de cualquier conducta humana, positiva o negativa, se debe partir del presupuesto esencial, de que en el ámbito penal del ordenamiento jurídico en un Estado de Derecho se deben respetar una serie de principios fundamentales. De entre los cuales se quieren destacar dos, el

⁸⁴ Tal fue el caso del famoso virus "Da Vinci", luego de investigar se determinó que tuvo como creador a un nacional de Filipinas y su lugar de acceso a Internet allí mismo, sin embargo dicho país no tiene legislación acerca de delitos informáticos, por lo cual la consecuencia ha sido la absoluta impunidad.

⁸⁵ Por ejemplo para EEUU como resultado de las polémicas USA PATRIOT ACT o para España, la Ley de Servicios de la Sociedad de la Información y Comercio electrónico (LSSICE).

principio de legalidad y la responsabilidad penal del individuo, por suscitar especial interés para las conductas en comento.

2.2.1. Principio de legalidad o reserva.⁸⁶

Resulta la razón más importante para tipificar, el principio angular de todo sistema jurídico-legal, de que no hay delito ni pena sin que la ley lo establezca previamente. *Nullum crimen, nulla poena sine lege*, señala el conocido aforismo latino.

Esta idea esencial es la que se conoce como el principio de legalidad o reserva y que la doctrina nacional concibe ampliamente, al vislumbrarlo como una garantía constitucional⁸⁷. Que la ley sea la única fuente del Derecho Penal se fundamenta en la necesidad de asegurar el respeto de la libertad y de la dignidad de los ciudadanos y de protegerlos frente a las posibles arbitrariedades, tanto de los legisladores, la judicatura y el ejecutivo.

A juicio del mismo penalista tendría un triple alcance:

- a) Sólo la ley penal puede crear delitos y establecer penas;
- b) La ley penal no puede operar retroactivamente, y
- c) La ley penal, al crear delitos y penas, debe referirse directamente a los hechos que constituyen aquéllos y a la naturaleza y límites de éstas”, es decir el principio de tipicidad.

Debe tenerse presente el hecho de que la inexistencia de normativa penal, no debe conducir a admitir la aplicación de la analogía como fuente del

⁸⁶ Se sigue el razonamiento de JIJENA, LEIVA, R. 1992. Chile la protección penal de la intimidad y el delito informático. Santiago, Chile, Editorial Jurídica de Chile. pp. 72-74.

⁸⁷ ETCHEBERRY, A. 1976. Curso de Derecho Penal. Santiago, Chile, Editorial Gabriela Mistral. 47p y siguientes.

Derecho Penal, método con el cual sencillamente se niega el principio de legalidad.

Nuestra Carta Fundamental vigente, en materia penal, consagra la igualdad y el principio de legalidad en los incisos 7º y 8º del artículo 19, en los siguientes términos:

“Ningún delito se castigará con otra pena que la que señale una ley promulgada con anterioridad a su perpetración, a menos que una nueva ley favorezca al afectado.

Ninguna ley podrá establecer penas sin que la conducta que se sanciona esté expresamente descrita en ella;”

Al tener rango constitucional, ninguna norma legal puede vulnerarlo, ya que ella sería impugnable por su inaplicabilidad.

Interesa retomar el elemento tipicidad, por el hecho de que es uno de los requisitos esenciales para sancionar una figura criminal su tipificación o consagración dentro del catálogo de tipos penales. Una condena penal no puede recaer legítimamente sobre una persona, a no ser que haya existido, con anterioridad al hecho una ley que autorizara la imposición de la pena por el mismo⁸⁸.

La tipicidad cumple una función reductora al seleccionar las conductas constitutivas de delito; además es la expresión técnico-penal del principio de legalidad; a su vez, garantiza un trato igualitario a los que estén en una misma

⁸⁸ NOVOA MONREAL, E. 1985. Curso de Derecho Penal, tomo 1, 2º edición. Santiago, Chile, Editorial Jurídica Cono Sur. pp. 308 y siguientes.

situación; y por último es “indiciaria de antijuricidad” porque los tipos describen conductas contrarias a derecho, que lesionan determinados bienes jurídicos, aunque eventualmente algunos actos típicos no sean antijurídicos en cuanto se compruebe la existencia de alguna causal de justificación.

Las conductas ilegítimas que buscamos darles un tratamiento penal, no pueden omitir el respeto a éste principio fundamental, en ninguno de sus alcances. Por lo tanto deben ceñirse al principio de legalidad, especialmente, en su manifestación de tipicidad, para poder ser perseguidas penalmente por la jurisdicción nacional, sin importar el lugar en que se hubieren cometido.

2.2.2. La responsabilidad penal individual y algunas observaciones acerca de la participación.

Es relevante reparar en estos puntos debido a que las conductas de intervención ilegítima de las comunicaciones electrónicas son cometidas, en nuestra hipótesis, por agentes de Estado extranjeros.

Atendidas las circunstancias, se podría abordar la discusión doctrinaria acerca de la posibilidad de responsabilidad penal de las personas jurídicas, sin embargo nosotros sostenemos la impropiedad de dichos postulados y a contrapunto, creemos que la responsabilidad penal es individual, pues ella es de hechos y las conductas ilícitas son cometidas por individuos, sin importar para los efectos de la conducta humana física punible si se han realizado bajo el alero de una organización. Desde otro punto de vista las personas jurídicas no tienen la materialidad para actuar por si mismas en el mundo físico y por lo tanto no pueden ser penalmente responsables.

No obstante no nos cerramos a la posibilidad de la procedencia de hipótesis de autoría mediata y participación, de los superiores jerárquicos de los agentes de las agencias internacionales de inteligencia y de terceros burócratas⁸⁹, o de la posibilidad de evaluar la procedencia de responsabilidad civil del Estado, frente a esas conductas ilegítimas cometidas por sus agentes.

2.2.3. La criminalidad informática.

Luego de presuponer el respeto a los principios destacados y los demás del ordenamiento jurídico-penal nacional e internacional, se procede a un intento de enmarcar las conductas ilegítimas apuntadas dentro de alguna variedad de conductas típicas acogidas por nuestra legislación interna⁹⁰, para así determinar la viabilidad de persecución penal de ellas por nuestros tribunales de justicia.

Dicha gama de tipos debe ser, sin duda, los que atienden la criminalidad informática. Para justificar esta elección se debe realizar un análisis doctrinario acerca de dichas figuras delictivas.

2.2.3.1. Delitos informáticos⁹¹

2.2.3.1.1. Concepto.

En cuanto al concepto de delitos informáticos cabe destacar que en la doctrina se presentan opiniones dispares. Mientras para algunos puede

⁸⁹ VILLEGAS DÍAZ y LAVÍN ESPINOZA. Op. cit. pp. 300-305.

⁹⁰ Así lo intenta la criticada, y en proceso de reforma, CHILE. Ministerio de Justicia. 1993. Ley 19.223: Tipifica figuras penales relativas a la informática. 7 de junio del 1993. [en línea] <www.bcn.cl> [consulta: 22 enero 2007].

⁹¹ VILLEGAS DÍAZ, M. y LAVÍN ESPINOZA, M.; op. cit., "Terrorismo e intervención penal en la red Internet...", se sigue generalmente el tratamiento de estos autores acerca del tema, pp. 214-229.

hablarse de “delito informático”, para otros, debe hablarse, en puridad técnica, de “delitos informáticos”.

2.2.3.1.1.1. “Delito Informático”.

2.2.3.1.1.1.1. Definiciones doctrinales.

En la primera postura encontramos a JIJENA LEIVA para quien “delito informático” es la “acción delictiva en la cual el computador es instrumento u objeto del hecho”⁹². La definición anotada coincide con precisión a la proporcionada por MORALES RÍOS⁹³.

Esta definición, al pretender englobar todas las conductas que cabrían dentro de la delincuencia informática, no permite delimitar el campo de ésta, ampliándose en demasía. Por lo demás, hacen alusión al objeto material de la conducta, elemento que no necesariamente ha de estar presente en una definición de carácter general.

Luego, TINAJEROS⁹⁴ lo define, de manera bien difusa, como” un acto ilegal, no ético o no autorizado que involucra el procesamiento de datos y la transmisión de los mismos”.

Delimitando aún más el concepto, DAVARA estima que se trata de “una acción que, reuniendo las características que delimitan el concepto de delito,

⁹² JIJENA LEIVA, R. Op. cit. 81p.

⁹³ Para este autor, el delito informático es “...toda acción delictiva en la cual el computador es el instrumento u objeto del hecho...”. Es idéntica a la proporcionada por JIJENA LEIVA, R. MORALES RÍOS, H. 1989. , ponencia en Congreso para la enseñanza del derecho, Madrid, 1989. Cit. por ABEDRAPO BUSTOS, E. 1996. Ley 19.223 sobre Delitos Informáticos. Memoria de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Chile, Facultad de Derecho, Universidad de Chile. 34p.

⁹⁴ TINAJEROS ARCE, E. 2006. Nuevas formas de delinquir en la Era Tecnológica: Primeras observaciones sobre Espionaje, Fraude y Sabotaje Informático. [en línea] Revista Electrónica Alfa-redi (98) <www.alfa-redi.com> [consulta: 16 de enero 2007]

sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software”⁹⁵.

También en esta postura se encuentran CASTILLO y RAMALLO, para quienes “delito informático” es toda acción dolosa que provoca un perjuicio a personas o entidades, y en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas⁹⁶. Similar es la definición de CAMACHO LOSA para quien delito informático es “toda acción dolosa que provoca un perjuicio a personas o entidades, sin que, necesariamente conlleve un beneficio material para su autor, o que, por el contrario, produce un beneficio ilícito a su autor aún cuando no perjudique de forma directa o inmediata a la víctima, y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas”⁹⁷.

Ambas definiciones, especialmente la última, parecen menos amplias que las anteriores, y por ende, mejores, no obstante la alusión al dolo directo puede ocasionar no pocos problemas dogmáticos, en relación a la eventualidad de producirse una conducta imprudente que pudiere merecer reproche penal. La adecuada restricción de las conductas queda de manifiesto cuando CAMACHO LOSA estima que no deben incluirse dentro del concepto de delito informático, aquellos hechos en los cuales los dispositivos informáticos son objeto de un delito de los tipificados en el Código Penal, como por ejemplo, la sustracción del hardware (soporte físico).

⁹⁵ Concepto extraído de: SEMINARIO de Delitos Informáticos en el marco del Diplomado en Derecho Informático de la Escuela de Graduados, Facultad de Derecho, Universidad de Chile, 2004.

⁹⁶ CASTILLO y RAMALLO. 1989. El delito informático. En: Congreso de Derecho Informático de la Universidad de Zaragoza. Cit. por JIJENA, L. Op. cit. pp. .81-82.

⁹⁷ CAMACHO LOSA, L. 1987. El Delito Informático. Madrid, España, Gráficas Cóndor. 25p.

Por otro lado, TÉLLEZ⁹⁸ conceptualiza al delito informático, de manera típica y atípica, entendiendo por la primera a “las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin” y por las segundas “actitudes ilícitas en que se tienen a las computadoras como instrumentos o fin”.

Por otro lado CALLEGARI⁹⁹ lo define como: “aquél que se da con la ayuda de la informática o de técnicas anexas”. Este concepto tiene la desventaja de solamente considerar como medio de comisión de esta clase de delitos a la informática, olvidándose la autora que también lo informático puede ser objeto de la infracción.

En nuestro país MUÑOZ NAVARRO, hace alusión al delito informático, al hablar de “fraude informático”, entendiendo por tal a todo acceso indebido a la información cometido con la intención de apoderarse o de modificar datos¹⁰⁰. Sin duda la definición de este autor es restrictiva, abarcando tan solo una de las diversas conductas delictivas que pueden caer en el campo de la delincuencia informática.

2.2.3.1.1.1.2. Definiciones institucionales.

La Organización para la Cooperación Económica y el Desarrollo estima que el delito informático o “*computer crime*” es “cualquier conducta ilegal, no ética o no autorizada, que involucra el procesamiento automático de datos, y/o

⁹⁸ TÉLLEZ VALDÉS, J. 1996. Los Delitos informáticos. Situación en México. En: Informática y Derecho (9) (10) y (11). Mérida, España, UNED, Centro Regional de Extremadura.

⁹⁹ CALLEGARI, N. Cit. por TÉLLEZ VALDÉS. Op. cit.

¹⁰⁰ MUÑOZ NAVARRO. Cit. por JIJENA LEIVA. Op. cit. 82p.

la transmisión de los mismos”¹⁰¹. Para el Departamento de Justicia norteamericano el delito informático es “cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática sea esencial para su comisión, investigación o persecución”¹⁰².

Dos cuestiones cabe resaltar respecto de estas definiciones.

En primer lugar, al señalar “cualquier acto ilegal” parece ser que se están refiriendo a una diversidad de conductas delictivas, lo que puede conducir a dos posibilidades: o bien concebir el delito informático como un solo delito con pluralidad de hipótesis, o bien una diversidad de delitos informáticos. Ninguna de las dos definiciones deja en claro este punto.

En segundo lugar, la definición de la Organización para la Cooperación Económica y el Desarrollo, si bien, a primera vista parece ser omnicompreensiva de las diversas conductas que podrían constituir la delincuencia informática, es demasiado vaga, impidiendo delimitar el campo de este tipo de delincuencia. Por su parte, la definición aportada por el Departamento de Justicia Norteamericano, en el fondo es restrictiva, ya que se excluyen una serie de comportamientos, en los cuales los agentes no poseen conocimientos informáticos.

2.2.3.1.1.1.3. Definiciones legales.

El Anteproyecto de la ley N° 19.223 sobre delitos informáticos, señaló que “delito informático” es “toda acción típica, antijurídica y culpable, para cuya consumación se utiliza o afecta una computadora o sus accesorios”. Al igual

¹⁰¹ Citada por JIJENA, L. Op. cit. 81p, MAGLIONA, C.-LÓPEZ, M. 1999. Delincuencia y Fraude Informático. Derecho Comparado y ley 19.223. Santiago, Chile, Editorial Jurídica de Chile. 37p.

¹⁰² Idem.

que la Organización para la Cooperación Económica y el Desarrollo, hace equiparable el delito informático al “*computer crime*”.

Esta definición es restrictiva, ya que reduce el ilícito informático únicamente a aquellas conductas vinculadas a los ordenadores que se encuentren tipificadas en la ley, excluyendo, por ende, todas aquellas que no se encuentren tipificadas, pero que por razones de lege ferenda deberían ser incluidas¹⁰³.

Finalmente, y según la historia fidedigna del establecimiento de la ley 19.223, el legislador habría señalado que el delito informático es, en sí mismo, una acción ilícita reprochable, y no un mero instrumento para cometer otros delitos. Una definición bastante vaga y que poco o nada puede acercarnos al concepto de los ilícitos que se cometen en el campo de la delincuencia informática.

2.2.3.1.1.2. “Delitos Informáticos”.

En la segunda postura, esto es, concebir la existencia no de un delito informático, sino de “delitos informáticos”, encontramos definiciones propuestas por la doctrina.

De este modo GONZÁLEZ¹⁰⁴ indica: “En términos generales, creo que... se diferencia entre los hechos en los que el sistema informático o sus elementos son el objeto material del delito y aquéllos otros en los que son el instrumento del mismo. En el primer caso, delitos contra el sistema informático

¹⁰³ En opinión similar: MAGLIONA, C.-LÓPEZ, M. Op. cit. 42p.

¹⁰⁴ GONZÁLEZ RUS, J. J. 1999. Protección penal de sistemas, elementos, datos, documentos y programas informáticos. [en línea]. Revista Electrónica de Ciencia penal y criminológica, (01-14). <<http://criminet.ugr.es/recpc/>> [consulta: 16 enero 2007].

o contra elementos de naturaleza informática se incluyen los comportamientos en los que cualquiera de estos componentes (tanto físicos -hardware- como lógicos -software y ficheros y archivos) resulta el objeto material de ilícitos patrimoniales, bien porque son en sí objeto específico de protección (terminales de comunicación, programas de ordenador, datos, informaciones, documentos electrónicos) bien porque pueden servir de soporte a elementos protegidos de manera general, pero en los que la aparición de implicaciones informáticas puede plantear peculiaridades dignas de atención específica (secretos de empresa, obras literarias o artísticas, datos con eventual valor probatorio recogidos en ficheros informáticos, etc.). En todo caso, diferenciando entre los delitos contra elementos físicos, que no plantean realmente problemas significativos, y los que afectan a elementos lógicos, cuya naturaleza suscita concretas y muy interesantes cuestiones.

En el segundo grupo se incluyen, en cambio, los delitos que se realizan por medio del sistema informático o utilizando elementos de naturaleza informática, que aparecen como el instrumento utilizado para la realización del ilícito, patrimonial o socioeconómico. Ello, tanto si el objeto de ataque es un elemento patrimonial cualquiera (dinero, en caso de las transferencias electrónicas de fondos o en la utilización de tarjetas de cajeros automáticos, por ejemplo) como cuando es también un sistema informático (introducción de virus, acceso ilícito a ordenadores y redes, etc.). En muchos supuestos concurrirán ambas perspectivas (daños a un sistema informático accediendo ilícitamente al mismo), lo que, en su caso, podrá dar lugar a eventuales concursos de delitos y hará preferente la contemplación desde la óptica de los delitos contra el sistema informático. Salvo que presenten problemas específicos, ningún comentario se hará cuando los medios informáticos sean simplemente una forma más de cometer delitos, sin que ello añada particularidad alguna al hecho (daños en una cadena de montaje, alterando el programa del ordenador que la controla, por ejemplo).”

Por otro lado, para VERA QUILODRÁN, los delitos informáticos son “conductas que atentan en forma grave a determinados bienes y derechos del individuo, que presentan una configuración específica y exclusiva de la actividad informática, y que han sido sometidos a una “tipología” técnica”¹⁰⁵.

La definición propuesta es lo suficientemente amplia como para englobar cualquier tipo de conducta vinculada a la informática, pero al no especificar cuáles son los bienes o derechos que resultan afectados, es casi imposible delimitar su ámbito de protección.

PARKER¹⁰⁶ también aporta definiéndolos como: “todo acto intencional asociado de una manera u otra a los computadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio”.

MAGLIONA y LÓPEZ estiman que “en puridad no puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común, su vinculación de alguna manera a ordenadores”¹⁰⁷. Y haciendo suyas las apreciaciones de ROMEO CASABONA¹⁰⁸ y GUTIÉRREZ FRANCÉS¹⁰⁹ estiman que los delitos relacionados con la delincuencia informática se caracterizan por su “especificidad”, carácter que viene dado por el “ordenador junto con sus funciones propias más importantes: el procesamiento y transmisión automatizados de datos y la confección y/o utilización de programas para tales fines. Cualquier conducta que no opere

¹⁰⁵ VERA QUILODRÁN, A. 1996. Delito e Informática (La informática como fuente de delito), Santiago, Chile, Ediciones Jurídicas La ley, 95p.

¹⁰⁶ PARKER D.B. 1987. *Computer crimes*. 1974. Cit. por ROMEO CASABONA, Carlos.; “Poder Informático y Seguridad Jurídica”, Fundesco, Madrid, España, 1987.

¹⁰⁷ MAGLIONA, C.-LÓPEZ, M. Op. cit. pp. 34-35.

¹⁰⁸ ROMEO CASABONA. Op. cit. pp.42-43

¹⁰⁹ GUTIÉRREZ FRANCÉS, M. L. 1991. Fraude Informático y Estafa. Madrid, España, Ministerio de Justicia, Secretaría General Técnica, Centro de Publicaciones. 63p.

sobre la base de estas funciones, aunque pueda resultar delictiva.... No poseerá ya esa especificidad...y deberá ser, por tanto, apartada del estudio de la delincuencia vinculada a la informática o tecnologías de la información. En este sentido es irrelevante que el ordenador sea instrumento u objetivo de la conducta, y que ésta esté criminalizada o merezca serlo por consideraciones político criminales”¹¹⁰.

Este concepto parece mas preciso que el primero anotado, ya que se encarga de señalar la “especificidad” en los delitos informáticos. No obstante, para arribar a una conclusión, es preciso revisar otras definiciones.

SIEBER estima que los delitos informáticos son todas las “lesiones dolosas e ilícitas del patrimonio relacionadas con datos procesados automáticamente”¹¹¹. Ya hemos señalado anteriormente que la alusión al dolo en lugar de aclarar un concepto, lo confunde y puede dar lugar a problemas dogmáticos, en relación a las conductas imprudentes que pudieran ser objeto de reproche penal.

TIEDEMANN estima que los delitos informáticos son “todos los actos antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático o de procesamiento de datos”¹¹².

La definición es amplia, y abarca cualquier clase de conducta relacionada con el campo de la delincuencia informática. Además deja abierta la posibilidad de que los delitos informáticos tipificados por la ley penal vigente no son todos ni los únicos posibles. Además, al señalar “socialmente perjudiciales”,

¹¹⁰ ROMEO CASABONA. Op. cit. pp.42-43.

¹¹¹ SIEBER, U. Cit. por GUTIÉRREZ FRANCÉS. Op. cit. 56p.

¹¹² TIEDEMANN, K. 1985. Poder económico y delito. Barcelona, España, Editorial Ariel. 122p.

parece acercarse a un enfoque material del bien jurídico afectado, concebido éste en términos generales como una “síntesis normativa determinada de una relación social concreta y dialéctica”¹¹³, esto es, un bien jurídico que nace de la confrontación de intereses sociales en conflicto.

Por otra parte, el concepto abarca el problema de la amenaza a la esfera privada del ciudadano, y a los daños patrimoniales producidos por el abuso de datos procesados automáticamente¹¹⁴.

En nuestro país, HUERTA y LÍBANO estiman que delitos informáticos son: “todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, tratándose de hechos aislados o una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente producirá de manera colateral, lesiones a distintos valores jurídicos, reportándose muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro”¹¹⁵.

Si bien esta definición tiene la ventaja de ser omnicomprendensiva de distintas modalidades delictivas, tiene la desventaja de aludir expresamente al dolo, por las razones ya anotadas, esto es, la posibilidad de la existencia de una conducta imprudente merecedora de sanción penal. Así por ejemplo, la intromisión no intencionada en sistemas de información de seguridad de un país, que produzca un perjuicio a dicho sistema.

¹¹³ Este concepto pertenece a BUSTOS, J. y HORMAZÁBAL, H. 1997. Lecciones de Derecho Penal, volumen I. Madrid, España, Editorial Trotta, 59p.

¹¹⁴ En esta opinión MAGLIONA, C. y LÓPEZ, M. Op. cit. 39p.

¹¹⁵ HUERTA, M. y LÍBANO, C. 1996. Delitos Informáticos. Chile. Editorial Jurídica Conosur Ltda. 116p.

2.2.3.1.1.3. Nuestra postura.

En primer lugar concordamos con VILLEGAS DÍAZ y LAVÍN ESPINOZA¹¹⁶, en que es correcto adoptar la postura de existencia de “delitos informáticos”. Pues no es una sola la modalidad de conducta delictiva la que engloban esta variedad de conductas delictivas. La interceptación de las comunicaciones electrónicas con fines ilegítimos es solo una variante de las conductas que constituyen estos tipos de delitos, como por otro lado, por nombrar un ejemplo, podría estar la conducta de destrucción de un sistema electrónico a través del “hacking”.

Una acepción que supera en gran parte las limitaciones de las anteriormente anotadas es la proporcionada por RODRÍGUEZ MERINO, para quien son delitos informáticos las “acciones típicas, antijurídicas y culpables, que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, como bien jurídico de naturaleza colectiva o macrosocial (abarcando otros intereses: propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos, etc.) en cualquiera de las fases que tienen vinculación con su flujo o intercambio (ingreso, almacenamiento, proceso, transmisión y/o regreso), contenida en sistemas informáticos de cualquier índole, sobre los que operan las maniobras dolosas”¹¹⁷.

Sin embargo la alusión al dolo, dificulta dogmáticamente la definición, pues no incluye las hipótesis de intervención negligente, que aunque con un menor disvalor no pueden abandonarse.

¹¹⁶ VILLEGAS DÍAZ Y LAVÍN ESPINOZA. Op. cit. pp. 220-221.

¹¹⁷ RODRÍGUEZ MERINO, D. 2003-2004. Criminalidad e Internet. En: MIGUEL ÁNGEL DAVARA RODRÍGUEZ (coordinador). XVIII Encuentros sobre Informática y Derecho. 2003-2004. Madrid, España, Universidad Pontificia Comillas. 370p. Cit. por VILLEGAS DÍAZ Y LAVÍN ESPINOZA. 220p.

Continuando con el análisis, la pregunta que luego hay que responder es acerca de la necesidad o innecesidad de tipificar figuras especiales de delitos informáticos o desde otro punto de vista si los ya existentes se justifican, o estos tipos son subsumibles en otros tradicionales ya vigentes.

De particular interés se presentan las reflexiones de VERA QUILODRÁN, que a pesar de que en su obra define los delitos informáticos de la manera que hemos anotado, realiza una detallada descripción de tipos legales vigentes en nuestro país dentro de los cuales podrían caber los delitos informáticos. Esto ocurre por ejemplo con el espionaje informático, figura que puede perfectamente ser incluida dentro de los arts. 109 inc 1, 246, 156, 242, 337, 284 del Código Penal.

Conclusiones que son de gran valor ya que eliminan el problema de la tipicidad de las conductas ilegítimas de intervención de las comunicaciones electrónicas por parte de agentes de Estado extranjeros, sin la necesidad de reforma de la ley 19223 y eliminan el problema de alcance interpretativo que pueda dar la judicatura de esta normativa a las conductas delictivas tratadas. Bastaría entonces, en nuestra opinión, recurrir a los tipos tradicionales simplemente. Y lo que es mas esperanzador VERA QUILODRÁN, no aborda el tipo del artículo 161 A vigente en el Código Penal, figura que en nuestra opinión perfectamente aborda las conductas delictivas de intervención ilícita y las hace penalizables en el ordenamiento penal chileno, sin necesidad de un gran esfuerzo interpretativo.

Lo importante es reconocer que “el avance tecnológico trae consigo también nuevos peligros, nuevas formas de ataque contra bienes jurídicos relevantes, con lo cual surge especialmente la pregunta por la capacidad de

reacción de los tipos penales tradicionales frente a formas de criminalidad desarrolladas al alero del desarrollo informático”¹¹⁸. Por eso, nos parece correcta la postura de CORCOY BIDASOLO¹¹⁹, en cuanto advierte como una de las posibilidades de reacción penal frente a las conductas de criminalidad informática, la necesidad de reinterpretar teleológicamente los tipos penales existentes.

Adoptada una postura ahora es necesario abordar las distintas modalidades que adoptan los delitos informáticos, desde la doctrina. De esta forma queremos determinar si la conducta de intervención de las comunicaciones electrónicas personales se comprende en alguna de ellas y así determinar su ilicitud o al menos ilegitimidad, paso previo desde una perspectiva penal material a convertirse en una conducta susceptible de someterse al imperio del Derecho Penal.

2.2.3.1.2. Clasificación de las conductas que componen los delitos informáticos.

Ya hemos dicho que los delitos informáticos contienen una serie de conductas punibles. Para objetos de nuestro estudio adoptaremos la clasificación doctrinaria de PARKER¹²⁰, pues a nuestro parecer es la que aborda de mejor manera un área altamente compleja y tecnologizada. Este autor distingue:

¹¹⁸ HERNÁNDEZ BASUALTO, H. 2001. Tratamiento de la criminalidad informática en el Derecho Penal chileno. Diagnóstico y Propuestas. Chile, Universidad Andrés Bello, 2001.

¹¹⁹ CORCOY BIDASOLO, M. 1989. El sabotaje informático. En: Congreso de Derecho Informático, junio de 1989, España, Zaragoza, Universidad de Zaragoza. Cit. por JIJENA, R. Op. cit., 78p.

¹²⁰ PARKER, D. B. 1974. Computer crime. Cit. por JIJENA LEIVA, R. 95p.

1- Modificación de documentos fuente (introducción de datos falsos o *data diddling*): consiste en manipular las transacciones de entrada al ordenador con el objeto de introducir movimientos falsos en todo o parte, o en eliminar transacciones verdaderas que deberían hacerse introducido¹²¹. Son particularmente difíciles de detectar y puede revestir las siguientes modalidades¹²²:

- Omisión del ingreso de ciertas informaciones
- Alteración de su contenido
- Inclusión de datos no autorizados
- Procesamiento duplicado

2- Cambios clandestinos en programas: Consiste en introducir modificaciones no autorizadas en ellos, alterando sus procesos¹²³.

3- Caballo de Troya: Consiste en introducir rutinas, conjuntos de instrucciones o sentencias en la codificación de un programa, no autorizadas, y que son activadas con una señal al cumplirse una condición predeterminada. Con ello se logra que el programa actúe en forma distinta a la que estaba prevista¹²⁴. Para utilizar este método se requiere de una cierta capacitación técnica, al menos, saber programar.

3- *Salami techniques (rounding down)*: Este método se utiliza en instituciones en las cuales hay movimientos de dinero, y consiste en la sustracción de

¹²¹ CAMACHO LOSA, L., Op. cit. 36p. MAGLIONA, C. y LÓPEZ, M. Op. cit. 46p.

¹²² JIJENA LEIVA, R. Op. cit. 96p.

¹²³ Ibid. 95p.

¹²⁴ Idem. Un ejemplo sería que en una entidad bancaria se introduce una modificación en el programa de cuentas corrientes, para que siempre que sea consultado el saldo de alguna cuenta determinada, aquel sea multiplicado por mil, diez, cien, etc.

pequeñas cantidades de activos de distintas procedencias haciendo un redondeo de las respectivas cuentas, depositándolas en otra u otras cuentas¹²⁵.

4- *Superzapping*: Se trata del uso no autorizado de un programa de utilidad para alterar, borrar, copiar, insertar, o utilizar en cualquier forma no permitida los datos almacenados en el ordenador o en los soportes magnéticos¹²⁶. A través de esta modalidad es posible alterar los registros de un fichero sin que quede constancia de esta modificación.

5- Puertas con trampas (*trap doors*): Los puntos débiles de que puedan adolecer los sistemas informáticos permiten su acceso eludiendo los controles normales. Este punto débil se denomina “puerta falsa” o “*trap door*”. Para introducirse al sistema se utilizan las interrupciones en la lógica de un programa (que los programadores elaboran para el chequeo del mismo en la fase del desarrollo para su depuración), las que pueden no haber desaparecido cuando los programas entren al proceso de producción normal y que debilitan su seguridad¹²⁷.

Dicho de otro modo, cuando los programas entran en proceso de producción normal se genera un problema, ya que no existe certeza de que todas esas “puertas falsas” han desaparecido. Los instrumentos de chequeo en la fase de desarrollo muchas veces no son eliminados, con lo cual las aplicaciones quedan con unas puertas de acceso por donde introducirse a los programas¹²⁸.

¹²⁵ Ibid. 96p. MAGLIONA C. y LÓPEZ, M. Op. cit. 47p.

¹²⁶ CAMACHO LOSA, L. Op. cit. 42p.

¹²⁷ JIJENA LEIVA, R. Op. Cit. 96p.

¹²⁸ MAGLIONA, C. y LÓPEZ, M. Op. cit. 48p.

La realización de esta conducta requiere por parte del autor, de una especial calificación técnica, puesto que solo un “especializado” podría encontrar (no crear) las “puertas falsas”, aunque cabe la posibilidad de que de manera accidental puedan encontrarse.

6- Bombas lógicas: La conducta consiste en introducir en un programa una serie de instrucciones no autorizadas para que en una fecha o circunstancia predeterminada se ejecuten, desencadenando la destrucción de la información que se encuentra almacenada en el ordenador, distorsionando el funcionamiento del sistema, provocando paralizaciones intermitentes, etc.¹²⁹.

Se trata de verdaderas “bombas de tiempo” ya que su objetivo es producir daños a futuro. Por las características de esta modalidad, no es infrecuente que la doctrina la asimile a una forma de sabotaje informático¹³⁰. Dentro de ella se ubica el denominado virus computacional.

7- Recogida de Residuos (*scavenging*): Consiste en recoger la información residual que queda impresa en un papel o almacenada en un disco o cinta magnética, después de la realización de un trabajo. Luego, solo puede hacerse de manera física o electrónica¹³¹. En el fondo, consiste en aprovecharse de los descuidos de los usuarios o técnicos informáticos para obtener información que ha sido abandonada sin ninguna protección como residuo de un trabajo real efectuado con autorización¹³².

8- Ataques asíncronos (*asynchronous attacks*): Desde el punto de vista técnico es el ataque más complejo, y consiste en aprovechar el funcionamiento

¹²⁹ CAMACHO LOSA, L. Op. cit. 44p.

¹³⁰ Así: JIJENA LEIVA, R. Op. cit. 96p. MAGLIONA, C. y LÓPEZ, M. Op. cit. 48p.

¹³¹ JIJENA LEIVA, R. Op. cit. 97p.

¹³² CAMACHO LOSA, L. Op. cit. 51p.

asíncrono de un sistema operativo, esto es, un programa o conjunto de programas básicos que posibilitan la gestión y control del funcionamiento global del ordenador, coordinando los sistemas periféricos que lo acompañan y comprobando que los procesos se ejecuten en el orden, momento y lugar adecuados¹³³. Estos programas funcionan de manera asíncrona, como por ejemplo, estableciendo filas de espera que se van desbloqueando en función de la disponibilidad de los datos que se estaban esperando, y basándose en los servicios que pueden realizar para los distintos programas en ejecución. El ilícito lo constituiría la alteración de este proceso, por ejemplo: hacer caer un sistema de tratamiento automatizado de información y manipulando los parámetros o condiciones en que deberá rearrancar el mismo¹³⁴.

9- Filtración o divulgación de datos (*data leakage*): Consiste en la sustracción de datos confidenciales en un sistema para copiarlos o simplemente para sustraerlos, para luego divulgarlos sin autorización¹³⁵.

La doctrina estima que ésta es una modalidad de espionaje informático¹³⁶, delito al cual nos avocaremos con especial dedicación.

10- Trasiego de personas (*piggybacking and impersonation*): Consiste en acceder a áreas controladas por medios electrónicos o mecánicos. En opinión de CAMACHO LOSA no se trata de un procedimiento de comisión de delitos informáticos, sino solo un medio de ejecución¹³⁷. Se suele incluir también el llamado "*impersonation*" que consiste en una especie de suplantación de personalidad¹³⁸.

¹³³ JIJENA LEIVA, R. Op. cit. 97p.

¹³⁴ Ídem.

¹³⁵ Ibídem.

¹³⁶ Así: JIJENA LEIVA, R. Op. cit. 98p. MAGLIONA, C. y LÓPEZ, M. Op. cit. 50p.

¹³⁷ CAMACHO LOSA, L. Op. cit. 57p

¹³⁸ MAGLIONA, C. y LÓPEZ, M. Op. cit. 50p.

11- Pinchado de líneas de teleproceso (*wiretapping*): Consiste en la intervención en las líneas de comunicación para conocer o manipular los datos que son transmitidos. En opinión de CAMACHO LOSA, “todo lo que se necesita es un pequeño “*cassette*” como grabador, una radio portátil AM/FM, un módem para remodular las señales telefónicas analógicas y convertirlas en digitales, y una pequeña impresora para listar la información que se ha captado”¹³⁹.

12- *Simulation and modeling*: Consiste en utilizar el ordenador como instrumento para planificar y controlar el delito, mediante técnicas de simulación de situaciones y de modelos de las mismas. De esta forma se pueden conocer las consecuencias previsibles de determinadas conductas¹⁴⁰.

Así, de especial relevancia se presenta para efectos de este estudio la filtración o divulgación de datos, pues lo consideramos junto con parte de la doctrina como una modalidad de espionaje electrónico. Por otro lado, sostenemos que la conducta de interceptación de comunicaciones personales electrónicas está inmersa en ella y que ECHELON, ENFOPOL y el programa CARNIVORE como sistemas de interceptación mundial de las telecomunicaciones la realizan sistemáticamente respecto la gran mayoría de las comunicaciones electrónicas de los ciudadanos del orbe, con consecuencia de afectación del derecho al secreto de la comunicaciones y de intereses comerciales, inclusive.

Los países suscriptores y avaladores de dicha Red de espionaje internacional deben responder políticamente de tales delitos, al menos, merecen el desaprobado general de la comunidad internacional, mientras que los

¹³⁹ CAMACHO LOSA, L. Op. cit. 60p.

¹⁴⁰ JIJENA LEIVA, R. Op cit. 98p.

miembros de las agencias de inteligencia que controlan técnicamente tales sistemas junto con los burócratas que los controlan políticamente deben ser merecedores de sanciones penales. Es por ello que se ha sondeado, hasta el momento, en el presente estudio, la viabilidad de un tipo penal o conjunto de ellos que permita desde la perspectiva de nuestro derecho interno, la persecución penal de dicho actos.

Luego de consideraciones acerca de los principios y acerca de los delitos informáticos se concluye que tales tipos existen y que se encuentran dispersos en la legislación nacional, en tipos tradicionales, pero respecto de los cuales se debe realizar una interpretación teleológica de acuerdo con los avances de la tecnología y la evolución de los comportamientos delictuales.

No obstante, desde una perspectiva penal-sustantiva, los problemas no se agotan en la búsqueda de un tipo, la labor interpretativa de la doctrina y judicatura acerca de éstos o la propuesta de lege ferenda de la creación de uno, existen otras interrogantes que complican la posibilidad de perseguir y condenar tales conductas intrusivas. En los siguientes apartados nos dedicaremos a analizar los problemas que son de mayor complejidad.

2.3. La aplicación de la ley penal en el espacio

La intervención ilegítima de las telecomunicaciones electrónicas personales por parte de agentes de Estado extranjeros encierra un problema dentro de la teoría de la aplicación de la ley penal en el espacio, pues es probable que al comunicarnos vía correo electrónico, el emisor o receptor se encuentren en determinado lugar fuera de los límites del país, del otro.

Lo que ocurre es que dicha transmisión “viaja” por las “autopistas de la información” de Internet, para hacer un enlace en los servidores de los proveedores de servicios, que se encuentran principalmente en territorio norteamericano, justamente en ese tránsito, al empalmar con el servidor se produce la interceptación ilegítima. Es decir, la comisión del delito ocurre en un país extranjero, en que, dichas conductas se encuentran jurídicamente justificadas, pero los titulares de los bienes jurídicos afectados se encuentran desperdigados por todo el orbe. Las preguntas consecuenciales que resultan son: ¿Se puede pretender la aplicación de la ley extranjera en nuestro país? ¿Cómo eficazmente perseguir dicha conducta, desde el ámbito del derecho interno?. Ya atenderemos a estas preguntas pero primero urge realizar un análisis acerca de la aplicación de la ley penal en el espacio, desde nuestro ordenamiento jurídico.

Siguiendo el razonamiento de gran parte de la doctrina nacional, y citando a GARRIDO MONTT¹⁴¹, la comisión de un delito tiene posibilidades de iniciarse en un lugar y consumarse en otro, que el sujeto que lo realizó se fugue del territorio del país o que haya venido del extranjero, o que el delito tenga consecuencias fuera del territorio donde se perpetró. Cuando alguna de estas alternativas se da, se plantean problemas de competencia entre los tribunales dentro de un país, pero cuando suceden en territorios de distintos Estados sobrevienen algunas complejidades al producirse problemas de soberanía.

Por consiguiente, en alternativas como las señaladas se crea un doble problema, primero determinar el Estado cuyos tribunales serán competentes para conocer del delito y castigar a los responsables y segundo, cuál es la ley

¹⁴¹ GARRIDO MONTT, M. 2003. Derecho Penal Parte General, tomo I. 1ª edición 2003. Santiago, Chile, Editorial Jurídica de Chile. pp. 125-150.

aplicable: la del que instruye el proceso, la de aquél en que se cometió el hecho o las del país cuya nacionalidad detenta el delincuente.

Para resolver estas materias existen reglas en el ordenamiento jurídico nacional, que se denominan en conjunto “derecho internacional penal”; en realidad son normas de derecho interno¹⁴² cuyo objetivo es precisar la aplicación de la ley penal nacional en el territorio y las situaciones excepcionales que la hacen aplicable extraterritorialmente.

2.3.1. Los principios sobre validez espacial de la ley penal chilena.

2.3.1.1. Principio básico: el principio de territorialidad.

Tal como sostiene POLITOFF¹⁴³, establece el artículo 5º del Código Penal (primera parte) que “la ley penal chilena es obligatoria para todos los habitantes de la República, incluso los extranjero”.

Este principio, está consagrado, en una u otra forma, en casi todos los sistemas legales, significa que la ley penal chilena se aplica a cualquiera que cometa un delito en nuestro territorio, jurídicamente y no geográficamente entendido, sin que sea obstáculo para ello la nacionalidad del hechor, de la víctima o de los bienes o derechos afectados por el delito. Se trata de una aplicación del principio de soberanía.

¹⁴² CURY URZÚA, E. 1988. Derecho Penal. Parte General, tomo 1. Santiago, Chile, Editorial Jurídica de Chile. 186p.

¹⁴³ POLITOFF LIFSCHITZ, S. 1997. Derecho Penal. Santiago, Chile, Editorial Jurídica Conosur. 138p.

Para determinar la aplicación territorial de la ley penal chilena es preciso dilucidar los conceptos de territorio, jurídicamente comprendido, y el del lugar en que se entiende cometido el delito.

Respecto de lo primero nos remitimos a los postulados de la doctrina nacional que coincide con casi absoluta unanimidad, acerca de los conceptos y el alcance de “territorio”¹⁴⁴.

El tema del lugar en que se entiende cometido el delito nos merece mayor atención. En atención a los postulados de CURY¹⁴⁵, por regla general, determinar el lugar de comisión y la consiguiente territorialidad o extraterritorialidad del hecho no presenta dificultades. Sin embargo, en algunos casos se complica, a causa de que la ejecución adopta formas complejas que comprometen a varios territorios. Como ejemplo, el ya citado, la interceptación ilegítima, en territorio norteamericano, de la correspondencia electrónica de un ciudadano de Chile, que desde nuestro país envía a su novia que se encuentra en Francia.

Para solucionar esta clase de problemas la doctrina ha propuesto fundamentalmente tres criterios distintos.

1). Según la teoría del resultado; el delito debe entenderse cometido en el lugar donde éste se ha producido. Su fundamento radica, sobre todo, en que la perturbación de la convivencia se deja sentir con toda su intensidad precisamente allí donde tiene lugar el resultado delictivo y en que sólo con la consumación se perfecciona por completo la conducta punible.

¹⁴⁴ Así se observa en: CURY, E; Op. cit. pp.189-192. POLITOFF, S. Op. cit. pp. 38-143. ETCHEBERRY, A. Op. cit. pp. 117-123. GARRIDO MONTT, M. Op. cit. pp. 127-132.

¹⁴⁵ CURY, E. Op. cit. pp. 192-194.

El punto de vista aludido ha encontrado considerable acogida en el pensamiento jurídico norteamericano. Quizás por eso, lo acepta también como fórmula alternativa el artículo 302 del Código de Bustamante, el cual, de no ser aplicable en su primera parte, ordena dar “preferencia al derecho de la soberanía local en que el delito se haya consumado”.

2). De acuerdo con la teoría de la actividad; el delito se comete allí donde se da principio a la ejecución de la conducta típica. Este punto de vista se basa en la idea de que el disvalor delictivo radica fundamentalmente en la acción y, por lo tanto, es al país, en donde ésta se realiza al que corresponde su enjuiciamiento.

Este criterio es recogido para fines del derecho interno por el artículo 157 del Código Orgánico de Tribunales¹⁴⁶, que señala: “Será competente para conocer de un delito el tribunal en cuyo territorio se hubiere cometido el hecho que da motivo al juicio.

El juzgado de garantía del lugar de comisión del hecho investigado conocerá de las gestiones a que diere lugar el procedimiento previo al juicio oral.

El delito se considerará cometido en el lugar donde se hubiere dado comienzo a su ejecución.

Sin perjuicio de lo dispuesto en el inciso segundo, cuando las gestiones debieren efectuarse fuera del territorio jurisdiccional del juzgado de garantía y se tratase de diligencias urgentes, la autorización judicial previa podrá ser concedida por el juez de garantía del lugar donde deban realizarse. Asimismo,

¹⁴⁶ CHILE. 1943. Ministerio de Justicia. Ley nº 7421: Código Orgánico de Tribunales. 9 Julio 1943 [en línea] <www.bcn.cl> [consulta: 22 enero 2007]. En adelante cuando nos refiramos al Código orgánico aludiremos al chileno.

si se suscitare conflicto de competencia entre jueces de varios juzgados de garantía, cada uno de ellos estará facultado para otorgar las autorizaciones o realizar las actuaciones urgentes, mientras no se dirimiere la competencia.

La competencia a que se refiere este artículo, así como la de las Cortes de Apelaciones, no se alterará por razón de haber sido comprometidos por el hecho intereses fiscales”.

No obstante, muchas veces, esta teoría puede conducir a conflictos que determinen la impunidad del delito, como en el caso de que el Estado en que se inició la ejecución carezca de interés en el castigo a causa de que la perturbación experimentada por su convivencia fue insignificante o inexistente.

3). Por último la teoría de la ubicuidad, en conformidad a la cual es competente para conocer del hecho tanto aquél país en que se ha realizado un acto de ejecución como aquél en que se produjo el resultado consumativo, indistintivamente.

Tal es la postura sostenida por la mayoría de la doctrina¹⁴⁷, que destaca en esta concepción la preservación de forma adecuada de la unidad de la valoración jurídica que ha de acordarse al hecho delictivo, permitiendo su enjuiciamiento conjunto por una de las leyes comprometidas; no obstante dicha teoría pueda crear algunos riesgos de infracción del principio *non bis in idem*. Pero en opinión de CURY¹⁴⁸, éstos dependen de circunstancias prácticas, las cuales, en determinados casos también podrían afectar a cualquiera de los otros criterios.

¹⁴⁷ Coinciden, entre otros CURY, E. Op. cit. 193p. POLITOFF, S. Op. cit. 155p. GARRIDO MONTT, M. Op. Cit. 133p.

¹⁴⁸ CURY, E. Op. cit. 133p.

Nosotros, para abordar la conducta de interceptación ilegítima de las comunicaciones electrónicas, adoptamos la teoría de la ubicuidad, pues en primer lugar, aunque consideramos que el delito se inicia en su ejecución y se consuma en territorio norteamericano, generalmente, las consecuencias del delito repercuten en el lugar en que se encuentran el emisor y el receptor del correo electrónico, y por lo tanto para dar una adecuada tutela penal a estos individuos se torna esencial no ignorar la afectación de los bienes jurídicos fundamentales de los individuos, como es el derecho al secreto en las comunicaciones. A su vez, por la calidad de derecho fundamental que éste posee, protegido por nuestra constitución, se hace obligatorio para todas las instituciones del Estado no escatimar esfuerzos para darle una adecuada protección, en la llamada dimensión objetiva de los derechos fundamentales¹⁴⁹.

2.3.1.2. Excepciones a la territorialidad de la ley penal.

A pesar de lo ya dicho, sin duda, la aplicación del principio de territorialidad de la ley penal chilena escapa a la situación fáctica en análisis; como ya determinamos anteriormente, creemos que el delito se inicia en su ejecución en territorio extranjero y se consuma, a su vez, en éste, puesto que los servidores de los proveedores de servicio de correo electrónico, se encuentran, casi en su totalidad, en territorio norteamericano o europeo y es en ese tránsito cuando se produce la interceptación. De esta manera, el concepto de territorio reconocido por nuestro ordenamiento jurídico, que concuerda con el de la gran mayoría del de los regímenes legales de los estados nacionales de todo el mundo, no tiene el alcance, para de acuerdo al principio de territorialidad comprender las conductas delictivas de intromisión.

¹⁴⁹ RODRÍGUEZ BLANCO, B. 1998. La estructura del derecho de las comunicaciones. En: El secreto de las comunicaciones: tecnología e intimidad, cap. III, Madrid, España, editorial. McGraw-Hill. 53p.

Sin embargo, excepcionalmente, la ley penal chilena pretende recibir aplicación extraterritorial basada en uno u otro principio de los restantes en la materia. Tales situaciones se encuentran expresamente reguladas, según lo preceptuado en los artículos sexto y 106 del Código Penal; sexto del Código Orgánico de tribunales; tercero del Código de Justicia militar¹⁵⁰; primero de la Ley n° 5.478; y alguna de las disposiciones de la ley de Seguridad Interior del Estado.

2.3.1.2.1. Aplicación del principio de personalidad o nacionalidad.

Consiste en que la aplicación de la ley penal se extiende a los nacionales de Chile, sin ser relevante el bien jurídico afectado en el delito, o que se haya cometido en territorio extranjero. Tiene dos dimensiones: una pasiva en que la víctima es de nacionalidad chilena, y otra activa, en que lo relevante es que el hechor sea un nacional.

Por supuesto para que reciba aplicación, requiere de una serie de requisitos legales y de eficacia, relativos a que el hechor del delito esté a disposición de los tribunales de justicia nacionales.

Siguiendo a GARRIDO MONTT¹⁵¹ y CURY¹⁵², entre otros, creemos que los bienes jurídicos afectados deben tener la calidad de individuales o particulares, entendido de que estos no sean de los que se destinan a tutelar intereses del Estado, pues éstos estarían cubiertos por el principio real o de defensa.

¹⁵⁰ CHILE. Ministerio de Justicia. 1944. Código de Justicia Militar. 12 diciembre 1944. [en línea] <www.bcn.cl> [consulta: 22 enero 2007]. En lo sucesivo cada vez que nos refiramos al Código de Justicia militar a secas, aludiremos al chileno.

¹⁵¹ GARRIDO MONTT, M. Op. cit., pp. 125-150.

¹⁵² CURY, E. Op. cit. 195p.

El principio de nacionalidad encuentra expresión en el artículo sexto, N° 6 del Código Orgánico de Tribunales, de acuerdo con el cual la ley chilena reclama jurisdicción para conocer de los delitos “cometidos por chilenos contra chilenos, si el culpable regresa a Chile sin haber sido juzgado por la autoridad del país en que delinquiró”.

CURY¹⁵³, destaca que no ha sido pacífico el fundamento de esta norma. Detalla que por un lado NOVOA¹⁵⁴ descarta la inclusión de dicha norma dentro de los casos de aplicación del principio de personalidad, a causa del carácter “supletorio”, que al principio atribuye la ley chilena. Por tal razón considera que se trata de una solución práctica, destinada a evitar la impunidad de atentados contra un bien jurídico chileno cuando el autor ha llegado a territorio nacional sin haber sido castigado en aquél en que se cometió el delito, y la extradición no es solicitada o no procede por cualquier razón.

Concuerda en gran medida ETCHEBERRY¹⁵⁵, pero parece considerar que la disposición aplica el principio real, pues aunque no lo dice expresamente, trata de ella bajo ese rótulo.

Por último el mismo CURY¹⁵⁶, opina que la disposición combina los principios de nacionalidad activo y pasivo, dándoles una vigencia supletoria. Se funda en el propósito de evitar la impunidad del autor cuando se niega su extradición en virtud de las cláusulas sobre no entrega del nacional que usualmente contienen los tratados relativos a la materia. Por esta razón no se ha contemplado el caso en que el hechor es un extranjero, ya que, tal evento, la

¹⁵³ Ibid. p.194.

¹⁵⁴ NOVOA MONREAL, E. Op. cit. pp. 168-169. Cit. por CURY E.; Ibídem

¹⁵⁵ ETCHEBERRY, A. Op. cit. 183p. Cit. por CURY E. Op. cit.194p.

¹⁵⁶ Idem.

extradición se otorgará de todas maneras y quien lo juzgará será el Estado en cuyo territorio se cometió el delito.

En la práctica, no obstante puede ocurrir que por cualquier razón no se otorgue la extradición del extranjero que delinquiró contra un chileno fuera del territorio nacional, y ha llegado a Chile sin ser juzgado en el lugar del hecho. En casos como esos se dará la extraña paradoja destacada por ETCHEBERRY¹⁵⁷, de que dicho extranjero no podrá ser juzgado por los tribunales chilenos. Para evitar esta situación absurda, sería necesario aceptar en estos casos una aplicación supletoria de la ley nacional posiblemente sometiéndola a requisitos más exigentes, como de querrela de la víctima

2.3.1.2.2. Aplicación del principio real o de defensa.

Determina la pretensión de aplicación extraterritorial de la ley penal chilena, basado fundamentalmente en la calidad del bien jurídico afectado, de esta forma sin importar el país en que se hubiere perpetrado el ilícito, si se afectan determinados bienes jurídicos la justicia chilena podrá perseguir tales delitos. Básicamente consisten en la protección de intereses estatales, con exclusión de los de particulares.

El principio real determina la aplicación de la ley penal chilena a hechos ocurridos en el extranjero en los casos a que se refieren los números 1,2 y 5 del artículo 6º del Código Orgánico de Tribunales, y el artículo 3º números 2 y 3 del Código de Justicia Militar.

De conformidad con algunas de esas disposiciones, quedan sometidos a la jurisdicción nacional los crímenes y simples delitos perpetrados fuera del

¹⁵⁷ ETCHEBERRY A. Op. cit. 183p. Cit. por CURY E. Ibid. 195p.

territorio de la república, “por un agente diplomático consular, en el ejercicio de sus funciones”; “la malversación de caudales públicos, fraudes y exacciones ilegales, la infidelidad en la custodia de documentos, la violación de secretos (y) el cohecho, cometidos por funcionarios públicos chilenos o extranjeros al servicio de la república”. Lo relevante es, en definitiva, ilustrar que, para el principio de defensa lo importante es la violación de un determinado tipo de bienes jurídicos, que por su particularidad solamente pueden ser trastocados por chilenos.

2.3.1.2.3. Aplicación del principio de universalidad.

Funda la aplicación extraterritorial de la ley penal chilena en razón de la violación de bienes jurídicos protegidos universalmente, que determinan la persecución penal de ciertos delitos sin importar del lugar de comisión que se trate. Además, se trata de atentados que por sus características son de difícil enjuiciamiento penal, ya sea por que se trata de “delitos en tránsito”, sus distintas etapas se desarrollan en distintos países, y que además generalmente se encuentran tipificados en tratados internacionales, o se perpetran en “tierra de nadie”. Como la trata de blancas, esclavos, el genocidio, por citar algunos de los ejemplos, o que se cometan en alta mar. El principio en que se cimienta es la colaboración internacional que los países guarden entre sí, para enfrentar atentados atroces a la humanidad.

El número 7 del artículo 6º del Código Orgánico de Tribunales, con arreglo al cual se aplica la ley chilena a la piratería, determina su aplicación aunque los hechos que la configuren se hayan realizado, como generalmente ocurre, fuera del territorio nacional. Se trata de una clara expresión del principio de universalidad, que busca dar tratamiento penal a este tipo de delitos que de otro modo se mantendrían impunes. También es manifestación el artículo 6º

número 8 de Código Orgánico de Tribunales, que contempla los casos incorporados por los tratados internacionales. En efecto, “estos generalmente se refieren a delitos que por su naturaleza comprometen el territorio de varios países, ya que su actividad presupone traslado de uno a otros...”.Respecto de ellos se ha consagrado por lo pronto el principio de universalidad en los artículos 307 y 308 del Código de Bustamante.

Para las materias que motivan nuestra investigación, creemos que el principio de territorialidad no permite la persecución penal del delito de interceptación ilegítima de comunicaciones personales, por las características propias del mismo. Sin embargo, la aplicación extraterritorial de la ley penal chilena es la vía, apoyada principalmente en el principio de universalidad. El delito en cuestión es uno de los que, por su naturaleza, requiere de la cooperación internacional para su enjuiciamiento penal eficaz. Por otro lado no puede ser indiferente para los distintos estados la conculcación impune de Derechos Fundamentales. Dicho de otro modo, la discusión de la soberanía en la aplicación de la ley penal de los distintos países debe ceder frente a intereses superiores de justicia mundial.

En nuestra opinión, el Derecho penal debe avanzar hacia su efectiva internacionalización, para hacer frente a las nuevas formas delictivas que permite el avance tecnológico. Se debe ungir órganos supranacionales de administración de justicia, aún contra la oposición de algunos países. Justamente, la labor de la comunidad internacional es superponer los Derechos Fundamentales y los intereses de justicia internacional sobre los intereses políticos y económicos de determinados estados.

2.4. Valor en Chile de las leyes penales extranjeras.

Esta es la otra vertiente del problema, recientemente defendimos la aplicación extraterritorial de la ley chilena, con los particulares supuestos que embargan nuestra investigación; ahora nos corresponde responder a las pretensiones de extraterritorialidad que guarda la USAPA, cuerpo normativo que brinda marco jurídico a la intervención “justificada”, en pos de vagos conceptos como la seguridad nacional. Mal vale sobreponer un criterio así de ambiguo a los Derechos Fundamentales.

Utilizando los razonamientos de CURY¹⁵⁸, en virtud del principio de soberanía de los estados, estos no aplican, en caso alguno, leyes penales extranjeras. Este punto de vista se encuentra expresamente reconocido en el artículo 304 del Código de Bustamante, según el cual “ningún estado contratante aplicará en su territorio las leyes penales de los demás”.

Desde estos principios jurídicos rechazamos la aplicación de tal normativa norteamericana en nuestro país, menos con fines atentatorios del derecho a la privacidad y al secreto en la comunicaciones. Es cierto que los Derechos Fundamentales pueden ser suspendidos o restringidos, frente a determinados acontecimientos extraordinarios, pero no creemos justificar la creación de un sistema mundial de interceptación de las telecomunicaciones, que carece de control democrático de cualquier índole, y que esconde intereses comerciales y políticos tras fines aparentemente altruistas. La seguridad nacional, la amenaza del “enemigo” son conceptos “pantalla” de intereses ocultos que por la misma condición no son para nada altruistas.

A continuación, es necesario darle respuestas a un problema técnico-penal, ¿De qué vía jurídica disponemos para requerir a un agente de estado

¹⁵⁸ CURY, E. Op. cit. pp. 197-198

extranjero para someterlo a nuestro ordenamiento jurídico frente a la comisión de un delito?.

2.5. La Extradición.

2.5.1. Concepto.

La doctrina nacional, de manera clara, ha logrado crear conceptos más o menos similares de extradición, lo que se diferencia principalmente es si se trata de una institución o de un acto. Así, GARRIDO nos dice que “...La extradición es la institución por la cual un Estado, denominado requerido, entrega a otro –el requirente- la persona que le solicita y que se encuentra en su territorio, para que el requirente lo procese penalmente o para que se cumpla una condena cuando ya lo ha sentenciado. Se califica de “activa”, en relación al país requirente, y de “pasiva”, respecto del requerido, que es quién debe hacer la entrega...”¹⁵⁹.

Por su parte, POLITOFF nos explica que “...La extradición es el acto por el cual un Estado entrega una persona a otro Estado que lo reclama para juzgarlo penalmente o para ejecutar una pena ya impuesta. En el primer caso se puede hablar de extradición para perseguir un delito y en el segundo caso de extradición para hacer efectiva una condena...”¹⁶⁰.

Por otra parte, ETCHEBERRY expone que “...Se llama extradición la institución jurídica en virtud de la cual un Estado entrega a otro Estado una persona que se encuentra en territorio del primero y que es reclamada por el

¹⁵⁹ GARRIDO MONTT, MARIO. Op. cit. 140p.

¹⁶⁰ POLITOFF L., S. Op. cit. 164p.

segundo para su juzgamiento en materia penal o para el cumplimiento de una sentencia cuando este en carácter de ya dictada...”¹⁶¹

2.5.2. Fuentes normativas de la extradición.

En primer lugar, los Estados pueden suscribir acuerdos o tratados internacionales para prevenir la circunstancia de la extradición. Ergo, la primera fuente serían los tratados internacionales suscritos por varios Estados. De tal modo, los tratados más representativos suscritos por Chile serían el Código de Bustamante y el Convenio de Montevideo de 1933. Ello sin perjuicio que hayan tratados bilaterales entre Estados para regular la extradición.

En segundo, los Estados suelen tener una normativa interna que prevenga o que trate la extradición. En este sentido, la legislación chilena, en el Código Procesal Penal contempla en el libro VI del título IV.

Finalmente, y de manera supletoria, cuando no hay tratados al respecto, entre los Estados rige la costumbre. Esta costumbre se basa en la idea o principio de reciprocidad, es decir, que si un Estado entrega a una persona, en el futuro ese Estado deberá estar dispuesto a entregar a una persona, del mismo modo, si lo requiriere.¹⁶²

2.5.3. Condiciones en que procede la extradición.

Para que la extradición tenga cabida, deben verificarse las siguientes circunstancias:

¹⁶¹ ETCHEBERRY. Op. cit. 134p.

¹⁶² Ibid. 135p. Lo mismo en POLITOFF. Op. cit. 167p.

- 1.- Debe haber una relación internacional entre ambos Estados, ya fuera de manera inequívoca mediante un tratado internacional, o al menos en razón del principio de reciprocidad.
- 2.- El hecho debe estar tipificado tanto en una Estado como en el otro. A esto se le denomina “Principio de la Doble Incriminación”. Según POLITOFF, ésta debe ser examinada en abstracto, vale decir, sin considerar causales de justificación o de exculpación.¹⁶³
- 3.- El hecho debe detentar una cuantía considerable en su pena. Así, no cabría hablar de extradición de delitos de poca significación o bagatela.
- 4.- El delito debe ser un delito común, por oposición a un delito político. Esto significa que si el delito fue realizado en el marco de una subversión contra la autoridad por considerarle injusta o ilegítima, no debe extraditarse dado que se supone que el juicio no sería justo.
- 5.- El delincuente, *prima facie*, siempre debiera extraditarse. Sin embargo, lo normal es que un Estado nunca extradite a sus ciudadanos nacionales. Ante esa realidad, el artículo 345 del Código de Bustamante establece una regla que indica que si no se concede la extradición de un nacional, el Estado que no la concedió debe juzgar a la persona en cuestión. Pese a ello, la aplicación de dicho código es limitada, por lo que muchos caso se quedarían sin una solución jurídica sistematizada y tendrían una solución eminentemente política.
- 6.- El delito no debe estar prescrito y no debe estar amnistiado.
- 7.- A la persona que se extradita no debe habersele juzgado, cumplido una condena, o no debe estar sustanciándose un procedimiento por los hechos que propician la extradición. Esta idea esta recogida en al artículo 358 del Código de Bustamante¹⁶⁴.

¹⁶³ POLITOFF. Op. cit. 169p

¹⁶⁴ CHILE. Ministerio de Relaciones Exteriores. 1934. Código de Derecho Internacional Privado Decreto nº 374 del Ministerio de Relaciones Exteriores. 25 abril 1934. [en línea] <www.bcn.cl> [consulta: 22 enero 2007].

2.5.4. Efectos de la extradición.

Hay que distinguir si se ha concedido o si no se ha concedido.

Si no se concede, tiene efecto de cosa juzgada y no puede volver a solicitarse la extradición de esa persona.

Si se ha concedido, se procede a enviar al extraditado al país que lo requirió, pero con las limitaciones siguientes: no se le puede juzgar por otros delitos que no hubieren sido denotados en la petición del país requirente, requisito que se le llama “Principio de Especialidad”¹⁶⁵; y que no se le puede condenar a pena de muerte, fundado esto en última instancia en principios humanitarios.¹⁶⁶

2.6. Aspectos procesales y penales relativos a la intervención en las telecomunicaciones.

El Estado, como se explicó en el capítulo anterior, tiene un rol fundamental y protagónico en la promoción de los Derechos Humanos, de modo que pasen a ser algo más que una pretensión programática, y constituyan realmente Derechos Fundamentales aceptados por todos los Estados que, al menos, aspiren a seguir el modelo de “Estado de Derecho”.

Por otra parte, también se relató que el Estado puede atentar contra el Derecho a la vida privada en el marco de su obligación de proteger a los ciudadanos y de ejercer el *Ius Puniendi*, vale decir, su obligación de perseguir los delitos que cometan los ciudadanos so resguardar la paz social.

¹⁶⁵ GARRIDO. Op. cit. 148p.

¹⁶⁶ Ídem.

Para dicho ejercicio, el Estado no puede actuar arbitrariamente y a destajo, sino que debe someter su acción al principal freno de su poder: la Constitución.

Como bien sabemos, la Constitución (en términos generales y relativos al Estado de Derecho contemporáneo) tiene una doble finalidad al respecto: regular el ejercicio del poder del Estado, y entregar garantías a los ciudadanos, de modo que vean protegida su integridad y su posibilidad de desarrollar una vida plena. Lo primero se concreta en la separación de poderes, y lo segundo en el establecimiento del catálogo de Derecho Fundamentales.

La ley debe estar en consonancia a la Constitución, sino su existencia como norma matriz del ordenamiento no tendría sentido. Por ende, y como corolario, la ley penal debe sujetarse a la Constitución.

Sin embargo, no sólo la ley penal de fondo (las conductas penadas) debe sujetarse a la Constitución, sino todo el procedimiento que implique investigar, acusar, juzgar, y ejecutar una conducta reprochable. Así, la ley procesal penal también debe sujetarse a la Constitución.

Ahora bien, centrándonos en nuestro tema de investigación, la principal circunstancia en la cual el Estado puede violar el derecho a la vida privada es en el ejercicio de la investigación de delitos.

De este modo, y en el marco de la llamada “guerra contra el terrorismo”, legislaciones como la USAPA desconocen este derecho fundamental al autorizar la intervención en las telecomunicaciones, sin resguardo del derecho a la vida privada.

Nuestro principal problema ahora es, más allá de la legitimación política y moral que tienen los Estados, determinar si existe una legitimación jurídica para que sea vulnerado nuestro derecho a la vida privada, en el marco de una investigación con fines penales. Para tal efecto, el propósito del siguiente acápite es doble: por una parte explicar principios o instituciones comunes a toda la órbita jurídica occidental, que rijan la formación del procedimiento penal, siendo éstas una piedra de tope a la intervención estatal en las telecomunicaciones privadas vía Internet; y por otra, establecer, en razón de los principios procesales penales, las bases de una persecución penal en los casos de violación de dicho derecho, en sede penal.

2.6.1. El proceso penal, su caracterización, y los principios que lo rigen.

2.6.1.1. Concepto de proceso penal y sus finalidades.

El proceso penal es, en términos de LEONE, "...el conjunto de actos encaminados a la decisión jurisdiccional, acerca de una *notitia criminis* o acerca de las condiciones requeridas para algunas de las providencias en orden a la represión del delito o a la modificación de las relaciones jurídicas penales preexistentes."¹⁶⁷. En términos jurídicos, nos parece ésta, una definición pertinente e idónea porque resume los elementos centrales del proceso, a saber, las ritualidades, en sentido abstracto, la decisión que debe tomar un órgano del Estado, y a lo que debe referirse dicha decisión.

¿Por qué no menciona dicha definición la protección o resguardo de los Derechos Fundamentales, o al menos, de los Derechos Humanos? Porque, en

¹⁶⁷ LEONE, GIOVANNI. 1963. Tratado de Derecho Procesal Penal, Tomo I. Traducción de SENTÍS MELENDO, SANTIAGO. Buenos Aires, Argentina, Ediciones Jurídicas Europa-América. 10p.

abstracto y de manera teórica, no es requisito *sine qua non* de un proceso esa protección. Así, podemos encontrarnos con procesos penales de determinados ordenamientos jurídicos donde se protegen los Derechos Humanos, y otros que dejan mucho que desear al respecto y no por eso son removibles de la categoría general de proceso penal. Por ejemplo, no podemos aseverar que un proceso como del Código Italiano de 1930, de tinte fascista (que posteriormente sería reformado), no es un proceso por atacar contra los Derechos Humanos.

Sin embargo, es una aspiración común de los Estados modernos, en razón del rol del Derecho como instrumento pacificador de las relaciones sociales, que el proceso penal se vea empapado del respeto y protección al ser humano. Un siglo XX vertiginoso, brutal, y fatalmente crudo, nos recuerda con sus genocidios y sus guerras, lo mismo que una cicatriz imborrable en nuestra memoria colectiva, que el poder punitivo del Estado debe tener en cuenta al ciudadano ordinario.

En ese sentido, ROXIN nos ayuda a entender lo anterior, de manera muy pertinente, con una curiosa analogía: "...En el procedimiento penal entran en conflicto los intereses colectivos e individuales entre sí, con más intensidad que en ningún otro ámbito, la ponderación de esos intereses, establecida por la ley, resulta sintomática para establecer la relación entre el Estado e individuo genéricamente vigente en una comunidad: "¡El derecho procesal penal es el sismógrafo de la Constitución del Estado!"¹⁶⁸

Menester es también no confundir proceso con procedimiento, para tal distinción MATURANA nos explica que "...La forma externa en la cual se debe desarrollar esta idea abstracta que es el proceso, compuesta de una secuencia

¹⁶⁸ ROXIN, CLAUS. 2000. Derecho Procesal Penal, Traducción de CÓRDOBA, GABRIELA E., y PASTOR, DANIEL R. Buenos Aires, Argentina, Editores del Puerto. 10p.

o serie de actos que permite arribar a una sentencia que solucionará el conflicto es el procedimiento... Entendemos por procedimiento “el conjunto de formalidades externas, de trámites y ritualidades establecidas por el legislador para efectos que se desarrolle el proceso.”¹⁶⁹

La tarea del Estado de perseguir los delitos, cometidos por sus ciudadanos o contra sus ciudadanos, encuentra en la legislación procesal penal una doble función: por un lado, perseguir y juzgar los delitos, y hacer ejecutar las penas que recayeren sobre los delincuentes, pero a la vez proteger a quién siendo investigado o juzgado no pudiera reprochársele una conducta digna de castigo. Siguiendo a ROXIN otra vez, “...la violencia penal puede significar también un gran peligro para aquel que siendo inocente, ha caído en sospecha. Por ello, con la aparición de un derecho de persecución penal estatal, surgió también, a la vez, la necesidad de erigir barreras contra la posibilidad del abuso del poder estatal...”¹⁷⁰. Esas barreras estarían determinadas, según lo estimamos, por la Constitución Política y por los tratados internacionales pertinentes.

2.6.1.2. Caracterización de los procesos penales.

Antes de determinar qué principios rigen en todo proceso respetuoso de los Derechos Humanos, y por lo tanto aplicable a todos los Estados (al menos de la órbita occidental), debemos detenernos a pensar el siguiente dilema que DAMASKA nos plantea: “No todas las diferencias en el marco institucional y en las formas de justicia son visibles a primera vista. Algunas subyacen bajo similitudes superficiales y sólo pueden descubrirse tras una revisión profunda.

¹⁶⁹ MATURANA MIQUEL, CRISTIÁN. 2004. Separata de Introducción al Nuevo Sistema Procesal Penal. Santiago, Chile, Central de Apuntes de la Facultad de Derecho de la Universidad de Chile. 16p.

¹⁷⁰ ROXIN. Op. Cit. 2p.

No ha de sorprender, entonces, que a veces se proclame el consenso respecto de puntos sobre los cuales los acuerdos no son más que logros retóricos... ..la unanimidad comienza a resquebrajarse en cuanto se consideran las implicancias de esas nociones y el significado operativo de la administración de justicia de esas naciones.”¹⁷¹ Según esto, si cada proceso tiene diferencias en cada Estado, y a su vez los consensos no parecen aunarse en sus propios términos al existir diferencias notables¹⁷² ¿Cómo identificar estos principios comunes?

La solución a tal problema radica en la configuración de procesos modelos, en abstracto, de los cuales se puedan extrapolar características y principios que configuren los procesos en concreto. Así, si bien en un primer orden no podremos extraer un conjunto de principios comunes, si podremos obtener una serie de categorías generales que nos ayudarán a retratar entidades que son muy disímiles entre sí.

De tal manera, la doctrina tradicionalmente ha seguido la dicotomía entre el procedimiento acusatorio e inquisitivo. Por ejemplo, MANZINI caracteriza esta dicotomía a propósito de la evolución del proceso penal en Italia, de una manera más aferrada a la experiencia itálica, valga la redundancia. Así expone que el proceso acusatorio es “...contradictorio, como el proceso civil, pero predomina en él la escritura, falta de debate público...,” etcétera.¹⁷³

¹⁷¹ DAMASKA, MIRJAN R. 2000. Las caras de la Justicia y el Poder el Estado, traducción de MORALES VIDAL, ANDREA, y RUIZ-TAGLE, PABLO. Santiago, Chile, Editorial Jurídica de Chile. 10p.

¹⁷² Cabe recordar nada más que nuestro antiguo proceso penal reunía la facultad de acusar y de juzgar en una sola persona, algo impensado en procesos de otros países. O bien, tomando un ejemplo de DAMASKA. Op. cit. 11p “...El hecho que la mayoría de los sistemas de common-law pongan restricciones más severas al acopio de pruebas en los casos criminales más que en los civiles, casi escapa a la comprensión de un abogado continental...”

¹⁷³ MANZINI, VICENZO. 1951. Tratado de Derecho de Procesal Penal, Tomo I, traducción SENTÍS MELENDO, SANTIAGO, y AYERRA RENDÍN, MARINO. Buenos Aires, Argentina, Ediciones Jurídicas Europa-América. 34p.

LEONE confecciona esta dicotomía antitética de manera más fina, pues estima que la principal diferencia entre ambos sistemas es que en el inquisitivo hay ausencia de mediación entre el juez y el imputado (entendiendo como esa mediación la defensa jurídica). En cambio, esa mediación o defensa existe en el acusatorio.¹⁷⁴ En coordinación con ello, piensa que el proceso acusatorio puro y el inquisitivo puro son totalmente opuestos.

Así, y a *grosso modo*, concibe en abstracto que un proceso penal acusatorio puro reconoce los siguientes principios: a.- la jurisdicción pertenece a un órgano estatal; b.- el poder de iniciativa (acusación) es de los privados y no del Estado; c.- Pasividad del tribunal para acusar (se requiere de una acusación para iniciar un procedimiento); d.- Ya iniciado el procedimiento, el órgano estatal no está condicionado por el impulso privado; e.- Pasividad del tribunal en la investigación, y en el aporte y selección de la prueba; f.- Existencia de contradictoriedad, oralidad y publicidad del debate; g.- libertad personal del acusado hasta la sentencia condenatoria.¹⁷⁵ MATURANA a ello agrega que "...el sistema acusatorio es el que primero aparece en el curso de la evolución histórica de la humanidad y rigió en Grecia, Roma, y diversos países hasta la Edad Media..."¹⁷⁶ En el mismo sentido, MANZINI distingue en la antigua Roma republicana entre la *accusatio* y la *cognitio* como diferencia entre la acusación y el juzgamiento, las cuales quedaban entregadas a entidades distintas.¹⁷⁷

De la misma manera, también concibe que el proceso inquisitivo puro tenga principios característicos, estos serían: a- Un mismo juez reúne la facultad de acusar, de investigar, y de juzgamiento; b.- El juez es de carácter

¹⁷⁴ LEONE. Op. cit. 20p, siguiendo a CARNELUTTI. Lezioni I, 158p.

¹⁷⁵ Ibid. pp. 21-22.

¹⁷⁶ MATURANA. Op. cit. 50p.

¹⁷⁷ MANZINI. Op. cit. 6p.

permanente; c.- El juez tiene libertad para buscar y adquirir las pruebas; d.- Proceso escriturado y secreto; e.- Existe una regulación legal de la prueba; f.- Existe doble grado de jurisdicción (primera y segunda instancia); h.- Hay nulidad de los actos en caso de ilegalidad en la constitución del juez, de inobservancia de las normas sustanciales, o de violación de la ley.¹⁷⁸

Finalmente, concluye que los procesos en concreto son procesos mixtos, y que en la vida real no existen procesos acusatorios o inquisitivos puros (o si existieran serían casos muy raros). Los procesos mixtos son una mezcla de los principios enunciados de manera antitética anteriormente, teniendo cabida el uno o el otro. A modo de ejemplo, LEONE caracteriza el proceso penal italiano de comienzo de los años 60' del siglo veinte de esta manera: a.- Necesidad de separar el juzgamiento de la acusación e investigación; b.- Necesidad de dos fases en el procedimiento: instrucción de escrituración y secreto, y otra de juicio, de oralidad y publicidad; c.- La crítica y adquisición de la prueba quedan en manos del juez.¹⁷⁹

DAMASKA, en complemento de lo anterior y realizando un ejercicio de Derecho procesal penal comparado, además de reconocer en abstracto la dicotomía de proceso adversarial puro e inquisitivo puro (le llama adversarial a lo que sería acusatorio)¹⁸⁰, se fija en las relaciones de poder que mantiene el Estado con sus ciudadanos, y para tal efecto desarrolla dos dicotomías de procesos en abstracto y puros para caracterizar, de manera más precisa, los procesos de las distintas tradiciones jurídicas del planeta. Entonces, establece la dicotomía de tribunales jerárquicos y tribunales paritarios, y la de tribunales que sólo resuelven conflictos y de tribunales que implantan políticas.¹⁸¹

¹⁷⁸ LEONE. Op. cit. pp. 23-24.

¹⁷⁹ Idem. 26p.

¹⁸⁰ DAMASKA. Op. cit. pp. 16-17.

¹⁸¹ Ibid. 24p y siguientes.

Luego de ello, ya comprendiendo como caracterizar los procesos penales en base a modelos abstractos, debemos enunciar de una manera más precisa los principios que forman el procedimiento y que se extraen de las dicotomías antes enunciadas.

2.6.1.3. Sobre los principios procesales penales en general.

TAVOLARI define a los principios procesales como "... las fórmulas a los que el pensamiento jurídico-político recurre, para estructurar un modo de realizar el *ius puniendi* estatal, en condiciones que permitan su ejercicio efectivo y fructuoso, sin mengua de las garantías y derechos que el desenvolvimiento cultural estima en un momento determinado, son los que corresponde asegurar al imputado y reconocer a la víctima"¹⁸². Del mismo modo, también es pertinente agregar que "...justamente en la medida en que estemos ante un verdadero principio (esto es, ante un elemento originario de lo esencial, de aquello que pertenece a la naturaleza de una cosa: en este caso, el proceso penal), dependerán de él muchas características del proceso y muy numerosos instrumentos procesales..."¹⁸³

Por su parte, ROXIN establece, a propósito de la legislación alemana, que todos los principios tienen un mandato superior del derecho procesal penal: el principio del proceso justo, establecido en los artículos 1º, 20, 28, y 66 de la Ley Fundamental Alemana, y en el artículo 6.1 de la Convención Europea para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Luego, y ahondando en su esquematización, él propone que se deben

¹⁸² TAVOLARI OLIVEROS, RAÚL. 2000. El Proceso en Acción. Chile, Editorial Libromar. 562p.

¹⁸³ DERECHO PROCESAL PENAL. 1999. por Andrés de la Oliva Santos "et al". Madrid, España, Editorial Centro de Estudios Ramón Areces S.A. 7p.

considerar los principios en la siguiente sistematización, considerando que son en parte rígidos y que cada principio tiene su antítesis teórica¹⁸⁴.

1.- Principios de la Iniciación del Procedimiento.

a.- Principio de la Oficialidad: El Estado tiene que perseguir los delitos de oficio. Su antítesis sería la acción penal privada, y la acción penal colectiva,

b.- Principio Acusatorio: Es la separación de la acusación e investigación del juzgamiento, vale decir, "...donde no hay acusador, no hay juez..."¹⁸⁵

c.- Principio de Legalidad: Es la obligación del Estado de perseverar en la persecución de delitos. Su atenuación viene dada por los delitos donde el reproche del hecho es insignificante.

d.- Principio del Juez Preestablecido por Ley.

2.- Principios de la Realización del Procedimiento.

a.- Principio de Investigación (Principio de Instrucción, Principio de Averiguación, y Principio de Verdad Material).

b.- Principio de Ser Oído conforme a la Ley.

c.- Principio de Celeridad, de Concentración en el Juicio Oral.

3.- Principios Probatorios.

a.- Principio de la Investigación.

b.- Principio de la Inmediación en la Producción de la Prueba.

c.- Principio de la Libre Valoración de la Prueba.

d.- Principio *In Dubio pro Reo*: En caso de duda se decidirá a favor del acusado¹⁸⁶.

¹⁸⁴ ROXIN. Op. Cit. 79p.

¹⁸⁵ Idem. 86p.

¹⁸⁶ Ibid.102p.

4.- Principios Referidos a la Forma.

- a.- Oralidad.
- b.- Publicidad.

2.6.1.4. Principios procesales penales en Chile.

Como es obvio y podría esperarse, Chile también detenta un proceso penal, y por lo tanto, existen principios que forman nuestro proceso penal.

La reciente reforma a la justicia penal ha hecho a los autores nacionales preguntarse sobre cuales serían los principios que caracterizarían al proceso penal nacional. Discusión que ciertamente está determinada, o al menos influenciada, por las categorías de análisis antepuestas.

TAVOLARI, en base al Proyecto de Código Procesal Penal Chileno, logra identificar los siguientes principios, clasificados a su vez en subcategorías diferenciadas:¹⁸⁷

A.- Principios Político Procesales:

- 1.- Principio de resguardo de los Derechos del imputado, lo que se puede expresar en la expresión *nulla poena sine iudicio* (no hay pena sin un juicio).
- 2.- Principio de resguardo de los Derechos de la víctima.
- 3.- Principio de eficaz administración de los recursos públicos de persecución penal, que a su vez se traduce en:
 - 3.1.- El archivo provisional, es decir, que si no hay una chance de éxito en la persecución de un delito, no debe

¹⁸⁷ TAVOLARI. Op. cit. pp. 565-582.

perseverarse en la investigación, sin perjuicio de que con la agregación de nuevos antecedentes ésta pueda reanudarse.

3.2.- Principio de oportunidad, que consiste en que si un delito por su insignificancia no comprometiére el interés público (bagatela), no debiera iniciarse su persecución.

B.- Principios Orgánicos:

1.- Separación de las funciones estatales de investigar, acusar, y sentenciar.

2.- Instrucción por el Ministerio Público.

3.-Juzgamiento por un tribunal letrado, colegiado de única instancia.

C.- Principios de Política Criminal:

1.-Justicia consensuada o Principio de disponibilidad de la justicia criminal, que a su vez se concreta en:

1.1.-Acuerdos reparatorios.

1.2.- Procedimiento abreviado.

D.- Principio Procesal Criminológico:

1.- Suspensión condicional del procedimiento.

E.- Principios o Reglas Técnicas del Procedimiento.

1.- La publicidad.

2.- La oralidad y la inmediación, que se manifiestan en la presencia ininterrumpida de jueces, fiscal, defensor, e imputado durante el juicio oral.

F.- Principios de Prueba:

En esta categoría el autor no desarrolla los principios en un punteo, mas comenta que, en razón de este principio, "...la posibilidad de discutir sobre las pruebas en presencia del tribunal, sin que puedan esgrimirse otras, termina configurando un régimen

de igualdad de posibilidades procesales a que se puede aspirar en el proceso penal...”¹⁸⁸ y agrega que “... los tribunales apreciarán la prueba con entera libertad, pero no podrán contradecir las reglas de la lógica, los conocimientos científicamente ni las máximas de la experiencia...”¹⁸⁹

Una clasificación de los principios procesales penales en Chile un poco más asertiva, y realizada sobre el código mismo y no sobre el proyecto, es la que realiza HORVITZ y LÓPEZ. Esta clasificación nos resulta valiosa porque “...se servirá de la doctrina extranjera en cuanto ella tiene de universal en la determinación del contenido de principios que son comunes a los diferentes sistemas procesales penales contemporáneos. A partir de allí, propondremos confrontar estas nociones con la forma en que dichos principios aparecen reconocidos en los tratados internacionales sobre Derechos Humanos ratificados por Chile.”¹⁹⁰ Esta idea, ya adelantada por estos autores, será capital en relación al sub-acápito siguiente, pues nos ayudará a compatibilizar nuestros principios con los comúnmente aceptados por los países occidentales al menos.

En fin, volviendo a la cuestión que nos es atingente ahora, esta clasificación distingue entre Principios y Garantías. Los primeros son una manifestación de la constitucionalización del Derecho procesal penal, y las segundas son opciones políticas que adopta el legislador procesal penal.¹⁹¹ Así, la clasificación, a modo enunciativo, general, y haciendo referencia los artículos del Código Procesal Penal en que se encuentran o manifiestan, sería del siguiente orden.¹⁹²

¹⁸⁸ Ibid. 581p.

¹⁸⁹ Idem.

¹⁹⁰ HORVITZ LENNON, MARÍA INÉS y LÓPEZ MASLE, JULIÁN. 2002. Derecho Procesal Penal Chileno, Tomo I. Santiago, Chile, Editorial Jurídica de Chile, 33p.

¹⁹¹ HORVITZ y LÓPEZ. Op. cit. 35p.

¹⁹² Ibid. pp. 35-102.

1.- Principios de Persecución Penal:

1.1.- Principio de oficialidad. (Artículo 53).

1.2.- Principios de investigación oficial y aportación de parte. (Artículo 3º)

1.3.- Principio acusatorio (Artículos 3º, 7º, 8º, y 9º).

1.4.- Principios de legalidad (Artículos 53 inciso 2º, 56, 77, 166, 175 “b”) y oportunidad (Artículo 170).

2.- Garantías Individuales ante la Persecución Penal:

2.1.- Garantías de la Organización Judicial.

2.1.1.- Derecho al juez independiente. (Artículo 195 del Código Orgánico de Tribunales.)

2.1.2.- Derecho al juez imparcial. (Artículo 1º)

2.1.3.- Derecho al juez natural. (Artículo 2º)

2.2.- Garantías Generales del Procedimiento.

2.2.1.- Derecho al juicio previo (artículo 1º)

2.2.2.- Derecho a ser juzgado dentro de un plazo razonable. (Artículo 247, a propósito del plazo para investigar)

2.2.3.- Derecho a defensa. (Artículo 8º)

2.2.4.- Derecho a presunción de inocencia. (Artículo 4º)

2.2.5.- Inadmisibilidad de la persecución penal múltiple o *non bis in idem*. (Artículo 1º inciso 2º).

2.3.- Garantías del Juicio.

2.3.1.- Derecho al juicio público. (Artículo 1º, y 376 letra “d”).

2.3.2.- Derecho al juicio oral. (Artículo 1º, y 291).

2.3.2.1.- Principio de inmediación. (Artículos 331, 332, 340, 344, y 329)

2.3.2.2.- Principio de continuidad y concentración. (Artículos 282 y 283).

2.6.1.5. Principios procesales penales que se podrían considerar comunes.

Como ya vimos antes, DASMASKA estima que no es común que los procesos compartan principios e instituciones comunes, y si lo hacen, más bien sería de manera programática. Sin embargo, y pese a esta realidad, esa constatación no es la que tomaremos como pilar en esta monografía por la razón que enunciábamos al comenzar este acápite: el Derecho tiene una vocación amplia e infatigable para buscar la paz en la humanidad, paz que se consigue reduciendo la brutalidad con que el hombre actúa cuando se ve dotado de poder. Esa vocación se ve reflejada en creación de tratados internacionales, comenzando con la Declaración Universal de Derechos Humanos, para concordar, al menos, en lo que es indignificante para el hombre. Podrá ser cierto que los Derechos Humanos son más programáticos que realidades aplicadas, pero no por ello debemos renunciar a su aplicación, sino, lisa y llanamente, estaríamos renunciando a la vocación socializadora del Derecho.

Al respecto, TAVOLARI asevera "...que el actual debate acerca de los principios del proceso penal, superados los antagonismos de modelos acusatorios e inquisitorios, por el triunfo de aquél, con las variantes que cada lugar y tiempo determinan, se centra en consignar aquellos que mejor recogen las garantías de los ordenamientos políticos que consagran..."¹⁹³, y ciertamente, en opinión nuestra, esas garantías son las que consagran los tratados internacionales y la Constitución Política.

¹⁹³ TAVOLARI. Op. cit. 582p.

Este mismo autor, de manera lúcida y ordenada, sistematiza los principios procesales penales que pueden ser extraídos de la Declaración Universal de Derechos Humanos, del Pacto de San José de Costa Rica, y del Pacto Internacional de Derechos Civiles y Políticos. A saber, la sistematización sería del siguiente tenor:¹⁹⁴

A.- Principios o Garantías Jurídico-Políticas:

- 1.- El Derecho a un Juez independiente e imparcial.
- 2.- El Derecho a un juez competente.
- 3.- El Derecho a la defensa.
- 4.- El Derecho a un recurso ante un tribunal superior.
- 5.- El Derecho al *non bis in idem*.
- 6.- El Derecho a indemnización por error judicial.
- 7.- El Derecho a un juicio público.

B.- Principios o Garantías Procesales:

- 8.- El Derecho a ser oído.
- 9.- El Derecho a ser informado de los cargos en su contra.
- 10.- El Derecho a la presunción de inocencia.
- 11.- El Derecho a la igualdad procesal.

C.- Principios o Garantías Procedimentales.

- 12.- El Derecho a juzgamiento en un plazo razonable (el Derecho a juzgamiento sin indebidas dilaciones).
- 13.- El Derecho a no ser obligado a declarar en su contra ni a declararse culpable.
- 14.- El Derecho a contar con la asesoría de un abogado defensor.
- 15.- El Derecho a presentar y rendir la prueba.
- 16.- El Derecho a contradecir la prueba contraria.

¹⁹⁴ Ibid. 563p.

17.- El Derecho a la libertad provisional, durante la sustanciación del juicio, según las condiciones que la ley determine.

Asimismo, nosotros debemos agregar que el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales¹⁹⁵, de conformidad al protocolo N° 11 de 1998, en sus artículos 5º, 6º, y 13 consagra estos mismos principios. Sin embargo, hay tres que no quedan expresados de manera manifiesta en dicho tratado, pero son deducibles, y por lo tanto, estarían presentes de manera indirecta. Estos principios no expresamente manifiestos serían: el Derecho al *non bis in idem*, el Derecho (del acusado) a no ser obligado a declarar en su contra ni a declararse culpable, y el Derecho a presentar y rendir la prueba.

De esta forma, la utilidad de esta clasificación del profesor TAVOLARI radica en que, de una u otra manera, vendría a determinar los principios procesales comúnmente aceptados por los Estados occidentales, y legitimados en tratados internacionales en observancia y respeto a los Derechos Humanos. Vale decir, serían un mínimo común denominador garantista aplicable a toda la órbita occidental.

Entonces, ese mínimo común, nos sirve para proyectar el objetivo de este acápite: establecer los principios que los Estados en el ejercicio de la persecución de delitos no deben violar, especialmente a propósito de la investigación de los delitos en Internet; y qué principios deben regir la persecución de los delitos cometidos a propósito de la intervención en las telecomunicaciones vía Internet.

¹⁹⁵ CONSEJO DE EUROPA. 1950. Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. 4 noviembre 1950. [en línea] <<http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/SpanishEspagnol.pdf>> [consulta: 22 de enero 2007].

CAPÍTULO III

LA ILEGALIDAD DE LA INTERVENCIÓN EN LAS TELECOMUNICACIONES POR PARTE DE AGENTES DE ESTADO EXTRANJERO

“...Los Estados Unidos son potentes y grandes.
Cuando ellos se estremecen hay un hondo temblor
que pasa por la vértebras enormes de los Andes.
Si clamáis, se oye como el rugir del león.
Ya Hugo a Grant lo dijo: Las estrellas son vuestras.
(Apenas brilla, alzándose el argentino sol
y la estrella chilena se levanta...) Sois ricos...”

RUBÉN DARÍO

Poema “a Roosevelt” , Cantos de Vida y Esperanza, 1905.

3.1. Palabras preliminares.

Estos versos de Rubén Darío, escritos hace poco más de cien años, nos ilustran, de una manera tan poética como franca, la actual situación que vivimos los ciudadanos comunes frente al tema de la intervención de nuestros correos electrónicos: la principal amenaza ante nuestro Derecho Fundamental y Humano, a la vida privada, en nuestras telecomunicaciones por Internet, es la intervención de las grandes potencias. Esta masiva intervención está detonada, ciertamente, por la llamada “guerra contra el terrorismo” impulsada de un modo protagónico por los Estados Unidos de América.

Ya en el capítulo I algo explicamos de esta actual circunstancia y nuevo orden mundial, pero ciertamente lo antedicho es una reiteración quizá necesaria, pues será uno de los presupuestos esenciales de la articulación de este capítulo. Nuestro objetivo ahora es determinar si es jurídicamente correcto que otros Estados, y en especial los Estados Unidos, revisen correspondencia electrónica sin que medie la debida autorización de los órganos jurisdiccionales

nacionales pertinentes, para efectos de una investigación con fines punitivos y penales, y para determinar ello, nos basaremos en la información vertida en los capítulos anteriores, por lo que habrá un constante referencia a lo ya andado.

En lo que concierne a la estructura y desarrollo del presente capítulo, primero revisaremos si es o no procedente que los jueces estadounidenses autoricen la intromisión en la correspondencia electrónica en virtud de la llamada Acta Patriota de los Estados Unidos. Para tales efectos, retomaremos los efectos de la ley penal, sustantiva y adjetiva, en el espacio, en razón del principio de territorialidad como regla general, y qué excepciones podría reconocer, las cuales adquieren especial relevancia ante la problemática territorial de Internet que parece irresoluta y que hace un duro contrasentido al antedicho principio de territorialidad.

Luego, dentro de esas excepciones, detallaremos el principio de jurisdicción universal como una eventual justificación y posible solución del problema, y junto a ello, determinaremos su contexto de aplicación de manera unilateral por los Estados Unidos y su improcedencia en el caso analizado, con especial énfasis a la jurisprudencia del tribunal constitucional chileno y en la Convención sobre la Cibercriminalidad.

Después, y continuando con las consecuencias de la problemática territorial de Internet, retrataremos la aplicación de técnicas criptológicas como una solución parcial y como una medida político-criminal de carácter preventivo a la intervención en las telecomunicaciones, pero que, sin embargo, no satisface la repuesta que buscamos, y que no sería sino otra cosa que un acto de resignación.

A continuación, adoptaremos una posición respecto a la legalidad de estas intromisiones en relación a los tratados internacionales que garantizan Derechos Humanos y a la Constitución de la República de Chile, dado que esos cuerpos normativos garantizan el Derecho a la vida privada, y que según la idea de superioridad normativa, tales intervenciones serían ilegales, al menos, en Chile, pese a su legalidad aparente (o quizá discutible) en los Estados Unidos.

3.2. Aplicación al problema de la ley penal en el espacio.

La extensión de Internet a casi la totalidad del planeta hace, cuanto menos, difícil establecer normas jurídicas que la ordenen, porque ningún poder legislativo nacional alcanza la extensión de la propia red y, de otra, porque su regulación a través de reglas del Derecho Internacional, exigiría la constitución de un poder o autoridad centralizada de carácter internacional, solución esta que de momento no se ve necesaria por los propios operadores, ni parece alcanzable materialmente en el corto plazo¹⁹⁶. Estas aseveraciones por supuesto que son extensivas a la problemática de aplicación de la ley penal en el espacio relacionada con la intervención de las telecomunicaciones electrónicas.

Considerando que ya hemos sentado los presupuestos de la discusión en el capítulo II, ahora corresponde realizar un ejercicio de aplicación de las teorías en la materia, al problema específico. Para eso vamos a proceder a ahondar en la toma de posición en los distintos puntos de discusión que ya se han planteado en capítulos anteriores.

¹⁹⁶ CLIMENT BARBERÁ, JUAN. 2001. La justicia penal en Internet. Territorialidad y competencias penales. En: Internet y derecho penal. Madrid, España, Consejo General del poder judicial, Editorial Lerko Print S.A. 65p

¿Dónde está Internet? o ¿dónde radica Internet? Estas respuestas han de ser, cuanto menos, ambiguas, ya que tendremos que convenir en que Internet es todos los sistemas, redes y subredes que se interconectan y cada uno de estos sistemas es de distintos titulares, con sus propias reglas jurídicas; del mismo modo que tendríamos que responder que Internet está en cada acceso, proveedor de servicio y en definitiva en cada máquina que interviene en el sistema y en todas ellas a la vez, de tal modo que los criterios de regulación territorial aplicables al conjunto del sistema no resultan viables, pese a los esfuerzos, infructuosos de momento, por alcanzar la regulación de la red de redes por parte de los distintos poderes públicos nacionales¹⁹⁷.

Para comenzar, en el contexto del principio de territorialidad de la ley penal, acerca de la problemática del lugar en que se entiende cometido el delito, con sus innegables repercusiones en aspectos penales materiales y procesales, adoptamos la teoría de la ubicuidad. En primer lugar, con fundamento en los argumentos ya señalados¹⁹⁸, y además considerando como elemento central la titularidad del derecho al secreto de las comunicaciones que asiste tanto al emisor como receptor de la comunicación. Desde otra perspectiva, nos parece de menor relevancia para el problema en cuestión la sujeción estricta a las teorías penales desarrolladas en el contexto de esta discusión, en comparación con razones de justicia de primer orden que representa la adecuada tutela de los Derechos Humanos fundamentales. Por otra lado, estamos contestes en las características técnicas propias de Internet, en el sentido de albergar un peligro inmanente para el derecho al secreto de las comunicaciones, es por esto, que nos parece de suma relevancia no escatimar esfuerzos para, jurídicamente, buscar una fórmula que otorgue una adecuada tutela, sin importar, primordialmente, las discusiones teóricas, es más, la

¹⁹⁷ Ídem.

¹⁹⁸ Ver capítulo II, acápite 2.3.1.1., número 3.

doctrina y la legislación deberían ampliar el desarrollo teórico considerando estas hipótesis de intervención de las telecomunicaciones electrónicas.

El Derecho ha de dar cumplida respuesta a las modificaciones de las relaciones sociales que constantemente se vienen produciendo a consecuencia de la innovación tecnológica, pues de lo contrario no cumpliría su papel de regulador de las relaciones sociales y comenzaría un peligroso alejamiento del propio colectivo social del que se deriva, y a la vez que regula y conforma¹⁹⁹.

El peso de la territorialidad del Derecho penal choca, pues, frontalmente, al menos en el terreno de los principios, con las características propias de Internet, de entre las cuales cabe destacar, lo que podría llamarse, la aterritorialidad connatural de la red de redes, atendido lo peculiar del propio contexto del llamado ciberespacio, que se crea y soporta por Internet²⁰⁰.

En lo que respecta a la aplicación extraterritorial de la ley penal hemos concluido anteriormente que, a nuestro parecer, la situación fáctica de intervención de las telecomunicaciones electrónicas escapa al principio de aplicación territorial por los argumentos ya señalados con antelación²⁰¹. No obstante, para profundizar en la materia, debemos proceder a analizar el tema desde dos perspectivas, primero en cuanto a la aplicación extraterritorial de la ley penal nacional para otorgar una adecuada tutela al secreto de las comunicaciones; y segundo desde la aplicación extraterritorial de la USAPA, que de entre sus características cabe destacar, para estos efectos, su pretensión de “justicia universal” justificante, en su lógica, de una intervención indiscriminada en las telecomunicaciones de todos los ciudadanos del orbe.

¹⁹⁹ CLIMENT BARBERÁ. Op.cit. 652p.

²⁰⁰ Ibid. 656p

²⁰¹ Ver también capítulo II, acápite 2.3.1.2.

Desde la primera perspectiva, en aplicación del principio de universalidad, propugnamos la aplicación extraterritorial de la ley penal nacional, tanto en sus aspectos materiales y procesales, en lo que guarda primordial importancia la posibilidad de persecución penal de los delitos cometidos por agentes de Estado extranjeros, en conculcación del derecho al secreto en las comunicaciones, por la jurisdicción de cualquier país, sin importar el lugar de su comisión. El delito es de aquellos que requiere, por su naturaleza, de la cooperación internacional, para su enjuiciamiento penal eficaz. La discusión de la soberanía debe ceder frente a intereses superiores de justicia mundial. En razón de todo esto es que afirmamos, en su oportunidad, la anhelada efectiva universalización del Derecho penal, al menos en cuanto a la persecución de los delitos que tratamos, para hacer frente a las nuevas formas delictivas que permite el avance tecnológico. Todo esto con la importante salvedad de preferir en primer lugar la creación de un Derecho Internacional Penal de Internet y la implementación de un órgano jurisdiccional supranacional que le sea accesorio.

Se trata de modelar instituciones jurídico-penales adaptables a la realidad dinámica de Internet. Ello comporta dos alternativas posibles: en primer lugar, la configuración tipos delictivos de Internet desde una ley penal internacional y encomendar su enjuiciamiento a órganos jurisdiccionales penales internacionales idóneos, cuya existencia o no, estudiaremos posteriormente. En segundo lugar, mantener la configuración tipos delictivos de Internet desde una ley penal internacional, y encomendar el enjuiciamiento de estos delitos a las jurisdicciones propias de los distintos Estados.

Las ventajas de la primera de las alternativas, delitos y jueces penales internacionales para Internet, son patentes desde el punto de vista de la seguridad jurídica, el decaimiento de la impunidad de Internet y de la

superación de los problemas a territorialidad de la red. Sin embargo, aunque los inconvenientes no se vislumbran más allá de los conflictos con las jurisdicciones nacionales, la viabilidad de esta alternativa no parece posible a corto plazo, ello por dos razones, la primera porque para la validez del sistema sería necesario que la totalidad de los Estados adoptarán el sistema, sin que quedaran territorios fuera del mismo a modo de paraísos penales de Internet; la segunda, porque aún cuando se consiguiera esta unanimidad respecto de la configuración de los delitos de Internet, no parece viable la constitución de órganos jurisdiccionales internacionales penales específicos para estos, a la vista de las dificultades que ha tenido el funcionamiento del Tribunal penal internacional para los delitos contra la humanidad, situación de suma relevancia que basta con ilustrar con la no ratificación aún del Tratado de Roma, por nuestro país y Estados Unidos, por citar algunos ejemplos²⁰².

En la segunda perspectiva, rechazamos la aplicación de las disposiciones de la USAPA con afanes extraterritoriales amparada en una pretensión unilateral de “jurisdicción universal”. En primer lugar basado en las argumentaciones de Derecho, otorgadas en el capítulo II, respecto al valor de la ley penal extranjera en Chile²⁰³.

Dicha legislación norteamericana responde a la idea que una mayor información supone necesariamente una mayor seguridad, y que dadas las actuales circunstancias internacionales, ésta debe prevalecer frente a los principios fundamentales de libertad e intimidad. A tal efecto, modifica numerosas leyes relativas a la congelación de fondos, secreto bancario entradas y registros en domicilios, intervención en las comunicaciones etc.

²⁰² CLIMENT BARBERÁ. Op.cit., pp. 659-660.

²⁰³ Ver capítulo II, acápite 2.4.

Dispone dicha ley, en lo que a Internet afecta y señalándolo de manera esquemática:

- 1) La equiparación de las comunicaciones por Internet a las comunicaciones tradicionales (por teléfono, etc.) reconociendo el desarrollo experimentado por las primeras y la necesidad de su regulación (sección 216).
- 2) Que cuando haya sospechas de actividad terrorista, las comunicaciones realizadas por Internet (al igual que el resto de las comunicaciones), podrán ser vigiladas con una única orden judicial federal para todo el territorio de Estados Unidos. Ello evita al FBI, la CIA o cualquier otra agencia de seguridad, tener que pedir una orden para cada estado y cada domicilio. Hasta ahora las órdenes judiciales sólo tenían eficacia dentro del territorio de la jurisdicción del juez autorizante (sección 216).
- 3) Además, un único permiso judicial permitirá intervenir todos aquellos teléfonos o direcciones de correo electrónico que puedan ser usados por un sospechoso de actividades terroristas.
- 4) Una sola orden judicial obligará a los proveedores de Internet a facilitar la dirección asignada por dicho proveedor al cliente, la dirección desde la que el cliente se conecte con el proveedor, cómo realiza el cliente el pago y cualquier otra información requerida (secciones 210 y 211).
- 5) Permite, además, a las empresas proveedoras de Internet revelar cuanta información tenga de un cliente cuando aprecien un riesgo inmediato de muerte o lesiones graves para las personas (sección 212).
- 6) Se tipifica el ciberterrorismo, definiendo al *hacker* como aquél que tiene la intención de provocar un daño, que será cualquier deterioro

de la integridad o disponibilidad de datos, programas o sistemas, y siendo indiferente la cuantía del daño causado, la cual solo afecta la pena.

- 7) Se incrementan notablemente las penas a los *hackers*: si atacan ordenadores protegidos (los de la defensa nacional, seguridad nacional, administración de justicia penal, comercio interestatal o con el extranjero o comunicaciones de los Estados Unidos) sean norteamericanos o de los países extranjeros, y cualquiera que sea la cuantía del daño causado, serán condenados a penas de hasta diez años de prisión cuando sea la primera condena, y hasta veinte años cuando haya reincidencia; en ataques a otros ordenadores, cuando éstos supongan pérdidas superiores a cinco mil dólares, se les impondrán penas de hasta cinco años de prisión (sección 814)²⁰⁴.

Luego, basta con recordar para ilustrar la amenaza, que según los criterios ya señalados con que trabajan las Agencias internacionales de Seguridad y la capacidad técnica que disponen, cualquier ciudadano o persona jurídica del mundo que se comuniquen a través de la red, pueden ser objeto de intervención. Fundada exclusivamente en criterios cuyo contenido son conceptos de derecho indeterminado, tales como la seguridad nacional o el orden público, que dependen directamente de la concepción que de ellos tengan las autoridades en el poder.

Por otro lado, la aplicación del principio de universalidad dispone justamente, entre otras cosas, que una de las labores de la comunidad internacional es superponer los Derechos Humanos fundamentales y los

²⁰⁴ PERARNAU MOYA, JOÁN. 2001. Internet amenazada. En: Internet y derecho penal. Madrid, España, Consejo General del poder judicial. Editorial Lerko Print S.A. pp 137-138.

intereses de la comunidad internacional de justicia sobre los intereses políticos, en este caso, de determinados Estados.

En última instancia, el criterio esencial que debe guiar la aplicación de la ley penal en el espacio es aquél que posibilite de la mejor manera posible el enjuiciamiento de las conductas atentatorias de los Derechos Humanos fundamentales, sin importar de quien provengan y el respeto irrestricto de las teorías jurídicas existentes. Dicho de otro modo, el Derecho por razones de justicia, libertad y dignidad debe oponerse a aquello que conculque derechos humanos y permitir el tratamiento penal de los delitos atentatorios de éstos, sin importar primordialmente el contenido de las teorías jurídicas en la materia, y en caso de inconcordancia de éstas la doctrina es la que debe adecuarse.

3.2.1. Primera hipótesis de solución: principio de jurisdicción universal.

A continuación, y como ya hemos venido esbozando, urge analizar una primera propuesta de solución a la intervención de las telecomunicaciones electrónicas realizadas por agentes de Estado extranjero, que dice relación con la implementación o validación de un sistema supranacional que contenga tipos penales y un órgano jurisdiccional especialmente destinados para dicho efecto. En definitiva, proponemos de *lege ferenda* la creación de la institucionalidad jurídico-penal pertinente, para el adecuado tratamiento de estas conductas criminales. Se trata de, en este sentido, interpretar y aplicar en la práctica el principio de universalidad ampliamente abordado a lo largo de ésta monografía.

Para tales propósitos, procederemos primero a analizar en lo pertinente el fallo del Tribunal Constitucional chileno, de características conservadoras, acerca del recurso de inaplicabilidad por inconstitucionalidad, presentado por un grupo de parlamentarios, con ocasión de la ratificación del tratado de Roma,

que dio origen al Tribunal Penal Internacional, de fecha ocho de abril de dos mil dos²⁰⁵.

En esa ocasión dicho órgano jurisdiccional falló acogiendo la petición de los parlamentarios, declarando la inconstitucionalidad del tratado, primordialmente fundado en:

“19°. Que, la naturaleza jurídica de la jurisdicción de la Corte Penal Internacional, de acuerdo al Preámbulo del Estatuto y al artículo 1º, transcritos en los considerandos 13º y 17º, es penal y complementaria de las jurisdicciones nacionales, pero, a juicio de los requirentes, aparece más bien como paralela o contradictoria a ellas;

20°. Que, un estudio del Tratado por el que se establece la Corte Penal Internacional nos lleva a la conclusión que dicho Estatuto no definió el significado del carácter complementario de la jurisdicción que se crea;

24°. Que, de un estudio de lo sustantivo o esencial de las disposiciones del Estatuto que se transcriben a continuación, resulta evidente que la Corte puede corregir lo resuelto por los tribunales nacionales de los Estados Partes, pudiendo, en consecuencia, decidir en contra de lo obrado por ellos y, en determinadas situaciones, de ausencia real o formal de dichos tribunales nacionales, sustituirlos;

35°. Que, la naturaleza jurídica de la jurisdicción de la Corte Penal Internacional atentaría por ello contra el principio de "soberanía nacional" establecido en el artículo 5º, del Capítulo I, de nuestra Constitución Política.

Dice este artículo:

²⁰⁵ TRIBUNAL CONSTITUCIONAL. 2002. Fallo sobre Tribunal Penal Internacional. [en línea], Revista "Ius et Praxis", v.8, nº 1, Talca, Chile. <www.scielo.cl> [consulta: 14 Octubre 2006].

"Artículo 5º. La soberanía reside esencialmente en la Nación. Su ejercicio se realiza por el pueblo a través del plebiscito y de elecciones periódicas y, también, por las autoridades que esta Constitución establece. Ningún sector del pueblo ni individuo alguno puede atribuirse su ejercicio.

El ejercicio de la soberanía reconoce como limitación el respeto a los derechos esenciales que emanan de la naturaleza humana. Es deber de los órganos del Estado respetar y promover tales derechos, garantizados por esta Constitución, así como por los tratados internacionales ratificados por Chile y que se encuentren vigentes.";

45º. Que, como la función jurisdicción es expresión del ejercicio de la soberanía, sólo la pueden cumplir las autoridades que la Constitución establece. El mandato de su artículo 5º, inciso primero, no admite dudas sobre el particular, sea que las autoridades jurisdiccionales a que alude se encuentren dentro o fuera del "Poder Judicial". De esta manera, a la Corte Penal Internacional el tratado, precisamente, le otorga jurisdicción para eventualmente conocer de conflictos ocurridos dentro del territorio de la República, y que deberían ser de competencia de algún tribunal nacional. Este específico reconocimiento de potestad jurisdiccional para ser ejercida por una autoridad no establecida por nuestra Carta, entra en frontal colisión con la norma recordada, por lo que hace evidente su inconcialibilidad;

58º. Que, en síntesis, el incorporar a un tribunal de justicia con competencia para resolver conflictos actualmente sometidos a la jurisdicción chilena, e incluirlo entre las "autoridades que esta Constitución establece", en concordancia con el artículo 74, ya citado, debe necesariamente ser autorizado por el Constituyente.

En consecuencia, para que la Corte Penal Internacional sea un tribunal establecido para juzgar delitos cometidos en Chile, debe incorporarse al sistema interno mediante una adecuación constitucional;”.

En suma, el tribunal declara inconstitucional el tratado de Roma por atentar contra el principio de soberanía reconocido por el constituyente en la Carta fundamental nacional vigente y declara la necesidad de una adecuación constitucional que posibilite su incorporación al marco jurídico nacional.

Por otro lado, para los demás tratados atinentes la suerte es similar, ninguno de los cuerpos normativos supranacionales que dan tratamiento sustantivo en la materia ha sido suscrito y ratificado por el Estado de Chile. Desde la propuesta de la elaboración de un sistema internacional penal la ratificación unánime por todos los Estados es esencial. Para ilustrar esto a continuación escogemos revisar el Convenio sobre Cibercriminalidad²⁰⁶ que en la actualidad “constituye sin duda el esfuerzo internacional más importante en contra de las actividades criminales cometidas a través de medios informáticos”²⁰⁷.

Esta convención, cuya elaboración tomó más de cuatro años, tiene como objetivos fundamentales los siguientes: (1) armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático; (2) proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de tales conductas delictivas; y (3) establecer un régimen dinámico y efectivo de cooperación internacional²⁰⁸. En especial nos

²⁰⁶ Convenio sobre Cibercriminalidad, 23.XI.2001Budapest. [en línea] <www.interpol.int/Public/TechnologyCrime/> [consulta: 20 septiembre 2006].

²⁰⁷ MUÑOZ ESQUIVEL, OLIVER. 2002. La Convención sobre delitos informáticos. [en línea] Revista de derecho Informático Alfa-Redi, (42). <www.alfa-redi.org> [consulta: 20 septiembre 2006].

²⁰⁸ Ídem.

gustaría destacar el artículo 3º, sección 1, capítulo II, que tipifica la “interceptación ilícita”, señalando: “Las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la interceptación, dolosa y sin autorización, cometida a través de medios técnicos de datos informáticos- en transmisiones no públicas- en el destino, origen o en el interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos. Las partes podrán exigir que la infracción sea cometida con una intención delictiva o también podrá requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático”.

Considerando el contenido del artículo citado, no se puede más que concluir que estamos en presencia de otro argumento para fundar nuestro rechazo por la pretensión unilateral de facto de “jurisdicción universal” contenida en la USAPA; puesto que Estados Unidos ha suscrito y ratificado este convenio y no puede, en extensión, desconocer su suscripción a un sistema internacional penal, al menos, en su aspecto sustantivo. Para conservar esta lógica es que debe adecuarse a un sistema procesal internacional que le sea complementario.

Debemos realizar una salvedad, el presente análisis del Convenio sobre la cibercriminalidad solamente implica nuestra adscripción a la hipótesis de solución en torno al principio de jurisdicción universal, pero en ningún caso, nos obsta ha señalar las flagrantes violaciones contra los Derechos Humanos fundamentales que contiene en sus disposiciones. Para ello adoptamos las

críticas que realiza la organización no gubernamental TREATY WATCH²⁰⁹, de entre las cuales destacamos:

- 1) El convenio carece de protección a la privacidad y las libertades civiles; de hecho la palabra “privacidad” no aparece en su articulado ninguna sola vez. Requiere de cooperación de los proveedores de servicios de Internet para la búsqueda y adquisición de información sin requerirse de la policía, para que se haga responsable del procedimiento. No solamente establece una carga injusta sobre los proveedores sino que permite la libre intervención de las agencias de inteligencia, motivando el uso de este poder indiscriminadamente, violando el principio de control de las autoridades, propio de un Estado de derecho democrático.
- 2) El convenio otorgaría nuevas facultades de intervención policiales; el tratado permitiría autorizar a los Estados contratantes dispositivos de intervención como *Carnivore*, con las consecuencias nefastas contra los Derechos Humanos fundamentales ya conocidas.

De tal forma, en nuestro ordenamiento jurídico no existe, en la actualidad, el reconocimiento de los tipos penales ni del órgano jurisdiccional para la implementación de un sistema penal eficaz que dé tratamiento integral, oportuno y garantista a las conductas de intervención indiscriminada en la red. Pero, a su vez, consideramos que las razones de soberanía argüidas por el Tribunal Constitucional no son “de peso” para que a futuro se someta el asunto a nueva discusión y se reconozca un sistema internacional penal para el tratamiento de la intervención indiscriminada de las telecomunicaciones

²⁰⁹ TREATY WATCH. *Eight reasons the International Cybercrime treaty should be rejected* [en línea] <www.treatywatch.org/about.html> [consulta: 20 septiembre 2006].

electrónicas, puesto que, en primer lugar, la naturaleza misma del recurso de inaplicabilidad no impide a que se someta de nuevo a discusión tal tema; segundo, el mismo artículo 5º en su último inciso reconoce como límite del ejercicio de la soberanía el respeto de los derechos esenciales que emanan de la naturaleza humana y también ahonda en el deber del Estado de respetar y promover tales derechos reconocidos por el ordenamiento jurídico nacional. Claramente permitir de la manera mejor posible el enjuiciamiento de las conductas atentatorias de los Derechos Humanos fundamentales, es expresión de estos mandatos y el ejercicio de la soberanía, un concepto jurídico indeterminado que muta en tanto la realidad social se modifique, no debe ser obstáculo para la adecuada protección de los Derechos Humanos; por último, y en lo que a hermeneútica legal se refiere, hacemos eco con la posición de minoría del ministro LIBEDINSKY²¹⁰.

Concluimos en que jurídicamente nada obsta a que a futuro esta realidad cambie y se creen, modifiquen los ya existentes, y ratifiquen los tratados necesarios para la configuración de un sistema internacional penal de Internet, por otro lado, concordamos con las razones de no viabilidad a corto plazo de CLIMENT BARBERÁ, pero las consideramos dificultades de orden político y que por ende son solucionables por dicha vía, ajena a los principios jurídicos que en nada obstan a la creación de un sistema penal tal.

Aplicando lo extraído a la pretensión unilateral de “jurisdicción universal” de Estados Unidos contenida en la USAPA, deberían aplicarse a ella las mismas razones jurídicas y políticas esgrimidas para rechazarla, y así declarar inaplicable dicha ley penal norteamericana en nuestro país y respecto nuestros ciudadanos. Sin embargo, alguien podría argumentar que nosotros mismos nos hemos encargado de desestimar tales razones y que propondríamos contra nuestras intenciones dicha aplicación, no obstante, para desvirtuar un

²¹⁰ Ídem.

argumento en tal sentido debemos agregar que la pretensión unilateral de la legislación norteamericana se hace con franco atentado de los Derechos Humanos fundamentales, pues autoriza, entre muchas cosas, la intervención indiscriminada de las telecomunicaciones en contra del derecho al secreto de las comunicaciones. En razón de esto y como hemos venido repitiendo, los Derechos humanos son la guía en última instancia de cualquier Estado de Derecho democrático, y no se puede aplicar normativa alguna que atente contra ellos. Es decir, ambas situaciones no pueden homologarse por razones de justicia superiores a cualquier otro criterio político o jurídico aplicable.

En suma, rechazamos la pretensión norteamericana unilateral de facto de “jurisdicción universal” contenida en la USAPA, por las razones políticas, jurídicas y de justicia superior, en último término, aludidas. Que a la actualidad se incrementan preocupantemente, de hecho, la tercera USAPA (2006) contempla la posibilidad de que cualquier soldado norteamericano pueda detener a un sospechoso de terrorismo en cualquier lugar del mundo, otra demostración de las aberraciones jurídicas que puede alcanzar el desquiciamiento del “tío Sam”.

Recientemente nos hemos referido a razones políticas que obstan la posibilidad de solución a la problemática de Internet, en torno a la intervención indiscriminada de las comunicaciones por parte de agentes de Estado extranjero, sin embargo, también existen otras razones con el mismo efecto de orden técnico, económico etc. que en los siguientes acápite procederemos a revisar.

3.3. Sobre la problemática territorial de Internet en disonancia con el principio de territorialidad del Derecho penal.

Ya latamente hemos discurrido sobre el principio de territorialidad y sobre sus excepciones, y sobre la improcedencia del principio de jurisdicción universal unilateral impulsado por los Estados Unidos con la USAPA. Ahora bien, sería bueno explicitar en que medida la rúbrica desmedida y transfronteriza de la red Internet teje un grueso contrapunto en relación a la protección de los Derechos Fundamentales y Humanos para las posibilidades fácticas de su resguardo.

Frente a los problemas fácticos de resguardo, huelga enfatizar medidas político-criminales preventivas que un usuario común puede utilizar, y en especial, haremos referencia especial a la criptología. Además, en este mismo sentido, haremos referencia a los problemas políticos que determinan trabas legales en su tratamiento legal en Estados Unidos.

3.3.1. El carácter transfronterizo de la red como elemento determinante de la problemática en cuestión.

Ya revisamos en el acápite 1.1.2.2. del capítulo primero que dos de las principales características de la Internet son ser una red globalizada y descentralizada, lo que a su vez determina su rúbrica transfronteriza, finalmente desencadenando en que no haya una jurisdicción nacional aplicable. Al convertirse la red en esta afortuna “tierra de nadie”, sólo aquel que disponga de mayores recursos y tecnología informática y telemática podrá influir decisivamente en ella. Así, podemos verificar la intervención en nuestros correos electrónicos, realizada por los Estados Unidos, con la red ECHELON y con el programa *Carnivore* de la CIA. También hay que agregar a esto que la bullada USAPA permite la intervención de los correos electrónicos siempre que un juez norteamericano lo autorice.

Esta desbocada intervención es claramente atentatoria a los Derechos Fundamentales y Humanos ya explicitados en el acápite 1.2.2. del capítulo primero, que es el Derecho a la vida privada, a la inviolabilidad del hogar y de la correspondencia, consagrada en el artículo 12 de la Declaración Universal de Derechos Humanos, en el artículo 17 del Pacto de Derechos civiles y Políticos de 1966, en el artículo 11 de la Convención Interamericana sobre Derechos Humanos o Pacto de San José de Costa Rica, en el 19 n° 4 y n° 5 de la Constitución Política de la República de Chile. Estos mismos derechos tienen un correlato en la ley penal en el artículo 161 A del Código Penal chileno.

Ahora bien, en atención a las normas procesales, y en relación a los principios comunes a todo el continente americano que expone el profesor TAVOLARI²¹¹ y que comparamos con los reconocidos en el Convenio Europeo para la protección de los Derechos humanos y de las libertades fundamentales, extrajimos los posibles principios procesales comúnmente aceptados en buena parte de la órbita occidental en el acápite 2.6.3.1. Esos principios, con la intervención de los Estados Unidos en virtud de la USAPA se ven vulnerados, en especial atención, los principios del Derecho a la defensa, el Derecho a ser oído, y el Derecho a la igualdad procesal.

En relación a estas normas y principios antedichos, la intervención antedicha sería claramente ilegal en función al derecho sustantivo general, lo que redundaría en que como estudiantes de Derecho, que creen en un mundo donde se respeten los Derechos Humanos, y quizá aún corriendo el riesgo de parecer pueriles e idealistas, no deberíamos hacer otra cosa sino repudiar dicha intervención.

²¹¹ Ver capítulo II, sub-acápite 2.6.1.

Pese a ello, el fenómeno del poder determina quién puede actuar y con qué posibilidades fácticas, mas justamente de ahí dimana la aspiración del Derecho de ser una disciplina cuya finalidad es la reducción de la barbarie humana limitando el poder de quién lo detentare. Sin embargo, frente a las flagrantes vulneraciones vistas, nos da la impresión de que la red, para estos efectos, se ha convertido en un verdadero espacio donde prima la voluntad de quién es más poderoso, en este caso los Estados Unidos mediante la ejecución de su política contra el terrorismo.

Pese a ello, la protección a que aspiramos es discutida, pues la intervención en los correos electrónicos es considerada por JIJENA LEIVA como algo que no es siempre digno de la tutela del derecho a la inviolabilidad de la correspondencia, en el sentido de que el administrador del correo tendría siempre acceso a revisar su contenido y sería como una simple tarjeta postal, salvo que el mensaje se enviara encriptado²¹² (la encriptación la revisaremos en el acápite siguiente). Para nosotros, esa no es la postura adecuada para tratar el problema, pues si bien todo administrador puede revisar los correos, no quiere decir que todo internauta los pueda revisar libremente como un postal. El acuerdo de privacidad dependerá de cada usuario con su administrador en el contrato de prestación servicio de correos, en el cual lamentable y normalmente el usuario no dispondrá de ese derecho frente al administrador por ser un contrato de adhesión. Con todo, el hecho que exista una clave para ingresar al correo da un ámbito protegido frente a todos lo demás internautas y frente a eventuales intrusos, ergo, el correo electrónico no tendría el estatus de un mera postal, empero sea fácilmente vulnerable y en los contratos de prestación de servicio de correo electrónico se atente. En este sentido PERARNAU MOYA

²¹² JIJENA LEIVA, RENATO. Sobre la Confidencialidad e Inviolabilidad de los Correos Electrónicos. [en línea] <<http://www.ecampus.cl/ecampus/home/htm/Textos/derecho/jijena/1/jijena1.htm>> [consulta: 3 noviembre 2006].

nos ilustra la situación de una manera pesimista, citando a ALVAREZ MARAÑÓN: "...a estas alturas, ya sabrá que en Internet no existe nada parecido la privacidad..."²¹³. En fin, si no es porque renunciamos a este derecho por la suscripción del servicio de correo, aquél se verá vulnerado eventualmente por la posibilidad técnica de que un tercero lo pueda interceptar y leer.

Frente a tan desafiante y complejo panorama... ¿Cómo podríamos nosotros, los ciudadanos chilenos, resguardar nuestro derecho a la vida privada y a la inviolabilidad de la correspondencia? La respuesta *ex post* y en sede judicial intentará ser la respuesta del capítulo siguiente. Sin perjuicio de ello, en el siguiente acápite denotaremos lo que *ex ante* puede hacer un ciudadano común para proteger su privacidad en base a las herramientas que nos ofrece la red. En extensión de esto, cabe recordar que dentro de las características de la red está la de ser controlada por los usuarios y la de ser abierta, lo que le confiere una profusa vocación para promover la democracia y reducir asimetrías de información, y finalmente, darnos armas de defensa ante esta invasión a nuestra vida privada.

3.3.2. La criptografía como una medida político-criminal de carácter preventivo frente a la intervención en las telecomunicaciones vía correo electrónico.

Ya en el acápite 1.1.4. explicamos algo en relación a la criptografía, o criptología, como un medio de asegurar la confidencialidad de un mensaje de correo a propósito de la firma electrónica como medio de autenticación del usuario emisor y de integridad del mensaje enviado. La criptología, es entonces,

²¹³ ALVAREZ MARAÑÓN, GONZALO. 2000. De Incógnito por Internet. PC World (168). 2000, España. Cit. por PERARNAU MOYA, JOÁN. Op. Cit. 137p.

una disciplina que busca el cifrado de mensajes para evitar que estos sean conocidos por todos mediante una clave o método de ocultamiento de la información contenida en el documento.

Esto adquiere vitalísima importancia frente al cómo evitar la intervención en las telecomunicaciones, dado que resulta obvio que en la medida que se pueden ocultar los mensajes nos aseguramos de que sean confidenciales. Aún cuando ya explicamos que no concordamos con lo que expone JIJENA LEIVA, afirma algo que es correcto y que es completamente rescatable: un mensaje encriptado no podrá ser interceptado (o interceptado con la misma facilidad) que un mensaje que no detente tal protección. Aún así cabe hacer un reparo: "... No existe un solo algoritmo criptográfico que sea inviolable. Incluso, si no hay manera de efectuar ataques criptoanalíticos, cualquier sistema de claves puede "reventarse" mediante el sencillo sistema de probar todas las claves posibles..."²¹⁴. Con todo, la criptografía es lo mejor que disponemos y es una herramienta que podemos utilizar para custodiar nuestra privacidad. En este sentido SANCHEZ ALMEIDA, con gran entusiasmo, dice "...Tenemos derecho a que nadie pueda leer lo que pensamos, a conspirar incluso. Ninguna revolución, ninguna declaración de derechos humanos hubiese sido posible, si el pensamiento disidente hubiese sido monitorizado desde el poder. Lejos del fin de la historia que abanderan los apóstoles del pensamiento único, hemos de reivindicar la criptografía como herramienta al servicio de la libertad. Necesitamos una trinchera frente al Gran Hermano, desde la que defender la esperanza de un mundo mejor. Un mundo en el que quepan todos los mundos."²¹⁵. También, GONZÁLEZ NAVARRO en el mismo sentido, y dando paso a lo que trataremos en seguida, asevera que "...las patologías propias de

²¹⁴ DÍAZ LEVANO y PERAZA DARVE. Op cit.

²¹⁵ SÁNCHEZ ALMEIDA, CARLOS. 2000. La Criptografía como Derecho. [en línea] Revista de Derecho Informático Alfa-Redi. <<http://www.alfa-redi.org/rdi-articulo.shtml?x=487>> [consulta: 3 noviembre 2006].

Internet disponen, por tanto, de un instrumento eficaz en la lucha contra los gobiernos, colectivos y asociaciones preocupados por los contenidos de la Red. El siguiente paso es evidente: restringir en la medida de lo posible la criptografía. Pero, y he ahí, el conflicto, la seguridad lleva aparejada la lesión al derecho del ciudadano a la privacidad, pues privacidad es en definitiva la esencia de la criptografía.²¹⁶

La criptografía como derecho no parecería ser una afirmación tan exagerada, siendo que es el medio protección a la vida privada más accesible y efectivo en las comunicaciones vía correo electrónico en la Internet. Pero tras la circulación comercial de los programas criptográficos hay un trasfondo político que empalma con la cuestión inicial de este acápite: la necesidad de hegemonía, en función de la llamada seguridad nacional, de los Estados Unidos. No todo es tan favorable, pues según ya lo decía GONZÁLEZ NAVARRO en la cita anterior, hay un problema político subyacente.

Básicamente, el problema del control y supervigilancia estatal para vulnerar los programas criptográficos que desarrollen sus empresas, y poder así tener un control sobre las telecomunicaciones, en los Estados Unidos deviene del primer gobierno Bill Clinton, cuando en 1993, y mediante la *National Security Agency* (en adelante N.S.A.), se pretendió crear un depósito “de llaves maestras” de sistemas criptográficos llamado *Key Escrow*, donde las llaves se depositarían en comisiones de confianza llamadas en inglés *Trusted Third Parties* (desde ahora T.T.P.'s). El sistema fracasó porque nadie quería confiar el secreto de su negocio a una entidad estatal, y la razón es obvia: el éxito de un sistema criptográfica radica en que no pueda ser descifrado, y si se le otorga al Estado la posibilidad de descifrarlo discrecionalmente, ese negocio no sería tan

²¹⁶ GONZÁLEZ NAVARRO. Op. cit. 161p.

rentable como se proyectó, lo que finalmente desencadena en un fuerte desincentivo a la inversión en ese giro.

El gobierno estadounidense, pese a ello, perseveró en sus intenciones de una manera más astuta, y estableció un sistema de incentivos económicos para las empresas que desarrollaren *softwares* de criptografía. Este consistía en otorgar licencias de exportación y licencias gubernamentales a cambio de las llaves maestras, que se almacenarían en el Key Recovery²¹⁷ (el nuevo nombre que se le dio al Key Escrow, que también funcionaría sobre las T.T.P.'s). Esto, sumado a la función de consejería que ejercen sobre la N.S.A, otros entes gubernamentales como *Bureau of Export Administration* (B.X.A.), que se encarga de la supervisión de las exportaciones de bienes y servicios norteamericanos, y que también ejerce sobre ella *The National Institute of Standards and Technology* (N.I.S.T.), que desarrolla normas técnicas aplicables a la industria y los servicios de las nuevas tecnologías de la información y de las telecomunicaciones. Esta intervención gubernamental apunta a la restricción en la comercialización de la criptografía masiva y avanzada fuera de los Estados Unidos, y también dentro de ella. Al respecto, GONZÁLEZ NAVARRO, asevera que "...el uso de las versiones americanas fuera de las fronteras se considera un delito muy grave, equiparable al tráfico de armas. En efecto, el carácter práctico y poco dado a la sutileza de los norteamericanos ha permitido el uso libre de una criptografía de grado medio para su exportación, en el sentido de algoritmos que usen claves relativamente cortas, restringiendo sin embargo con carácter general la encriptación fuerte..."²¹⁸

La consecuencia de lo antedicho es inteligible: los Estados Unidos sostienen una preocupación muy marcada respecto a la intervención en las

²¹⁷ Ibid. 172p.

²¹⁸ Ibid. 158p.

telecomunicaciones, y para ello son capaces de colocar obstáculos al comercio de software criptográfico. Como ya explicamos, buena parte de este afán viene determinado por la llamada guerra contra el terrorismo, y otro motivo, quizá presunto, de esta intervención, es la obtención de información económica estratégica, lo que podría derivar en la adopción de medidas proteccionistas implícitas para el comercio de Estados Unidos, así, lo denuncia COSTA al explicitar los fines que, al menos, guarda el sistema “Hortensia III” para espionaje corporativo en Europa²¹⁹. De ello nada nos asegura que no hubiere usado a Echelon para intervenir asuntos corporativos revelando información relevante y confidencial. Así, podemos concluir que hay más intereses comprometidos que la sola seguridad nacional.

Finalmente, también concluimos que la criptografía sería una medida político-criminal de carácter preventivo, parcial, respecto de la intervención foránea, ya fuera por una intervención amparada por la USAPA ya fuera frente a cualquier intervención en general, y por lo tanto, parece sensato utilizar métodos sencillos de criptografía disponibles en la red Internet, incluso gratuitamente. También sería bueno tomar en cuenta los consejos de PERARNAU MOYA para hacer nuestra navegación en Internet más segura y no exponernos innecesariamente a que nuestra privacidad sea violentada. Esos consejos, *a grosso modo*, son:

1.- Ser sensato y nunca entregar el nombre ni otros datos personales, salvo en compras vía Internet.

2.- Borrar periódicamente los archivos temporales y las *cookies* de la memoria de nuestro ordenador.

²¹⁹ COSTA. Op. cit.

3.- Navegar con un anonimizador, que es un software que oculta nuestro número IP frente a otros usuarios o frente a páginas que registran nuestros datos.

4.- Utilizar un programa que detecte *web bugs* y *spywares*, que serían programas que se alojan en nuestros ordenadores y que envían información sobre nuestro ordenador a otros ordenadores, ya fuere con fines de inteligencia o con fines comerciales.

5.- Instalar un cortafuego en el ordenador, de modo de evitar intromisiones indeseadas.

6.- Encriptar el correo electrónico, como ya lo explicamos antes.

7.- No ejecute programas que no hayamos registrado antes con un antivirus.

8.- Tenga siempre respaldos de la información que considere relevante²²⁰.

3.4. Reflexiones sobre la ilegalidad de la intervención en las telecomunicaciones.

Luego de desarrollar el esquema del presente capítulo, no podemos más que afirmar la ilegalidad de la intervención de las telecomunicaciones electrónicas autorizadas por la normativa de la USAPA, en contra del derecho a la inviolabilidad de las comunicaciones, concretado en el derecho al secreto de éstas, del que son titulares nuestros ciudadanos.

La revisión acerca de la aplicación de la ley penal en el espacio, avanza en tal sentido, ya que, por diversos argumentos, se determina la ilegitimidad de la pretensión de jurisdicción “universal” unilateral y de facto de los Estados Unidos. Principalmente debido a que no es conforme a Derecho pretender el

²²⁰ PERARNAU MOYA. Op. cit. pp. 142-143.

establecimiento de un sistema jurisdiccional, a espaldas del que se quiere configurar a nivel supranacional que a su vez apoya parcialmente, y lo que es más grave, contrario a los Derechos Humanos fundamentales.

En desprecio de esta pretensión se procedió al análisis de algunas hipótesis de solución. Por un lado se reflexionó acerca de la preferencia, en orden a la configuración de un sistema penal internacional adecuado para la persecución de la conducta de intervención indiscriminada en las telecomunicaciones en la red, constituido a través de tratados internacionales, que contenga los tipos penales y un órgano jurisdiccional especiales para las conductas atentatorias, provengan de privados o agentes del poder público de cualquier Estado. Apoyados en el principio de universalidad de la aplicación de la ley penal, pues consideramos, fundados en la naturaleza de los delitos y las características técnicas de Internet, que requiere para su tratamiento de la cooperación de la comunidad internacional, que debe, en todo caso, anteponer la tutela de los Derechos Humanos por sobre los intereses particulares de cualquier Estado. A pesar de nuestra intención inicial estamos contestes en las dificultades políticas, económicas y técnicas de la implementación de un sistema penal tal, por esto es que, en defecto de esta hipótesis, optamos por un tratamiento sustantivo penal supranacional apoyado en las jurisdicciones nacionales de los distintos países, que con fundamento en el principio de universalidad brinde un efectivo tratamiento penal sin importar el lugar de comisión del delito, considerando de primera relevancia la titularidad del derecho a la inviolabilidad de las comunicaciones, tanto del receptor como el emisor. Sin embargo, consideramos conforme a Derecho nuestra intención inicial y que las dificultades de otra índole son solucionables, eventualmente, por otras vías ajenas a lo jurídico.

Dentro de esta hipótesis de solución analizamos la sentencia del Tribunal Constitucional que declaró inconstitucional el tratado de Roma y el Convenio

sobre la Cibercriminalidad, instituciones, que a pesar de las críticas a cuestas, configuran un comienzo para la intención de crear un sistema internacional que persiga las conductas delictivas asociadas con la intervención indiscriminada de las comunicaciones. No ignoramos las críticas y de hecho las consideramos valiosas para que a futuro se cree un sistema eficaz y respetuoso de los Derechos Humanos fundamentales.

Luego, con ocasión del análisis de las características técnicas de la Red, su aterritorialidad y carácter transfronterizo, marcan un peligro inmanente para la protección de la privacidad de las telecomunicaciones electrónicas y por ende se convierte en “caldo de cultivo” para la intervención indiscriminada por parte de hackers y agentes de Estado. Sin embargo, el Derecho no puede claudicar en estas intenciones y mientras los esfuerzos no sean fructuosos, los ciudadanos del mundo nos encontramos indefensos frente al poder inconmensurable de las autoridades, realidad que se materializa en la actuación flagrante de las potencias en contra del derecho al secreto en las comunicaciones del que somos titulares cada uno de nosotros, albergado en las constituciones y tratados internacionales vigentes.

En el contexto de este escenario es que ensayamos otra hipótesis de solución: La criptografía o criptología. A falta de la eficacia de la heterotutela, los ciudadanos no merecemos mantenernos desprotegidos, por eso tenemos el derecho a proveernos algún medio de protección preventiva, que en este caso se traduce en la encriptación de la información que intercambiamos en los correos electrónicos. No obstante, los esfuerzos de las autoridades apuntan a dificultar estos mecanismos de seguridad, realidad que configura otro escenario de injusticia que a ningún jurista puede mantener indiferente. En suma, defendemos el derecho a la criptografía que tiene todo internauta para así hacer efectiva de algún modo su privacidad. Por ello es que en última instancia otorgamos una serie de consejos prácticos para que cualquier persona pueda

proveerse algún nivel de protección cuando haga uso de medios de comunicación electrónicos.

Pero, aún en la práctica, una pregunta clave subsiste: ¿A través de qué mecanismos jurídicos el nacional afectado en su derecho a la inviolabilidad de las telecomunicaciones electrónicas frente a la intervención por parte de un agente de Estado extranjero, puede hacerlo efectivo?. Atendiendo que las posibilidades de reacción de un sólo individuo generalmente se limitan a las instituciones de justicia nacionales. El siguiente capítulo intentará darle respuesta satisfactoria a esta interrogante.

CAPÍTULO IV.

ALTERNATIVAS DE PERSECUCIÓN PENAL NACIONALES E INTERNACIONALES

“...Al León le pareció que no estaría mal dar un susto al Mago, de modo que dejó escapar un tremendo rugido, tan feroz y espantoso que Toto saltó alarmado y fue a dar contra el biombo que había en el rincón, haciéndolo caer. Al oír el estrépito, los amigos miraron hacia allí y en seguida se sintieron profundamente asombrados al ver, en el sitio que hasta entonces ocultaba el biombo, a un viejecillo calvo y de arrugado rostro que parecía tan sorprendido como ellos...

...¿Acaso no eres un gran mago? Preguntó Dorothy. En absoluto querida. No soy más que un hombre común...”

LYMAN FRANK BAUM
El Mago de Oz,

4.1. Palabras preliminares.

La pequeña Dorothy, el espantapájaros, el leñador, y el león, creían fehacientemente que el Mago de Oz solucionaría sus problemas, pero se hallaron ante una gran decepción al enterarse que el mago no era más especial que ellos, y que poco o nada podría hacer. En un sentido parecido, ahora nos toca la oportunidad de abordar, y de manera concreta, las posibilidades de defensa en sede penal que tiene un ciudadano ordinario para resguardar su derecho a la vida privada y a la inviolabilidad de las telecomunicaciones vía correo electrónico.

La sorpresa que nos encontramos en esta dilucidación fue la muy parecida a la que se llevó esa improvisada tropa cuando vio al mago en su real magnitud: tanto fiscales, juzgados de garantía, Cortes de Apelaciones, e incluso la

mismísima Corte Suprema, poco o nada pueden hacer para protegernos de las intervenciones masivas en los correos electrónicos impulsadas por los estados extranjeros.

Para denotar la carencia que vertebra este capítulo, primero revisaremos los tipos penales afines, que son los del artículo 161 A y el del artículo 2º de la ley 19.223 sobre delitos informáticos; también se realizará una pertinente crítica de estos. En segundo lugar, se pasará revista a como operaría el proceso penal de conformidad al Código Procesal Penal, y cómo no ofrece una persecución penal afín a estas vulneraciones. A continuación, revisaremos posibilidades de defensa en el contexto internacional, con referencia a la Comisión y a la Corte Interamericana de Justicia, y pasando revista también al Convenio del Cibercrimen, aún no adoptado por Chile. Para terminar, se revisará que la posibilidad de entablar una acción de protección es muy poco viable, por lo que determinaremos que la protección de estos derechos, en el caso de la intervención masiva de los correos electrónicos, es nula.

4.2. Los tipos de la legislación chilena.

4.2.1. Generalidades.

Para iniciar un análisis en cuanto a los mecanismos jurídicos existentes a los cuales puede recurrir un nacional frente a la intervención de sus comunicaciones electrónicas privadas, con las características que hemos descrito, debemos sondear acerca de la existencia de tipos presentes en el ordenamiento jurídico nacional que lo protejan ante tal eventualidad. Dicho en otras palabras, realizaremos la búsqueda, desde una perspectiva penal material, de un tipo que nos pueda servir para combatir aquellas intervenciones que nos parecen ilegítimas, puesto que vulneran Derechos fundamentales.

Sin embargo, y previo a dicho análisis, debemos advertir que no toda intervención en las comunicaciones electrónicas es ilegítima e ilegal para nuestra ley. El propio ordenamiento jurídico nacional contempla hipótesis en que dicho procedimiento sería legal, no obstante se trata de circunstancias fácticas delimitadas por la propia ley y que a su vez, para su ejecución debe cumplirse con una especial investidura y una serie de requisitos copulativos que la misma ley contempla. Con esta aproximación estamos haciendo referencia al artículo 222 del Código Procesal Penal que dispone, en su inciso primero:

“Interceptación de las comunicaciones telefónicas. Cuando existieren fundadas sospechas, basadas en hechos determinados de que una persona hubiere cometido o participado en la preparación o comisión, o que aquélla preparare actualmente la comisión o participación en un hecho punible que mereciera pena de crimen, y la investigación lo hiciere imprescindible, el juez de garantía, a petición del ministerio público, podrá ordenar la interceptación y grabación de sus comunicaciones telefónicas o de otras formas de telecomunicación.”

A continuación el incisos siguientes restringen aún mas la medida de investigación, puesto que señalan que la orden de interceptación “sólo podrá afectar al imputado o persona respecto de las cuales existieren sospechas fundadas, basadas en hechos determinados, de que aquellas sirven de intermediarias de dichas comunicaciones, y asimismo, de aquellas que facilitaren sus medios de comunicación al imputado o sus intermediarios”(inciso segundo).

Del mismo modo se regula como circunstancia especial la comunicación del imputado con su abogado en el inciso tercero, la que no podrá ser

restringida de ningún modo, salvo que el juez de garantía lo ordenare, “por estimar fundadamente, sobre la base de antecedentes de los que dejará constancia en la respectiva resolución, que al abogado pudiere tener responsabilidad penal en los hechos investigados”.

El inciso cuarto prosigue señalando los requisitos de la orden de interceptación, que cuentan la indicación circunstanciadamente del nombre, la dirección del afectado por la medida y señalar la forma de interceptación y la duración de la misma que no podrá exceder de sesenta días. “El juez podrá prorrogar este plazo por períodos de hasta igual duración, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en los incisos precedentes”.

El inciso quinto²²¹ prosigue: “Las empresas telefónicas y de comunicaciones deberán dar cumplimiento a esta medida, proporcionando a los funcionarios encargados de la diligencia las facilidades necesarias para que se lleve a cabo con la oportunidad con que se requiera. Con este objetivo los proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a seis meses, de los números IP de las conexiones que realicen sus abonados. La negativa o entorpecimiento a la práctica de la medida de interceptación y grabación será constitutiva del delito de desacato. Asimismo, los encargados de realizar la diligencia y los empleados de las empresas mencionadas en este inciso deberán guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento”.

²²¹ CHILE. Ministerio de Justicia. 2005. 20.074: Modifica los Códigos Procesal Penal y Penal. 14 noviembre 2005. [en línea] <www.bcn.cl> [consulta: 22 enero 2007]. También: CHILE. Ministerio de Justicia. 2004. 19.927: Modifica el Código Penal, el Código Procedimiento Penal y el Código Procesal Penal en materia de delitos de pornografía infantil. 14 enero 2004. [en línea] <www.bcn.cl> [consulta: 22 enero 2007].

Por último remata el inciso final señalando que si las sospechas consideradas para la orden de interceptación se disiparen o hubiere transcurrido el plazo de duración fijado para ellas, ella deberá ser interrumpida inmediatamente.

La ley es clara y restrictiva para permitir la intervención de las comunicaciones; se debe tratar de un medio de investigación en el marco de un proceso penal, llevado a cabo a petición de un fiscal con autorización y orden previa y detallada por resolución de un juez de garantía; resolución que debe ser fundada en base a sospechas fundadas en hechos determinados; con señalación circunstanciada del nombre, la dirección, la forma de interceptación y su duración, que está limitada en su prolongación.

En suma, el ordenamiento jurídico nacional contempla la utilización legal de esta medida solamente en el cumplimiento de estos requisitos y en ningún caso más. De este modo, la intervención indiscriminada que realizan los agentes de Estado extranjero, sobre las comunicaciones de nuestros conciudadanos, en el contexto de la USAPA, sería a todas luces ilegal y por lo tanto merecedora de protección penal. De ahí la necesidad de investigar acerca de la existencia de tipos penales que puedan otorgar esta cobertura.

Las leyes atinentes a esta materia son la nº 19.223 y 19.423, del año 1993 y 1995, respectivamente y la Constitución Política, con su artículo 19 nº 5 en relación con el artículo 20. Ya desde un comienzo nos parecen normas de muy larga data, sobretodo para lo dinámico que ha sido el desarrollo de la delincuencia informática a nivel mundial y porque no contemplan, especialmente, los últimos acontecimientos en torno a la flagrante violación de los derechos fundamentales efectuada indiscriminadamente por agentes de

Estado extranjero. A continuación realizaremos una revisión de aquellos, más en detalle.

4.2.2. Párrafo 5 título III, libro II del Código Penal: el artículo 161-A del Código Penal.

Introducido al Código Penal el año 1995, a través de la Ley nº 19.423 publicada el veinte de Noviembre de 1995, consecuencia del conocido incidente de intervención de las comunicaciones telefónicas a Sebastián Piñera, producto de la moción del senador Miguel OTERO²²²; buscaba otorgar una adecuada protección al derecho a la vida privada e inviolabilidad de las comunicaciones. Dicho artículo dispone: “Se castigará con la pena de reclusión menor en cualquiera de sus grados y multa de 50 a 500 Unidades Tributarias Mensuales 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 o comunicaciones 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.

Igual pena se aplicará a quién difunda las conversaciones, comunicaciones, documentos, instrumentos, imágenes y hechos a que se refiere el inciso anterior.

²²² COMISIÓN DE CONTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. 1993. Informe, recaído en el proyecto de ley, iniciado en moción del honorable senador señor Otero, que modifica el Código Penal a fin de cautelar efectivamente la privacidad de las personas, nº 2.241, de 16 de Junio de 1993. [en línea] <www.sil.senado/docsil/info2241.doc> [consulta. 29 noviembre 2006].

En caso de ser una misma la persona que los haya obtenido y divulgado, se aplicarán a ésta las penas de reclusión menor en su grado máximo y multa de 100 a 500 Unidades Tributarias Mensuales.

Esta disposición no es aplicable a aquellas personas que, en virtud de ley o de autorización judicial, estén o sean autorizadas para ejecutar las acciones descritas”.

Nosotros sostenemos la aplicación de este tipo a la situación de intervención de las comunicaciones electrónicas en tratamiento. No obstante para ello debemos realizar algunas precisiones ya que “claro está que el tipo del artículo ha sido redactado en forma defectuosa y contiene un número considerable de elementos normativos, necesitados, por ello, de una complementación valorativa...²²³” .

En primer lugar, detrás de estos tipos se busca la protección de la vida privada y la inviolabilidad de las comunicaciones privadas, reconocidas constitucionalmente. Una de las manifestaciones concretas de dichos bienes jurídicos es el derecho al secreto en las comunicaciones. Elemento que es central en nuestra posición respecto la protección de las comunicaciones electrónicas. La Corte de Apelaciones de Santiago falla considerando tales elementos, con ocasión del mediático caso de Alejandro Guillier como editor de la estación de televisión Chilevisión y la ministro en visita Gabriela Pérez²²⁴:

²²³ SEGUNDA SALA DE LA CORTE SUPREMA. 2004. Sentencia, de fecha seis de enero de 2004, considerando 5º, en expediente caratulado “Guillier con Pérez”, Rol Nº 5.604-03. [en línea] <www.lyd.com/noticias/sentencias/recurso_amparo_caratulado.pdf> [consulta: 30 de Noviembre del 2006]

²²⁴ SEGUNDA SALA DE LA CORTE DE APELACIONES DE SANTIAGO. 2003. Sentencia, de fecha veintidós de diciembre de 2004, considerando 12º, letra a), en expediente caratulado “Guillier con Pérez”, Rol Nº 33.865-2003. [en línea] <www.lyd.com/noticias/sentencias/recurso_amparo_caratulado.pdf> [consulta: 30 noviembre 2006]

“a- Que respecto de la primera (Ley 19.423), y examinada las actas legislativas, correspondientes, se desprende de manera categórica que durante el trámite parlamentario que condujo a la dictación de la ley... quedaron debidamente plasmadas las siguientes motivaciones del legislador: que la separación de lo privado y lo público es lo que determina el bien público que debe cautelarse; que no hay que confundir los actos que se realizan en privacidad de aquellos que se ejecuten en lugares públicos o de libre acceso al público; que el sujeto que será objeto de la sanción será el que indebidamente y por cualquier medio se introduzca o entrometa en la privacidad que da lugar, la oficina, los recintos y vehículos particulares y lugares que no sean de libre acceso al público, por ser estos los espacios donde ésta se ejerce y adquiere vida...”

En segundo, a pesar, de que una de las conductas que se busca darle protección penal, mediante este tipo es la captación, interceptación, grabación o reproducción de conversaciones o comunicaciones de carácter privado, que sean de carácter telefónicas o vivenciales, nada obsta a que se amplíe la cobertura hasta las comunicaciones electrónicas, que en nada se separan en cuanto al aspecto de privacidad que guardan las comunicaciones telefónicas y tampoco en sus aspectos esenciales. Ambas son teledirigidas, requieren del soporte de tecnología, tienen un(os) emisor(es) y un(os) receptor(es) que confían en su confidencialidad, en ambos casos la conducta de interceptarlas requiere de un ánimo doloso y de un soporte tecnológico de determinada sofisticación. De hecho el espíritu detrás de la ley pretende incluir todo tipo de comunicaciones, con la gran salvedad de que no sean de carácter públicas, lo que grafica la ley con que se realicen “en recintos particulares o lugares que no sean de libre acceso al público”.

Luego hay que abordar el alcance de la expresión “recintos particulares o lugares que no sean de libre acceso al público”. Respecto a “recintos”, acudimos a la definición del Diccionario de la Real Academia Española²²⁵, que lo define como: “Espacio comprendido dentro de ciertos límites”. Al agregarle la característica de particulares parece tan sólo incluirle el rasgo de que en aquél espacio delimitado no cualquiera pueda ingresar, pues no es público. A su vez la expresión “lugares que no sean de libre acceso al público” no viene sino tan sólo a buscar ampliar la idea de recintos particulares, hasta lo que no alcance el primer concepto. La diferenciación parece tener el ánimo de buscar omnicomprensión respecto los lugares de comisión de la conducta típica. Al respecto reiteramos que el ánimo de la ley es excluir los lugares de acceso público y no requiere de la materialidad del lugar para la comisión del delito.

Con esto queremos recalcar que el tipo perfectamente se puede enmarcar en un recinto virtual, tal como es el correo electrónico, que es de carácter privado, por ser un medio homologable a la correspondencia tradicional y sus características técnicas, como por ejemplo, el disponer de una contraseña, para restringir el acceso a su contenido exclusivamente a su usuario. Para reafirmar tal realidad el informe de la Comisión de Constitución, Legislación, Justicia y Reglamento, ya citado²²⁶, encargó un informe acerca del proyecto de ley al abogado penalista y profesor de la cátedra en la Pontificia Universidad Católica de Chile, Manuel Guzmán Vial, que entre sus conclusiones expresó: “En relación con las disposiciones de esta iniciativa de ley, apunto que por los numerandos 1º y 2º del artículo 161 A se enfatiza la circunstancia de que el reproche de la acción punible está centrado en un lugar determinado, como la casa, oficina, recinto o vehículo.

²²⁵ Consultado en diccionario de la Real Academia de la Lengua Española. [en línea] <www.rae.es> [consulta: 29 noviembre de 2006].

²²⁶ COMISIÓN DE CONTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. Op. cit, 11p.

Sin desconocerse que tal modalidad es significativa, pues la víctima se siente en tales casos amparada por un entorno de resguardo, le pareció que el núcleo de la acción delictiva está constituido por la injerencia del tercero en la órbita de la intimidad, sin la autorización del sujeto pasivo.

De esta suerte, el enunciado de los tipos propuestos dejaría fuera de la censura penal, a las acciones que ocurrieran en lugares públicos. Así, la conversación privada que se tiene en un lugar público, y que es, por ejemplo, grabada desde distancia, clandestinamente, no se sancionaría, lo que importaría dejar en la impunidad un hecho atentatorio contra la intimidad. Por ello, creyó apropiado sancionar "al que por cualquier medio capte, grabe o reproduzca conversaciones, sin autorización de los que intervienen en ellas", esto es, de forma que no se haga mención al lugar en que se realiza la acción".

Aparte de lo anterior, queremos destacar un elemento que asiste al artículo 161-A. El artículo 157 del Código Procesal Penal, respecto de las medidas cautelares reales que pueden solicitar la víctima o el Ministerio Público, se remite al Código de Procedimiento Civil²²⁷. Y a su vez dispone, que al deducir la demanda civil, la víctima podrá solicitar que se decrete una o más de dichas medidas. Dicho esto, sostenemos, que a pesar de que ninguna de las medidas precautorias contempladas en el Código de Procedimiento Civil, nos parecen lo suficientemente específicas para proteger la privacidad de las comunicaciones electrónicas, en vísperas del ejercicio de una acción penal o civil o durante el curso del juicio; sostenemos que el artículo 298 del Código de Procedimiento Civil, consagra la posibilidad de ejercer una medida precautoria genérica, tal como se desprende de su articulado:

²²⁷ CHILE. Ministerio de Justicia. 1902. Ley nº 1552: Código de Procedimiento Civil. 30 agosto 1902. [en línea] <www.bcn.cl> [consulta: 22 enero 2007]. En adelante cuando nos refiramos al Código de Procedimiento Civil, aludiremos al chileno.

“Podrá también el tribunal, cuando lo estime necesario y no tratándose de medidas expresamente autorizadas por la ley, exigir caución al actor para responder de los perjuicios que se originen”.

Con ello la ley reconoce la posibilidad de considerar otras medidas precautorias, mientras exista el *fumus boni juris* y el peligro de que la acción que se haya interpuesto o se vaya interponer, no vaya a poder tener los efectos deseados, para el actor. A su vez, la mención de la exigencia de caución sólo al actor, en nada obstaría para que en el caso de la intervención indiscriminada de las telecomunicaciones electrónicas por agentes de Estado extranjero, sea el Estado o el sujeto pasivo quien deba otorgar las garantías para que cese la intervención, por las características técnicas de la conducta delictiva bajo tratamiento. Es más proponemos que, por lo mismo, el Estado sea en la abrumante mayoría de los casos, el llamado a otorgar dichas garantías para que cese la perturbación.

4.2.3. La Ley nº 19.223.

Ley especial publicada el siete de junio del año 1993, con motivo de darle tratamiento penal a los delitos informáticos, “tiene como antecedente directo la legislación francesa, en particular la Ley N° 88-19, de 5 de enero de 1988, relativa al Fraude Informático”²²⁸. Para dichas conductas criminales, en la actualidad, se trata de la única respuesta penal en el ordenamiento jurídico nacional, siendo francamente insuficiente y de mala calidad. La doctrina concuerda unánimemente en ello, tal como expondremos luego.

Pero antes, su breve articulado dispone:

²²⁸ MAGLIONA, CLAUDIO. 2002. Delincuencia informática en Chile. Proyecto de ley. [en línea] Revista de Derecho Informático Alfa-Redi (50) <www.alfa-redi.org> [30 de noviembre de 2006] 1p.

“Artículo 1°.- 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.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2°.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

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

Especial atención merece el artículo 2° de la ley, que según nuestro parecer, podría servirnos para otorgar protección al nacional usuario de una casilla de correo electrónico, frente a la intervención ilegítima por parte de agentes de Estado extranjero. Sin embargo la ley dispone del “que con ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma...”. Frente a esta terminología usada, no

obstante, nosotros creemos que se extiende la protección más allá que los sistemas de tratamientos de datos; la información son datos y los correos electrónicos son un medio de comunicación personal que busca darle un tratamiento confidencial a dicha información.

Por otro lado realizando un breve análisis del tipo objetivo de este artículo, siguiendo a HUERTA MIRANDA²²⁹; éste clasifica las conductas típicas contenidas en la ley, entre las cuales nos interesa:

“C. Acceso indebido a la información contenida en un sistema de tratamiento de la misma

De acuerdo con el Diccionario de la Real Academia española²³⁰, acceso es la entrada o paso a un lugar.

Por su parte el adverbio “indebido” entrega la idea de ilicitud, injusticia, carencia de equidad, no autorizado.

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 perjuicio de terceros.

²²⁹ HUERTA MIRANDA, Marcelo. Figuras delictivo informáticas tipificadas en Chile. S.a. S. num. [en línea] Revista de Derecho Público de la Contraloría General de la República de Chile. <www.bcn.cl> [30 noviembre 2006] 10p.

²³⁰ Consultado en diccionario de la Real Academia de la Lengua Española. [en línea] <www.rae.es> [consulta: 29 noviembre de 2006].

Desde esta perspectiva, el acceso indebido implica una violación de “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 delincuente, sin embargo, una vez en el sistema, el agente se apodera, conoce o utiliza la información confidencial a que no tenía acceso”.

A pesar de lo dicho, y como adelantamos previamente, dicha ley ha merecido una crítica generalizada por parte de la doctrina debido a, su deficiente tipificación, lo insuficiente que es en cuanto a su cobertura y los gruesos errores conceptuales en que incurre. En ello concuerda, JIJENA LEIVA²³¹ señalando: “Poniendo de relieve sus innumerables errores de forma y de fondo -al igual que lo hicimos mediante informes remitidos al Parlamento entre los años 1991 y 1993, en forma previa a su promulgación-, muy en particular al no haberse entendido cuáles son los bienes jurídicos que requieren ser resguardados frente a la criminalidad informática, y al haberse dado muestra de un notable desconocimiento y falta de manejo conceptual - eliminándose incluso la expresión "automatizado" de los tipos penales-, se concluye en que el único destino posible de este cuerpo legal de tan sólo cuatro aislados artículos es que él sea derogado”.

Por otro lado MAGLIONA²³² aporta, con otro cariz, proponiendo la complementación de la ley N° 19.223: “Sin lugar a dudas el texto de la Ley N° 19.223 es actualmente insuficiente para combatir la delincuencia informática en Chile. La Ley fue creada en 1993, año en que el fenómeno Internet aún no lograba desarrollarse en el país. Por lo cual, el legislador al momento de tipificar

²³¹ JIJENA LEIVA, R. 2004. La criminalidad informática. Análisis de la ley 19.223, sus antecedentes y modificaciones en curso. [en línea] <www.sdi.bcn.cl/partners/e-derecho/Ponencias/ver_po/p55> [consultado con fecha 5 de diciembre de 2006].

²³² MAGLIONA, C. Delincuencia Informática... Op. cit. 6p.

las conductas, no pudo dimensionar el cambio que produciría Internet en nuestra sociedad, y en el comportamiento de los delincuentes. A lo menos, creemos que debe estudiarse *i)* la sanción de los delitos de fraude informático, acceso no autorizado, creación y distribución de virus o programas dañinos, y falsificación informática; *ii)* la reformulación de los tipos de sabotaje informático, alteración de datos y apoderamiento de información; y *iii)* la incorporación de conceptos esenciales para una correcta aplicación de la ley. Junto con lo anterior, debe hacerse un esfuerzo para incorporar al país a las iniciativas internacionales que se están realizando con el objeto de sancionar la delincuencia informática de manera global, mediante la cooperación internacional de todos los países. Internet permite realizar un delito en Chile desde cualquier país del mundo. Es por ello, que la única forma de protegerse frente a delincuencia informática, es la cooperación internacional”.

Concordamos plenamente con estas últimas reflexiones de MAGLIONA, pues por ese lado es que vislumbramos la solución a la conducta delictiva que motiva este trabajo, realidad que venimos analizando desde capítulos anteriores.

Más en específico MAGLIONA²³³, plantea críticas respecto a la conducta típica del artículo 2 que nos interesa: “Sin perjuicio de lo anterior, la figura de acceder sin autorización a un sistema de tratamiento de información, constituye delito individualmente considerada, en muchas legislaciones. En este sentido, creemos que junto a las conductas sancionadas por el artículo n° 2 de la ley n° 19.223, se debe tipificar la figura de acceso no autorizado sin la concurrencia de un elemento subjetivo. Debe bastar con el acceso sin autorización o sin derecho a un sistema de tratamiento de información, concepto que comprende a los sitios *web* en Internet.

²³³ Ibid. pp. 8-9.

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

Del mismo modo, MENESES DÍAZ²³⁴ brinda una interesante enumeración de críticas básicas que se realizan a la ley, que se resumen en tres puntos clave.

El primero dice relación con la confusión entre delitos informáticos y delitos computacionales. “Para autores como HERRERA BRAVO²³⁵ que sigue en este sentido a Renato Jijena - la primera denominación correspondería a aquellos ilícitos que atentan contra los datos digitalizados y contra los programas computacionales contenidos en un sistema. Los segundos, en cambio, serían delitos de carácter convencional que estarían ya establecidos en el Código Penal.

Tal posición, se fundamentaría en lo dispuesto en el artículo 1º de la ley Nº 19.223 que señala: “El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes...”.

²³⁴ MENESES DÍAZ, C. 2002. Delitos informáticos y nuevas formas de resolución del conflicto penal. [en línea] Revista de Derecho Informático Alfa-Redi (51) <www.alfa-redi.org> [30 noviembre 2006], pp. 2-3.

²³⁵ HERRERA BRAVO, R. 1993. Reflexiones sobre los Delitos Informáticos motivadas por los desaciertos de la Ley Chilena Nº 19.223. [en línea] <<http://www.ctv.es>> [consulta: 30 noviembre 2006].

Del análisis de dicho artículo, se desprende que a partir de éste, se pretende sancionar a quienes destruyan o inutilicen el equipo o aparato computacional y sus partes piezas o componentes, en circunstancias que, 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 daños²³⁶.

Segundo, la ubicación fuera del Código Penal, a lo que al respecto dice en resumidas palabras: “La dictación de leyes aisladas, necesariamente 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 informático²³⁷”.

Y en último lugar, deja sin regulación ciertos delitos informáticos, a lo que aporta: “existe consenso en la doctrina en cuanto a que nuestra normativa, contempla sólo dos modalidades delictivas: el sabotaje informático (artículos 1° y 3°) y el espionaje informático (artículos 2° y 4°) dejando de lado las figuras del fraude informático, la del acceso no autorizado o *hacking* directo y la piratería de programas”.

En el marco de éste último punto es que nosotros propugnamos la creación de un tipo, en nuestro ordenamiento jurídico, que contemple la conducta delictiva de intervención de las comunicaciones electrónicas por parte de agentes de Estado extranjero.

²³⁶ MENESES DÍAZ. Op. cit. 2p.

²³⁷ Ibid. 3p.

En suma, nos hacemos partícipes de algunas de las críticas, en cuanto a la derogación de esta ley, la incorporación de los tipos especiales de los delitos informáticos al Código Penal vigente, la aclaración conceptual de los “verdaderos” delitos informáticos, como aquellos que tengan como objeto afectar la integridad y el tráfico de información, y no aquellos que ya estén cubiertos por los tipos penales tradicionales y la creación de tipos que contemplen todas las formas de criminalidad informática, incluyendo, por supuesto, la que nos convoca.

4.2.4. La Constitución: el recurso de protección.

Aunque no se trata de un tipo penal, nos ofrece un medio de protección posible para la intervención indiscriminada de las comunicaciones. En primer lugar en el artículo 19 n° 4 y 5, respectivamente, reconocen el derecho a la vida privada, la honra de la persona y de su familia; y la inviolabilidad del hogar y de toda forma de comunicación privada, como regla general. Por otro lado el artículo 20 de la Constitución consagra el recurso de protección, técnicamente una acción, puesto que su objetivo es dar inicio a un proceso frente a los Tribunales Superiores de justicia para que “el que por causa de actos u omisiones arbitrarios o ilegales sufra privación, perturbación o amenaza en el legítimo ejercicio en los derechos y garantías establecidos en el artículo 19 números..., 4º, 5º..., podrá ocurrir por si o por cualquiera a su nombre, a la Corte de Apelaciones respectiva, la que adoptará de inmediato las providencias que juzgue necesarias para restablecer el imperio del derecho y asegurar la debida protección del afectado...”²³⁸.

²³⁸ Extracto del artículo 20 de: CHILE. 1980. Constitución Política de la República de Chile.

El informe anual sobre los Derechos Humanos en Chile del año 2004 nos expone acerca del recurso de protección²³⁹: “Suele decirse que una de las innovaciones mas relevantes de la Constitución de 1980 la constituye la instauración de un mecanismo de resguardo de los Derechos fundamentales expedito y ágil. El recurso de protección, cuyo antecedente se encuentra en el Acta constitucional N° 3 sobre derechos y deberes constitucionales (decreto ley n° 1552 del año 1976), fue pretendidamente concebido como el remedio que se requería para cambiar la situación de indefensión en que se encontraban las personas frente a los abusos, en especial, se decía, aquellos abusos de la autoridad administrativa que quedaban sin sanción, ya que los tribunales contencioso-administrativos que contemplaba la Constitución de 1925 nunca fueron creados por el legislador. De esta manera, era imperioso dotar a los ciudadanos de una vía jurisdiccional que sirviera de medio de tutela de los derechos básicos, en especial, dado que el amparo (o *habeas corpus* que sí existía desde la Carta de 1833) no era suficiente para la debida protección de los derechos y libertades fundamentales...”

A continuación prosigue señalando respecto de sus características: “En primer término, se trata de una acción que algunos han llamado “informal”, por cuanto puede ser interpuesta por cualquier persona – natural, jurídica y aún por entes colectivos sin personalidad jurídica (como por ejemplo un centro de alumnos)- incluso sin ser abogado, y no sólo a favor de ella sino a nombre de otro (sin que sea necesario como ocurre en los demás procedimientos acreditar la presentación). En seguida se ha destacado la celeridad del procedimiento, toda vez que con la sola presentación del recurso la Corte solicita a quién es demandado (“recurrido”) un informe, y una vez, que éste es evacuado, la causa es alegada por los abogados de las partes. No hay, a diferencia de los

²³⁹ INFORME ANUAL SOBRE LOS DERECHOS HUMANOS EN CHILE. 2004: Sistema judicial y protección de derechos. [en línea] Universidad Diego Portales. <www.bcn.cl> [consulta: 29 noviembre 2006] pp. 26-28.

procedimientos comunes, un período de prueba, porque, como lo han señalado la jurisprudencia y la doctrina especializada, el recurso de protección es un procedimiento de emergencia, cautelar de derechos, que demanda una pronta acción por parte de la Justicia ante situaciones graves de violación de derechos básicos.

Por otro lado, la posibilidad de que pueda deducirse de cualquier forma “por escrito, en papel simple y aún por teléfono o télex”²⁴⁰-, incluso mediante un formulario que se encuentra en la Secretaría de las Cortes de Apelación, parece ser una genuina muestra de la materialización del derecho de acceso de la justicia de todas las personas”.

Al tenor de la Constitución no puede ser más claro, la intervención indiscriminada de las comunicaciones electrónicas, por parte de agentes de Estado extranjero, sin siquiera el conocimiento ni autorización de quienes son los únicos usuarios de dichos medios de comunicación²⁴¹, es un cúmulo de actos arbitrarios e ilegales que generan la privación de derechos fundamentales, expresamente protegidos con esta acción constitucional.

Se sostiene la arbitrariedad e ilegalidad de tales intervenciones fundado en que, como ya hemos visto, existe una vía legal predeterminada para la interceptación de comunicaciones de ciudadanos chilenos. Requisitos que en los casos que denunciarnos no se cumplen de ninguna manera.

De este modo los Tribunales superiores de justicia están obligados a restablecer el imperio de la ley, frente a estas violaciones, una vez interpuesta

²⁴⁰ CHILE. Corte Suprema de Justicia.1992. Auto Acordado sobre la Tramitación del Recurso de protección de garantías constitucionales. 27 de Junio de 1992 (modificado por el auto acordado de 4 de Mayo de 1998).

²⁴¹ Incluso habiéndolo resultaría cuestionable, puesto ahí se ingresa a la discusión acerca de la libre disposición de estos derechos, por parte de sus titulares.

la “acción” de protección, para de este modo tomar las medidas para que cesen y en consecuencia asegurar la debida protección del afectado.

4.3. Posibilidades de persecución penal conforme al Código Procesal penal.

En este acápite revisaremos, en la legislación procesal penal vigente, que la posibilidad de dar persecución efectiva no es tal, y que toda instancia tendería a agostarse sin obtener resultados fructíferos, o al menos, alentadores. De guisa tal, explicaremos que probablemente procedería el archivo provisional, como actitud primaria del fiscal. También cabría aplicar el principio de oportunidad del artículo 170 del Código Procesal. Luego, revisaremos que aunque fuera procedente la formalización del imputado, no podría operar la extradición por no existir la doble tipicidad requerida, y por exigirse una cierta cuantía de pena que el artículo 161 A y que el artículo 2º de la ley 19.223 del Código Penal, no detentan.

Con todo, y aunque se procediera de las formas ya descritas, se deberían franquear sendos problemas probatorios, para finalmente terminar este acápite con una breve reflexión de las perspectivas de un procedimiento de esta envergadura.

4.3.1. Archivo provisional y principio de oportunidad.

Normalmente, para intervenir las telecomunicaciones de manera legal en Chile, deberemos estar a lo estipulado en los artículos 222 y 223 del Código Procesal Penal. Cuando ello, no ocurre, se podría cometer alguno de los tipos ya revisados en el acápite anterior.

Si alguien comete uno de los tipos ya descritos y se ve afectado, quién sabe que sus telecomunicaciones vía correo electrónico están siendo intervenidas o han sido intervenidas, debe denunciar tal hecho ante Carabineros o ante el Ministerio Público conforme al artículo 172 y 173 del Código Procesal Penal. Dada la complejidad del tema y la sobrecarga de otro tipo de denuncias que soportan Carabineros, estimamos conveniente denunciar directamente ante el Ministerio Público. Igualmente es recomendable, entregar la mayor cantidad de antecedentes necesarios para facilitar a la fiscalía la prosecución exitosa de manera exitosa la investigación en cuestión, y quizá sortear los problemas probatorios que se explicarán más adelante.

Ahora bien, dada esta compleja demostración (tema que será explicado más adelante), sumado a que si un individuo no tiene como aportar antecedentes concluyentes y que la investigación debe realizarse primordialmente desde su ordenador en el momento que se intervinieron los correos electrónicos, es muy probable que dicha investigación pase al archivo provisional del artículo 167 del Código Procesal Penal²⁴², pues no habrían antecedentes que permitieren desarrollar actividades conducentes al esclarecimiento de los hechos.

También, estimamos, cabría aplicar el principio de oportunidad del artículo 170 del Código Procesal Penal²⁴³, por cumplirse los requisitos de

²⁴² CHILE. Ministerio de Justicia. 2000. Código Procesal Penal. 12 de Octubre del 2000. Artículo 167, inciso primero: "Archivo provisional. En tanto no se hubiere producido la intervención del juez de garantía en el procedimiento, el ministerio público podrá archivar provisionalmente aquellas investigaciones en las que no aparecieren antecedentes que permitieren desarrollar actividades conducentes al esclarecimiento de los hechos..."

²⁴³ Ibid. Artículo 170, inciso primero: "Principio de oportunidad. Los fiscales del ministerio público podrán no iniciar la persecución penal o abandonar la ya iniciada cuando se tratare de un hecho que no comprometiere gravemente el interés público, *a menos que la pena mínima asignada al delito excediere la de presidio o reclusión menores en su grado mínimo* o que se tratare de un delito cometido por un funcionario público en el ejercicio de sus funciones..." Las cursivas son nuestras.

cuantía mínima establecidos en la ley, que corresponden a la pena de 61 días (reclusión o prisión menores en su grado mínimo).

4.3.2. Formalización de la investigación e improcedencia de la extradición.

Antes que todo, para poder formalizar a un imputado se le debe poder individualizar e identificar y comunicarle la circunstancia de su investigación²⁴⁴. Luego, el anonimato que ofrece Internet, que fue revisado como una de las características de Internet en Capítulo I, nos dificultará la tarea de sobremanera. Todo descansará en nuestras posibilidades probatorias.

En caso que la investigación pudiere formalizarse, en primer lugar, deberemos descartar inmediatamente la procedencia de los acuerdos reparatorios porque no se cumple con el requisito de ser una vulneración de carácter patrimonial (el derecho a la vida privada y la inviolabilidad de la correspondencia no son bienes patrimoniales), conforme al inciso segundo del artículo 241 del Código Procesal Penal²⁴⁵.

En el caso de la suspensión condicional del procedimiento, siguiendo el artículo 237²⁴⁶ letra a), la cuantía máxima necesaria es de tres años de privación de libertad, y la pena máxima para este delito es de cinco años para el tipo del artículo 161 A, por lo que, en principio, no debería proceder. En cambio, esta pena es de 3 años para el tipo del artículo 2º de la ley 19.223, por lo que

²⁴⁴ Ibid. Artículo 229.- Concepto de la formalización de la investigación. La formalización de la investigación es la comunicación que el fiscal efectúa al imputado, en presencia del juez de garantía, de que desarrolla actualmente una investigación en su contra respecto de uno o más delitos determinados.

²⁴⁵ Ibid. Artículo 241, inciso segundo: "...Los acuerdos reparatorios sólo podrán referirse a hechos investigados que afectaren bienes jurídicos disponibles de carácter patrimonial, consistieren en lesiones menos graves o constituyeren delitos culposos...."

²⁴⁶ Ibid. Artículo 237, inciso segundo: "La suspensión condicional del procedimiento podrá decretarse: letra a).- Si la pena *que pudiere imponerse al imputado*, en el evento de dictarse sentencia condenatoria, no excediere de tres años de privación de libertad...".

eventualmente podría proceder. Con todo, la pena es la pertinente al caso concreto y no en abstracto, es decir, conjugando todas las posibles atenuantes y agravantes del caso particular²⁴⁷, por lo que, en conclusión, en ambos casos podría proceder. Al respecto, en el Instructivo 36 del Ministerio Público nos dice que "...Será necesario, entonces, que los fiscales realicen una ponderación de las eventuales atenuantes y agravantes que podrían aplicarse al caso concreto a efecto de evaluar adecuadamente la procedencia de la aplicación de esta salida alternativa... ...Con tal objeto, deberán considerarse el grado de participación que ha cabido al imputado y la circunstancia de encontrarse el delito en estado de tentativa, consumado o frustrado, en los casos que estas circunstancias influyen en la determinación de la pena..."²⁴⁸

Luego, atendiendo a que el Ministerio Público debe perseverar con la investigación, y se tuvieren resultados auspiciosos de ésta para nuestros fines y no se ha utilizado una de las salidas alternativas antedichas, deberemos intentar solicitar la extradición del agente de Estado extranjero que interviene nuestras telecomunicaciones de correo electrónico.

4.3.3. Improcedencia de la solicitud de extradición.

Luego, ya atendido que el Ministerio Público debe perseverar con la investigación formalizada porque no ha operado una salida alternativa, y si se tuvieren resultados auspiciosos de ésta para nuestros fines, el paso siguiente es intentar la extradición activa del agente de Estado extranjero que interviene nuestras telecomunicaciones de correo electrónico. Se trata de buscar la aplicación del procedimiento de extradición activa expuesto en el artículo 431 y

²⁴⁷ Eso se desprende de la expresión "...que pudiere imponerse al imputado..." del mismo artículo 273 antes mencionado.

²⁴⁸ CHILE. Fiscalía Nacional. 2000. Instructivo General N° 36 Sobre Criterios de Actuación e Instrucciones en Materia de Suspensión Condicional del Procedimiento, Santiago, 15 Diciembre del 2000.

siguientes del Código Procesal Penal, enunciado de manera general en Capítulo II de este estudio. Pese a ello, no se cumple con el requisito mínimo de cuantía exigido en el artículo 431²⁴⁹, pues para dar curso a una extradición la conducta incriminada debe detentar una pena mínima de un año, siendo que tanto la pena mínima, tanto la del artículo 161 A como la del artículo 2º de la ley 19.223, son de sesenta y un días (reclusión menor en su grado mínimo). Ergo, no cabría una extradición activa

Aún así, e hipotéticamente existiendo la cuantía necesaria para poder dar curso a una extradición ella no sería posible, dado que no concurre la doble tipicidad necesaria para dar curso a un procedimiento de esta índole, principio ya explicado en Capítulo II. Esto es así, porque, según la USAPA, esta conducta típica en Chile estaría legalmente avalada en los Estados Unidos.

De esta manera, la única forma posible de llegar a formalizar la investigación de un agente extranjero que intervenga ilícitamente nuestras telecomunicaciones, es que pisare suelo chileno por voluntad propia.

4.3.4. Las dificultades probatorias.

¿Cómo se puede probar que hemos sido víctimas de una intromisión a nuestro correo electrónico? ¿Se puede dotar a un computador de sistemas tales que puedan dar fe de que nuestros correos han sido violados? El tema es de suyo complejo y al respecto se ha discutido casi nada dentro el medio jurídico

²⁴⁹ CHILE. Código Procesal Penal... Op. cit. Artículo 431, inciso primero: "...Procedencia de la extradición activa. Cuando en la tramitación de un procedimiento penal se hubiere formalizado la investigación por un delito que tuviere señalada en la ley una pena privativa de libertad cuya duración mínima excediere de un año, respecto de un individuo que se encontrare en país extranjero, el ministerio público deberá solicitar del juez de garantía que eleve los antecedentes a la Corte de Apelaciones, a fin de que este tribunal, si estimare procedente la extradición del imputado al país en el que actualmente se encontrare, ordene sea pedida. Igual solicitud podrá hacer el querellante, si no la formulare el ministerio público...".

nacional. Sin embargo, en Latinoamérica algo se ha dicho al respecto. En ese sentido, hay quienes ya exponen y avalan la importancia del peritaje informático²⁵⁰, pues la información es muy volátil y la consecuencial alterabilidad de la evidencia, intrínseca a los ordenadores actuales, hacen que el problema probatorio sea lo más difícil. Pese a ello, si a lo anterior le agregamos los problemas que devienen de las características de Internet, hacen el tema adquiera carices infranqueables.

Sin embargo, es posible determinar salvar esos problemas, al menos en la teoría, cumpliendo cuatro requisitos necesarios para que una prueba electrónica asequible sea completamente procedente. Estos son a saber, siguiendo a CANO MARTÍNEZ²⁵¹: la autenticidad, que es la “...no alterabilidad de los medios originales, (que) buscan confirmar que los registros aportados corresponden a la realidad evidenciada...”²⁵²; la confiabilidad, que es aquello que “nos dice si efectivamente los elementos probatorios aportados vienen de fuentes que son creíbles y verificables...”; la completitud o suficiencia, que es “...la presencia de toda la evidencia necesaria para adelantar el caso...”²⁵³; y finalmente, la conformidad con las leyes y reglas del poder judicial, que no es sino otra cosa que sea una prueba lícita y respetuosa de lo que las leyes prescriban.

Para tales efectos, el mismo autor nos dice que para cumplir esos requisitos se debe “...Desarrollar esta características en arquitecturas de cómputo, requiere afianzar y manejar destrezas de correlación de eventos en

²⁵⁰ Un panorama referencial está en: CANO MARTÍNEZ, JEIMY JOSÉ. 2005. Estado del Arte del Peritaje informático en Latinoamérica. [en línea] Revista de Derecho Informático Alfa-Redi. <<http://www.alfa-redi.org/>> [consulta: 4 diciembre 2006].

²⁵¹ CANO MARTÍNEZ, JEIMY JOSÉ. 2003. Admisibilidad de la Evidencia Digital: Algunos Elementos de Revisión y Análisis. [en línea] Revista de Derecho Informático Alfa-Redi (61), <<http://www.alfa-redi.org/>> [consulta: 4 de diciembre 2006].

²⁵² Idem.

²⁵³ Idem.

registros de auditoria. Es decir, contando con una arquitectura con mecanismos de integridad, sincronización y centralización, es posible establecer patrones de análisis que muestren la imagen completa de la situación bajo revisión...”²⁵⁴. La implementación de mecanismos de integridad que revelen una información auténtica, de sincronización para determinar su confiabilidad, y de centralización para establecer criterios de suficiencia. Ahora bien, la configuración de estos mecanismos ya es un tema que escapa a nuestros conocimientos, y pende de lo que analistas de sistemas e informáticos puedan desarrollar al respecto, es decir, ya es un tema que pertenece a la dimensión de los hechos, y no a la del derecho.

Con todo, cabe agregar que gracias a que se avala la apreciación de la prueba conforme a la sana crítica²⁵⁵, sumado a la libertad de utilización de los medios probatorios²⁵⁶, estos medios probatorios tendrían un pleno asidero, pudiendo, conforme a su idoneidad, demostrar un intervención en las telecomunicaciones electrónicas vía e-mail.

Lamentablemente, en este acápite queda demostrado que el proceso penal nacional no puede hacerse cargo de manera efectiva de la intervención masiva en las telecomunicaciones electrónicas vía Internet, aunque haya una factibilidad técnica que permita demostrar esas intervenciones, no sin pagar un alto costo para un ciudadano común y corriente con conocimientos informáticos suficientes para navegar en la red. Al parecer, la Comisión y Corte

²⁵⁴ Idem.

²⁵⁵ CHILE. Código Procesal Penal. Op. Cit. Artículo 297 del Código Procesal Penal, inciso primero: “Valoración de la prueba. Los tribunales apreciarán la prueba con libertad, pero no podrán contradecir los principios de la lógica, las máximas de la experiencia y los conocimientos científicamente afianzados...”

²⁵⁶ Ibid. Artículo 295 del Código Procesal Penal: “Libertad de prueba. Todos los hechos y circunstancias pertinentes para la adecuada solución del caso sometido a enjuiciamiento podrán ser probados por cualquier medio producido e incorporado en conformidad a la ley.”

Interamericana de Derechos Humanos podrían darnos algunas luces de un camino a seguir para solucionar estos problemas.

4.4. La justicia internacional.

4.4.1. Preámbulo.

Ya hemos analizado las vías de reclamación jurídicas que tiene un ciudadano chileno frente a la intervención indiscriminada de sus comunicaciones electrónicas, desde la perspectiva del nuevo proceso penal de la reforma. Claro queda que las posibilidades eficaces de investigación y procesamiento, albergadas por dicho sistema, son escasas, puesto que el fiscal y los jueces se enfrentan a dificultades procedimentales de la más diversa índole. De ahí nace la necesidad de explorar las opciones que otorgan los sistemas internacionales de justicia creados por los Convenios internacionales, ya que, como en repetidas veces hemos dicho, tales delitos requieren de la cooperación internacional para su adecuado tratamiento penal.

Para estos fines es que ahora nos dedicaremos a revisar las alternativas que ofrecen la Convención americana sobre Derechos Humanos²⁵⁷, (o “Pacto de San José de Costa Rica”) la Corte Interamericana que se le asocia y el sistema europeo con el Convenio sobre Cibercriminalidad²⁵⁸ y la Corte Penal Internacional²⁵⁹.

4.4.2. La Convención americana sobre Derechos Humanos y la Corte Interamericana de Derechos Humanos.

²⁵⁷ Suscrito en Costa Rica, el 22 de Noviembre de 1969.

²⁵⁸ CONSEJO DE EUROPA. 2001. Convenio sobre Cibercriminalidad. 23 de Noviembre del 2001. [en línea] < <http://conventions.coe.int/treaty/en/Treaties/Html/185-SPA.htm> > [consulta: 23 enero 2007].

²⁵⁹ NACIONES UNIDAS. 1998. Estatuto de Roma de la Corte Penal Internacional. 17 julio 1998. [en línea] < <http://www.derechos.net/doc/tpi.html> > [consulta: 23 enero 2007].

Tal tratado ratificado por Chile²⁶⁰, consagra en su artículo 11, en exactos términos que el artículo 17 del Pacto Internacional de Derechos civiles y políticos:

“1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.”

A su vez, en su parte II, llamada “medios de la protección”, crea la Comisión Interamericana de Derechos Humanos y la Corte Interamericana de Derechos Humanos. Especial interés, como en un principio esbozamos, nos merece este último órgano, particularmente en lo que respecta a sus competencias. En este punto destacamos el artículo 61 n° 1, cuyo tenor indica:

“1. Sólo los Estados Partes y la Comisión tienen derecho a someter un caso a la decisión de la Corte”. Respecto a este asunto debemos especificar que sólo se puede recurrir a dicho órgano jurisdiccional una vez agotados los recursos dentro de la jurisdicción interna del país miembro, lo que francamente, luego de los diversos análisis realizado, resultaría la regla general, en el caso de intervención de las comunicaciones tratado, en que la justicia nacional se ve privada de medios eficaces para el eventual control de tal realidad conculcadora de derechos fundamentales.

²⁶⁰ Con fecha 8 de Octubre de 1990.

A su vez, el artículo 63 n° 1, señala: “1. Cuando decida que hubo violación de un derecho o libertad protegidos en esta Convención, la Corte dispondrá que se garantice al lesionado en el goce de su derecho o libertad conculcados. Dispondrá asimismo, si ello fuera procedente, que se reparen las consecuencias de la medida o situación que ha configurado la vulneración de esos derechos y el pago de una justa indemnización a la parte lesionada”.

Por otro lado y por último destacamos, el artículo 68, que dispone: “1. Los Estados Partes en la Convención se comprometen a cumplir la decisión de la Corte en todo caso en que sean partes. 2. La parte del fallo que disponga indemnización compensatoria se podrá ejecutar en el respectivo país por el procedimiento interno vigente para la ejecución de sentencias contra el Estado”.

De esa manera, la Corte también contempla la posibilidad de indemnizaciones compensatorias civiles, una alternativa interesante, también, para el caso de la intervención indiscriminada de las comunicaciones electrónicas.

Acerca de la consagración de este derecho por dicho cuerpo legal debemos realizar algunas precisiones; las que extraemos de la doctrina, siguiendo a ÁLVAREZ VALENZUELA y CERDA SILVA²⁶¹: “El tramado que configura en nuestro ordenamiento jurídico el derecho a la inviolabilidad de las comunicaciones privadas, está compuesto tanto por normas de rango

²⁶¹ ÁLVAREZ VALENZUELA D. y CERDA SILVA A. 2005. Sobre la inviolabilidad de las comunicaciones electrónicas. Ley N° 19.927 que tipifica los delitos de pornografía infantil. En: [en línea] Anuario de Derechos Humanos. 2005. Santiago Chile. Centro de Derechos Humanos, Facultad de Derecho, Universidad de Chile, consultado en <www.anuariocdh.uchile.cl/anuario1/13inviolabilidad-comunic-electronica.pdf> [consulta: 3 de Diciembre 2006]. pp. 139-141.

constitucional como por disposiciones incluidas en diversos tratados internacionales sobre derechos humanos, suscritos y ratificados por Chile, los que en su conjunto tienen la fuerza normativa de límites de la soberanía del Estado y que conforman, al decir de Humberto Nogueira, un verdadero bloque constitucional de derechos fundamentales.

Como podemos observar, el derecho a la inviolabilidad de las comunicaciones reconocido en la Constitución difiere en su formulación respecto de las normas de los acuerdos constitucionales citados, toda vez que contiene elementos de neutralidad tecnológica que le permiten ampliar su campo de aplicación, no limitándose al elemento “correspondencia” utilizado por estos últimos, el cual podría ser objeto de interpretaciones inapropiadamente restrictivas. En efecto, tanto el Pacto de San José de Costa Rica como el Pacto internacional de Derechos civiles y políticos son instrumentos internacionales creados a mediados del siglo XX, momento histórico donde el grueso de las comunicaciones eran realizadas por medios epistolares y telegráficos, ambos comprendidos dentro del concepto de “correspondencia” utilizado en ellos- conforme a la definición del Diccionario de la Real Academia de la Lengua Española²⁶²-; se refiere “al conjunto de cartas que se reciben o expiden” entendiéndose a su vez carta al “papel escrito y ordinariamente cerrado, que una persona envía a otra para comunicarse con ella”. No obstante, en ambas definiciones el elemento central subyacente es la comunicación, siendo la correspondencia y/o la carta sólo uno de los múltiples medios por el cual dicha comunicación se materializa.

No debemos olvidar que la protección que le brindan los instrumentos internacionales sobre Derechos Humanos a la correspondencia es una

²⁶² Consultado en diccionario de la Real Academia de la Lengua Española. [en línea] <www.rae.es> [consulta: 29 noviembre de 2006].

especificidad dentro de la protección otorgada de la vida privada de toda persona, lo cual, conforme a la interpretación extensiva que debe hacerse de los derechos y libertades fundamentales, nos permite sostener que la protección se refiere a la comunicación en si misma, prescindiendo del medio por el cual se verifica.

Como vemos, no se trata de que cualquier acto de comunicación sea protegido por el constituyente; se trata de un tipo de comunicación específica: la comunicación privada. Esta es según el Diccionario de la Real Academia²⁶³ aquella “que se ejecuta a la vista de pocos, familiar y domésticamente, sin formalidad alguna ni ceremonia alguna. Particular y personal de cada uno”. En tanto particular es entendido como lo que no es público. En consecuencia cuando hablamos de comunicación privada, estamos hablando de una comunicación verbal, escrita o por medio de señas, que tiene un carácter personal, que no es pública, en la que se proyecta la intimidad de una persona a otro (que puede ser una o varias personas), que ha sido escogido de manera singular por el emisor y donde no importa la forma o el medio donde se materialice la comunicación.

En conclusión, para que una comunicación sea objeto de protección bajo el bloque constitucional de Derechos Humanos conformado por la garantía contenida en el numeral 5 del artículo 19 de la Constitución y por las normas pertinentes de los instrumentos internacionales antes mencionados es necesario que: i) sea una acción comunicativa entre personas, y, ii) sea un acto no público, entre personas determinadas o determinables.

²⁶³ Ídem.

Bajo esta interpretación, las principales comunicaciones entre personas que se realizan por medios electrónicos están ampliamente garantizadas constitucionalmente. Así, el correo electrónico, los sistemas de mensajería instantánea, la telefonía IP etc., gozan de protección constitucional y penal en tanto su interceptación, registro o grabación ilegítima, se encuentran prohibidas y penadas por la ley”.

Concluyendo, de la misma forma con los autores, en la debida protección que otorga este instrumento internacional a la privacidad de las comunicaciones electrónicas y compartiendo las certeras precisiones que los mismos realizan, no podemos obviar un problema evidente que se genera al querer aplicarle la cobertura jurídica deseada a una gama de agentes de Estado extranjeros. Obviando el problema del lugar de comisión de los delitos, abordado en capítulos anteriores, colisionamos con que muchos de los países que participan activamente en los sistemas mundiales de intervención de las comunicaciones electrónica, léase ECHELON, o el software “CARNIVORE”, no han ratificado la Convención americana de Derechos Humanos. De la información que hemos obtenido en Internet²⁶⁴ se revela que: tan sólo Estados Unidos lo suscribió y que Canadá ni siquiera concurrió a ese acto; ambos creadores y activos miembros de tales sistemas dentro del espectro territorial americano. Nada ocurre, de la misma forma con los países europeos que han configurado un sistema de interceptación paralelo (si es que no en la actualidad estamos en presencia de un sistema interconectado universal de intervención de las comunicaciones electrónicas), ni Gran Bretaña, Australia y Nueva Zelanda, también miembros partícipes de la creación de ECHELON.

²⁶⁴ Dato consultado en: [en línea] <www.oas.org/juridico/spanish/firmas/b-32.htm> [consulta: 3 diciembre 2006].

Sabidas cuentas, de la forma de vinculación de los distintos países y sus respectivos ordenamientos jurídicos a los instrumentos internacionales conforme a las reglas del Derecho Internacional, se niega la posibilidad de recurrir al contenido de esta normativa y a la Corte interamericana de Derechos Humanos a que dio origen, para accionar en contra de ciudadanos de países que no han ratificado la Convención, y del mismo modo se impide la posibilidad de la valiosa cooperación internacional en la persecución de estos delitos que brindaría la Corte Interamericana de Derechos Humanos. Nuevamente tropezamos con la imperiosa necesidad de la creación o la consolidación de sistemas de justicia internacionales, para prohibir y sancionar las violaciones a los derechos humanos, que, en este sentido, y en la actualidad, se cometen flagrantemente.

4.4.3. Hacia una jurisdicción internacional para el tratamiento de estos delitos. Análisis crítico del Convenio sobre Cibercriminalidad y el Tribunal Penal Internacional.

Se trata de otra posibilidad de disponer de un sistema internacional de justicia para el tratamiento de los delitos cometidos por agentes de Estado extranjeros frente a la intervención de las comunicaciones electrónicas. En este sentido, parece que deberíamos seguir la lógica utilizada en el Convenio sobre la Cibercriminalidad, pero dado que no es un cuerpo normativo respetuoso de los Derechos Fundamentales, no nos parece que sea una alternativa viable de punición de estos ilícitos. Del mismo modo, también resulta sumamente exagerado intentar incluir este tipo de violaciones normativas en el Tratado de Roma, dado que se ocupa del tratamiento de crímenes de lesa humanidad, y al menos, según nuestro parecer, este no es el caso en comento. De esta

forma, parece necesario apuntar a la creación de una institucionalidad internacional novedosa que resuelva este vacío legal

La doctrina nacional no es ajena a estos raciocinios, al respecto de pronuncia MAGLIONA²⁶⁵: “La naturaleza misma de los delitos cometidos a través de Internet hace imposible su persecución, si no existe la colaboración internacional entre los países. Se trata de delitos cuya ejecución puede ser realizada en un país distinto a aquel en que se reflejan los daños. Por ello, una conducta lesiva debe ser delito en cada jurisdicción. Así, no obstante de respetar las legislaciones locales, los Estados deben definir delitos informáticos basados en un modelo común. Chile debe participar en las iniciativas internacionales contra la delincuencia informática.”

Este tipo de esfuerzo internacional se enfoca desde la perspectiva de la persecución de los delitos informáticos, tipos que se enmarcan perfectamente en las conductas delictivas que se busca erradicar. Nos referimos a la Convención sobre la Cibercriminalidad²⁶⁶ suscrita con éxito el 8 de noviembre de 2001 en el Consejo de Europa, que reúne a 41 países, junto a otros Estados no miembros como Estados Unidos, Canadá, Japón y Sudáfrica. Se trata del primer tratado internacional sobre delitos en Internet.

Siguiendo con los razonamientos de MAGLIONA²⁶⁷ “la Convención pretende punir las conductas dirigidas en contra de la confidencialidad, integridad y la disponibilidad de los sistemas computacionales, redes e información computacional, como el mal uso de dichos sistemas, redes e información, mediante la penalización y adopción de medidas necesarias para

²⁶⁵ MAGLIONA. Delincuencia informática. Op. cit. 12p.

²⁶⁶ Cuyo texto fue consultado en: [en línea] www.conventions.coe.int/Treaty/en/Treaties/Html/185-SPA.htm [consulta: 4 diciembre 2006].

²⁶⁷ MAGLIONA. Delincuencia informática. Op. cit. pp.11-13.

combatir efectivamente dichas conductas, mediante la facilitación de la detección, investigación y procesamiento de las mismas, tanto a nivel nacional como internacional, junto a una rápida y confiable cooperación internacional”.

Para estos efectos está organizada en cinco títulos, los que deberán ser incorporados a los ordenamientos jurídicos nacionales de los países que se suscriban a la convención. El título nº 1 se trata de delitos en contra de la confidencialidad, integridad y disponibilidad de sistemas e información computacional. Se sanciona el acceso no autorizado, la interceptación de datos, la alteración de datos, la intervención de sistemas y el mal uso de instrumentos (incluyendo virus computacionales) para cometer las conductas antes mencionadas. Luego el título nº 2 se refiere a delitos relacionados con la informática. Se sanciona la falsificación informática y el fraude informático. El título nº 3, a su vez, trata de delitos relacionados con el contenido. Se sanciona la difusión de pornografía infantil. El título nº 4 busca atender a los delitos relacionados con las infracciones a la propiedad intelectual y derechos conexos. Se sanciona la difusión de obras protegidas en infracción a las normas sobre propiedad intelectual y derechos conexos. Por último el título nº 5 trata los delitos relacionados con la colaboración y encubrimiento de las conductas mencionadas en los títulos anteriores. En este título se contempla además la posibilidad de hacer responsables a las personas jurídicas por las conductas realizadas en su beneficio por personas naturales.

Por otro lado también contiene normas comunes al procedimiento, investigación, prueba (recopilación de datos informáticos en tiempo real, interceptación de datos, etc.) y competencia, que deberán adoptar los Estados.

En cuanto a cooperación internacional también adopta posiciones, señala las normas generales que regularán dicha cooperación, normas sobre extradición, mutua asistencia, normas sobre cooperación en la investigación y

prueba de delitos informáticos. La Convención otorga a la policía la posibilidad de obligar a empresas a conservar datos de divulgación, tráfico y conexión, para poder rastrear el origen de un ataque informático.

Respecto a esto último subyace nuestra crítica fulminante acerca de éste cuerpo normativo, a pesar de que contiene tipos interesantes para darle tratamiento a las conductas delictivas de intervención indiscriminada de las comunicaciones electrónicas, en cuanto, respecto a los procedimientos de investigación y mutua asistencia asociados a la cooperación internacional, cae en afectación de los derechos fundamentales. Nuevamente MAGLIONA²⁶⁸ nos coopera en ilustrar esta realidad: “Grupos defensores de la privacidad y de los Derechos Humanos objetaron el borrador de la Convención, por la falta de resguardos procesales para proteger los derechos de las personas, y por la posibilidad de que leyes nacionales de los países suscriptores impongan restricciones a la privacidad, al anonimato y a la encriptación de datos”. La organización no gubernamental “*Global Internet Liberty Campaign*” (GILC), en su documento “Carta de la *Global Internet Liberty Campaign* (GILC) al Consejo de Europa acerca de la Convención sobre ciberdelitos, versión 24.2²⁶⁹”, de fecha doce de diciembre de 2001, señala un conjunto de críticas profundamente detalladas, clasificadas en varios puntos fundamentales.

En primer lugar señala: “El 18 de octubre de 2000 escribimos una carta en nombre de un amplio número de organizaciones de la sociedad civil para indicar nuestra oposición a la propuesta Convención sobre Ciberdelitos. En aquella carta presentábamos nuestra oposición a los temas relacionados con la criminalización de herramientas, la cuestión de la responsabilidad legal, las

²⁶⁸ Íbid. 13p.

²⁶⁹ GLOBAL INTERNET LIBERTY CAMPAIGN. 2001. Carta de la *Global Internet Liberty Campaign* (GILC) al Consejo de Europa acerca de la Convención sobre Ciberdelitos, versión 24.2 de fecha 12 de diciembre de 2001. [en línea] <www.gilc.org/privacy/coe-letter-1200-es.html> [consulta: 4 diciembre 2006].

sanciones sobre propiedad intelectual, a desarrollar la asistencia legal mutua y el aumento de la capacidad investigadora. Argumentábamos que la versión 2.2. de la convención representaba los intereses de las fuerzas de orden público y no ofrecía posibilidades para el control y la supervisión. El resultado final era una manifiesta falta de consideración a las libertades civiles”²⁷⁰.

A continuación destacamos en su primer apartado llamado “las excepciones plantean un problema de mayor envergadura”, las recomendaciones críticas realizadas²⁷¹:

- “Continuamos defendiendo que el uso de poderes invasivos ha de aplicarse sólo en caso de crímenes graves.
- La proporcionalidad es un concepto que ha de definirse a un nivel internacional, uniformemente, unilateralmente y en referencia a la jurisprudencia del Tribunal Europeo de Derechos Humanos.
- El acercamiento del actual borrador permitiendo excepciones y reservas en países individuales es erróneo y peligroso para los Derechos Humanos pues no es capaz de postular un límite aceptado a las intrusiones a la privacidad que estarían dentro de los objetivos de este tratado.
- Pedimos que la criminalidad dual sea un prerrequisito para todas las formas de asistencia mutua, y que estos crímenes se establezcan de forma específica.
- También pedimos la adición de un régimen consistente de protección a las libertades civiles dentro de las capacidades y poderes investigadores”.

²⁷⁰ Idem.

²⁷¹ Idem.

Las valiosas críticas desarrolladas por este documento no se detienen allí, luego en el apartado titulado "Poderes de Invasión"²⁷², indica:

"Continuamos oponiéndonos a los poderes y capacidades de interceptación y preservación de los datos sin un control suficiente.

- El artículo 19.4 continúa permitiendo la auto-incriminación al ordenar que un individuo que tiene conocimiento de los métodos de seguridad aplicados a datos de interés, tenga que ofrecer toda la información necesaria para registrar y requisar. Nos sigue preocupando que esto pueda ser una puerta para que los gobiernos accedan a las claves de descifrado con lo que se podría violentar el artículo 5º de la Convención Europea de Derechos Humanos.
- El artículo 20 sobre el acceso a los datos concernientes al tráfico no admite las características invasivas de esos datos, así como la división entre datos concernientes al contenido y al tráfico. De la misma forma no se define "datos concernientes al contenido".
- El añadido del artículo 20.2. acerca de recolección en tiempo real y la grabación de los datos a través de métodos técnicos parece ser una puerta para permitir sistemas como *Carnivore*.
- El añadido del artículo 21.2. permite -de forma similar "la recolección y grabación en tiempo real de datos de contenido a través de medios técnicos".

Recomendaciones acerca de estos poderes:

- Pedimos el establecimiento de límites claros para aquellos poderes y capacidades que impliquen situaciones en las que las

²⁷² Idem.

libertades civiles estén en compromiso. En particular, esperamos que esas técnicas invasivas se usen solamente en el caso de crímenes graves y donde esté claramente prevenida la auto-incriminación, así como otros derechos fundamentales, como la intimidad o la libertad de expresión tal y como se establecen en la Convención Europea de los Derechos Humanos, La Declaración Universal de los Derechos Humanos y el Convenio Internacional de Derechos Civiles y Políticos.

- Consideramos que la recolección de los datos concernientes al tráfico es una práctica invasiva y pedimos constreñimientos uniformes suficientes previos a la recolección.
- Pedimos una definición clara de "datos concernientes al contenido" y que se diferencien de los "datos concernientes al tráfico".
- Pedimos que se limiten los poderes de interceptación y el uso de herramientas para la recolección de datos de forma que se limite absolutamente la invasividad. Recomendamos que los artículos 20.2. y 21.2. sean reemplazados por un artículo protector que asegure que, si se usan medios técnicos, estos medios han de recoger solamente los datos de tráfico del usuario bajo investigación, obtener sólo los datos legalmente permitidos, impedir la modificación de los datos y respetar la división entre tráfico y contenidos. Si esto no puede asegurarse mediante una investigación independiente, estas técnicas han de considerarse ilegales (similar al artículo 3º) y no puede producirse ningún tipo de acceso o distribución de datos.
- La interceptación de las comunicaciones es una técnica invasiva que se usa a menudo contra disidentes y activistas pro Derechos Humanos en todo el mundo. Seguimos pidiendo que no se

establezca este requerimiento en una red de comunicaciones moderna, especialmente ahora que estas redes se están todavía definiendo y moldeando.

- El Consejo de Europa ha establecido públicamente la diferencia entre retención y preservación de datos. Sin embargo, considerando la discusión entre los G8 y recientemente en el Reino Unido, creemos que esta distinción requiere protecciones explícitas. Queremos que se observe el respeto internacional por la protección de datos tal y como recoge la Convención del Consejo de Europa de 1981 sobre protección de datos y la directiva de la Unión Europea para la protección de datos de 1995, y aplicar estos instrumentos a los datos concernientes al tráfico.

También ha de establecerse en esta convención un tope dentro del cual estas técnicas de investigación sean aceptables: un acceso injustificado y el almacenamiento masivo de datos son graves invasiones a nuestras libertades civiles”.

Del mismo modo, hacemos eco, en las críticas señaladas en el apartado “Extraterritorialidad indebida”²⁷³:

“La Convención contiene diversas afirmaciones sobre extraterritorialidad, recogidas especialmente en dos enunciados:

- El artículo 23 permite un alcance supranacional para los estados firmantes. Aunque hay una excepción en el sub-artículo 23.2. Como hemos expresado antes, si existe una excepción es porque a menudo esta medida va demasiado lejos.

²⁷³ Idem.

- La nota 29 que trata de la asistencia mutua según descrito en el artículo 27, especifica que "el hecho de que el sistema legal del miembro requerido no recoja un determinado procedimiento no es un argumento suficiente para rechazar la aplicación del procedimiento requerido por el otro miembro". Como resultado, los estados firmantes pueden ser obligados a actuar más allá de sus medios.

Recomendaciones sobre extraterritorialidad: pensamos que todas las indicaciones sobre extraterritorialidad son graves invasiones a la soberanía de las naciones con relación a la protección de los derechos de los individuos.

- Pedimos que se retire la nota 29 y que la filosofía que la apoya se considere no democrática.
- Requerimos que a los estados sólo se les permita actuar según métodos que son legales, resultado de acuerdos democráticos, como recoge la Convención Europea de Derechos Humanos; de otra forma, ello permitiría el uso de medias extremas extraterritorialmente, como podría ser el acceso del Reino Unido a claves de descifrado a partir de la ley RIP 2000 recientemente aprobada.
- Recomendamos la inclusión de una cláusula sobre la asistencia mutua que declara que cuando el miembro A pide ayuda al miembro B, B no pueda actuar usando medidas más poderosas que aquellas que se permiten en la jurisdicción de A, y el miembro B sólo puede actuar basándose en las leyes vigentes allí.

No queremos que la asistencia mutua aparezca como un arbitrio entre estados en la que tiene lugar diversas negociaciones para descubrir poderes y capacidades cada vez más grandes y más bajos niveles de protección".

Las aseveraciones antes citadas, nos parecen de vital importancia, por ello nos hemos permitido citar tal documento en forma extensiva, pues reflejan con gran precisión nuestras aprehensiones acerca del Convenio sobre Cibercriminalidad.

En suma, se torna urgente su modificación para que éste albergue el debido respeto y protección de los Derechos Humanos, en especial, el derecho a la privacidad y al secreto de las comunicaciones. Por otro lado, es necesaria la creación de un órgano jurisdiccional que trate los delitos que nos convocan.

4.5. Procedencia de una Acción de Protección en resguardo del Derecho a la Vida Privada, y a la Inviolabilidad de la Correspondencia.

La aplicación directa de la Constitución de 1980 ha marcado una pauta distinta en la defensa de los Derechos Fundamentales, en obsequio de la protección del ciudadano común, ofreciendo una garantía tal como es la acción de protección establecida en el artículo 20 de la carta fundamental. Nosotros somos de la opinión que esta acción, que ha perdido buena parte su auge, ganado en la década de los 90 del siglo pasado, en virtud del Auto Acordado sobre tramitación y fallo del recurso de protección de las garantías constitucionales, dictado por la Corte Suprema en junio de 1992 y modificado el nueve de junio de 1998; que ha dificultado de manera ostensible su admisibilidad (especialmente, en relación a la modificación de 1998).

Con todo, esta acción podría sernos de mucha utilidad para los propósitos de nuestra monografía, no en el sentido de perseguir penalmente a un agente extranjero, sino como un medio útil para la protección de de los

derechos vulnerados: a la vida privada y la inviolabilidad de las telecomunicaciones.

Así, podemos contemplar sin muchas dilaciones que se cumplen los requisitos mínimos establecidos por el artículo 20 de la Constitución: Existe un acto arbitrario e ilegal que es la intromisión no autorizada por el juzgado de garantía en nuestras telecomunicaciones; en este caso, la vulneración se verifica en sede de perturbación de un Derecho fundamental; además, también todo ciudadano tiene un legítimo ejercicio de esos derechos en el tráfico diario en la red.

De la misma manera, el sujeto legitimado activamente para impulsar esta acción es la persona natural a quién le resultaren intervenidas sus telecomunicaciones. Sin embargo ¿Cómo determinamos la legitimación pasiva? ¿A quién debemos demandar? Todo apunta a que *prima facie* se demande al sujeto que interviene las telecomunicaciones, en este caso, el agente de Estado extranjero. No obstante, en términos generales actúa por cuenta ajena, recibiendo ordenes de un superior, en el marco de una institución. También, y desde una perspectiva del sentido común, es sólo un engranaje de una compleja maquinaria de inteligencia, por lo que si se ve imposibilitado de intervenir los correos, puede hacerlo perfectamente otro sujeto. En fin, deberíamos determinar como legitimado pasivo a la institución extranjera que realiza las intervenciones, pero... ¿Podría realmente ser legitimado pasivo la NSA, la CIA, o el FBI? ¿Podría la Corte de Apelaciones, o la Corte Suprema, eventualmente, ordenar el cese de una intervención de esta índole? Al parecer, se observa que nada podría hacer un tribunal nacional por carecer de necesarias facultades, por lo que en este primer aspecto la demanda no podría proliferar.

También se debe solicitar al tribunal que vele por la inviolabilidad de la correspondencia y por el derecho a la vida privada. En este sentido, las medidas más asequibles que se podrían adoptar, para proteger al afectado, serían otorgar cuentas de correo electrónico nuevas, con anonimizadores y sistemas criptográficos afines. Una medida de mayor envergadura, como es el llamado a un Estado extranjero para que deje de revisar el correo electrónico de manera ilegal desde la perspectiva del Derecho chileno, parece poco probable, tanto por su inviabilidad de implementación real por los problemas políticos que acarrearía, como por la restricción de las atribuciones de los tribunales nacionales a conocer, fallar, y hacer ejecutar lo juzgado sólo los conflictos suscitados dentro del territorio nacional.

La aterritorialidad de Internet se vuelve a convertir entonces en un molesto convidado que no podemos expulsar de nuestras divagaciones.

Y aún suponiendo que tenemos un legitimado pasivo idóneo, tenemos que revisar el problema de determinar cuál es el tribunal competente para conocer de la acción de protección, dado que la ley establece que deberá ser el del lugar donde se hubiere cometido el acto ilegal o arbitrario²⁷⁴, está opinión es plenamente consonante con lo vertido en N° 1 el auto acordado de 1992²⁷⁵ ya mencionado. ¿En dónde ocurre realmente esa perturbación? Si un agente de Estado extranjero perpetra una violación de la correspondencia electrónica ¿El acto perturbador se posiciona en el país del agente, o en el domicilio del afectado? Ninguna de las leyes ya revisadas regula el problema en cuestión. Al

²⁷⁴ MATURANA MIQUEL, CRISTIÁN. 2003. Santiago, Chile. Los Recursos, Central de Apuntes de la Escuela de Derecho de la Universidad de Chile. 305p.

²⁷⁵ CORTE SUPREMA DE JUSTICIA, Auto Acordado. Op. cit.: N° 1:°.- El recurso o acción de protección se interpondrá ante la Corte de Apelaciones en cuya jurisdicción se hubiere cometido el acto o incurrido en la omisión arbitraria o ilegal que ocasionen privación, perturbación o amenaza en el legítimo ejercicio de las garantías constitucionales respectivas, dentro del plazo fatal de quince días corridos contados desde la ejecución del acto o la ocurrencia de la omisión o, según la naturaleza de éstos, desde que se haya tenido noticias o conocimiento cierto de los mismos, lo que se hará constar en autos.”

menos, está claro que los efectos del acto ocurren en Chile, y que su ejecución es fuera de nuestro país, como se explicó en la cuestión de la territorialidad, en capítulos anteriores.

Nuestra opinión es que, para estos efectos, y dado el nulo resguardo en sede penal ya explicado, debiera atenderse a donde se producen los efectos de la acción ilegal o arbitraria. Más, nos parece que la procedencia de esta acción se vería trucada en la realidad, y sería desechada por la incompetencia del tribunal, en razón del criterio restrictivo, ya mencionado, que han adoptado las Cortes de Apelaciones y la Corte Suprema, que es fruto del mencionado auto acordado.

Así, y con todo, parece casi nulo que una acción de protección tenga un resultado efectivo, ya fuere tanto por la incompetencia del tribunal por efectuarse el acto fuera del territorio nacional, por las menesterosas medidas que podría adoptar en pro de la privacidad de un ciudadano común y corriente, y también por las dificultades de perseguir al legitimado pasivo. Tristemente, si a esto le intentamos dar una cuota de mayor realismo, a un ciudadano ordinario le costaría más barato invertir dinero en adquirir *softwares* que mejoraren las condiciones de seguridad y de inviolabilidad de su privacidad electrónica, que gastar dinero en sede judicial para defender sus intereses. Quizá si se demandara bajo un *litis consorcio* activo entre muchos sujetos, podría lograrse otro resultado, pero la competencia de las Cortes de Apelaciones vuelve a ser el problema otra vez, y sólo nos quedaría terreno para una especulación de lo improbable

CONCLUSIONES

La intervención en las telecomunicaciones electrónicas por parte de los agentes de Estado extranjero es una realidad, así lo demuestra la evidencia ya analizada a lo largo del presente trabajo. Es más, la violación a los Derechos Fundamentales, específicamente el derecho a la vida privada y su manifestación concreta en el derecho al secreto en las comunicaciones, está institucionalizada, ya que está entregada a agencias de inteligencias de determinadas potencias, donde tiene un rol preponderante Estados Unidos y la Unión Europea, miembros fundadores de la red ECHELON e ENFOPOL, respectivamente. Del mismo modo han desarrollado *softwares* de intervención como el temido “Carnivore”.

El camino ha sido largo y lleno de reflexiones. En un principio nos planteamos una serie de hipótesis y objetivos, que fuimos corroborando o descartando. En primer lugar efectivamente existen medios de protección jurídicos de los derechos a la privacidad e inviolabilidad del correo electrónico, en el ordenamiento jurídico nacional e internacional, reflejados principalmente en la Constitución Política de la República y en los tratados internacionales ratificados por Chile, tales como la Convención americana sobre los Derechos Humanos y la Declaración Universal de Derechos políticos y civiles; sin embargo, no son eficaces, por no existir los mecanismos jurídicos de protección adecuados. Agreguemos a esto, que los Estados Unidos en el transcurso de la llamada “Guerra contra el terrorismo” han desarrollado una política expansionista, en sus atribuciones de investigación y persecución de los delitos que ellos estiman lesivos a sus intereses políticos, en ese sentido, fácticamente han consagrado, unilateralmente, el principio de jurisdicción universal, tal como se ve reflejado en la U.S.A Patriot act y el Convenio sobre el Cibercrimen; de

forma tal, que poseen poder para respaldar sus pretensiones políticas y de paso, violan, flagrantemente, Derechos fundamentales.

Específicamente, nuestro ordenamiento jurídico contempla tipos afines para la persecución de esta clase de delitos, a saber, el artículo 161-A del Código Penal, la ley N° 19.223, sobre “delitos informáticos. Además, en sede adjetiva, se dispone del procedimiento de extradición, el cual es útil para nuestros fines, inmerso en el nuevo proceso penal. Sin embargo, no parecen adecuados, desde una perspectiva penal material, los tipos albergados en la legislación chilena. Los errores conceptuales, la insuficiencia en las hipótesis cubiertas y la antigüedad de las leyes vigentes en la materia, tornan dificultoso, jurídicamente hablando, un adecuado tratamiento penal de estas conductas delictivas. Por otro lado, desde una perspectiva procesal, no se dispone de la doble tipicidad requerida, ni tampoco se cumplen los requisitos de cuantía del artículo 431 del Código Procesal Penal, que en suma hacen improcedente la extradición activa para estos casos concretos.

Con todo, y aún suponiendo la existencia de un procedimiento eficaz, el problema probatorio es evidente, no por su imposibilidad fáctica, sino por los costos que debería franquear el ciudadano común para aportar antecedentes fehacientes, que den pie, a la fructificación de una investigación penal, con la consecuente formalización de un eventual imputado.

Se analizaron otras vías alternativas, a las que pueda recurrir el ciudadano común, para reclamar la protección de su privacidad y secreto de las comunicaciones, frente a una intervención indiscriminada de sus telecomunicaciones electrónicas. En el ámbito jurisdiccional local, la acción de protección, resultaría en el plano teórico como eficaz, puesto que tiene el soporte de la Constitución, que la consagra como la acción cautelar por

excelencia y la misma Carta Fundamental, en el artículo 19 N° 5 reconoce el derecho a la inviolabilidad las comunicaciones. No obstante, en el plano práctico, el Autoacordado sobre la tramitación del recurso de protección, modificado el año 1998, restringe la procedencia de éste, y más aún establece como competencia de la Corte de Apelaciones, del lugar donde se verifica la perturbación. ¿Existen Cortes de Apelaciones competentes, para nuestro ordenamiento, en Missouri, Nebraska, Massachussets, Baviera o en Okinawa?. Al parecer no, y justamente en el extranjero se verifica el lugar de la comisión del delito.

En otra vertiente, existen instrumentos internacionales que podrían tutelar la privacidad de nuestros ciudadanos. Nos referimos a la Convención americana sobre Derechos Humanos, con sus órganos de la Comisión y, particularmente la Corte interamericana de Derechos Humanos. Sin embargo, como bien es sabido, los tratados internacionales, según las reglas del Derecho Internacional, requieren de la adhesión de los países, para entenderse por eficaces en el plano del derecho interno de los Estados ratificantes. Ello, respecto del particular, no ocurre con las naciones americanas, miembros de la red de intervención internacional de las telecomunicaciones; tornando muy improbable, jurídicamente, la persecución penal de los delitos. Lo mismo ocurre con el Convenio sobre el Cibercrimen, el cual no goza de la ratificación de nuestro país, apartándolo como parte integrante del Derecho nacional.

Respecto a los objetivos específicos del estudio, con intranquila satisfacción, logramos describir los principales problemas procesales y penales alusivos a la intervención en las telecomunicaciones electrónicas y demostrar su ineficacia. En nuestras pesquisas encontramos una nula jurisprudencia nacional e internacional respecto al tema en comento; la doctrina nacional (de la cual no somos ajenos), a su vez, se encuentra en un estado embrionario acerca

de la discusión sobre la intervención de las telecomunicaciones electrónicas, realidad que contrasta con el contexto iberoamericano y anglosajón, donde el tema, si bien no detenta una lata discusión, se encuentra ostensiblemente mejor tratado.

También, con poco asombro y mucho desconcierto, analizamos la principal legislación extranjera que propugna la intervención de las telecomunicaciones, en específico, nos referimos a la U.S.A. Patriot act y al Convenio sobre la Cibercriminalidad; evidenciamos sus rasgos atentatorios contra los Derechos Humanos y Fundamentales que se extienden a nuestros conciudadanos, principalmente debido a las pretensiones de aplicación extraterritorial unilateral que guarda, o dicho de otro modo, efectivamente, buscan influenciar al ordenamiento jurídico nacional chileno.

Evaluamos los mecanismos de protección nacionales a nivel de protección de la privacidad de las telecomunicaciones vía Internet, sin sorprendernos al notar la insuficiencia e ineficacia para estos efectos. Por lo tanto, es nuestra labor y responsabilidad como autores hacernos cargo, al menos en la teoría y en la especulación, de estas insuficiencias.

Las insuficiencias son críticas, mas nuestro propósito no es el pesimismo sino la solución de problemas concretos. Así, en el corto plazo y con independencia de las contingencias políticas imperantes, concluimos que la forma inmediata y más efectiva de resguardar los derechos a la privacidad y a la inviolabilidad de la correspondencia es la adopción de medidas político-criminales preventivas, respaldada con programas anonimadores y criptográficos. Si bien estos mecanismos de seguridad son vulnerables, al menos dan mayor tranquilidad que la de dejar nuestra correspondencia desnuda y visible. El acceso a estos medios, pensamos, debiera ser asegurado

por el Estado, ya fuera con una entrega directa o mediante incentivos económicos al desarrollo e internación de software de seguridad. Ahora bien, el grado de intervención del Estado podría verse limitado por el principio de subsidiaridad, tan bullado en el desarrollo del Derecho chileno, en relación a nuestro modelo económico imperante, mas esta discusión es quizá anticiparse a una actuación que el Estado aún no ha desarrollado, por lo que cuando suceda, cabrá plantearse y continuar con la discusión alusiva a las medidas político-criminales de carácter preventivas asistida en pro del resguardo de los derechos mencionados.

Del mismo modo, estamos en contra de toda política de limitación a la producción y tráfico de *softwares* de seguridad y anonimización, pues es una actividad necesaria para el resguardo de la vida privada y de la inviolabilidad de las telecomunicaciones. Si bien estos mecanismos de seguridad pueden ser usados por grupos violentos para la consecución de sus fines, no deberíamos preguntarnos cómo reprimirlos vulnerando los derechos de todos, sino estudiando las causas verdaderas del problema; es decir, no todos los ciudadanos debemos pagar el precio de la proliferación de la violencia como consecuencia de una imprudente conducción política, y en este caso concreto, una actividad política imprudente y expansionista de los Estados Unidos.

Sin embargo, y proyectándose en el futuro, el Derecho se ve en la obligación de brindar soluciones de protección eficaces, puesto que esa es su principal labor como herramienta de solución de conflictos sociales, y porque en la actualidad los existentes son francamente insuficientes. Más aún cuando en las conductas delictivas tratadas se vulneran gravemente los Derechos Humanos. Se trataría de una de las grandes deudas que mantiene la comunidad internacional con los internautas, la de otorgar medios de protección jurídicos coherentes y que tengan la fortaleza suficiente para restringir la

intervención de las telecomunicaciones electrónicas personales, exclusivamente a aquellos casos que dichas comunicaciones guarden el peligro real de ser vehículo de cobertura logística de peligros inminentes para la paz, la democracia y estabilidad política de nuestros países. Sostenemos que, una cooperación internacional real, coherente y eficaz es el único medio, para que en el largo plazo, se adopten las medidas jurídicas pertinentes en pos de una adecuada protección de la privacidad electrónica, para que de este modo, los ordenamientos jurídicos de los distintos países se uniformen con base en un único modelo, y así, se avance en el resguardo universal de los Derechos Humanos. Creemos que la cooperación internacional es el único medio, porque la naturaleza de la comisión de estos delitos, generan, que por regla general, el acto de comisión se realice en el territorio de un país, pero las consecuencias gravosas se manifiestan en otros tantos. A su vez, los Derechos Humanos deben servir de criterio universal de justicia, que se anteponga a la discusión de la aplicación de la ley penal en el espacio. Es decir, la soberanía de los países debe ceder frente a razones de justicia material superiores, que subyacen en los dichos derechos.

En razón de estas argumentaciones es que proponemos de *lege ferenda* la derogación y sustitución por otra ley de buena calidad, o al menos la modificación de la ley N° 19.223, sobre delitos informáticos, debido a: lo doctrinariamente atrasada que está, los errores conceptuales en que incurre y lo inespecífica que es para contemplar la gran gama de modalidades de ilícitos que se pueden cometer gracias a los avances de la informática. Debemos, en este punto, apoyar a los juristas nacionales, que ya larga y fulminantemente, la han criticado. Es decir, los legisladores nacionales deben acoger estas críticas técnico-jurídicas, reformular sus políticas legislativas para enfrentar los delitos informáticos, y por su puesto, contemplar la hipótesis de intervención

indiscriminada de las telecomunicaciones electrónicas realizadas por agentes de Estado extranjeros.

Otro tanto similar, alternativamente, podría ocurrir con el artículo 161-A del Código Penal, incorporado por la ley N° 19.423.

Respecto a si nos parece necesario reducir los requisitos de cuantía para que la extradición fuera procedente, parece necesario advertir que es atentatorio contra el garantismo, pues se debiera del mismo modo rebajar las cuantías para extradiciones de otros delitos, por lo que se generan mayores y variadas hipótesis de extradición y punición. En consecuencia, podría ser más perjudicial la solución al problema que el problema mismo.

En cuanto al análisis de la acción de protección, el problema de la legitimación pasiva es la improcedencia fáctica y jurídica del cese de las intervenciones estudiadas. Y aun solucionándose ese escollo, queda también el problema de la competencia de la Corte de Apelación a la del lugar donde se encuentra el afectado, y no a la del lugar donde se verifica la vulneración. Ergo, la acción de protección es inidónea para solucionar este tipo de problemas.

En el ámbito internacional, pareciera también procedente restringir las competencias arrogadas por la U.S.A. Patriot act para que sea respetuosa de los Derechos Fundamentales de nuestros conciudadanos. Así mismo, es deseable que nuestros legisladores y tribunales de justicia se enfrenten a las pretensiones de extraterritorialidad unilateral de los Estados Unidos de América, entre otros motivos, para resguardar los Derechos Humanos y Fundamentales que nuestros antepasados han conseguido a costa de largas luchas y decepciones, y que son el estandarte de la inagotable vocación del Derecho por reducir la brutalidad y la violencia en la existencia de la humanidad.

BIBLIOGRAFÍA

1. ABEDRAPO BUSTOS, E. 1996. Ley 19.223 sobre Delitos Informáticos. Memoria de Licenciado en Ciencias Jurídicas y Sociales. Santiago, Chile, Facultad de Derecho, Universidad de Chile.
2. ADAME MARTÍNEZ, MIGUEL ANGEL. 1998. Derecho en Internet. Sevilla, España, Edit. Mergablum.
3. ALDUNATE, EDUARDO. 2005. La Colisión de Derechos Fundamentales. Revista Derecho y Humanidades (11). Santiago, Chile, Facultad de Derecho, Universidad de Chile.
4. ALVÁREZ GONZÁLEZ, JOSÉ JULIÁN. 2005. Colisión entre los Derechos Fundamentales a la libre expresión y a la intimidad y dignidad humana en los Estados Unidos y Puerto Rico. Revista Derecho y Humanidades (11). Santiago, Chile., Facultad de Derecho, Universidad de Chile.
5. ÁLVAREZ VALENZUELA D. y CERDA SILVA A. 2005. Sobre la inviolabilidad de las comunicaciones electrónicas. Ley N° 19.927 que tipifica los delitos de pornografía infantil. En: [en línea] Anuario de Derechos Humanos. 2005. Santiago Chile. Centro de Derechos Humanos, Facultad de Derecho, Universidad de Chile, consultado en www.anuariocdh.uchile.cl/anuario1/13inviolabilidad-comunic-electronica.pdf > [consulta: 3 de Diciembre 2006].

6. BARATTA, ALESSANDRO. 1986. Requisitos Mínimos del respeto de los derechos humanos en la ley penal. Revista Nuevo Foro Penal (34), Bogotá, Colombia.
7. BARROSO, PORFIRIO y LOPÉZ TALAVERA, MARÍA DEL MAR. 1998. La Libertad de Expresión y sus Limitaciones constitucionales, Madrid, España, Editorial Fragua.
8. BELDA PÉREZ- PEDRERO, Enrique. 1998. El Derecho al secreto de las comunicaciones. [en línea] Parlamento y Constitución. Anuario (2). <www.dialnet.unirioja.es/servlet/articulo?codigo=197133> [consulta: 13 enero 2007].
9. BUSTOS RAMÍREZ, J. 2005. La Política Criminal y el Derecho Penal. En: Lecciones de Derecho Penal. Parte primera. En: Obras Completas, volumen II, Lima, Perú, Edit. Aranzadi.
10. BUSTOS, J. y HORMAZÁBAL, H. 1997. Lecciones de Derecho Penal, volumen I. Madrid, España, Editorial Trotta.
11. CAMACHO LOSA, L. 1987. El Delito Informático. Madrid, España, Gráficas Cóndor.
12. CAMPBELL, DUNCAN. 2001. Silencio, se espía. [en línea] El Correo de la UNESCO, marzo, 2001. <http://www.unesco.org/courier/2001_03/sp/doss10.htm>, [consulta: 6 de enero del 2007].

13. CANO MARTÍNEZ, JEIMY JOSÉ. 2003. Admisibilidad de la Evidencia Digital: Algunos Elementos de Revisión y Análisis. [en línea] Revista de Derecho Informático Alfa-Redi (61), <<http://www.alfa-redi.org/>> [consulta: 4 de diciembre 2006].
14. CANO MARTÍNEZ, JEIMY JOSÉ. 2005. Estado del Arte del Peritaje informático en Latinoamérica. [en línea] Revista de Derecho Informático Alfa-Redi. <<http://www.alfa-redi.org/>> [consulta: 4 diciembre 2006].
15. CHILE. Ministerio de Justicia. 1855. Código Civil. 22 noviembre 1855. [en línea] <www.bcn.cl> [consulta: 22 enero 2007].
16. CHILE. Ministerio de Justicia. 1874. Código Penal. 12 noviembre de 1874. [en línea] <www.bcn.cl> [consulta: 22 enero 2007].
17. CHILE. Ministerio de Justicia. 1902. Ley nº 1552: Código de Procedimiento Civil. 30 agosto 1902. [en línea] <www.bcn.cl> [consulta: 22 enero 2007].
18. CHILE. Ministerio de Relaciones Exteriores. 1934. Código de Derecho Internacional Privado Decreto nº 374 del Ministerio de Relaciones Exteriores. 25 abril 1934. [en línea] <www.bcn.cl> [consulta: 22 enero 2007].
19. CHILE. 1943. Ministerio de Justicia. Ley nº 7421: Código Orgánico de Tribunales. 9 Julio 1943 [en línea] <www.bcn.cl> [consulta: 22 enero 2007]. En adelante cuando nos refiramos al Código orgánico aludiremos al chileno.

20. CHILE. 1948. Declaración Universal de Derechos Humanos. 10 diciembre 1948. [en línea] <<http://www.ddhh.gov.cl/>> [consulta: 22 enero 2007].
21. CHILE. 1980. Constitución Política de la República. 24 octubre 1980. [en línea] <www.bcn.cl> [consulta: 22 enero 2007].
22. CHILE. 1989. Pacto de Derechos Civiles y Políticos. 29 abril 1989. [en línea] <www.bcn.cl> [consulta: 22 enero 2007].
23. CHILE. Convención americana sobre Derechos Humanos, denominada “Pacto de San José de Costa Rica” .1991. Presidente de la República, PATRICIO AYLWIN AZOCAR. 5 enero 1991. [en línea] < www.bcn.cl> [consulta: 23 enero 2007].
24. CHILE. Corte Suprema de Justicia.1992. Auto Acordado sobre la Tramitación del Recurso de protección de garantías constitucionales. 27 de Junio de 1992 (modificado por el auto acordado de 4 de Mayo de 1998).
25. CHILE. Corte Suprema de Justicia.1992. Auto Acordado sobre la Tramitación del Recurso de protección de garantías constitucionales. 27 de Junio de 1992 (modificado por el auto acordado de 4 de Mayo de 1998).
26. CHILE. Fiscalía Nacional. 2000. Instructivo General N° 36 Sobre Criterios de Actuación e Instrucciones en Materia de Suspensión Condicional del Procedimiento, Santiago, 15 Diciembre del 2000.

27. CHILE. Fiscalía Nacional. 2000. Instructivo General N° 36 Sobre Criterios de Actuación e Instrucciones en Materia de Suspensión Condicional del Procedimiento, Santiago, 15 Diciembre del 2000.
28. CHILE. Ministerio de Justicia. 2000. Ley n° 19.696: Código Procesal Penal. 12 octubre 2000. [en línea] <www.bcn.cl> [consulta: 22 enero 2007].
29. CHILE. Ministerio de Justicia. 2004. 19.927: Modifica el Código Penal, el Código Procedimiento Penal y el Código Procesal Penal en materia de delitos de pornografía infantil. 14 enero 2004. [en línea] <www.bcn.cl> [consulta: 22 enero 2007].
30. CHILE. Ministerio de Justicia. 2005. 20.074: Modifica los Códigos Procesal Penal y Penal. 14 noviembre 2005. [en línea] <www.bcn.cl> [consulta: 22 enero 2007].
31. CLIMENT BARBERÁ, JUAN. 2001. La justicia penal en Internet. Territorialidad y competencias penales. En: Internet y derecho penal. Madrid, España, Consejo General del poder judicial, Editorial Lerko Print S.A.
32. COMISIÓN DE CONTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO. 1993. Informe, recaído en el proyecto de ley, iniciado en moción del honorable senador señor Otero, que modifica el Código Penal a fin de cautelar efectivamente la privacidad de las personas, n° 2.241, de 16 de Junio de 1993. [en línea] <www.sil.senado/docsil/info2241.doc> [consulta. 29 noviembre 2006].

33. CONSEJO DE EUROPA. 1950. Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. 4 noviembre 1950. [en línea] <<http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/SpanishEspagnol.pdf>> [consulta: 22 de enero 2007].
34. CONSEJO DE EUROPA. 2001. Convenio sobre Cibercriminalidad. 23 de Noviembre del 2001. [en línea] <<http://conventions.coe.int/treaty/en/Treaties/Html/185-SPA.htm>> [consulta: 23 enero 2007].
35. COSTA, SILVIO. 2003. El sistema ECHELON de espionaje global o la ley del todo vale. [en línea] Rebelión. <<http://www.rebellion.org/cibercensura/costa210103.htm>> [consulta: 17 enero 2007].
36. CURY URZÚA, E. 1988. Derecho Penal. Parte General, tomo 1. Santiago, Chile, Editorial Jurídica de Chile.
37. DAMASKA, MIRJAN R. 2000. Las caras de la Justicia y el Poder el Estado, traducción de MORALES VIDAL, ANDREA, y RUIZ-TAGLE, PABLO. Santiago, Chile, Editorial Jurídica de Chile.
38. DE VEGA, PEDRO. 1998. Mundialización y Derecho Constitucional, para una palingenesia de la realidad constitucional. En: Memorias del VI Congreso Iberoamericano de Derecho Constitucional: 15 al 17 de abril de 1998. Santa Fe de Bogotá, Colombia, Universidad Externado de Colombia.

39. DEL PIAZZO, CARLOS. 2006. Los Derechos Humanos ante las Nuevas Tecnologías. [en línea]. Revista de Derecho Informático Alfa-Redi. Num. 48 <<http://www.alfa-redi.org/rdi-articulo.shtml?x=1478>>. [consulta: 5 diciembre 2006].
40. DERECHO PROCESAL PENAL. 1999. por Andrés de la Oliva Santos “et al”. Madrid, España, Editorial Centro de Estudios Ramón Areces S.A.
41. DIAZ ELIAS. 1976. Socialismo Democrático y Derechos Humanos. En: FERNANDO TORRES (Editor). Política y Derechos Humanos. Valencia, España.
42. DÍAZ LEVANO, CAROLINA, y PERAZA DARVE, MARÍA LAURA. 2005. La Criptografía: "Una guerra de Piratas y Corsarios". [en línea] Revista de Derecho Informático Alfa-Redi, Num. 82. [<http://www.alfa-redi.org/rdi-articulo.shtml?x=950>]. <<http://www.alfa-redi.org/rdi-articulo.shtml?x=950>>, [consulta: 15 enero 2007].
43. ESTADOS UNIDOS DE AMÉRICA. 2001 Patriot Act. Senado de los Estados Unidos. 24 octubre 2001. [en línea] Ciber P@is. <www.palomallaneza.com/ciber/usapa.htm>, [consulta: 3 julio 2006].
44. ETCHEBERRY, A. 1976. Curso de Derecho Penal. Santiago, Chile, Editorial Gabriela Mistral.
45. FERNÁNDEZ ALLER, CELIA y SUÁREZ SÁNCHEZ DE LEÓN, JOAQUÍN MARÍA. 1999. Informática para Abogados. Madrid, España, Ediciones Anaya Multimedia S.A.

46. FERRAJOLI, LUIGI. 1995. El Derecho Penal Mínimo. En: Prevención y Teoría de la Pena. Juan Bustos (director) Santiago, Chile, Ed. Jurídica Conosur Ltda.
47. FERRAJOLI, LUIGI. 2000. El garantismo y la filosofía del derecho. Colombia. Universidad Externado.
48. FERREYROS SOTO, C. 1996. Aspectos metodológicos del delito informático. Mérida, España, ID UNED.
49. GARCÍA-HUIDOBRO, JOAQUÍN. 2005. Conflicto de Derechos. Revista Derecho y Humanidades (11). Santiago, Chile, Facultad de Derecho, Universidad de Chile.
50. GARRIDO MONTT, M. 2003. Derecho Penal Parte General, tomo I. 1ª edición 2003. Santiago, Chile, Editorial Jurídica de Chile.
51. GLOBAL INTERNET LIBERTY CAMPAIGN. 2001. Carta de la *Global Internet Liberty Campaign* (GILC) al Consejo de Europa acerca de la Convención sobre Ciberdelitos, versión 24.2 de fecha 12 de diciembre de 2001. [en línea] <www.gilc.org/privacy/coe-letter-1200-es.html> [consulta: 4 diciembre 2006].
52. GONZÁLEZ NAVARRO, BLAS ALBERTO. 2001. Criptología y libertades públicas. En: LOPEZ ORTEGA, JUAN JOSÉ (Compilador). Internet y Derecho Penal. Madrid, España Cuadernos de Derecho Judicial, Consejo General del Poder Judicial. pp. 147-237. 152p.

53. GONZÁLEZ RUS, J. J. 1999. Protección penal de sistemas, elementos, datos, documentos y programas informáticos. [en línea]. Revista Electrónica de Ciencia penal y criminológica, (01-14). <<http://criminet.ugr.es/recpc/>> [consulta: 16 enero 2007].
54. GONZÁLEZ, JUAN CARLOS. 2001. UNA COMISIÓN DE LA EUROCÁMARA confirma la existencia de ECHELON. [en línea] El Mundo, España, jueves 8 de Marzo, 2001. <<http://www.elmundo.es/navegante/2001/03/08/seguridad/984041457.html>>. [consulta: 6 enero 2007].
55. GUTIÉRREZ FRANCÉS, M. L. 1991. Fraude Informático y Estafa. Madrid, España, Ministerio de Justicia, Secretaría General Técnica, Centro de Publicaciones.
56. HASSEMER, W. 1999. Perspectivas del derecho penal futuro.
57. HERNÁNDEZ BASUALTO, H. 2001. Tratamiento de la criminalidad informática en el Derecho Penal chileno. Diagnóstico y Propuestas. Chile, Universidad Andrés Bello, 2001.
58. HERRERA BRAVO, R. 1993. Reflexiones sobre los Delitos Informáticos motivadas por los desaciertos de la Ley Chilena Nº 19.223. [en línea] <<http://www.ctv.es>> [consulta: 30 noviembre 2006].
59. HORVITZ LENNON, MARÍA INÉS y LÓPEZ MASLE, JULIÁN. 2002. Derecho Procesal Penal Chileno, Tomo I. Santiago, Chile, Editorial Jurídica de Chile.

60. HUERTA MIRANDA, Marcelo. Figuras delictivo informáticas tipificadas en Chile. S.a. S. num. [en línea] Revista de Derecho Público de la Contraloría General de la República de Chile. <www.bcn.cl> [30 noviembre 2006].
61. HUERTA, M. y LÍBANO, C. 1996. Delitos Informáticos. Chile. Editorial Jurídica Conosur Ltda.
62. INFORME ANUAL SOBRE LOS DERECHOS HUMANOS EN CHILE. 2004: Sistema judicial y protección de derechos. [en línea] Universidad Diego Portales. <www.bcn.cl> [consulta: 29 noviembre 2006].
63. JIJENA LEIVA, R. 2004. La criminalidad informática. Análisis de la ley 19.223, sus antecedentes y modificaciones en curso. [en línea] <www.sdi.bcn.cl/partners/e-derecho/Ponencias/ver_po/p55> [consultado con fecha 5 de diciembre de 2006].
64. JIJENA LEIVA, RENATO. Sobre la Confidencialidad e Inviolabilidad de los Correos Electrónicos. [en línea] <<http://www.ecampus.cl/ecampus/home/htm/Textos/derecho/jijena/1/jijena1.htm>> [consulta: 3 noviembre 2006].
65. JIJENA, LEIVA, R. 1992. Chile la protección penal de la intimidad y el delito informático. Santiago, Chile, Editorial Jurídica de Chile.
66. LAGO, MARÍA. SOLEDAD. 2001. Sistemas mundiales de interceptación de las comunicaciones. En: Programa de actualización de Derecho Informático, Curso de posgrado de Régimen jurídico de los bancos de

datos, Buenos Aires, Argentina, Universidad de Buenos Aires, Facultad de Derecho.

67. LEONE, GIOVANNI. 1963. Tratado de Derecho Procesal Penal, Tomo I. Traducción de SENTÍS MELENDO, SANTIAGO. Buenos Aires, Argentina, Ediciones Jurídicas Europa-América.
68. MAGLIONA, CLAUDIO. 2002. Delincuencia informática en Chile. Proyecto de ley. [en línea] Revista de Derecho Informático Alfa-Redi (50) <www.alfa-redi.org> [30 de noviembre de 2006].
69. MANZINI, VICENZO. 1951. Tratado de Derecho de Procesal Penal, Tomo I, traducción SENTÍS MELENDO, SANTIAGO, y AYERRA RENDÍN, MARINO. Buenos Aires, Argentina, Ediciones Jurídicas Europa-América.
70. MATURANA MIQUEL, CRISTIÁN. 2002. Responsabilidad de los proveedores de acceso y de contenido en Internet. Revista Chilena de Derecho Informático Facultad de Derecho, Universidad de Chile, Santiago, Chile.
71. MATURANA MIQUEL, CRISTIÁN. 2003. Santiago, Chile. Los Recursos, Central de Apuntes de la Escuela de Derecho de la Universidad de Chile.
72. MATURANA MIQUEL, CRISTIÁN. 2004. Separata de Introducción al Nuevo Sistema Procesal Penal. Santiago, Chile, Central de Apuntes de la Facultad de Derecho de la Universidad de Chile.

73. MENESES DÍAZ, C. 2002. Delitos informáticos y nuevas formas de resolución del conflicto penal. [en línea] Revista de Derecho Informático Alfa-Redi (51) <www.alfa-redi.org> [30 noviembre 2006].
74. MONTAÑÉS PARDO, Miguel Ángel. 1999. La intervención de las comunicaciones. Doctrina jurisprudencial. España, Editorial Aranzadi.
75. MOYA GARCÍA, RODRIGO. 2003. Libertad de expresión en la red Internet. Revista Chilena de Derecho Informático, Facultad de Derecho, Universidad de Chile, Santiago, Chile.
76. MUÑOZ ESQUIVEL, OLIVER. 2002. La Convención sobre delitos informáticos. [en línea] Revista de derecho Informático Alfa-Redi, (42). <www.alfa-redi.org> [consulta: 20 septiembre 2006].
77. NACIONES UNIDAS. 1998. Estatuto de Roma de la Corte Penal Internacional. 17 julio 1998. [en línea] <<http://www.derechos.net/doc/tpi.html>> [consulta: 23 enero 2007].
78. NOVOA MONREAL, E. 1985. Curso de Derecho Penal, tomo 1, 2º edición. Santiago, Chile, Editorial Jurídica Cono Sur.
79. PARLAMENTO EUROPEO investiga. 2004. [en línea] *News Room* del Parlamento Europeo. 2 de abril 2004. <<http://www.europarl.europa.eu/highlights/es/108.html>> [consulta: 6 enero 2007].
80. PATRIOT ACT. 2006. [en línea] Ciber P@is. <www.palomallaneza.com/ciber/usapa.htm>, [consulta: 3 julio 2006].

81. PECES-BARBA, G. 1999. Curso de Derechos Fundamentales. Teoría General. Madrid. España. Universidad Carlos III, Boletín Oficial del Estado de Madrid.
82. PERARNAU MOYA, JOÁN. 2001. Internet amenazada. En: Internet y derecho penal. Madrid, España, Consejo General del poder judicial. Editorial Lerko Print S.A.
83. PEREZ DEL VALLE, C. 1996. Sociedad del Riesgo y reforma penal, en Poder Judicial, 2ª y 3ª Época, Consejo General del Poder Judicial.
84. PIZZOLO CALOGERO. 1998. La relación constitución-globalización. Una visión desde el derecho constitucional americano. En: Memorias del VI Congreso Iberoamericano de Derecho Constitucional, 15 al 17 de Abril de 1998. Santa Fe de Bogotá, Colombia, Universidad de Externado de Colombia.
85. POLITOFF LIFSCHITZ, S. 1997. Derecho Penal. Santiago, Chile, Editorial Jurídica Conosur.
86. REUSSER, CARLOS. 2003. Internet, Conceptos Generales. Santiago, Chile, Centro de Estudios de Derecho Informático, Universidad de Chile.
87. RODRÍGUEZ BLANCO, B. 1998. La estructura del derecho de las comunicaciones. En: El secreto de las comunicaciones: tecnología e intimidad, cap. III, Madrid, España, editorial. Mcgraw-Hill.

88. RODRÍGUEZ MERINO, D. 2003-2004. Criminalidad e Internet. En: MIGUEL ÁNGEL DAVARA RODRÍGUEZ (coordinador). XVIII Encuentros sobre Informática y Derecho. 2003-2004. Madrid, España, Universidad Pontificia Comillas.
89. RODRÍGUEZ RUIZ, B. 1998. El secreto de las comunicaciones: tecnología e intimidad. Monografía. Madrid, España, Editorial McGraw-Hill.
90. ROMEO CASABONA, Carlos.; “Poder Informático y Seguridad Jurídica”, Fundesco, Madrid, España, 1987.
91. ROXIN, CLAUS. 2000. Derecho Procesal Penal, Traducción de CÓRDOBA, GABRIELA E., y PASTOR, DANIEL R. Buenos Aires, Argentina, Editores del Puerto.
92. SÁNCHEZ ALMEIDA, CARLOS. 2000. La Criptografía como Derecho. [en línea] Revista de Derecho Informático Alfa-Redi. <<http://www.alfa-redi.org/rdi-articulo.shtml?x=487>> [consulta: 3 noviembre 2006].
93. SEGUNDA SALA DE LA CORTE DE APELACIONES DE SANTIAGO. 2003. Sentencia, de fecha veintidós de diciembre de 2004, considerando 12º, letra a), en expediente caratulado “Guillier con Pérez”, Rol Nº 33.865-2003. [en línea] <www.lyd.com/noticias/sentencias/recurso_amparo_caratulado.pdf> [consulta: 30 noviembre 2006].
94. SEGUNDA SALA DE LA CORTE SUPREMA. 2004. Sentencia, de fecha seis de enero de 2004, considerando 5º, en expediente caratulado

- “Guillier con Pérez”, Rol N° 5.604-03. [en línea] <www.lyd.com/noticias/sentencias/recurso_amparo_caratulado.pdf> [consulta: 30 de Noviembre del 2006].
95. TAVOLARI OLIVEROS, RAÚL. 2000. El Proceso en Acción. Chile, Editorial Libromar.
96. TÉLLEZ VALDÉS, J. 1996. Los Delitos informáticos. Situación en México. En: Informática y Derecho (9) (10) y (11). Mérida, España, UNED, Centro Regional de Extremadura.
97. TIEDEMANN, K. 1985. Poder económico y delito. Barcelona, España, Editorial Ariel.
98. TINAJEROS ARCE, E. 2006. Nuevas formas de delinquir en la Era Tecnológica: Primeras observaciones sobre Espionaje, Fraude y Sabotaje Informático. [en línea] Revista Electrónica Alfa-redi (98) <www.alfa-redi.com> [consulta: 16 de enero 2007].
99. TREATY WATCH. *Eight reasons the International Cybercrime treaty should be rejected* [en línea] <www.treatywatch.org/about.html> [consulta: 20 septiembre 2006].
100. TRIBUNAL CONSTITUCIONAL. 2002. Fallo sobre Tribunal Penal Internacional. [en línea], Revista “*Ius et Praxis*”, v.8, n°1, Talca, Chile. <www.scielo.cl> [consulta: 14 Octubre 2006].

101. UNITED STATES OF AMERICA. What is the War on Terrorism? S.a. [en línea] <<http://www.whitehouse.gov/infocus/nationalsecurity/faq-what.html>> [consulta: 19 enero 2007].
102. VERA QUILODRÁN, A. 1996. Delito e Informática (La informática como fuente de delito), Santiago, Chile, Ediciones Jurídicas La ley.
103. VIGOROUX, A. 2002. Del Deber de Retención de los Datos de Tráfico relativos a las Comunicaciones Electrónicas. [en línea] Revista de Derecho Informático (49). <www.alfa-redi.org/rdi-articulo.shtml?x=1462> [consulta: 13 enero 2007].
104. VILLEGAS DIAZ, MYRNA. 2001. Terrorismo: Un problema de Estado, tratamiento jurídico en la legislación comparada. Especial referencia a los delitos de terrorismo en las legislaciones de Chile y España. Tesis de Doctor en Derecho. Salamanca, España, Área Penal, Departamento de Derecho Público, Universidad de Salamanca.
105. VILLEGAS DÍAZ, M. y LAVÍN ESPINOZA, M. 2005. Terrorismo e intervención penal en la red Internet .Uso de las tecnologías de la información y las comunicaciones en la represión penal del terrorismo. [en línea] Departamento de Investigación, Universidad Arcis. <<http://derecho.universidadarcis.cl/index.php?option=content&task=view&id=8&Itemid=45>> [consulta: 17 enero 2007].