BOLETÍN Nº 2.974-19

INFORME DE LA COMISIÓN DE CIENCIAS Y TECNOLOGÍA RECAÍDO EN EL PROYECTO DE LEY QUE MODIFICA LA LEY Nº 19.223, QUE TIPIFICA FIGURAS PENALES RELATIVAS A LA INFORMÁTICA.

HONORABLE CÁMARA:

Vuestra Comisión de Ciencias y Tecnología pasa a informaros el proyecto de ley, en primer trámite constitucional y reglamentario, iniciado en moción de los Diputados señores: Darío Paya Mira, Juan Bustos Ramírez, Sergio Correa de la Cerda, Camilo Escalona Medina, Andrés Egaña Respaldiza, Pablo Longueira Montes, Rosauro Martínez Labbé, Iván Moreira Barros, Iván Norambuena Farías y Patricio Walker Prieto, que modifica la ley Nº19.223, de 1993, que tipifica figuras penales relativas a la informática.

I.- CONSTANCIA PREVIA.-

Al proyecto de ley en informe, no se le ha hecho presente el trámite de urgencia, por parte del Ejecutivo.

Asimismo, no corresponde votar su articulado con quórum especial ni ser conocido por la Comisión de Hacienda.

* * * * * * * *

II.- MENCIÓN DE LAS PERSONAS ESCUCHADAS POR LA COMISIÓN.-

La Comisión contó con la participación permanente y activa del señor Fernando Londoño, abogado del Ministerio de Justicia y de la señora Alejandra Moya, abogada de la Subsecretaria de Telecomunicaciones, quienes en representación del Ejecutivo entregaron sus observaciones sobre la iniciativa legal y absolvieron las consultas de los señores Diputados.

Asimismo, la Comisión recibió a las siguientes personas quienes, en representación de sus instituciones proporcionaron su opinión:

-4 Don Fernando Londoño, abogado del Ministerio de Justicia;
-5 Doña Alejandra Moya, abogada de la Subsecretaria de Telecomunicaciones;
-6 Don Guillermo de la Vega Ivovic, Gerente de Servicios Empresariales de la Asociación Chilena de Empresas de Tecnologías de Información A. G. (ACTI);
-7 Don Rodrigo Rojas, abogado de la empresa SONDA;
-8 Don Armando Muñoz Moreno, Comisario, Jefe de la Jefatura de Comunicaciones de la Policía de Investigaciones de Chile;
-9 Don Alvaro Morales Torres, Subjefe de la Jefatura de Comunicaciones de la Policía de Investigaciones de Chile;
-10 Doña Lorena Donoso, abogada, profesora de Derecho Informático de la Universidad de Chile;
-11 Don Héctor Hernández, abogado, profesor de Derecho Penal de las Universidades Andrés Bello y Alberto Hurtado;
-12 Don Max Weinstein, Presidente de la Asociación de Proveedores de Internet;
-13 Don Jorge Martina Aste, Gerente General de la empresa Terra;
-14 Don Waldo Maldonado, Director de Tecnología de la empresa Terra, y
-15 Don Cristián Maturana, Fiscal de la empresa Entel.

* * * * * * * *

III.- ANTECEDENTES GENERALES.-

Es un hecho reconocido y aceptado que la tecnología de comunicación, almacenamiento y procesamiento electrónico de datos ha tenido, en la última década, un asombroso cambio, siendo el más significativo la creación de la Red, que permite transacciones comerciales, financieras, culturales y ha incidido fuerte en la educación, la información y la entretención.

La legislación existente hace una década, establecía que afectar datos contenidos en un sistema era considerado más grave que la destrucción del sistema mismo. Ahora, con la creación de la Red, los sistemas

pasan a una posición dominante y es así que afectar un sistema puede ser infinitamente más grave que afectar un dato.

Todo lo anterior concluye que ante la importancia que tiene para la vida social y económica del país esta nueva realidad económica, se hace necesario revisar y actualizar los mecanismos legales de protección de la misma.

Pero, junto con la realidad expuesta también, han aparecido conductas antisociales que buscan apropiarse de información, recursos financieros o propiedad intelectual ajena, o tan sólo se pretende causar daño a terceros.

Es así que han aumentado los crímenes cibernéticos, los que se aprende muy fácil a cometerlos, requieren de pocos recursos y plantean complejos problemas al momento de determinar la jurisdicción competente para investigar y sancionarlos.

Los gobiernos, instituciones, empresas o personas ante la ausencia de protecciones legales adecuadas, sólo pueden acudir a mecanismos técnicos para protegerse de robos y otros delitos, pero la realidad muestra que estas medidas son insuficientes y superadas con mucha facilidad.

Se ha podido constatar que los países que no disponen de mecanismos de protección legal para defenderse de estas amenazas corren riesgo de no poder competir en un mundo en que un porcentaje creciente de negocios y servicios implican transacciones, comunicaciones y uso de datos y procesos electrónicos.

* * * * * * * *

IV.- SÍNTESIS DE LAS IDEAS CENTRALES O FUNDAMENTALES DEL PROYECTO DE LEY EN INFORME.-

Nuestro país adolece de vacíos legales en la materia, lo que hace necesario resolver con prontitud y es así que conductas claramente ilegales no tienen sanción alguna.

Cabe destacar de entre estas conductas, el caso del acceso no autorizado a un ambiente electrónico, el que carece de sanción en nuestra legislación. Es así que el robo de un objeto físico desde un sector privado deja un rastro evidente, como es la falta de dicho objeto, en el caso electrónico el rastro no existe, ya que los datos e información que le interesen al delincuente no son sustraídos físicamente, sino que pueden ser copiados o vistos, sin que quede rastro alguno.

Lo antes expuesto, justifica sancionar el hecho de acceder sin autorización a sistemas de datos, procesamiento o comunicación electrónica, con el objeto de establecer una barrera de protección.

Se hace necesario que nuestra legislación garantice los derechos de las personas respecto de la versión cibernética de los delitos. En este sentido, la moción instituye el delito por acceso no autorizado.

Para materializar lo antes expuesto, se propone modificar la ley Nº 19.223, que tipifica figuras penales relativas a la informática.

Se hace presente que durante la discusión de esta iniciativa legal, se propusieron indicaciones para modificar su texto manteniendo la idea matriz, en el sentido de dejar establecido en el Código Penal, los delitos antes referidos, con la sanción correspondiente.

* * * * * * * *

V.- PERSONAS QUE FUERON ESCUCHADAS POR LA COMISIÓN Y QUE ENTREGARON SUS OBSERVACIONES SOBRE EL PROYECTO DE LEY EN INFORME.-

1.- Señor Rodrigo Rojas, abogado de la empresa SONDA.-

Expresó que la ley Nº 19.223 estableció dos tipos penales. El primero el sabotaje informático y el segundo, espionaje informático.

Con relación a las observaciones a la ley citada, ésta presenta algunos problemas:

De acuerdo con la opinión de la doctrina, se reconocían en el texto de la ley N° 19.223 algunos problemas o defectos. En general existe cierto consenso en que la mencionada ley, presentaba los siguientes problemas:

1.- El primero, aunque de tipo estrictamente formal, esta vinculado con el hecho de que se trata de una ley extracódigo, que es una practica no recomendable, pues habría sido preferible incorporar estos tipos penales a nuestro Código Penal.

2.- Presenta un problema conceptual al incluir dentro de la expresión sistema de tratamiento de información tanto al hardware como al software, aunque el proyecto original sólo se refería al soporte lógico o programas.

3.- La circunstancia anterior podría prestarse para lo que la doctrina llama concurso aparente de leyes penales.

4.- Otro de los cuestionamientos formulados por los críticos de la ley N° 19.223 se refería a las penas contempladas para los distintos tipos penales. Respecto de este aspecto existe también cierto consenso en que la penalidad podría ser aumentada para proteger de un modo más enérgico las importantes inversiones y los temibles efectos de algunos de estos delitos.

5.- Por último, los autores consideran que la ley N° 19.223 es insuficiente para combatir el delito informático. Sobre el particular se critica que la ley no castigue lo que se denomina acceso indebido o mero acceso y un gran aspecto que se encuadra dentro del llamado fraude informático.

Con respecto al proyecto de ley que modifica la ley N° 19.223 nuestra opinión es muy favorable, pues las modificaciones incluidas en su articulo único tienden a corregir algunos de los problemas u observaciones que se le hacían a la ya citada ley.

En efecto, con la nueva redacción de los artículos 1°, 2° y 3° de la ley N° 19.223 se reestructuran completamente los tipos penales, agrupándolos de modo diferente, corrigiendo algunas imprecisiones del texto anterior e incluyendo entre ellos, el conocido, mero acceso.

Con el esquema propuesto, en el nuevo articulo 1° se consagra el acceso indebido a un sistema electrónico de almacenamiento o procesamiento de datos, o a través del cual se provee un servicio electrónico de comunicaciones. Con esta proposición se corrige el tema del acceso no autorizado, se precisa el hecho de que debe tratarse de un sistema de tratamiento "electrónico" lo que sin duda es un avance, aunque se mantiene la imprecisión respecto del hardware y el software. Por otra parte, lo que consideramos un avance se consagra una multa a beneficio fiscal, y se hace expresa mención al derecho a exigir el pago de las indemnizaciones que correspondan conforme a las reglas generales.

En el inciso segundo se agrega el tipo de efecto que pueda tener el referido acceso indebido, con respecto a los datos almacenados o al funcionamiento del sistema, aun sin la intención de causar alteración, con una penalidad aumentada, lo que también les parece acertado.

Con respecto al nuevo articulo 2° si el propósito de acceder al sistema, es apoderarse de los datos, conocerlos indebidamente u obtener ventaja comercial o se ejecute excediendo una autorización, también se establece una penalidad aumentada al igual que multas de mayor cuantía. En general se manifiesta de acuerdo con la propuesta, sin perjuicio de que el uso de expresiones como la de "ventaja comercial" puede generar problemas de interpretación.

Por último, se reestructura el tipo penal, estableciendo que la destrucción o inutilización de un sistema de almacenamiento o procesamiento de datos, obstaculice o modifique su funcionamiento o modifique o destruya los datos contenidos en él, sufrirá una pena aún más alta que la anterior. Sobre este punto, creemos conveniente se precise que debe tratarse de sistemas de tratamiento automatizado o electrónico, como se hace en el articulo primero, pues de lo contrario se repite el error referido en los antecedentes.

Para concluir, y sin perjuicio de que su estudio puede resultar más complejo, podría evaluarse la conveniencia de regular el llamado fraude informático, pues se trata de una realidad que no siempre podrá ser encasillada dentro de los tipos penales de nuestro Código Penal.

Sostiene que una de las críticas que la doctrina hace a la ley N° 19.223 es que no sancionó el acceso indebido o no autorizado y si bien este simple acceso puede no provocar ningún daño, por el solo hecho de generar una oportunidad de peligrosidad, puede ser sancionado, como por ejemplo acceder a una propiedad privada o abrir una carta ajena, aunque no se lea. En ese sentido, estima que este proyecto es beneficioso y su opinión es favorable.

Hay algunos problemas que reconocen la doctrina y que deberían abordarse, en orden a que la ley debería utilizar correctamente la expresión de “sistema de tratamiento electrónico” y no de “sistema automatizado” que significaría que no es manual y que lo mencionaba el proyecto original, por lo que es pertinente agregar en el artículo 1° la expresión “sistema de tratamiento electrónico”, aunque reconoce que el día de mañana se puede inventar algo que no es electrónico, que puede ser inalámbrico.

* * * * * * * *

2. Señor Fernando Londoño, abogado del Ministerio de Justicia.-

Expresa que el Ministerio de Justicia lleva algunos meses estudiando la problemática de los nuevos delitos informáticos e incorporando el fraude informático, el hurto y falsificación de documentos electrónicos, el tema del hackeo y lo que abarca la moción en estudio.

Señala que hay dos modelos comparados para regular el tema de los delitos informáticos. Un primer modelo es hacerlo mediante leyes especiales, y crear un pequeño derecho penal informático. Ese modelo sólo fue implementado por Francia, en 1998, y no trabaja sobre la base de los bienes jurídicos que han sido afectados, como en el caso de fraude informático que es el patrimonio o en el ingreso no autorizado, que es la intimidad, en el caso de los documentos, que es la falsedad, etcétera, sino que trabaja sobre la base de atribuir calidad de bien jurídico a un objeto específico nuevo, que es la información automatizada o los datos y, en concreto, sobre esa hipótesis se trabaja.

Otra técnica, que es la que se ha seguido en la mayoría de los países, como Italia, España y Alemania y recientemente Francia se estaría incorporando a este sistema. Este modelo se basa en los bienes jurídicos. Es decir, se incorpora en los tipos penales tradicionales, ya por el objeto

material o por la forma de comisión, lo que es propiamente informático y esto tiene dos ventajas muy claras:

1.- Permite hacerse cargo de la coherencia del sistema del punto de vista de los bienes jurídicos. Por ejemplo, cuando se altera o daña un dato y no es lo mismo alterar un dato para apropiarse de dinero que alterarlo para otros fines. Respecto del fraude informático, que implica entrar a una cuenta corriente y a través de un proceso computacional adueñarse de los fondos del cuentacorrentista y al tratarse en el contexto de los bienes jurídicos protegidos en el Código Penal, permite hacer una calificación coherente, que, en este caso, es el fraude informático y el bien jurídico que se protege es el patrimonio y no el daño que se hace al sistema. Ahora bien, si hay violación a la intimidad, no es que se proteja el daño a los datos, sino que la intimidad es la afectada, como bien jurídico protegido.

Añade que el Ministerio de Justicia ha trabajado, además, con este modelo, porque es el que se ha impuesto con éxito en otros países.

Una segunda ventaja de este modelo es que permite un acceso normal y expedito a los abogados, ya que no hay jurisprudencia y los tipos son nuevos y los abogados y jueces se resisten a aplicar los tipos aparecidos en leyes especiales y los abogados y jueces se atreven mucho más a entrar en la discusión, sobre todo que hay jurisprudencia extensa, referida al Código Penal. Además el utilizar el referido Código permite un tratamiento mucho más amplio, ya que la ley N° 19.223 lo único que protege es un bien jurídico, material autónomo denominado dato y no se protege el patrimonio, la intimidad, la veracidad de la información.

Señaló el señor Londoño, que se debe trabajar sobre la base del Código Penal porque allí hay una coherencia en relación con los bienes jurídicos protegidos, lo que permite que las penas se coloquen adecuadamente y que primeramente se deben buscar fórmulas alternativas, porque se espera demasiado del Derecho Penal, porque sus resultados y alcances son muy limitados. Por ejemplo, cuando se incrementaron en Chile los hurtos de Cédula Nacional de Identidad, inmediatamente se plantearon mociones para regular aquello, con tipos penales específicos, pero al final los bancos exigieron huella digital para abrir cuentas corrientes y eso significó en pocos meses una

disminución notable de hurtos de cédulas de Identidad, lo mismo sucede con el tema del robo o hurto de radios de autos, cuando aparecieron las radios desmontables, disminuyó ese tipo de delitos.

* * * * * * * *

3.- Señor Armando Muñoz Moreno, Comisario Jefe de la Jefatura de Comunicaciones de la Policía de Investigaciones de Chile.-

Señala que todo ésto es un fenómeno nuevo, que va creciendo explosivamente y hay que estar alerta. Felicita el hecho que se haya presentado un proyecto de esta naturaleza, que incluya el acceso no autorizado o hacking directo, que llena un vacío en nuestra legislación pero debe precisarse la no-autorización. Por ejemplo, un señor que va a hacer una transacción en un cajero automático, ingresa sus datos y el sistema le valida o autoriza la transacción, pero esa información puede ser capturada por diversas tecnologías, pero sin embargo al ser esa información coherente con los registros será, en consecuencia, una transacción autorizada por el sistema, por lo que debería precisarse que debe ser sin autorización del titular.

En relación con la no-autorización, sostiene que existen mecanismos que requieren de una inversión y costo. Por ejemplo, en ISAPRES, para que no haya suplantación de personas, se están creando tarjetas con claves o huella digital y así se reducen los riesgos, pero es un problema de costos y la tecnología va a ayudar a que se disminuyan estos problemas.

Señala que respecto del segundo inciso del artículo 1° debiera estructurarse como un artículo independiente, incluyendo todos los “propósitos” mencionados en el nuevo artículo 2º, más el motivo incluido en el actual artículo 4º, es decir, la difusión o revelación.

Expresa que el punto mencionado anteriormente tiene el siguiente fundamento, al referirse a “... tenga el propósito de ....”. Se pregunta si ese término se refiere al dolo. Añade que si la respuesta es afirmativa, entonces quedan fuera de esta figura las acciones de hacking que tuvieron como consecuencia la ventaja comercial, conocimiento indebido, etc. pero que no hubo intención de provocarlo (“coartada”), aunque ello desde el punto de vista técnico

es casi imposible, ya que se requieren una serie de “actividades computacionales” que no podrían ejecutarse “sin intención”.

Respecto de profesionales del área informática, hay una sanción por tener los conocimientos específicos, que les permite actuar con mayor facilidad. Es el caso del policía que comete un delito, que tiene una pena mayor, por el hecho de ser policía.

Expresa que todos los programas que circulan por Internet son desarrollados por informáticos, que son ocupados por personas que no son informáticos, esto es, los usuarios de Internet .

Luego se pregunta qué pasa con una banda profesional internacional, con mucho financiamiento, que incorpora en los cajeros automáticos diferentes elementos para capturar datos, tales como notebooks de última generación, lectores, cámaras, polvo en los teclados. Se detiene esta banda, pero no alcanzaron a utilizar los datos que obtuvieron, entonces qué sucede con esa banda que si bien capturó información, pero no la utilizó.

Con respecto al tema de los virus informáticos, señaló que existen los virus troyanos, que son programas camuflados y es complicado legislar en ese aspecto.

Explica que estos son verdaderos “trozos de código” (archivos ejecutables, instrucciones lógicas, etc.) que se ingresan a un sistema, por diferentes medios, pero que en calidad de encubiertos del verdadero propósito del acceso original. Agrega que los propósitos de éstos son innumerables, de allí que la comunidad informática los clasifica en virus: troyanos, las bombas lógicas, que son aquellas que ejecutan ciertas acciones después de un tiempo determinado, etcétera.

* * * * * * * *

4.- Señora Lorena Donoso, abogada, profesora de derecho informático en la Universidad de Chile.-

La experiencia de la ley N° 19.223, en que se intenta crear un nuevo bien jurídico protegido sindicado como la pureza

de la información contenida en un sistema de tratamiento, parece ser no muy adecuada, considerando que hay otros bienes jurídicos involucrados en la materia, ya que en esa ley se podrían ver identificados varios de esos bienes jurídicos protegidos, contenidos en el Código Penal.

Sostiene que ya hay armonía en la doctrina, en términos generales, en cuanto a la punibilidad de cada uno de estos bienes, respecto de la informática.

Añade que, además, la legislación española es más ambiciosa en estos aspectos, ya que prevé la posibilidad de cometer delitos contra las personas a través de medios informáticos, básicamente lesiones, que podrían cometerse, por ejemplo por medio de un video juego, que podría alterar las lesiones síquicas de las personas o provocar la muerte, a propósito de los juegos de rol, ya que se podría condicionar a una persona a cometer un cierto ilícito. También se sanciona las conductas terroristas a través de redes y para todo ello se ha modificado el Código Penal, para adecuarlos a los nuevos tiempos. En consecuencia, la tendencia es modernizar los Códigos Penales, que están anquilosados.

Agrega que la experiencia nacional indica que en los años de vigencia de la ley N° 19.223 no ha tenido gran aplicación

Señala que discrepa del hecho de que la no-aplicación se deba a que los jueces no entienden este precepto legal, puesto que le ha tocado tramitar causas referidas a delitos informáticos y no fueron pocos los casos en que se procedió por delito de daño del Código Penal y no hubo forma de convencer al juez que había ley especial que podía aplicarse, porque se veían los daños físicos, pero no los hechos al soporte lógico. Piensa que el armonizar en general las penas en el Código Penal es una labor mayor.

Lo más adecuado es armonizar las figuras penales actuales de la ley N° 19.223 al Código Penal y luego elaborar una legislación que sea neutra desde el punto de vista tecnológico y que sea equivalente al funcionamiento extra sistema interno nacional.

Expresa que al momento de modificar el Código Penal, debe haber claridad respecto de los bienes jurídicos que se afectarán, en

orden a hacerlas comprensivas desde una perspectiva técnica, pero sin entrar a una casuística que las haga inaplicable cuando aparezca nueva tecnología.

Plantea temor en el sentido que siempre se pretenda crear legislación especial cuando surge un problema concreto, como por ejemplo si sale algo en las noticias, se pretende legislar sobre eso de inmediato, y eso trae perjuicio enorme.

En todo caso, reformar el Código Penal es un esfuerzo que vale la pena llevar a cabo y estima que no debería ser demasiado largo. Recuerda que la nueva modificación al Código Penal español, para abordar el tema del terrorismo en la red sólo duró dos años.

Indica que debe haber una mínima intervención o adecuación a los tipos ya consolidados en la normativa penal, como por ejemplo que no es concebible estafar a una máquina, porque no hay engaño posible.

Sostiene que la red es un elemento que, de alguna forma, ha cambiado el escenario de nuestros tiempos. Existe en este aspecto una extensa literatura norteamericana que se refiere al Ciber espacio y el espacio público que es susceptible de ser apropiado por que están en el mundo físico y la legislación, lo que debe hacer es establecer las normas de sana convivencia y debe considerarse como un lugar en que nos vamos a desenvolver de una determinada forma, por lo que no parece ser lo regulable, sino que las relaciones que allí se potencien. Eso se ve, por ejemplo, cuando uno abre una correspondencia, puede incluso romper esa carta, pero no suceden los mismos con la violación de un correo electrónico, puesto que muchas veces se puede abrir o ver un correo de ese tipo y nadie se enterará y la información subsiste en el sistema y de ahí la necesidad de sancionar el mero acceso y en ese sentido el espacio cobra una razón importante, más que por las consideraciones penales, por la vía de la criminología, en el sentido de dificultades de persecución y de establecer desde donde se cometió el ilícito. Por ser una forma de regular la convivencia humana en un lugar específico, justifica aún más el considerar las mínimas adecuaciones necesarias de los tipos tradicionales de la convivencia en el espacio físico.

* * * * * * * *

5.- Señor Héctor Hernández, abogado, profesor de Derecho Penal de las Universidades Andrés Bello y Alberto Hurtado.-

Señala que en el tema en debate hay dos modelos. Uno es construir a partir de la informática, es decir aparece un nuevo tema social, que produce desafíos de adaptación jurídica, por lo que se debería crear un Derecho Penal para ese problema, en que no se consideran para nada los bienes jurídicos y la tradición, sino que hay una reacción directa a la nueva realidad y se crea un Derecho Penal ad hoc y eso es lo que hace Francia y en los demás países tales como Alemania, Italia, Portugal, España, se adapta el Código Penal ya existente a los desafíos que plantea la informática.

La informática en materia penal lo que hace es poner a disposición nuevas herramientas o nuevas formas de afectar bienes jurídicos tradicionales y en definitiva, simplemente se adaptan las disposiciones antiguas a los nuevos requerimientos, Agrega que se están afectando derechos tradicionales como la intimidad, la inviolabilidad de las comunicaciones o del hogar, o la propiedad; en consecuencia, hay delitos de daños que suponen la destrucción de objetos materiales, pero ahora hay objetos valiosos que no se les podría aplicar el tipo del daño o engañar a través de computadores, se podría incluir en la estafa. Chile siguió el modelo francés, que habitualmente ocasiona graves fricciones con el sistema de valoraciones del Código Penal y es artificial porque en vez de analizar qué bienes jurídicos afecta, simplemente sigue la novedad del nuevo producto o del nuevo fenómeno social y si se sigue así nada obstaría que el día de mañana se tenga un Derecho Penal especial para la telefonía celular, para las vacaciones de tiempo compartido, etcétera. Añade que para los jueces es más práctico y asimilable seguir trabajando con un Código, adecuado a nuevas exigencias. Además las contradicciones con las valoraciones del Código Penal hacen que simplemente los jueces vean la ley especial como algo lejano y no practicable, ya que no se entiende por qué un tipo de manipulación debe castigarse con penas severas si no hay claridad respecto de lo que se está protegiendo y al modificarse el Código Penal en esta materia, no se está castigando una maniobra informática per se, sino que a través de la informática se ha atentado en contra de la intimidad o la propiedad de una persona. La razón legítima de la intervención judicial se va a encontrar, en la medida que quede patente que se está protegiendo patrimonio, intimidad o propiedad y lo que se está reprimiendo son las nuevas formas de afectar contra los bienes jurídicos tradicionales, que están legitimados en el sistema del Código Penal y se hace

más fácil una represión efectiva y lo que han hecho los españoles, los alemanes e italianos van en esa línea, y lo que se pretende hacer es adaptar nuestro antiguo Código Penal, con objeto de proteger los bienes jurídicos tradicionales, ante estos nuevos cambios y necesidades.

Indica que no se pretende hacer una modificación integral del Código Penal, ya que puede durar muchos años, sino lo que se debe hacer es un esfuerzo de adaptación que puede ser relativamente sencillo, puesto que no se requiere para todos los posibles ilícitos o los bienes jurídicos, sino que para algunos, en que el objeto material antes no existía. Es decir, todo lo que es protección de la propiedad, contra apropiación o destrucción siempre se pensó como objetos corporales, pero hoy en algunos casos no son aplicables esos tipos tradicionales.

Destaca que la informática es una herramienta importante en nuestras vidas, pero las cosas básicas van a seguir siendo las mismas. Por ejemplo, no se aprecia por qué la intimidad va a ser protegida con más o menos severidad, simplemente porque el soporte es distinto. Que duda cabe si se destruye una red de información, se puede hacer un tremendo daño con una pequeña intervención o afectar el patrimonio de una persona, pero debe haber proporcionalidad entre la pena y el daño informático, ya que no es lo mismo destruir una base de datos de una empresa que una receta de cocinas y esa proporcionalidad no se hace en la ley N° 19.223 y sólo se protege el dato.

Es clara y razonable la proporcionalidad que se da en las penas del Código Penal, ya que cuando se destruyen cosas de poco valor, las penas son relativamente bajas y cuando son de alto valor, las penas aumentan. Ahora bien, cuando a través de la informática, se logra una modificación de una situación patrimonial y ocasiona perjuicio a alguien se da la misma situación y eso se observa en el delito de estafa, cuando, por ejemplo la suma defraudada es alta, la pena es mayor.

Expresa que se debe precisar qué es lo que se quiere proteger. Es decir, por qué es grave destruir la base de datos del hospital y lo grave se da con el propio hospital y su administración y no con la informática. En ese ejemplo, en la medida que se puedan valorar los datos contenidos y que se destruyeron, el daño va a ser mayor, por lo que en el bien jurídico protegido es la propiedad. En estos casos, se le puede agregar a los tipos tradicionales

calificaciones, pero que el legislador deje en claro qué es lo que pretende proteger en definitiva, ya que la informática es un medio que sirve para fines valiosos y esos fines deben protegerse.

Señala que respecto de la no aplicación de la ley N° 19.223, se debe, a su juicio, no tanto a desconocimiento de los jueces, sino que a la desvinculación con razones poderosas de legitimación con el Derecho Penal son muy relevantes, pero además porque necesariamente se trata de nuevos conceptos, en orden a formulaciones legales que son muy amplias, que abarca cualquier cosa. Es decir, son tipos penales muy extensos. Analógicamente, se puede pensar de cómo se puede estafar a alguien a través de medios informáticos, sustrayendo fondos de una cuenta corriente, y eso es una forma especial de estafa o apropiación indebida y de afectar el patrimonio y perfectamente puede suceder.

Concluye que la ley N° 19.223 es insuficiente y va a seguir siéndolo, si es que se aprueba la moción propuesta, por lo que debe haber un debate más profundo y estudiar áreas en que la informática va a estar presente. Resume diciendo que son pequeñas modificaciones al Código Penal, que no van contra las valoraciones tradicionales.

* * * * * * * *

6.- Señor Max Weinstein, Presidente de la Asociación de Proveedores de Internet.-

Señala que respecto de Internet, se le asocia a algo visible, referido a las páginas web, pero va mucho más allá que eso.

Comenta que el servicio más usado en Internet es el correo electrónico, que se asimila a una llamada telefónica; también hay otros servicios como los boletines que se asocian a las informaciones; los foros de conversación (news look), que se asimilan a una conversación en una plaza; los chat, que se traduce en la conversación de persona a persona. Cada servicio tiene un trato distinto y quien emite información es responsable de su contenido.

Algunos ISP[1] son proveedores de contenidos y otros de servicio de acceso a Internet, pero no intervienen en los tráficos, por lo que es muy complejo la posibilidad de controlar a los ISP.

Con respecto de los correos electrónicos, es difícil saber qué se dice o hace a través de ese medio, por lo que una política restrictiva no operaría.

Con relación a los casos de pedofilia detectados por Internet, el asunto es que los delincuentes operan sobre la base de la confianza que adquieren de los menores y a partir de allí, obtienen información, que luego publican en la red.

Relata que en Estados Unidos, empezaron a aparecer contratos de control, para evitar la pornografía, y si bien es ilegal el uso de computadores para acceder a ese tipo de material, se estima inconstitucional la aplicación de estos contratos, porque atentaba contra el derecho de la libre expresión. En definitiva, piensa que en esta aldea global en que se ha convertido Internet, es difícil legislar sobre algo que es de uso mundial. Es difícil controlarlo todo y revisar el tráfico de navegación tiene un gran costo, que alguien debe asumir. Igualmente es complicado ver qué se limita. Añade que la conexión de filtros, tiene aspectos ventajosos en orden a limitar contenidos no deseados, pero las desventajas están dadas por el hecho que se exigen claves y el control de acceso es muy engorroso.

Están de acuerdo que se debe apoyar el combate al Ciber crimen, pero las conductas en la red son difíciles de controlar, como sucede con los teléfonos en que se llama y se corta de inmediato y sólo se puede detectar el origen de la llamada que se hace.

Expresa que almacenar las conexiones que hace cada usuario, entre otros problemas, sería entrometerse en la vida privada de los usuarios.

Manifiesta que están siempre dispuestos a colaborar con la Policía de Investigaciones, pero hay ISP que dependen de otros para funcionar, que son los llamados ISP virtuales, que, por ende, no guardan

[1] **Internet Service Provider**.: Empresas proveedoras de acceso a Internet.

información y otros ISP sencillamente no llevan registros del tráfico de sus usuarios.

* * * * * * * *

7.- Señor Jorge Martina Aste, Gerente General de la empresa Terra.-

Expresa que se debe tener una visión general de Internet. Hay que distinguir los proveedores de acceso y proveedores de contenido de Internet. En el primer caso, se deja pasar la información y en el segundo, se ofrecen servicios de información.

Señala que el tema de la seguridad y el de los contenidos se soluciona privilegiando la educación en la familia, en que se enseña al entorno a navegar por la red; además de la educación en los colegios. El tema de los filtros se supera rápidamente por la tecnología. Aún más, han ofrecido filtros de contenido a 200 mil personas, sólo 200 personas lo han contratado y eso es un síntoma que debe llamar la atención.

Respecto al almacenamiento de la información, destaca que es absolutamente factible, pero el punto es de costos y quién los asume.

Se ha percatado que hay predisposición de las empresas que dan servicios de Internet a colaborar.

Relata que el acceso a los servicios y contenido es abierto, excepto subscripciones a contenidos de pago. Es caro y difícil seguir y perseguir a sitios que publican contenidos no deseados, puesto que los sitios cambian día a día.

Expresa que todo los que publican tienen o una dirección IP[2] válida o un dominio válido vigente conocido y la responsabilidad del contenido publicado debe ser del que publica la información y, en definitiva, la decisión de acceso al contenido es una decisión del usuario final.

---

[2] **Internet Protocol**: Formato para conexiones de computadores con la red de Internet.

Señala que no comparte algunas materias del proyecto sobre la responsabilidad por los contenidos de Internet, toda vez que no se puede intervenir en la transmisión y hacer responsable de su mal uso a los proveedores. Respecto de los filtros de contenido, éstos se ofrecen en el mercado abierto, por lo que es inoperante obligar a los ISP a ofrecer ese producto. Añade que la labor de los ISP es hacer que circulen los contenidos, los que se dan libremente.

Precisa que la responsabilidad última en el tema de los contenidos, la tiene la familia. En los colegios, lo mínimo que deben hacer es instalar los mejores filtros de contenidos del mercado.

Con respecto a las medidas para solucionar el tema de la seguridad y el buen uso depende exclusivamente de la educación que se dé a la familia y del trabajo mancomunado de los ISP, con la Subsecretaria de Telecomunicaciones, el Ministerio de Educación y los colegios.

Acerca del proyecto de privacidad de datos, un punto fundamental está dado por la forma de verificar el consentimiento que deben otorgar los padres en esta materia. Eso debería hacerse por una gestión personal del padre, en que concurra a firmar un documento de autorización a su hijo menor de 14 años, de lo contrario no habría forma de comprobar el referido permiso. En Estados Unidos, para estos casos, se exige tarjeta de crédito, pero nada obsta a que se den datos falsos. En Europa, recién se está tratando este tema tangencialmente.

En el caso de Terra siempre se piden los datos y a los menores de 13 años se les exige autorización de los padres, pero no se les puede obligar a que den información verdadera.

Señala que Terra Chile ha desarrollado arquitecturas y tiene instalado sistemas orientados a garantizar la confiabilidad de sus sistemas y servicios. Se han contratado empresas certificadoras que auditen la calidad de la seguridad de los servicios que se ofrecen. Se han definido políticas internas orientadas a garantizar, en alguna medida, la seguridad de los servicios ofrecidos a sus clientes. Dada la complejidad y lo dinámico del servicio, este trabajo es permanente en el tiempo.

Indica que Terra Chile guarda un determinado número de registros (logs) de los servicios accedidos durante su operación. Luego, indica que 30 millones de páginas vistas al mes, equivalen a 1.500 millones de registros mensuales; 10 millones de registros diarios del servidor de correo electrónico equivalentes a 100.000 casillas de e-mail activas; el proceso de un registro tiene un costo promedio de $2; procesar la información anterior tiene un costo mensual de $3.600 millones de pesos equivalentes a cinco millones de dólares mensuales y esta cantidad de registros no incluye otros servicios en Terra como: IRC, Streaming, ftp, news, etcétera.

Luego, precisa que lo caro es procesar la información al haber datos, porque se requiere CPU (Unidad de Proceso Central) y diversos software.

Señala que no se guarda información respecto de lo que hace el cliente o conmutado y, sólo por una cuestión de seguridad, Terra Chile posee un registro de la conexión de sus usuarios, que incluye fecha, hora y dirección IP asignada, que la tiene guardada entre cuatro y seis meses. Esta información es facilitada a los tribunales de justicia cuando es solicitada.

Destaca que el almacenamiento de datos es mucho más barato que su procesamiento; no obstante que para registrarlos se requiere una maquinaria y programas especiales y luego se procesan.

Expresa que si una página web contiene un delito, se debe recurrir al tribunal, para solicitarle a esa empresa que retire esa información, por orden judicial.

* * * * * * * *

8.- Señor Cristián Maturana, Fiscal de la empresa Entel.-

Expresa que en Chile se ha modificado la Constitución Política de la República en materia de censura, ajustándose a tratados internacionales. Internet es un canal de expresión e impedir que circule o restringirlo en algunas áreas, importaría una censura y ello sería ilegal y cualquier restricción en esta materia requiere autorización judicial. Añade que si la ley

entrega a los ISP cualquier control en cuanto a acceso o contenido sería inconstitucional y ello sólo se puede hacer mediante orden judicial.

Indica que en la reforma procesal penal, la Policía de Investigaciones tiene acceso rápido a los fiscales para obtener medidas, si es que hay indicios de algún delito informático, especialmente si se hace a través de la red.

Expresa que el tráfico de navegación en Internet es tan grande y a tan alta velocidad, que el costo de almacenamiento es irreal. Aclara que ni Internet ni los ISP han generado delitos. Lo que pasa que se utiliza la red como medio para cometerlos. Indica que el usuario de una computadora personal es responsable por su uso, aunque sea anónimo, pero no se puede bloquear el acceso a la información, ya que se requiere orden de un juez. Precisa que el propio computador podría registrar y almacenar la información que se ha obtenido por la red y eso sería más fácil. No obstante ello, reconoce que en la informática, existen muchos medios para ocultarse y actuar en forma anónima, por lo que muchas veces resulta muy difícil pesquisar a alguien que haya cometido un delito por la red; aún más se puede actuar desde fuera de Chile.

Señala que su empresa se preocupa constantemente por el tema de seguridad en Internet y se coordinan permanentemente con la Policía de Investigaciones, para abordar este aspecto.

Opina que también los fabricantes de computadoras pueden adoptar medidas para que la información del usuario no se borre, aunque reconoce que esa misma información se puede ocultar.

Indica que es más seguro el tráfico de Internet a través de banda ancha que en forma conmutada.

Expresa que efectivamente se guarda información, pero el crecimiento del tráfico en Internet cada día es más grande, por lo que no habrá capacidad computacional para almacenarla y también se da el problema del procesamiento del tráfico.

Con relación a la autorregulación, destaca que varias empresas del rubro de la informática ofrecen a los padres filtros y programas de

Internet ya filtrados, pero el problema es cultural, puesto que tiene que haber un control o protección de los hijos también. Destaca además que su empresa es líder en la venta de filtros, pero la gente derechamente no los contrata.

Explica que Internet se basa en la autorregulación que le dan los propios ISP y no por las leyes que pudieran regularlo, toda vez que Internet tiene un desarrollo que va mucho más rápido que la norma legal.

Reconoce que existe una importante labor de coordinación entre los ISP y la Subsecretaría de Telecomunicaciones en el desarrollo de Internet.

Si bien es partidario de poner luces rojas en el tema de la seguridad en Internet, pero no en todas las esquinas. Entel tiene filtro de contenidos en más de 25 millones de sitios.

Aclara que hoy están en condiciones de tener una capacidad de almacenamiento de 2 millones de usuarios que naveguen unas cinco horas diarias, en que se generan unos 12 millones de eventos, por lo que es muy difícil dar información a la Policía de Investigaciones.

El mejor control que puede existir es poner una password o clave en el computador personal y, de esa manera, se restringe totalmente el acceso a navegar por Internet, en cambio los filtros no dan seguridad total, en orden a que pueden ser burlados con nueva tecnología.

Precisa que el mundo vertical de Internet es sólo el medio mediante el cual se cometen los delitos, desde el mundo físico.

* * * * * * * *

9.- Señor Alvaro Morales Torres, Subcomisario Jefe de la Brigada Investigadora del Ciber Crimen de la Policía de Investigaciones de Chile.-

Comenta que respecto de las transacciones o eventos, hay una cantidad de información que policialmente no es importante, ellos sólo utilizan un cinco por ciento de esa información; además que ellos solicitan a los ISP las direcciones IP en un horario determinado.

Recuerda que hace un año atrás hicieron una propuesta de almacenamiento de registros, asumiendo sus costos, pero nada ha pasado al respecto. Aclara que a ellos no les interesa el contenido de la información, sino quien ocupa el IP.

Precisa que saber la información de acceso del usuario no implica vulnerar la privacidad. En estos casos, lo que se requiere es actuar con prontitud, toda vez que los hackers borran todo tipo de huellas y, por ende, los registros.

* * * * * * * *

VI.- DISCUSIÓN DEL PROYECTO DE LEY EN INFORME.-

a) En general.

La Comisión realizó un detenido estudio de la iniciativa legal en informe, en el que participaron diversos señores Diputados, integrantes de la Comisión como de los representantes del Ejecutivo.

El Diputado señor Darío Paya Mira, uno de los autores de la moción, entregó los fundamentos de la misma. Expresa que viene a suplir un vacío en la legislación vigente, toda vez que no hay sanción para el acceso no autorizado en ambientes electrónicos. Además, pone al día y complementa, en esta materia, a la ley N° 19.223, de 1993.

Expresa que esta ley sanciona la eliminación de documentos, pero no la del sistema, que es mucho más grave.

Destaca que hay delitos informáticos, que deben ser atacados por medios no tradicionales, porque si bien son fáciles de cometer y con pocos recursos tecnológicos y económicos, los daños son enormes y cuesta pesquisarlos, por lo tanto deben existir protecciones legales, ya que las defensas y herramientas jurídicas actuales son limitadas.

De esta manera, se pretende sustituir los primeros tres artículos de la referida normativa legal y mantener el artículo 4°, agregando una nueva figura delictual, que es el acceso no autorizado, que se sanciona:

1.- Por el solo hecho de ingresar a un sistema informático, sin autorización, sin que haya daños. Puede suceder que uno ingrese a un medio informático, observe la información y luego salga de ese sistema, y se configuraría una suerte de hurto.

2.- Cuando consta que alguien ingresa al sistema informático, sin permiso, se causa daño y se paraliza el sistema, aunque no haya habido intención.

3.-Cuando habiendo ingresado sin autorización, se prueba que se hizo con fines ilícitos.

En esta moción se establecen sanciones penales y pecuniarias, a beneficio fiscal y de los afectados. Agrega que las normas propuestas, a su juicio, son autosuficientes, para sancionar este delito. Hace presente, que se tuvo a la vista la legislación europea, especialmente las normas de la Comunidad Económica Europea y la legislación norteamericana, que contemplan expresamente el delito de acceso no autorizado. Aclara que algunas legislaciones distinguen entre almacenar y procesar información, al momento de configurarse el delito.

Precisa que en este tipo de delitos el aspecto policial es clave y ha conversado este asunto no sólo con agentes policiales especializados, sino que con personas proveedoras del servicio de Internet, que le han indicado que sólo durante un determinado tiempo conservan los registros de navegación y luego borran esa información. Sostiene que muchas veces los ataques provienen del extranjero. Agrega que el Congreso Nacional recibe unos 300 intentos diarios de acceso no autorizado desde fuera de Chile, especialmente de Sao Paulo, Brasil.

El tema es difícil en la práctica, reconoce que se puede hacer algo, aprobando este proyecto. Con él, además, se puede alejar a todos aquellos que por deporte se dedican a alterar o hurtar información.

El Ejecutivo, a través de la señora Alejandra Moya, abogada de la Subsecretaría de Telecomunicaciones y del señor Fernando Londoño, abogado del Ministerio de Justicia, entregaron la posición que, al respecto, sustentan.

Recuerda que la ley Nº 19.223, del año 1993 introdujo la penalización de diversos delitos vinculados al ámbito informático, protegiendo la información contenida en redes informáticas.

Agrega que dicha ley no olvida una serie de problemas que genera la utilización de medios informáticos para la Comisión de delitos considerados tradicionales, o bien, en que dichos medios constituyen el objeto material de protección (fraude informático, apropiaciones indebidas de telecomunicaciones, falsificación de documentos electrónicos, clonación y alteración de tarjetas de crédito), los que en la actualidad generan el riesgo de quedar desprotegidos frente a conductas similares, cometidas por medios materiales o dirigidos a vulnerar objetos de protección material. Es así como, por ejemplo, hoy no se penaliza el hurto en cajeros automáticos, la distracción de fondos desde cuentas corrientes mediante medios informáticos.

Lo anterior demuestra que la ley N°19.223 ha resultado de muy escasa aplicación a la fecha, por dificultades propias de la técnica penal utilizada, el limitado alcance de la normativa y el desconocimiento por parte de los actores del sistema de la materia tratada (jueces y abogado particularmente)

El Ejecutivo apoya la iniciativa legal en informe pero, estima más acertado proponer modificaciones penales que resuelvan los vacíos detectados en la ley N°19.223, la cual proponen su derogación y el establecimiento en su reemplazo de figuras típicas en el Código Penal, que consideren todos los delitos que son posibles cometer con medios informáticos o cuya base se encuentra precisamente en la protección de datos o sistemas informáticos.

Para tal efecto, se propone modificar los artículos 146, 193, 197, 248, 468, 470, 485, 486 y 487 del Código Penal.

El señor Diputado Egaña comenta que este es un tema complejo, pero los pasos que se están dando son importantes. Piensa que por el hecho que se legisle se van a evitar abusos, que se hacen por alumnos de algunos colegios o de facultades de ingeniería de universidades.

Estima que esta es una señal para las empresas que tienen información sensible, para que se preocupen, porque este será un delito que posee acción pública, aunque muchas de estas entidades no denuncian por una cuestión de prestigio.

Recuerda que, al principio, el hurto de base de datos se hacia por diskettes y no por sistemas computacionales, por temor a dejar rastros, como sucedió en Almacenes París de Concepción, que a través de diskette se vendió información.

* * * * * * * *

Votación de la idea de legislar en general.-

La Comisión aprobó por asentimiento unánime, la idea de legislar de la iniciativa legal en informe, con la participación de los Diputados señores: Andrés Egaña; Camilo Escalona; Carlos Ignacio Kuschel; Rosauro Martínez; Iván Moreira; Darío Paya; Edmundo Villouta y Patricio Walker.

* * * * * * * *

b) En particular.

Artículo único (moción).-

"Artículo único: Modificase la ley Nº19.223, de 1993, que tipifica figuras penales relativas a la informática."

1) Sustitúyase el artículo primero de la ley Nº19.223 por el siguiente:

"Artículo 1º.- El que sin autorización acceda a un sistema electrónico de almacenamiento o procesamiento de datos, o a través del cual se provee un servicio electrónico de comunicaciones sufrirá la pena de presidio menor en sus grados mínimo a medio, una multa de beneficio fiscal de 50 a 100 Unidades Tributarias Mensuales

y una multa del mismo monto a beneficio de cada uno de los afectados, sin perjuicio de las indemnizaciones de perjuicio que se puedan reclamar de conformidad a la ley.

Cuando con motivo de dicho acceso se produzca una alteración de los datos almacenados o del funcionamiento del sistema se aplicará a quien incurra en él, aun sin la intención de causar dicha alteración, la pena de presidio menor en su grado medio y las multas indicadas en el inciso anterior."

2) Sustitúyase el artículo segundo de la ley 19.223 por el siguiente:

"Artículo 2º.- Cuando el acceso no autorizado descrito en el artículo anterior tenga el propósito de apoderarse de datos, conocerlos indebidamente, obtener. ventaja comercial, o se ejecute excediéndose una autorización vigente, se aplicará la pena de presidio menor en sus grados medio a máximo, y las multas respectivas serán de 200 a 500 Unidades Tributarias Mensuales."

El señor Diputado Paya formuló indicación para sustituir los Nºs 1 y 2 de la moción, que reemplazan el texto de los artículos 1º y 2º de la ley Nº 19.223, por el siguiente:

"1.- Sustitúyase el articulo 146 del Código Penal, por el siguiente:

"Articulo 146. El que por cualquier medio abriere o registrare la correspondencia o los papeles de otro sin su voluntad o accediere a la información de otro contenida en redes, soportes lógicos o sistemas de tratamiento automatizado de información sin su voluntad sufrirá la pena de presidio menor en sus grados medio a máximo si divulgare o se aprovechare de los secretos que ellos contienen, y en el caso contrario la de reclusión menor en sus grados mínimo a medio.

Esta disposición no es aplicable entre cónyuges, ni a los padres, guardadores o quienes hagan sus veces, en cuanto a los papeles, cartas o información contenida en redes, soportes lógicos o sistemas de tratamiento automatizado de información, de sus hijos o menores que se hallen bajo su dependencia.

Tampoco es aplicable a aquellas personas a quienes por ley, reglamento o contrato les es lícito instruirse de comunicaciones o informaciones ajenas".

II Para reemplazar el número 3 del proyecto por los siguientes:

2.-Incorpórese el siguiente numeral 9, nuevo, al artículo 485 del Código Penal:

"9º Destruyendo, alterando, inutilizando o dañando de cualquier otro modo los datos, programas o documentos electrónicos de otro contenido en redes, soportes lógicos o sistemas de tratamiento automatizado de la información".

III.- Sustitúyase el inciso primero del artículo 487, por el siguiente:

"Los daños no comprendidos en los artículos anteriores, serán penados con reclusión menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales. Igual pena se impondrá al que impidiere u obstaculizare el funcionamiento de un sistema de tratamiento automatizado de la información".

El señor Diputado Walker formuló indicación para sustituir, en la indicación del Diputado señor Paya, el artículo 146, por el siguiente:

“Artículo 146.- Sustitúyase el artículo 146 del Código Penal, por el siguiente

“Articulo 146. El que por cualquier medio abriere o registrare la correspondencia o los papeles de otro sin su voluntad o accediere a la información de otro, contenida en redes, soportes lógicos o sistemas de tratamiento automatizado de información sin su voluntad, sufrirá la pena de reclusión menor en sus grados mínimo a medio si divulgare o se aprovechare de los secretos que ellos contienen, y en el caso contrario la de reclusión menor en sus grados mínimo.

Esta disposición no es aplicable entre cónyuges, ni a los padres, guardadores o quienes hagan sus veces, en cuanto a los papeles, cartas o información contenida en redes, soportes lógicos o sistemas de tratamiento automatizado de información, de sus hijos o menores que se hallen bajo su dependencia.

Tampoco es aplicable a aquellas personas a quienes por ley, reglamento o contrato les es lícito instruirse de comunicaciones o informaciones ajenas".

Señala el señor Diputado Walker que comparte el texto de la indicación del señor Diputado Paya, con la salvedad de que no apoya las penas impuestas en ella, dado que las considera un poco altas. Informa que son las mismas que se pretenden contemplar para sancionar el delito de pornografía, en especial, cuando es transmitido por la red.

Con relación a la indicación del señor Diputado Paya, la Comisión analizó el alcance que podría tener la palabra “contrato” que figura en el inciso tercero.

El señor Diputado Escalona manifestó su inquietud por el alcance que podría tener, el que podría llegar a permitir que exista violación de información ajena.

El representante del Ejecutivo, señor Fernando Londoño señaló que en el proyecto de ley que estudia el Ministerio de Justicia, sobre la misma materia, se considera una excepción al alcance del término “contrato”, ya que tiene vinculación con las relaciones laborales de una empresa.

En atención al debate habido, el señor Diputado Paya formuló indicación para agregar después de la palabra “contrato”, la siguiente frase: “con el titular de la información”.

- La Comisión rechazó por un voto a favor, tres en contra y una abstención la indicación del señor Diputado Walker.

- Respecto de la formulada por el señor Diputado Paya para sustituir el texto del artículo 146 del Código Penal, más la adecuación presentada por el mismo señor Diputado, se aprobó por asentimiento unánime.

- En los mismos términos, se dieron por rechazados los Nº 1 y 2 de la moción.

* * * * * * * *

Articulo 3º (Moción).-

3) Sustitúyase el artículo tercero de la ley Nº19.223 por el siguiente:

“Artículo 3º.- El que maliciosamente destruya o inutilice un sistema de almacenamiento o procesamiento de datos, obstaculice o modifique su funcionamiento, o modifique o destruya los datos contenidos en él sufrirá la pena de presidio menor en su grado máximo y las multas indicadas en el artículo anterior.”

El señor Diputado Paya formuló indicación para reemplazar el Nº3 del proyecto, por el siguiente:

“2.- Incorpórese el siguiente numeral 9°, nuevo, al artículo 485 del Código Penal:

“9º.- Destruyendo, alterando, inutilizando o dañando de cualquier otro modo los datos, programas o documentos electrónicos de otros contenidos en redes, soportes lógicos o sistemas de tratamiento automatizado de la información".

Asimismo, presentó el señor Diputado Paya otra indicación para sustituir el inciso primero del artículo 487, por el siguiente:

"Los daños no comprendidos en los artículos anteriores, serán penados con reclusión menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales. Igual pena se impondrá al que impidiere u obstaculizare el funcionamiento de un sistema de tratamiento automatizado de la información".

- La Comisión aprobó, sin debate y por asentimiento unánime las dos indicaciones antes referidas.

- En los mismos términos, rechazó el Nº 3 de la moción.

* * * * * * * *

El señor Diputado Paya formuló una indicación, del siguiente tenor:

"Agréguese un artículo 2° al proyecto de ley en informe, con la redacción que se indica:

"Artículo 2°.- Derógase la ley N° 19.223, publicada en el Diario Oficial, el 7 de junio de 1993, que tipifica figuras penales relativas a la informática."

El señor Fernando Londoño, abogado del Ministerio de Justicia expresa que es importante precisar para los efectos de la historia de la ley y, por ende, de dejar constancia en el informe, que, en relación con los daños que esa norma establece, se entiende que ellos están incorporados en el estatuto general de daños a la propiedad que tiene el Código Penal y que se hace extensible a los daños a los hardware o a las máquinas computacionales, porque esta ley que se pretende derogar incluye tanto los daños a datos virtuales como al mundo físico, que son las máquinas. En consecuencia, a futuro, se debe entender que la destrucción de computadores cabe en la hipótesis genérica de daños a la propiedad física, contemplada en nuestro estatuto penal.

- La Comisión aprobó, por asentimiento unánime, la indicación antes referida.

* * * * * * * *

La Comisión acordó, por unanimidad, dejar constancia en el informe, la activa y eficiente participación que les cupo en la discusión de esta iniciativa legal tanto al señor Fernando Londoño, abogado del Ministerio de Justicia como a la señora Alejandra Moya, abogada de la Subsecretaría de Telecomunicaciones.

* * * * * * * *

VII.- EL PROYECTO DE LEY EN INFORME NO TIENE NORMAS DE CARÁCTER ORGÁNICO CONSTITUCIONAL O DE QUÓRUM CALIFICADO.-

VIII.- NO CORRESPONDE QUE LA COMISIÓN DE HACIENDA DEBA CONOCER DE ESTA INICIATIVA LEGAL.-

IX.- EL PROYECTO DE LEY FUE APROBADO EN GENERAL, POR UNANIMIDAD.-

X.- ARTÍCULOS E INDICACIONES RECHAZADAS POR LA COMISIÓN.-

1.- Artículo único de la moción.-

"Artículo único: Modificase la ley Nº19.223, de 1993, que tipifica figuras penales relativas a la informática."

1) Sustitúyase él artículo primero de la ley Nº19.223 por el siguiente:

"Artículo 1º.- El que sin autorización acceda a un sistema electrónico de almacenamiento o procesamiento de datos, o a través del cual se provee un servicio electrónico de comunicaciones sufrirá la pena de presidio menor en sus grados mínimo a medio, una multa de beneficio fiscal de 50 a 100 Unidades Tributarias Mensuales y una multa del mismo monto a beneficio de cada uno de los afectados, sin perjuicio de las indemnizaciones de perjuicio que se puedan reclamar de conformidad a la ley.

Cuando con motivo de dicho acceso se produzca una alteración de los datos almacenados o del funcionamiento del sistema se aplicará a quien incurra en él, aun sin la intención de causar dicha alteración, la pena de presidio menor en su grado medio y las multas indicadas en el inciso anterior."

2) Sustitúyase el artículo segundo de la ley 19.223 por el siguiente:

“Artículo 2º.- Cuando el acceso no autorizado descrito en el artículo anterior tenga el propósito de apoderarse de datos, conocerlos indebidamente, obtener. Ventaja comercial, o se ejecute excediéndose una autorización vigente, se aplicará la pena de presidio menor en sus grados medio a máximo, y las multas respectivas serán de 200 a 500 Unidades Tributarias Mensuales.””

3) Sustitúyase él artículo tercero de la ley Nº19.223 por el siguiente:

“Artículo 3º.- El que maliciosamente destruya o inutilice un sistema de almacenamiento o procesamiento de datos, obstaculice o modifique su funcionamiento, o modifique o destruya los datos contenidos en él sufrirá la pena de presidio menor en su grado máximo y las multas indicadas en el artículo anterior.”

2.- Del señor Diputado Walker para sustituir, en la indicación del Diputado señor Paya, el artículo 146, por el siguiente:

“Artículo 146.- Sustitúyase el artículo 146 del Código Penal, por el siguiente

“Articulo 146. "El que por cualquier medio abriere o registrare la correspondencia o los papeles de otro sin su voluntad o accediere a la información de otro, contenida en redes, soportes lógicos o sistemas de tratamiento automatizado de información sin su voluntad, sufrirá la pena de reclusión menor en sus grados mínimo a medio si divulgare o se aprovechare de los secretos que ellos contienen, y en el caso contrario la de reclusión menor en sus grados mínimo.

Esta disposición no es aplicable entre cónyuges, ni a los padres, guardadores o quienes hagan sus veces, en cuanto a los papeles, cartas o información contenida en redes, soportes lógicos o sistemas de tratamiento automatizado de información, de sus hijos o menores que se hallen bajo su dependencia.

Tampoco es aplicable a aquellas personas a quienes por ley, reglamento o contrato les es lícito instruirse de comunicaciones o informaciones ajenas".

* * * * * * *

Vuestra Comisión de Economía, Fomento y Desarrollo os propone que aprobéis el siguiente:

P R O Y E C T O D E L E Y:

“**Artículo 1°.-** Modificase el Código Penal de la siguiente forma:

“1.- Sustitúyase el artículo 146, por el siguiente:

“Articulo 146.- El que por cualquier medio abriere o registrare la correspondencia o los papeles de otro sin su voluntad o accediere a la información de otro contenida en redes, soportes lógicos o sistemas de tratamiento automatizado de información sin su voluntad sufrirá la pena de presidio menor en sus grados medio a máximo si divulgare o se aprovechare de los secretos que ellos contienen, y en el caso contrario la de reclusión menor en sus grados mínimo a medio.

Esta disposición no es aplicable entre cónyuges, ni a los padres, guardadores o quienes hagan sus veces, en cuanto a los papeles, cartas o información contenida en redes, soportes lógicos o sistemas de tratamiento automatizado de información, de sus hijos o menores que se hallen bajo su dependencia.

Tampoco es aplicable a aquellas personas a quienes por ley, reglamento o contrato con el titular de la información les es lícito instruirse de comunicaciones o informaciones ajenas.”

“2.- Incorpórese el siguiente numeral 9°, nuevo, al artículo 485:

“9° Destruyendo, alterando, inutilizando o dañando de cualquier otro modo los datos, programas o documentos electrónicos de otros contenidos en redes, soportes lógicos o sistemas de tratamiento automatizado de la información".

“3.- Sustitúyase el inciso primero del artículo 487, por el siguiente:

“Los daños no comprendidos en los artículos anteriores, serán penados con reclusión menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales. Igual pena se impondrá al que impidiere u obstaculizare el funcionamiento de un sistema de tratamiento automatizado de la información".

Artículo 2°.- Derógase la ley N 19.223, publicada en el Diario Oficial el 7 de junio de 1993, que tipifica figuras penales relativas a la informática”.

* * * * * * * *

Se designó Diputado Informante al señor **Darío Paya Mira.**

Acordado en sesiones de fecha 19 de junio; 3, 10, 17 y 31 de julio de 2002, con asistencia de los Diputados señores: Darío Paya Mira (Presidente), Sergio Correa de la Cerda, Andrés Egaña Respaldiza, Camilo Escalona Medina, Rodrigo González Torres, Jorge Tarud Daccarett (en reemplazo del Diputado señor Enrique Jaramillo Becker); Carlos Ignacio Kuschel Silva, Rosauro Martínez Labbé, Iván Moreira Barros, Edmundo Villouta Concha y Patricio Walker Prieto.

Sala de la Comisión 8 de agosto de 2002.

LUIS PINTO LEIGHTON
Secretario de la Comisión

ÍNDICE

* * * * * * * *