SESIONES ORDINARIAS

2002

ORDEN DEL DIA Nº 639

COMISIONES DE LEGISLACION PENAL Y DE COMUNICACIONES E INFORMATICA

Impreso el día 25 de julio de 2002

Término del artículo 113: 5 de agosto de 2002

SUMARIO: **Régimen** de delitos informáticos.

1. – **Di Leo** y **otros.** (2.772-D.-2001.)
2. – **Fontdevila** y **otros.** (1.299-D.-2002.)
3. – **Ferrari de Grand** y **Chaya.** (1.815-D.-2002.)

Dictamen de las comisiones

Honorable Cámara:

Las comisiones de Legislación Penal y de Comunicaciones e Informática han considerado los proyectos de ley de los señores diputados Di Leo y otros, Fontdevila y otros, y Ferrari de Grand y Chaya sobre Régimen de Delitos Informáticos y han tenido a la vista los proyectos de ley de los señores diputados Cardesa y otros (expediente 299-D.-2001), Cafiero (J. P.) (expediente 385-D.-2001), Godoy (expediente 1.185-D.-2001), Martínez (S.) (expediente 5.061-D.-2001), Corchuelo Blasco (expediente 7.316-D.-2001), Roggero y otros (expediente 2.585-D.-2002), Rubini (expediente 2.629-D.-2002), Herzovich y otros (expediente 2.871-D.-2002) y Molinari Romero (expediente 3.335-D.-2002); y, por las razones expuestas en el informe que se acompaña y las que dará el miembro informante, aconsejan la sanción del siguiente

PROYECTO DE LEY

El Senado y Cámara de Diputados,…

Artículo 1° – A los fines de la presente ley se entiende por:

Sistema informático: todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio.

Dato informático o información: toda representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático o de banda informática.

Art. 2° – *Acceso no autorizado.* Será reprimido con pena de prisión de quince días a seis meses, si el hecho no constituye un delito más severamente penado, el que ilegítimamente y a sabiendas accediera por cualquier medio, a un sistema o dato informático, sin que medie autorización del propietario o excediéndose de los límites de la autorización conferida.

La pena será de un mes a un año de prisión si el autor revelare, divulgare o comercializare la información accedida ilegítimamente.

Art. 3° – *Espionaje informático.* Será reprimido con prisión de un mes a un año, si el hecho no constituye un delito más severamente penado, el que interceptare, interfiriere o accediere a un sistema informático para obtener datos de forma no autorizada, violando la reserva o secreto de la información de dicho sistema.

La pena será de un año a cuatro años de prisión si los datos o la información obtenida constituyere secreto político o militar concerniente a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación.

En los supuestos de los dos párrafos anteriores, la pena se elevará al doble tanto en su mínimo como en su máximo si se revelaren, divulgaren o comercializaren los datos o la información obtenida.

Art. 4° – *Daño o sabotaje informático.* Será reprimido con prisión de seis meses a cuatro años, si el hecho no constituye un delito más severamente penado, el que maliciosamente destruyere, inutilizare, modificare, borrare, hiciere inaccesible o de cualquier modo y por cualquier medio, obstaculizare

el funcionamiento normal de un sistema o dato informático.

Si el hecho pusiere en peligro la seguridad de una nave, aeronave, tren, o cualquier otro medio de transporte público de personas o de cargas, o el normal funcionamiento de las comunicaciones, de la provisión de agua, del suministro de electricidad, de la prestación del servicio de salud o de cualquier otro servicio público, la pena de prisión será de 3 a 10 años.

Art. 5° – *Piratería informática.* Será reprimido con prisión de un mes a seis años el que se apropiare, descargare o usare, indebidamente la información contenida en un sistema informático.

Si la información constituyere secreto político o militar concerniente a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación, la pena será de uno a seis años de prisión.

Art. 6° – *Fraude informático.* Será reprimido con prisión de uno a seis años, el que con ánimo de lucro y valiéndose de cualquier ardid o engaño, perjudicare patrimonialmente a otro mediante la utilización de un sistema informático, sea modificando datos, sea introduciendo datos falsos o verdaderos o cualquier elemento extraño que sortee los procedimientos de seguridad del sistema.

La pena será de dos a seis años de prisión en los siguientes casos:

1. Si el perjuicio recae en alguna administración pública.
2. Cuando se obtuviere en provecho propio o de tercero el desvío de fondos provenientes de cuentas corrientes, cajas de ahorro, plazos fijos, valores en custodia o cualquier otro tipo de activo financiero.
3. Cuando para sí o para tercero se simulare la realización de pagos no efectuados en realidad, o la existencia de bienes, créditos o deudas.

Art. 7° – *Medios destinados a cometer delitos.* Será reprimido con prisión de tres meses a tres años, quien entregare a otro, distribuyere, vendiere o publicitare equipos de cualquier índole o programas de computación destinados a facilitar la comisión de los delitos previstos en la presente ley.

Art. 8° – Cuando el autor o responsable de los ilícitos antes mencionados sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo de la condena.

Art. 9° – En todos los casos de los artículos anteriores, si el autor de la conducta fuese el responsable de la custodia, operación, mantenimiento o seguridad de un archivo, registro, sistema o dato informático, la pena se elevará un tercio del máximo y la mitad del mínimo.

Art. 10. – Comuníquese al Poder Ejecutivo.

Sala de las comisiones, 11 de julio de 2002.

Margarita R. Stolbizer. – Pablo A. Fontdevila. – Franco A. Caviglia. – Pedro J. Calvo. – José G. L'Huillier. – Julio C. Moisés. – Guillermo E. Johnson. – Rafael E. Romá. – Roberto J. Avalos. – Angel E. Baltuzzi. – Daniel A. Basile. – Juan P. Baylac. – Jesús A. Blanco. – Carlos A. Caballero Martín. – Carlos A. Castellani. – Juan C. Correa. – María L. Chaya. – Hernán N. L. Damiani. – Marta I. Di Leo. – María del Carmen Falbo. – Alejandro O. Filomeno. – Miguel A. Insfran. – Gracia M. Jaroslavsky. – Arnoldo Lamisovsky. – Juan C. López. – Laura C. Musa. – Benjamín R. Nieto Brizuela. – Ricardo F. Rapetti. – Gabriel L. Romero. – Héctor R. Romero. – Juan M. Urtubey.

INFORME

Honorable Cámara:

Las comisiones de Legislación Penal y de Comunicaciones e Informática al considerar los proyectos de ley de los señores diputados Di Leo y otros, Fontdevila y otros, y Ferrari de Grand y Chaya sobre Régimen de Delitos Informáticos y habiendo tenido a la vista los proyectos de ley de los señores diputados Cardesa y otros (expediente 299-D.-2001), Cafiero (J. P.) (expediente 385-D.-2001), Godoy (expediente 1.185-D.-2001), Martínez (S.) (expediente 5.061-D.-2001), Corchuelo Blasco (expediente 7.316-D.-2001), Roggero y otros (expediente 2.585-D.-2002), Rubini (expediente 2.629-D.-2002), Herzovich y otros (expediente 2.871-D.-2002) y Molinari Romero (expediente 3.335-D.-2002), creen innecesario abundar en más detalles que los expuestos en los fundamentos que los acompañan por lo que los hacen suyos y así lo expresan.

Margarita R. Stolbizer.

FUNDAMENTOS

1

Señor presidente:

De la relación informática-delito podemos distinguir dos tipos de ilícitos: los delitos computacionales y los delitos informáticos.

Cuando los delincuentes de delitos tradicionales comienzan a utilizar como medio de comisión de ilícitos las tecnologías de la información, se produce una informatización de los tipos tradicionales, naciendo el delito computacional, que sólo son ilícitos convencionales que ya están regulados en el Código Penal.

También se crean conductas nuevas, no tipificadas en el Código Penal, y esto es lo que hace necesario crear nuevos tipos de delitos, los denominados delitos informáticos.

Es necesario distinguir entre software y hardware; el primero es el elemento lógico del sistema informático (programas), y el segundo es el elemento material (maquinaria, aparatos, etcétera).

Respecto del elemento lógico (software), por su naturaleza jurídica, escapa a la esfera de protección penal común, necesitando una tutela especial cuando las acciones punibles son realizadas mediante la ejecución de medios de tecnología computacional.

En cambio el elemento material (hardware), por su naturaleza de bien mueble, implica que al consumarse, deba ser sancionado por la figura del delito que corresponda (no son delitos distintos el robo de una lámpara que de una impresora).

A nivel internacional, no existe una definición propia del delito informático, pero muchos han sido los esfuerzos de los expertos para llegar a una conclusión al respecto.

Nidia Callegari, especialista en derecho informático, mexicana, define el delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

Para otros, delitos informáticos son "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático".

Para nosotros la definición más acertada sería la expuesta por el doctor Rodolfo Herrera Bravo en la ponencia presentada en el X Congreso Latinoamericano y II Iberoamericano de Derecho Penal y Criminología, celebrado en la Universidad de Chile en agosto de 1998, que sostiene que delito informático es "toda acción típica antijurídica dolosa cometida mediante el uso normal de la informática, contra el soporte lógico o software, de un sistema de tratamiento automatizado de la información".

Por lo tanto estaremos ante un delito informático cuando se atenta dolosamente contra los datos digitalizados y contra los programas computacionales contenidos en un sistema.

Los delitos informáticos tipificados en este proyecto son los reconocidos por las Naciones Unidas, y ellos son:

–El acceso no autorizado a la red es un delito mediante el cual el delincuente obtiene sin autorización acceso a la red, a un servidor o un archivo, aprovechando las deficiencias en las medidas vigentes de seguridad, en los procedimientos del sistema, o por cualquier medio.

Generalmente se hacen pasar por usuarios legítimos y utilizan ilegítimamente contraseñas o *passwords*.

Un ejemplo de ello sería el de quien, usando la contraseña de otro, ingresa a un servidor y usa gratuitamente Internet sin abonar lo que le corresponde.

En cambio el acceso no autorizado a servicios y sistemas informáticos puede realizarse mediante el espionaje, el sabotaje o la piratería.

–El espionaje informático es un delito que consiste en obtener sin autorización datos almacenados en un fichero automatizado, en virtud de lo cual se produce la violación de la reserva o secreto de la información de un sistema. (Por ejemplo, interceptando la información que circula en línea a través de las líneas telefónicas.)

Comprende el acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correo electrónico.

Entre los casos más famosos podemos citar el acceso al sistema informático del Pentágono y la divulgación a través de Internet de los mensajes remitidos por el servicio secreto norteamericano durante la crisis nuclear en Corea del Norte en 1994, respecto a campos de pruebas de misiles.

–El sabotaje informático es el acto de destruir, borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el normal funcionamiento del sistema, con medios computacionales.

Ejemplo: introduciendo un virus informático.

Fraude informático es la incorrecta utilización del resultado de un procesamiento automatizado de datos, mediante la alteración en cualquiera de las fases de su procesamiento, engañando a un ordenador, con ánimo de lucro y en perjuicio de un tercero.

–El fraude informático se puede cometer: mediante la manipulación de los datos de entrada, la manipulación de programas, la manipulación de los datos de salida y por manipulación informática.

Manipulación de los datos de entrada: este tipo de fraude informático es también conocido como sustracción de datos, no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

Manipulación de programas: el delincuente debe tener conocimientos técnicos de informática. Este delito consiste en modificar programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado es el denominado "caballo de Troya", que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Manipulación de los datos de salida: se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

Fraude efectuado por manipulación informática: es una técnica especializada que se denomina "técnica del salchichón", en la que "rodajas muy finas" de transacciones financieras se van sacando repetidamente de una cuenta y se transfieren a otra.

–Falsificaciones informáticas: las computadoras pueden utilizarse para realizar falsificaciones de documentos de uso comercial o personal.

Las fotocopiadoras computarizadas en color a base de rayos láser hacen copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

Por todo lo expuesto y dado que el potencial de aprovechamiento de la informática, para la información, la educación, el entretenimiento y la actividad económica a escala mundial es muy importante, es necesario garantizar un correcto equilibrio entre la garantía de la libre circulación de la información y la protección del interés público.

En consecuencia, solicito de mis pares la aprobación del presente proyecto.

Marta I. Di Leo. – Juan P. Baylac. – Carlos Maestro. – María G. Ocaña. – Margarita R. Stolbizer. – Marcelo J. A. Stubrin. – Julio A. Tejerina.

2

Señor presidente:

Las nuevas tecnologías de la información y la comunicación serán las responsables de cambios revolucionarios en las relaciones sociales, las interacciones científicas y las transacciones económicas, siempre que se promueva la colaboración efectiva de los sectores públicos y privados, la transparencia y neutralidad tecnológicas, pero, por sobre todo, se resguarde la intimidad y el derecho a la privacidad de las personas.

La informática nos rodea y es un fenómeno irreversible. Se encuentra involucrada en todos los ámbitos de la interacción humana, desde los más importantes a los más triviales, generándose lo que en la doctrina norteamericana se denomina *computer dependency*. Sin la informática las sociedades actuales colapsarían. Es instrumento de expansión ilimitada e inimaginable del hombre y es, a la vez, una nueva forma de energía, e inclusive de poder intelectual.

La "tecno-era" o "era digital" y su producto, la sociedad de la información, han impulsado un cambio de paradigma social y cultural, impactando drásticamente en la estructura socioeconómica y provocando un rediseño de la arquitectura de los negocios y la industria. Asimismo, surgió una nueva configuración de delitos, los llamados delitos informáticos, que es necesario tipificar, clasificar e incorporar al digesto legal argentino.

Naturalmente que el derecho, como orden regulador de conductas, no queda exento del impacto de las nuevas tecnologías, destacándose la imposibilidad de adaptar dócilmente los institutos jurídicos vigentes y los viejos dogmas a estos nuevos fenómenos.

Las tecnologías de la información han abierto nuevos horizontes al delincuente, incitando su imaginación, favoreciendo su impunidad y potenciando los efectos del delito convencional. A ello contribuye la facilidad para la comisión y encubrimiento de estas conductas disvaliosas y la dificultad para su descubrimiento, prueba y persecución.

La información, en consecuencia, ha adquirido un valor altísimo desde el punto de vista económico, constituyéndose en un bien sustrato del tráfico jurídico, con relevancia jurídico-penal por ser posible objeto de conductas delictivas (acceso ilegítimo, sabotaje o daño informático, espionaje informático, etcétera) y por ser instrumento de comisión, facilitación, aseguramiento y calificación de los ilícitos tradicionales.

Las Naciones Unidas tipificaron los delitos informáticos de la siguiente manera:

– Acceso no autorizado a la red.
– Espionaje informático.
– Sabotaje informático.
– Fraude informático.

A nivel internacional, no existe una definición propia del delito informático, pero muchos han sido los esfuerzos de los expertos para llegar a una conclusión al respecto.

Nidia Callegari, especialista mexicana en derecho informático, define al delito informático como "aquel que se da con ayuda de la informática o de técnicas anexas". Otra definición la aporta el doctor Rodolfo H. Bravo en la ponencia presentada en el X Congreso Latinoamericano y II Iberoamericano de Derecho Penal y Criminología, celebrado en la Universidad de Chile en 1998, que sostiene que delito informático es "toda acción típica antijurídica dolosa cometida mediante el uso normal de la informática, contra el soporte lógico o software, de un sistema de tratamiento automatizado de la información".

Podemos diferenciar entre dos tipos de violación de la privacidad en Internet. El primero de ellos es la recolección de datos personales con fines comerciales: su objetivo es la creación de bases de datos con perfiles del potencial consumidor y las direcciones de correo para el envío de publicidad (*spam*) o el desarrollo de políticas editoriales y de *marketing* de los sitios web. Allí, los principales dilemas éticos están en la validez de la recolección de datos, debido a que es realizada sin el consentimiento de los usuarios, y su venta a terceros. Un segundo tipo de transgresión de la privacidad en la red es la vigilancia de los usuarios por parte de los organismos de seguridad de los gobiernos y de los empleadores. Esto consiste en un monitoreo del tráfico por la web y la intercepción del correo electrónico.

Por eso, el Area de Etica del Centro de Estudios Mediales (CEM) de la Facultad de Ciencias de la Comunicación e Información de la Universidad "Diego Portales" realizará una serie de estudios sobre la privacidad en Internet. De esta manera se espera entregar herramientas reales a los usuarios para que puedan evitar los problemas comunes que aca-

rrea el hecho de que terceros puedan recolectar y vender información personal.

Pese a que el artículo 13 de la Declaración Universal de Derechos Humanos de 1948 reconoce el derecho a la vida privada y rechaza la intromisión en la vida familiar, domicilio o su correspondencia, en Internet se han alcanzado niveles casi insospechados en la pérdida de la privacidad.

En los primeros días de abril de 2000, CNN informó que el servicio de inteligencia inglés, MI5, estaba en condiciones de interceptar los mails y acceder a toda información que lean, reciban o escriban los navegantes británicos. Sin embargo, esta práctica puede ser llevada a cabo por cualquier persona o empresa, tenga o no una página web, debido a que, según Gonzalo Alvarez (Alvarez, Gonzalo, 1999, "¿Intimidad?", en *Criptonomicón* del Instituto de Física Aplicada del CSIC), "cada vez que se visita un sitio web, se suministra de forma rutinaria una información que puede ser archivada por el administrador del sitio". Generalmente, este seguimiento de las actividades de los navegantes se realiza a través del uso de las llamadas *cookies*. Ellas son un pequeño volumen de datos que un servidor web envía al disco duro de su computador cada vez que entra a un sitio.

Según la normativa de privacidad de Yahoo, el buscador que según distintos estudios concentra entre el 50 y el 60 por ciento de todas las visitas a la web, las *cookies* sirven para "recordarnos quién es usted y obtener acceso a la información de su cuenta (almacenada en nuestros equipos), para ofrecerle un servicio mejor y más personalizado". También sirven para calcular el tamaño de la audiencia, "ayudar a que las empresas de Yahoo Tiendas puedan controlar las visitas y las ventas…, medir algunos parámetros de tráfico, las secciones de la red de sitios web de Yahoo visitados y los filtros de visita utilizados". Como podemos observar, las *cookies* no sólo identifican las páginas que visitó, sino que también permiten saber cuánto tiempo se detuvo en cada una de ellas y cuáles son las que prefiere. Además, sirven para identificar el tipo de monitor que está usando, cuál es el *browser* que tiene instalado y cuál es el sistema operativo que ocupa. Incluso, a través de las *cookies*, se puede saber cuál es la versión que tiene del *browser* o navegador y del sistema operativo. Además, permiten individualizar el computador desde el que se está navegando. Gonzalo Alvarez afirma que esto se realiza al rastrear el computador que se está ocupando y averiguar la dirección IP, que no es más que una suerte de certificado de residencia en Internet, por decirlo de alguna manera sencilla.

Sin embargo, María Luisa Fernández (Fernández, María Luisa, 1998, *Nuevas tecnologías, Internet y derechos fundamentales*, Editorial McGraw Hill, Madrid, España, página 143) asegura que el peligro que encierra el uso de las *cookies* es que "el comportamiento del usuario puede ser observado por el proveedor, el cual puede acumular información personal sobre los gustos, preferencias y comportamiento del mismo sin su consentimiento".

Si miramos ese problema desde la perspectiva del sitio web, la elaboración de perfiles permite entregar un mejor servicio, mucho más personalizado. Un claro ejemplo de lo anterior es la revista electrónica "CNET News". Esta acostumbra enviar e-mails a sus lectores en los que les dice: "como usted ha demostrado tener interés en tal o cual tema, le enviamos esta invitación especial". En cambio, desde el punto de vista del usuario, podrían estar siendo vulneradas sus libertades, sobre todo cuando no está claro el destino de dichos perfiles. Además, no existe un consenso sobre su utilización y su venta o traspaso a terceros. El punto está en que cualquier sitio web puede recolectar información personal a través de las *cookies* sin que el usuario se entere. Esto se debe a que la *cookie* es enviada cada vez que un usuario entra a una página, y a que los navegadores más populares, como Microsoft Explorer y Netscape Navigator, están configurados "por defecto" o desde la "fábrica" para aceptar todas las *cookies* de manera automática. Es por eso que la mayoría de los usuarios ni siquiera sabe de la existencia de las *cookies* y que sin su consentimiento se están elaborando perfiles, los que incluso pueden ser vendidos a otras empresas o sitios web.

"Como podemos observar, la pérdida de la privacidad en Internet se produce en distintos niveles debido a la variedad de formas que entregan los medios digitales para recolección y procesamiento de los datos personales. En ella intervienen actores tan diversos como los gobiernos, la empresa privada, los empleadores, los ISP y los mismos sitios web." (Oscar Jaramillo Castro, periodista chileno, es colaborador de sala de prensa. Es doctor (C) en ciencias de la información de la Universidad Complutense de Madrid. Coordinador del Área de Etica del Centro de Estudios Mediales (CEM) de la Universidad "Diego Portales".)

En virtud de lo anteriormente expuesto, consideramos que el bien jurídico tutelado en los delitos informáticos es la información en todos sus aspectos (verbigracia: propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos), entendiendo que su ataque supone una agresión a todo el complejo entramado de relaciones socio-económico-culturales, esto es, a las actividades que se producen en el curso de la interacción humana en todos sus ámbitos, y que dependen de los sistemas informáticos (transporte, comercio, sistema financiero, gestión gubernamental, arte, ciencia, relaciones laborales, tecnologías, etcétera).

En consecuencia, puede entenderse por delitos informáticos a aquellas acciones típicas, antijurídicas y culpables que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, en cualquiera de las fases que tie-

nen vinculación con su flujo o tratamiento, contenida en sistemas informáticos de cualquier índole sobre los que operan las maniobras dolosas. Ahora bien, la información, como valor a proteger, ha sido tenida en consideración por el derecho penal en otras ocasiones. Sin embargo, se lo ha hecho desde la óptica de la confidencialidad, pero no como un nuevo bien jurídico tutelado, abarcativo de varios intereses dignos de protección penal. Piénsese si no en las normativas sobre violación de secretos profesionales o comerciales, o la más reciente legislación sobre hábeas data, de confidencialidad en la información y en el derecho público provincial, por las Constituciones de las provincias del Chaco y de La Rioja, entre otras tantas normas que dentro de regímenes específicos resguardan a la información con una especial protección.

Asimismo, se busca, de alguna manera, cubrir las lagunas legales que fueron quedando luego de la incorporación de cierta protección a determinados intangibles en nuestro derecho positivo nacional. Va de suyo que éste no es un proyecto general y omnicomprensivo de todas aquellas acciones antijurídicas, sino que busca dar una respuesta en un campo específico del derecho positivo, como lo es el derecho penal.

Se decidió privilegiar la claridad expositiva, el equilibrio legislativo y apego al principio de legalidad, evitando caer en una legislación errática que terminara en un mero recogimiento de la casuística local o internacional, evitando tomar figuras del derecho comparado sin antes desmenuzarlas y analizar estrictamente el contexto en donde se desarrollaron y, finalmente, ponderar cómo jugarían dentro del esquema general vigente en la República Argentina.

Este proyecto abraza el principio de la mínima intervención en materia penal, buscando incriminar únicamente las conductas que representen un disvalor de tal entidad que ameriten movilizar el aparato represivo del Estado. En más de una oportunidad una determinada conducta ilegítima será merecedora de un castigo extrapenal, sea a través del régimen de la responsabilidad civil, del derecho administrativo o la materia contravencional.

Para proteger penalmente el bien jurídico tutelado de la información se propone la creación de tres tipos de delitos básicos, con sus correspondientes agravantes, a saber:

a) El acceso ilegítimo informático o intrusismo informático no autorizado *(hacking)* que supone vulnerar la confidencialidad de la información en sus dos aspectos: exclusividad e intimidad;

b) El daño o sabotaje informático *(cracking)*, conducta que va dirigida esencialmente a menoscabar la integridad y disponibilidad de la información, y

c) El fraude informático, hipótesis en la cual se utiliza el medio informático como instrumento para atentar contra el patrimonio de un tercero, que se incluye en esta ley por su propia especificidad que impone no romper la sistemática de este proyecto de ley especial, y por la imposibilidad de incorporarla a los delitos contra la propiedad contemplados en el Código Penal.

A) *Acceso ilegítimo informático*

En el artículo 1º se ha optado por incorporar esta figura básica, en la que por acceso se entiende todo ingreso no consentido, ilegítimo y a sabiendas a un sistema o dato informático. Es una figura básica toda vez que su aplicación se restringe a aquellos supuestos en que no media intención fraudulenta ni voluntad de dañar, limitándose la acción a acceder a un sistema o dato informático que se sabe privado o público de acceso restringido y del cual no se posee autorización. Así, se concluye que están excluidos de la figura aquellos accesos permitidos por el propietario u otro tenedor legítimo del sistema.

Consideramos apropiada aquí la fijación de una pena de multa, atento que se trata de una figura básica que generalmente opera como antesala de conductas más graves, por lo que no amerita pena privativa de la libertad, la que por la naturaleza del injusto habría de ser de muy corta duración. Este criterio resulta acorde con el de las legislaciones penales más modernas (Alemania, Austria, Italia, Francia, España), que ven en la pena de multa el gran sustituto de las penas corporales de corta duración, puesto que no menoscaban bienes personalísimos como la libertad, ni arrancan al individuo de su entorno familiar y social o lo excluyen de su trabajo. En este sentido, las recomendaciones del VI Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, Caracas, Venezuela, 25 de agosto de 1980, Subcomisión de la Comisión II, y García Basalo, J. Carlos, *Las crisis de las penas privativas de libertad. Sistemas supletorios*, Congreso Panamericano de Criminología, Universidad del Salvador, 6/10-11-79, ponencia III.

En cuanto a los elementos subjetivos de la figura, se añade un ánimo especial del autor para la configuración del tipo, que es la intencionalidad de acceder a un sistema de carácter restringido, es decir, sin consentimiento expreso o presunto de su titular.

En el último párrafo de este artículo se contempla como agravante de esta figura la circunstancia que los sistemas o datos informáticos sean concernientes a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos, en cuyo caso se duplican los montos mínimo y máximo de la multa. El fundamento de la agravante es la importancia de los sistemas e información comprometida, ya que están involucrados en el correcto funcionamiento de servicios vitales para la Nación, sin los cuales se pondría en jaque la convivencia común, en especial en los núcleos urbanos.

En el artículo 2º se contempla la pena de un mes a dos años de prisión si el autor revelare, divulgare o comercializare la información, como modalidad más gravosa de afectación del bien jurídico tutelado por la circunstancia que supone la efectiva pérdida de

la exclusividad de la información, penalidad concordante con la descripción típica introducida por la ley 25.326, la que incorpora al Código Penal el artículo 157 bis.

En el último párrafo de este artículo se contempla para esta figura agravada la misma agravante del artículo anterior, referida a los sistemas e información vitales para la Nación, imponiendo en este caso pena de tres meses a tres años de prisión.

B) *Daño o sabotaje informático*

En cuanto a la protección propiamente dicha de la integridad y disponibilidad de un sistema o dato informático, el artículo 3º tiene por objeto llenar el vacío que presenta el tipo penal de daño (artículo 183 del Código Penal) que sólo contempla las cosas muebles. En nuestro país la jurisprudencia sostuvo que el borrado o destrucción de un programa de computación no es una conducta aprehendida por el delito de daño, pues el concepto de cosa es sólo aplicable al soporte y no a su contenido (C. N. Crim. Corr., Sala 6ª, 30-4-93, "Pinamonti, Orlando M.", "J.A." 1995-III-236). Dicha solución es aplicable también a los datos o información almacenada en un soporte magnético.

Al incluir los sistemas y datos informáticos como objeto de delito de daño se busca penalizar todo ataque, borrado, destrucción o alteración intencional de dichos bienes intangibles. Asimismo, la incriminación tiende también a proteger a los usuarios contra los virus informáticos, caballos de Troya, gusanos, *cancer routines*, bombas lógicas y otras amenazas similares.

Se prevé para este delito una pena de un mes a un año de prisión. La figura proyectada constituye un delito subsidiario, ya que la acción de dañar es uno de los medios generales para la comisión de ilícitos, pero esta subsidiariedad está restringida exclusivamente a los casos en que el delito perpetrado por medio de la acción dañosa esté "más severamente penado".

En el artículo 4º se contempla la figura agravada, previendo especialmente las consecuencias del daño cuando se daña un sistema o dato informático del sector público, de los servicios públicos, del sistema financiero y del sistema científico. La trascendencia pública, inmanente a las obligaciones del Estado, así como la especialidad de la información protegida ameritan agravar la pena en estas hipótesis a una pena de tres meses a cuatro años de prisión.

C) *Fraude informático*

En el artículo 5º se ha pensado el delito de fraude informático como un tipo autónomo y no como una figura especial de las previstas en los artículos 172 y 173 del Código Penal. En este sentido, se entendió que en el fraude informático la conducta disvaliosa del autor está signada por la conjunción de dos elementos típicos, ausentes en los tipos tradicionales de fraudes previstos en el Código: el ánimo de lucro y el perjuicio patrimonial. El ánimo de lucro es el elemento subjetivo del tipo que distingue el fraude informático de las figuras de acceso ilegítimo informático y daño informático, en los casos en que la comisión de las conductas descritas en estos tipos trae aparejado un perjuicio patrimonial.

El medio comisivo del delito de fraude informático consiste en la manipulación o despliegue de cualquier artificio tecnológico semejante sobre un sistema o dato informático. Se ha optado por definir la conducta que caracteriza este delito como una "manipulación" o "artificio tecnológico semejante" en el entendimiento de que dichos términos comprenden tanto la acción de supresión, modificación, adulteración o ingreso de información falsa en un sistema o dato informático.

Se contempla para esta figura una pena de un mes a seis años de prisión, penalidad concordante con las de los artículos 172 y 173 del Código Penal.

En el artículo 6º el hecho se agrava y corresponde una pena de dos meses a seis años de prisión, cuando el fraude informático recae en alguna administración pública.

D) *Disposiciones comunes*

Como artículo 7º, bajo el título de "Disposiciones comunes", se dispone la pena accesoria de inhabilitación para el desempeño de cargos públicos, cuando el autor de los delitos informáticos tipificados en el presente proyecto sea un funcionado público en ejercicio de sus funciones. Ello en razón de la mayor responsabilidad y respeto a la legalidad que incumbe a las personas que se desempeñan en la función pública, por lo que se consideró oportuno establecer una pena accesoria de inhabilitación por el doble del tiempo de la condena.

Como artículo 8º se dispone la elevación de la pena de prisión en un tercio del máximo y la mitad del mínimo cuando el autor tenga la denominada "posición de garante", esto es, cuando quien realiza las conductas delictivas es aquel que tiene a su cargo la custodia u operación del sistema, en razón de las responsabilidades y deberes que le incumben, puesto que usa sus conocimientos, estatus laboral o situación personal para cometer cualesquiera de los delitos tipificados en el presente proyecto de ley.

Como artículo 9º se ha creído necesario, por el tipo de ley especial de que se trata, redactar un glosado que facilite la comprensión de la terminología utilizada. Se definen los dos términos centrales, en torno de los cuales giran los tipos definidos, con el mayor rigorismo, a los fines de acotar los tipos en salvaguarda del principio de legalidad, pero, a la vez, con la suficiente flexibilidad y vocabulario técnico, con el objeto de no generar anacronismos en razón de la velocidad con la que se producen los cambios tecnológicos, tratando de aprehender todos los fenómenos de las nuevas tecnologías de la información.

Se ha comprobado, fruto de debates producidos en otras latitudes, que la inmensa cantidad de las conductas ilegítimas que se buscan reprimir atenta contra uno u otro de estos dos conceptos definidos. Consiguientemente, se decidió –siguiendo la Convención del Consejo de Europa sobre Cyber Crime– que, demarcando con nitidez ambos conceptos y haciéndolos jugar dentro de la tipología elegida, se lograba abarcar en mayor medida las conductas reprochables, sin perder claridad ni caer en soluciones vedadas por principios centrales del derecho penal: a saber, principio de legalidad y principio de prohibición de la analogía.

Independientemente de lo manifestado, se debe tener presente que si bien el dato informático o información, tal cual está definido en esta ley especial, es sin duda un intangible, y que –solo o en conjunto con otros intangibles– puede revestir cierto valor económico o de otra índole, no debe, por ello, caerse en el error de –sin más– asociarlo a lo que en los términos del derecho de la propiedad intelectual se entiende por obra protegida (verbigracia: *software*). Si bien una obra protegida por el régimen de la propiedad intelectual, puede almacenarse o transmitirse a través de una red o de un sistema informático y –eventualmente– ser objeto de una conducta de las descritas por esta ley, no toda información –según se define aquí– es una obra de propiedad intelectual y por ende goza del resguardo legal que otorga dicho régimen de protección especial.

En el artículo 10, como política de legislación criminal, se ha optado por incluir estos delitos en una ley especial y no mediante la introducción de enmiendas al Código Penal, fundamentalmente para no romper el equilibrio de su sistemática y por tratarse de un bien jurídico novedoso que amerita una especial protección jurídico-penal.

Adicionalmente, este esquema tiene la bondad de permitir la incorporación de nuevas figuras que hagan a la temática dentro de su mismo seno sin tener que volver a discernir nuevamente con el problema de romper el equilibrio de nuestro Código Penal, que viene siendo objeto de sucesivas modificaciones. Este esquema también se ha seguido en países como los Estados Unidos, donde se tiene una alta conciencia de que la carrera tecnológica posibilita nuevas formas de cometer conductas disvaliosas y merecedoras de un reproche penal.

Para finalizar, destacamos que el presente proyecto de ley está basado en el anteproyecto de ley de delitos informáticos que la Secretaría de Comunicaciones, por resolución 476/2001, sometió a consulta pública. Asimismo, para su redacción se consideraron las propuestas contenidas en los expedientes 299-D.-01 (T.P. Nº 3), Cardeza, Enrique G. y otros; 1.185-D.-01 (T.P. Nº 18), Godoy, Norma; 2.772-D.-01 (T.P. Nº 53), Di Leo Marta I. y otros; 5.762-D.-01 (T.P. Nº 130), García, Francisco A.; 7.316-D.-01 (T.P. Nº 186), Corchuelo Blasco, José M.

Por todo lo expuesto, solicito a mis pares me acompañen en la aprobación del presente proyecto de ley.

Pablo A. Fontdevila. – Franco A. Caviglia. – María del Carmen Falbo.

3

Señor presidente:

Se ha presentado un sinnúmero de iniciativas para legislar sobre esta nueva forma de delincuencia, muy empeñoso ha sido el esfuerzo de los legisladores que han trabajado años anteriores, aunque su esmero nunca culminó con la sanción de una ley en este sentido; esos antecedentes han sido tenidos en cuenta a la hora de redactar el presente proyecto, que intenta ser un aporte al vacío legal que presenta el ordenamiento jurídico argentino en esta materia.

El derecho penal no puede estar ajeno al impacto que ha significado el desarrollo de las tecnologías informáticas en todas las esferas de la vida de la sociedad. La necesidad de contar con una ley específica sobre el tema se ha hecho evidente a medida que ha avanzado la tecnología, y poder contar con ella sería una gran ventaja respecto del tema penal, ya que se evitaría caer en el riesgo de la aplicación analógica, que está siempre presente frente a los avances de la ciencia.

Las diversas formas de aparición de la criminalidad informática propician la aparición de nuevas lesiones a bienes jurídicos, susceptibles de reproche penal, y por lo tanto hace necesario la creación de tipos penales adecuados.

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de las computadoras con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad son algunas de las conductas relacionadas con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

Un análisis de las legislaciones que se han promulgado en diversos países arroja que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras, e incluso en algunas de ellas se ha previsto formar órganos especializados que protejan los de-

rechos de los ciudadanos amenazados por el uso indebido de las computadoras.

Desde hace aproximadamente diez años la mayoría de los países europeos ha hecho todo lo posible para incluir dentro de la ley la conducta punible penalmente, como el acceso ilegal a sistemas de computación, la difusión de virus o las estafas a través de la red.

En virtud de las consideraciones expuestas, señor presidente, es que solicito el tratamiento del presente proyecto.

Teresa H. Ferrari de Grand. – María L. Chaya.

ANTECEDENTES

1

PROYECTO DE LEY

El Senado y Cámara de Diputados,...

DELITOS INFORMATICOS

Artículo 1º – *Acceso no autorizado a la red*. Será reprimido con prisión de 15 días a 6 meses el que se conectare indebidamente o realizare la conexión por accidente y decida voluntariamente seguir conectado a una red, un servidor o un archivo.

Art. 2º – *Espionaje informático*. Será reprimido con prisión de 15 días a 6 meses el que interceptare, interfiriere o accediere a un sistema de tratamiento de la información para obtener datos de forma no autorizada, ya sea por motivo de lucro o simple curiosidad.

Si los datos o la información obtenida constituyeren secreto político o militar concerniente a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación, la pena será de 6 meses a 3 años de prisión.

Se impondrá la misma pena cuando la información obtenida perteneciere a un sistema informático de grandes empresas.

En el supuesto de los dos párrafos anteriores, las penas se elevarán al doble si maliciosamente revelare o difundiere los datos o la información obtenidos.

Si estas conductas fueren cometidas por un funcionario público que se hubiere valido de su cargo para realizarlas, sufrirá además inhabilitación especial perpetua.

Art. 3º – *Sabotaje informático*. Será reprimido con prisión de 6 meses a 4 años el que maliciosamente destruyera, inutilizare, modificare o borrare funciones o datos de computadoras con intención de obstaculizar el funcionamiento normal del sistema, empleando medios computacionales.

Art. 4º – *Piratería informática*. Será reprimido con 1 mes a 6 años de prisión el que se apropiare, descargare o usare, indebidamente, la información contenida en un soporte lógico o software.

Si la información constituyere secreto político o militar concerniente a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación, la pena será de 1 a 6 años de prisión.

Si el hecho fuere cometido por un funcionario público que se hubiere valido de su cargo para cometerlo, sufrirá, además, inhabilitación especial perpetua.

Art. 5º – *Fraude informático o manipulaciones no autorizadas de datos*. Será reprimido con prisión de 2 a 6 años el que, valiéndose de cualquier ardid o engaño, alterare sin autorización el resultado de un procesamiento automatizado de datos, en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y perjudicando patrimonialmente a un tercero, ya sea sustrayendo datos, ingresando datos falsos, manipulando programas computacionales con fines ilícitos o alterando datos procesados.

Si el hecho fuere cometido por un funcionario público que se hubiere valido de su cargo para cometerlo, sufrirá además inhabilitación especial perpetua.

Art. 6º – *Falsificaciones informáticas*. Será reprimido con prisión de 1 a 6 años el que alterare o falsificare datos de los documentos almacenados en forma computarizada, ya sean personales o comerciales.

Art. 7º – Incorpórense las disposiciones de esta ley al Código Penal en el Libro Segundo (De los delitos) como título XIII, Delitos informáticos.

Art. 8º – Comuníquese al Poder Ejecutivo.

Marta I. Di Leo. – Juan P. Baylac. – Carlos Maestro. – María G. Ocaña. – Margarita R. Stolbizer. – Marcelo J. A. Stubrin. – Julio A. Tejerina.

2

PROYECTO DE LEY

El Senado y Cámara de Diputados,…

DELITOS INFORMATICOS

CAPÍTULO I

Acceso ilegítimo informático

Artículo 1º – Será reprimido con pena de multa de un mil quinientos a treinta mil pesos, si no resultare un delito más severamente penado, el que ilegítimamente y a sabiendas accediere, por cualquier medio, a un sistema o dato informático de carácter privado o público de acceso restringido.

La pena de multa se duplicará, tanto en su mínimo como en su máximo, si la conducta se dirigiese a sistemas o datos informáticos concernientes a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos.

Art. 2º – En el caso del artículo 1º de la presente ley, la pena será de un mes a dos años de prisión si

el autor revelare, divulgare o comercializare la información accedida ilegítimamente.

La escala penal será de tres meses a tres años si la conducta se dirigiese a sistemas o datos informáticos concernientes a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos.

CAPÍTULO II

Daño informático

Art. 3º – Será reprimido con prisión de un mes a un año, siempre que el hecho no constituya un delito más severamente penado, el que ilegítimamente y a sabiendas alterare de cualquier forma, destruyere, inutilizare, suprimiere o hiciere inaccesible, o de cualquier modo y por cualquier medio, dañare un sistema o dato informático.

Art. 4º – En el caso del artículo 3º de la presente ley, la pena será de tres meses a cuatro años de prisión si el daño fuera cometido contra un sistema o dato informático concerniente al sector público, servicio público, sistema financiero o sistema científico.

CAPÍTULO III

Fraude informático

Art. 5º – Será reprimido con prisión de un mes a seis años el que con ánimo de lucro, para sí o para un tercero, mediante cualquier manipulación o artificio tecnológico semejante a un sistema o dato informático, obtenga la transferencia no consentida de cualquier activo patrimonial o la cancelación de débitos en perjuicio de otro.

Art. 6º – En el caso del artículo 5º de la presente ley, si el perjuicio recae en alguna administración pública la pena será de dos a seis años de prisión.

Disposiciones comunes

Art. 7º – Cuando el autor o responsable de los ilícitos antes mencionados sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo de la condena, salvo en el caso del artículo 1º de la presente ley en que la accesoria de inhabilitación será de seis meses.

Art. 8º – En todos los casos de los artículos anteriores, si el autor de la conducta fuese el responsable de la custodia, operación, mantenimiento o seguridad de un archivo, registro, sistema o dato informático, la pena se elevará un tercio del máximo y la mitad del mínimo.

Art. 9º – A los fines de la presente ley se entiende por:

– *Sistema informático:* todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio.

– *Dato informático o información:* toda representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático.

Art. 10. – Quedan incorporadas las disposiciones de la presente ley al Código Penal de la Nación.

Art. 11. – Comuníquese al Poder Ejecutivo.

Pablo A. Fontdevila. – Franco A. Caviglia. – María del Carmen Falbo.

3

PROYECTO DE LEY

El Senado y Cámara de Diputados,...

LEY DE DELITOS INFORMATICOS

Artículo 1º – *Del acceso no autorizado.* Será reprimido con prisión de un mes a seis meses, si el hecho no constituye un delito más severamente penado, quien accediere a una computadora o sistema de computación que no le pertenezcan; ya sea directamente, o a través de otra computadora o sistema de computación; sin que medie autorización del propietario o excediéndose de los limites de la autorización conferida.

La pena será de dos meses a dos años, en los siguientes casos:

1. Cuando el acceso fuera obtenido respecto de datos de una entidad financiera, o de empresas administradoras de tarjetas de créditos, o de información comercial o industrial de cuya revelación se pudiera derivar ventajas comercial o industrial para determinadas personas o entidades.
2. Cuando del hecho se deriva interferencia, dificultad u obstrucción del uso legal de una computadora o sistema de computación por parte de terceros.
3. Cuando se hubiere accedido a información contenida en una base de datos pertenecientes al gobierno nacional, gobiernos provinciales o municipales o sus dependencias, siempre que tales bases de datos sean de su uso exclusivo.

Art. 2º – *De la violación al correo electrónico.* Será reprimido con prisión de quince días a seis meses, el que abriere indebidamente un mensaje enviado a través del correo electrónico o mediante el sistema de *chat room* que no le esté dirigido o se impusiera de su contenido o copiare indebidamente dicho mensaje, aunque no esté protegido por encriptado, o suprimiere o desviare de su destino un mensaje electrónico que no le esté dirigido.

La prisión será de un mes a un año, si se comunicare a otro o publicare el contenido de un mensa-

je electrónico al que se accediera en los términos del párrafo anterior.

Art. 3º – *Daño a datos informáticos.* Será reprimido con prisión de quince días a un año, si el hecho no constituye un delito más severamente penado, quien sin expresa autorización del propietario de una computadora o sistema de computación; o excediendo los límites de la autorización conferida, voluntariamente y por cualquier medio destruyere, alterare, hiciere inutilizable o produjera pérdida de datos informáticos.

La pena será de tres meses a cuatro años, en los siguientes casos:

1. Cuando la destrucción, alteración o pérdida de datos trajera aparejada pérdidas económicas superiores a $ 100.000.
2. Cuando fuera cometida contra datos pertenecientes a organismos de defensa nacional, seguridad interior o inteligencia.
3. Cuando tuviera lugar respecto de datos guardados en establecimientos asistenciales y destinados a, o relacionados con, la atención de los pacientes.
4. Cuando el hecho fuera cometido respecto de datos destinados a facilitar o posibilitar la prestación de servicios públicos.
5. Cuando lo que se destruyere, alterare, hiciere inutilizable o produjere pérdida fuere información contenida en una computadora o sistema de computación, con o sin salida externa, mediante el envío de mensajes por e-mail.

La prisión será de dos a cuatro años si la conducta descripta en el apartado anterior se efectuare mediante la venta o distribución de programas al público.

Art. 4º – *De la estafa informática.* Será reprimido con prisión de un mes a tres años quien, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consiga la transferencia no consentida de cualquier activo patrimonial en perjuicio de un tercero.

La pena será de dos a seis años, en los siguientes casos:

1. Cuando se obtuviere en provecho propio o de terceros el desvío de fondos provenientes de cuentas corrientes, cajas de ahorro, plazos fijos, valores en custodia, o cualquier otro tipo de activo financiero.
2. Cuando para sí o para terceros se simule la realización de pagos no efectuados en realidad, o la existencia de bienes, créditos o deudas.
3. Cuando para obtener un provecho propio o de terceros, se modifique de cualquier modo el contenido de registros de cualquier índole existentes en una computadora o sistema de computación.
4. Cuando se tuviere el acceso a secretos industriales, con miras a su explotación en beneficio propio o de terceros.

Art. 5º – *Pornografía infantil.* Será reprimido con prisión de seis meses a tres años el que, por medio de una computadora o sistema de computación, exhiba, transmita o comercialice material pornográfico relativo a la persona o a la imagen de un menor de edad, aunque mediare el consentimiento de la víctima.

Art. 6º – Comuníquese al Poder Ejecutivo.

Teresa H. Ferrari de Grand. – María L. Chaya.