MOCIONES PARLAMENTARIAS EN EL AMBITO DEL DERECHO INFORMATICO*

Renato Javier Jijena Leiva [1]

Hoy en día el manejo de la información almacenada computacionalmente, especialmente aquella que contiene datos relevantes de las personas -información nominativa- puede significar no sólo una eventual violación al derecho a la intimidad y a la propiedad de éstas, a través de su comercialización, adulteración, manipulación, etc., sino que se puede transformar en un instrumento de poder sobre las personas por parte del Estado, e incluso de los particulares. Por ello, la necesaria y hoy prácticamente inexistente tutela de esa información. Estas razones, y otras desarrolladas en el presente trabajo, dan pie al profesor Jijena para efectuar una crítica a los proyectos legislativos atingentes al tema y que actualmente se discuten en el Congreso, previo introducirnos en la problemática del Derecho Informático, el cual se preocupa de la tutela señalada. En primer término analiza la moción Viera Gallo, la cual es agudamente criticada tanto por los defectos de fondo como de forma o técnica legislativa de que adolece el proyecto. En este punto es interesante el hecho que el profesor no sólo se dirige contra el proyecto legal, sino que también centra su crítica en la errada forma en que se ha entendido y discutido el problema a nivel de la Comisión respectiva de la Cámara de Diputados. En seguida, analiza la moción Bosselin-Pizarro. Pese a considerar que este proyecto es bastante superior al anterior, el autor también lo critica por las falencias de fondo que presenta. El profesor Jijena termina con dos reflexiones: la primera se refiere al ámbito de tutela que debe considerarse respecto de la información nominativa, a saber, el constitucional (a través de la acción de protección), el civil (a través de la responsabilidad contractual y extracontractual), el administrativo y el penal. La segunda reflexión se refiere a la necesidad de que se dicte una ley de tutela de datos que asuma todas las variantes del problema. Para ello, el autor señala una serie de características y puntos que debería contener dicha ley.

I. Generalidades.

El presente estudio tiene por objeto analizar, críticamente, los fundamentos, las características, las bondades, los defectos y la trascendencia de dos iniciativas parlamentarias que, a la fecha, se han presentado para su tramitación a la Cámara de

---

* Se incorporan como anexo a este trabajo, los 2 proyectos de ley que constituyen el objeto de análisis del artículo.

[1] Profesor Escuela de Derecho Universidad Católica de Valparaíso. Diplomado del CREI y la Universidad de Zaragoza.

Diputados del Congreso Nacional. Lamentablemente y no obstante su directa relación -digámoslo desde ya- la Comisión de Constitución, Legislación y Justicia de la Honorable Cámara no ha tenido a bien analizarlas en forma conjunta.

En julio de 1991 el diputado José Viera Gallo presentó a tramitación una moción para tipificar el delito informático, contenida en el Boletín Nº 412-07, la que actualmente está siendo analizada en el Senado -donde sabemos será objeto de modificaciones-; en agosto del mismo año, los parlamentarios Hernán Bosselin y Sergio Pizarro presentaron otra moción, contenida en el Boletín Nº 452-07, en la que recogieron un proyecto de ley elaborado durante la pasada administración, por una comisión ad-hoc del Ministerio de Justicia del Sr. Hugo Rosende, sobre protección del tratamiento automatizado de datos personales y criminalidad informática.

Parte de nuestras consideraciones y propuestas están contenidas en dos informes que, privadamente y en representación del Centro de Estudios y Asistencia Legislativa -CEAL- de la Universidad Católica de Valparaíso, hemos hecho llegar a los miembros de la Comisión pertinente en la Cámara de Diputados. Sin pretender repetir el contenido de un libro que en febrero de este año nos ha publicado la Editorial Jurídica de Chile, del mismo -titulado *Chile, la protección penal de la intimidad* y *el delito informático*- retomamos ahora varias ideas y elementos fundamentales. Lo dicho, creemos, explica la existencia de pocas referencias específicas a pie de página.

II. Fundamentos del tema y conceptos relevantes.

Antes de analizar el contenido de las mociones, pertinente es formular algunos comentarios, apuntados a aclarar y poner de manifiesto la trascendencia e implicancias de la materia en estudio.

A. La informática es la ciencia del tratamiento electrónico o automatizado de la información y está llamada a solucionar fenómenos como "la explosión informativa" del mundo moderno. Reiteradamente hemos afirmado que los computadores constituyen la amenaza por excelencia contra el derecho a la intimidad; ciertamente, la masificación en el uso de ordenadores (el término resulta de la traducción del vocablo francés "ordinateur") ha enfatizado un problema preexistente: el que la acumulación de información personal en bases y bancos de datos posibilita la injerencia en la vida privada de las personas..., por cuanto quien recopila la información obtiene una imagen inmaterial respecto de aquel cuyos datos son recolectados.

Porque no todo conjunto organizado de datos es relevante para las personas y la sociedad, se hace necesario determinar cuál es la información cuyo control constituye una forma de poder, que es transada -libremente- en el mercado, que constituye un bien económico, que ayuda a la toma de decisiones, que eventualmente será "hurtada" y que puede llegar a ser mal usada por un Estado para oprimir a sus nacionales. Al responder esta interrogante, surgen los bie-

nes jurídicos que primordialmente requieren de tutela.

La intimidad, reflejada en la información nominativa de un sistema informático, constituye el núcleo esencial de la personalidad y es preciso defenderlo de la intrusión o la manipulación de los grupos de poder que emergen en la sociedad de masas. Porque la intimidad se ha convertido en un gran negocio de información.

En la doctrina del Derecho Informático se habla de una "libertad informática", para aludir a la facultad de implementar sistemas electrónicos con información nominativa y, por ende, recolectar, procesar, almacenar y difundir datos de tal naturaleza, ...siempre bajo dos condiciones, porque no puede ser absoluta: que se cumpla con algún procedimiento previo de autorización o registro para su constitución y que se otorgue a toda persona el derecho de acceso a las bases y bancos de datos, que contengan información que les concierna (la libertad informática se traduce en una auténtica facultad de control de la información personal, para los titulares de la misma).

Es ante la necesidad de tutelar la privacidad de las personas o la información nominativa procesada electrónicamente, que en el Derecho Comparado han surgido las denominadas leyes de protección de datos, data protection act o atenschutz; buscan armonizar dos intereses en conflicto: la necesaria confidencialidad para determinadas informaciones y la eventual accesibilidad a la misma, consagrándose, en casi todas, sanciones penales para la violación de sus principios esenciales. Porque es en el ámbito de las limitaciones al uso de la informática donde deben tipificarse delitos, para sancionar las conductas que lesionen derechos dignos de tutela penal; así, la trascendencia de la intimidad, en cuanto bien jurídico a tutelar, requiere de la especial protección que otorga el derecho penal, máxime porque la facultad de no ver lesionada la privacidad, mediante el uso indebido de la informática, no queda garantizada efectivamente en conformidad al ordenamiento jurídico vigente.

En cuanto a la situación del problema en nuestro país, nos parece un gran error seguir considerando que estamos en el campo del "derecho-ficción". Chile camina aceleradamente a convertirse en una sociedad informatizada. Mas que en ningún país de Centro y Sud-América, puede comprobarse en la vida cotidiana la importancia y la eficacia de contar con sistemas informáticos; también debiera existir conciencia sobre los posibles abusos que pueden cometerse con los mismos. Es necesario, por ende, regular normativamente el uso -y sancionar administrativa y penalmente el eventual abuso- que se haga de información relevante sobre los chilenos, para evitar que el poder informático sea un instrumento de opresión del Estado o un instrumento de mercantilismo y lucro para algunos sectores: porque la autonomía de la vida privada puede ser violada, tanto por los particulares como por los agentes de la Administración.

Así, tratándose del sector privado, no todos los chilenos saben de la informa-

ción que, sobre nosotros, algunas empresas comerciales de servicios -en España denominadas "corredoras de listas"- recopilan y comercializan libre y a veces arbitrariamente; pensemos, por ejemplo, la cantidad de antecedentes que entregamos cuando se llena una solicitud de crédito en una multitienda o un simple formulario para ser socio de un club de video, en el listado de suscriptores del diario El Mercurio, etc. También se comercializan en nuestro país los datos de los archivos del Servicio Electoral, ya que en virtud del artículo 25 de la ley 18.556 -norma que habría que derogar-, son públicos los correspondientes a las inscripciones electorales. Es sobre la base de esta información que diversas empresas pueden realizar marketing vía el denominado sistema de "mailing" (correo) directo; y ella puede ser recopilada contra la voluntad de la persona a que aluden, puede ser errónea o puede ser maliciosamente alterada, ...sin que su titular posea algún mecanismo efectivo y específico de tutela.

Desde la perspectiva del sector público, por cierto que un Estado moderno requiere, para cumplir sus fines promocionales y asistenciales y con miras al bien común de la sociedad, información sobre sus nacionales. Pero debe evitarse que esta gran fuente de poder en manos del gobierno de turno, e incrementada notablemente en Chile después del último censo, eventualmente se revierta contra ellos.

Mención especial hay que hacer sobre el proyecto de ley que crea la Dirección de Seguridad e Informaciones, también en actual tramitación legislativa. No obstante que los parlamentarios se han preocupado expresamente de resguardar la privacidad de las personas, al considerar la existencia de una Comisión permanente y al consagrar la posibilidad de recurrir a la justicia del crimen, al parecer no se ha reparado en los riesgos que pueden derivarse del hecho de contemplarse la existencia de un banco de datos centralizado. Una de las interrogantes a responder sería la siguiente: ¿cómo podrán saber los titulares de los datos nominativos almacenados, por ejemplo, si ellos son exactos, si están actualizados, si se están utilizando en su contexto y si han dado pie a que sean entre-cruzados con otros sistemas para la elaboración de "perfiles de personalidad"?; se exige la promulgación de una ley de protección de datos que consagre, para los particulares, las garantías que emanan del "derecho de acceso", tal como lo hace el proyecto recogido en la moción de los diputados Bosselin y Pizarro y que más abajo analizaremos.

B. Consideraciones sobre la criminalidad informática.

Ante las interrogantes de si es necesaria la creación de nuevas formas penales que salgan al paso de posibles extralimitaciones en el uso de la informática, o de si estamos en presencia de un fenómeno tecnológico que requiere la intervención del "ius puniendi" del Estado, ...la respuesta debe ser afirmativa. Porque la computación, no obstante lo trascendente que ha sido y seguirá siendo para las modernas sociedades, va camino de convertirse en una variable cada vez más presente en los delitos, situación que se agrava, por cuanto los tipos penales que actualmente existen no subsumen,

porque no pueden hacerlo, los hechos ilícitos realizados por medio del computador o contra un sistema de tratamiento automatizado de información. Por la complejidad del medio informático, por las posibilidades que él otorga para desarrollar nuevas figuras delictivas o perfeccionar las existentes, por las nuevas modalidades de comisión, por los bienes jurídicos involucrados y porque la legislación penal vigente no contempla todos los posibles delitos informáticos, ...creemos que es imprescindible tipificar una figura específica.

El delito informático no ha sido objeto de una elaboración conceptual suficientemente perfilada. Por la falta de tradición jurídica de esta temática, una de las principales trabas para la confección de un tipo legal específico obedece a lo difícil que resulta encontrar una definición que comprenda todas las posibles modalidades de criminalidad informática. Retomando los elementos de la definición clásica de delito y para entender la figura, podemos concebirlo como toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema informático.

Concluimos en que lo que requiere de amparo son los contenidos informativos de un sistema, la información en sí misma, sin apellidos, ...que será objeto de tratamiento automatizado, que está siendo procesada o que está almacenada en bases y bancos de datos. La concebimos pues, genéricamente. Pero este es un primer acercamiento. Hay que dar otro paso. *Hay que darle contenido y atender a su naturaleza o a la finalidad en virtud de la cual un conjunto de datos han sido organizados informáticamente y, proyectando la concepción genérica a otros bienes jurídicos afectados, preguntarse cuáles son las especies de información que, en definitiva, reclaman de la tutela del ordenamiento jurídico en general y penal en particular:* si la información es nominativa o relacionada con las personas se atenta contra la intimidad; de ser económica o representar valores, se atenta contra la propiedad o el patrimonio; y de ser estratégica o relacionada con la seguridad o la soberanía de un Estado contra lo que hemos denominado la intimidad nacional.

Pero también la información en si misma es el objeto material del ilícito. El soporte lógico informático (datos y programas, "bits" o dígitos binarios, meros impulsos eléctricos...) constituye el objeto directamente afectado por un delito propiamente informático, no obstante ser intangible, incorporal, inapropiable o inaprehensible físicamente.

Algunas clasificaciones posibles.

1. a) Son delitos contra medios informáticos, contra un sistema informático, aquellos en que el ordenador es el objeto directo del ilícito.

Se exige una distinción fundamental: una cosa es el soporte o los elementos físicos del sistema (hardware o equipos, partes o componentes) y otra el elemento o

soporte lógico del mismo (datos y programas o software). Así, son delitos contra el soporte físico el hurto de "tiempo-máquina", los atentados contra las redes de transmisión de datos (interferencia o perturbación maliciosa), la destrucción de instalaciones informáticas, la sustracción de soportes de almacenamiento, etc. Son delitos contra el elemento lógico, v.gr. los programas "virus" o las bombas lógicas, la copia de software, el "atisbo" o visionado de datos en pantalla, la apropiación de información -para lo cual basta la mera copia sin privación permanente para el eventual afectado- y la manipulación o alteración de datos.

b) Son delitos con o mediante medios informáticos aquellos en que el ordenador es el instrumento usado para la ejecución del ilícito. Algunos podrían haberse realizado por medios distintos de los informáticos (sin manipulación del soporte lógico) -apareciendo la computación como una específica herramienta de comisión-; otros sólo son posibles con ellos.

Para aclarar la idea: generalmente los delitos contra medios informáticos son cometidos, valga la redundancia, con medios informáticos, pero puede ocurrir que los instrumentos para perpetrarlos no sean computacionales, como cuando acercándole un imán se destruye la información de un disco o de una cinta magnética.

2. Por la reciente doctrina que aborda el tema, se distinguen básicamente cuatro modalidades de ilícitos:

Se denominan fraude informático las manipulaciones de programas y datos -al ingresarlos, procesarlos o estando almacenados-.

Se llama sabotaje informático a la destrucción o inutilización del sistema: La verdad es que constituyen propiamente hipótesis de sabotaje informático los casos en que se destruyen directamente los elementos lógicos (datos y programas), porque la destrucción -daños o incendio- de un P.C., de un P.S., de una unidad de disco, de un disco duro, diskette o cinta magnética..., son hipótesis captables por los tipos del Derecho Penal común, ya que son cosas corporales muebles.

Es espionaje informático la obtención ilícita de información, dolosamente y sin autorización.

Se llama hurto de horas de computador o tiempo-máquina al uso del ordenador no autorizado o con fines, tiempos y propósitos distintos de los indicados.

Relación con los tipos tradicionales.

En relación a los delitos contra el soporte lógico, los tipos tradicionales de delitos contra la propiedad -y, por cierto, los pocos contra la intimidad- deben ser descartados por la intangibilidad del objeto material afectado. Ellos no alcanzan a

sancionar el apoderamiento de los elementos lógicos del sistema, porque los programas y datos contenidos en el ordenador no son "cosas muebles" susceptibles de integrar las modalidades de delitos patrimoniales: no olvidemos que los datos o bits son meros impulsos electrónicos. Nos parece que el tipo de daños del artículo 484 podría tener aplicación, en cuanto admitiéramos que lo determinante en él es que el objeto afectado, independientemente de su naturaleza material o inmaterial, sea susceptible de ser dañado y pueda ser objeto del derecho de propiedad; sin embargo, los problemas que se presentan son la avaluación del perjuicio ocasionado y la determinación de la pena, que en el Código Penal aparece muy reducida para sancionar la gravedad de los ilícitos informáticos.

Tratándose de *atentados contra el soporte físico*, éste si puede ser objeto material y jurídico de los delitos tradicionales contra la propiedad, con la salvedad del hurto de horas de computador (y afirmamos que es atípico el uso indebido de los elementos físicos del sistema, principalmente porque no hay ánimo de apoderamiento de la cosa).

Una distinción puede servir de ejemplo para resumir y aclarar lo expuesto sumariamente.

- El hurto de valores, por ejemplo mediante la transferencia electrónica de activos de cuentas bancarias (intangibles, asientos contables), es un ilícito que podría haber sido cometido con prescindencia de la computación y que atenta contra el patrimonio del titular de la cuenta y de la entidad financiera. Porque el bien jurídico afectado es la propiedad, en cuanto información patrimonial, para sancionarlo, bastaría establecer un aumento de la penalidad para la ejecución con medios computacionales de los delitos previstos en el Código Penal o en leyes especiales, como lo hace el artículo 30 del proyecto recogido por los diputados Bosselin y Pizarro.

- El hurto de información es una hipótesis típica de espionaje informático. La información es el bien jurídico que requiere de amparo y el objeto material del ilícito. No debe olvidarse que al tipificarse un delito específicamente informático lo que se busca es tutelar el soporte o los elementos lógicos del sistema, ...datos y programas o instrucciones.

- Mayoritariamente se piensa que el delito informático alude al "pirateo" de programas computacionales. Se exige una distinción. El "hurto de programas" no existe en el ordenamiento jurídico penal chileno; en nuestro país, en virtud del artículo 80 letra b de la ley de propiedad intelectual, sólo se sanciona, como delito contra los derechos autorales y no como delito informático, la copia ilegal de programas, siempre y cuando sea con fines de venta o comercialización posterior.

III. Sobre el Derecho Informático: referencia.

Otra distinción es fundamental. Los temas de la protección del tratamiento automatizado de datos y la criminalidad informática son dos tópicos del denominado Derecho Informático y no de la Informática Jurídica. Aquel surge, reclamando autonomía, al considerarse a la informática como objeto del análisis jurídico; la segunda, comprende a todas las posibles aplicaciones de la tecnología del procesamiento electrónico de información y de la telemática en el trabajo de los juristas, v.gr., automatización de oficinas y tribunales, implementación de bancos de datos legales y jurisprudenciales, desarrollo de sistemas expertos legales, etc. [2]

IV. Moción del diputado Viera Gallo.

Conozcamos el texto de los tan sólo cinco artículos inicialmente propuestos:

Artículo 1: El que indebidamente destruya, inutilice, obstaculice, impida o modifique el funcionamiento de un sistema automatizado de tratamiento de información sufrirá la pena de presidio menor en su grado máximo.

Si como consecuencia de estas conductas se afectasen los datos contenidos en el sistema, en algunas de las formas señaladas en el artículo cuarto, la pena será la indicada en éste aumentada en un grado.

Artículo 2: El que sin derecho intercepte, interfiera, o acceda a un sistema automatizado de tratamiento de información será castigado con presidio menor en su grado medio.

Artículo 3: El que revele, transmita o se apodere indebidamente de la información contenida en un sistema automatizado de tratamiento de la misma incurrirá en la pena de presidio mayor en su grado mínimo.

Si quien realiza estas conductas es el responsable del sistema la pena se incrementará en un grado.

Artículo 4: El que indebidamente introduzca, transforme, desfigure, altere, dañe o destruya los datos contenidos en un sistema automatizado de tratamiento de información será castigado con presidio mayor en su grado medio.

Artículo 5: Si las conductas de los artículos anteriores son efectuadas con ánimo

---

[2] Un análisis sobre el concepto, las particularidades, los tópicos relevantes y la relativa autonomía de este nuevo ámbito para el conocimiento jurídico, puede consultarse en nuestro libro recién referido.

de lucro, la pena se aumentará en un grado.

A. Aspectos positivos.

1. Debe elogiarse la inquietud por abordar el tema de la criminalidad informática.

2. La referencia en los tipos propuestos a los datos, que en cuanto se organizan en atención a su naturaleza o con una determinada finalidad constituyen información, es acertada.

3. Se establecieron penalidades altas, con lo cual se logra tanto un efecto disuasivo como una tutela efectiva.

B. Reparos de fondo.

1. El diputado Viera Gallo ha dicho que en Chile todavía la delincuencia es subdesarrollada [3]; sin embargo, es una realidad ya cotidiana el mal uso o abuso que se hace de la información -sobre todo nominativa- contenida en bases y bancos de datos. Téngase presente, además, la gran zona oscura o cifra negra que rodea estos ilícitos, porque primero son pocos los delitos descubiertos y, en segundo lugar, menos aún son los denunciados, para evitar perjudicar la reputación de los afectados.

La realidad chilena ha demostrado cómo la falta de tipificación puede dejar prácticamente impunes hipótesis que serían delitos si existiera la legislación adecuada. Recuérdese, ya de 1986, el denominado "Fraude a la Polla Gol", en que dos exfuncionarios de la empresa adulteraron previamente los instrumentos de juego (información destinada a ser procesada) alimentando dolosamente los equipos. Paradojalmente, por no estar tipificadas este tipo de figuras, en definitiva fueron encargados reos y condenados por un tipo residual del fraude por engaño, cuya penalidad es mínima. En Chile también se han cometido delitos vía canales "telemáticos" (el término resulta del maridaje entre las telecomunicaciones y la informática). En 1985 quedó al descubierto en Santiago una cuantiosa estafa a varias líneas aéreas, perpetrada por un argentino que, vía satélite, hurtó y alteró información de la red internacional utilizada para la reserva y comercialización de pasajes.

2. Llama la atención el que sólo se establecen sanciones penales, las más drásticas de un ordenamiento jurídico y que implican privación de libertad, sin que se consagren previamente los principios que debieran ampararse -v.gr., la confidencia-

[3] Así lo afirmó en una entrevista concedida al matutino EL Diario, el 26 de julio de 1991.

lidad de los datos- o las prohibiciones a respetar y las obligaciones a cumplir. Incluso la presentación de la moción, luego de constatar la gravedad que reviste el revelar información almacenada en un sistema informático, alude a la posibilidad de que excepcionalmente la ley lo permitiere o autorizare expresamente; y la duda surge fuerte: ¿en qué tipo de norma se está pensando?; ¿en una que regule globalmente el procesamiento de datos y que consagre el "secreto informático" o en alguna normativa actualmente vigente en Chile?.

También es inexacto afirmar que el resguardo legal desarrollado en el Derecho Comparado haya consistido en el establecimiento de delitos o sanciones penales. Si tan sólo nos atenemos a los países citados por el diputado Viera Gallo en la presentación de su moción, que son los mismos que nosotros analizamos y exponemos en nuestro libro citado al iniciar este estudio, vemos que en todos ellos se ha optado, en primer lugar, por la promulgación de leyes de protección de datos.

3. El bien jurídico "información" no ha surgido con el uso de las modernas tecnologías computacionales, como señala la presentación de la moción. Simplemente él se ha revalorizado, cualitativa y cuantitativamente, pasando a ser un bien inmaterial de gran valor económico -susceptible de apropiación y de tráfico patrimonial- y una forma de poder. Pero la existencia de bancos de datos es anterior y no exclusiva a la informática.

4. En la moción había parcialidad y confusión al momento de considerar los posibles bienes jurídicos afectados por la criminalidad informática. El problema se mantiene después del debate en Comisión.

a) Desde un principio se nos hizo inadecuado atender a "la información en cuanto tal", sin otorgarle una carga o contenido valorativo en atención a su naturaleza específica: porque no todo conjunto organizado de datos reviste igual importancia; porque no requieren de la misma tutela un banco de datos que almacene, por ejemplo recetas de cocina o un listado de algunos discos que se guardan en casa, versus los archivos del Registro Civil.

También es errado creer que, mediante la tipificación de un delito, se tutela el que los datos sean "idóneos, puros y de calidad". Estas notas deben resguardarse mediante la instrumentalización o consagración de garantías como las facultades que emanan del derecho de acceso -corregir, actualizar, conocer la finalidad de la recolección, apercibir, etc.-, todas las cuales les competen a cada uno de los titulares de los respectivos datos y son consagradas en leyes que protegen su tratamiento automatizado. Lo que debe tutelarse, sobre todo penalmente, es la recolección, procesamiento, almacenamiento y difusión de información de contenidos especiales y relevantes para la sociedad; debe evitarse el mal uso o abuso de información verdadera, idónea, pura y fidedigna.

Y el diputado Viera Gallo ha dejado de lado el punto; cuando concurrió al debate en Comisión, según consta en la página 3 del primer informe, expresamente señaló que no buscaba sancionar los delitos que pudieran ser cometidos utilizando la información que contienen los sistemas automatizados, especialmente en cuanto afectaren la vida privada de las personas. Y yo me preguntó: ¿porqué entonces se propuso un artículo 2º para sancionar hipótesis de espionaje informático?.

Cierto es, que la segunda nota a pie de página del informe señala que esta materia estaría tratada por otro proyecto de ley -el recogido por Bosselin y Pizarro-; pero si se constató la directa relación entre ambos, ¿porqué no se abordaron en conjunto, máxime cuando éste último contiene un Título completo sobre delitos informáticos?.

En el error, la Comisión fue más clara en su segundo informe, cuando señala que al legislarse "no debe importar el tipo de información, sino las acciones delictuales para obtenerla".

Para demostrar que en el estudio previo a la presentación de la moción no se logró entender lo que es la criminalidad informática -al no considerar la naturaleza o las distintas especies de información- y la confusión, por ejemplo entre lo que es el objeto material y los bienes jurídicos afectados, retomemos el ejemplo que Viera Gallo señala en la presentación de su iniciativa de ley: la información contenida en los bancos de datos de una AFP. Existen en ellos antecedentes sobre los imponentes, los montos de sus cotizaciones, sus beneficios, las condiciones en que se acogieron a los mismos (v.gr. por estar enfermos de SIDA), es decir, información nominativa y patrimonial, sobre la persona y su patrimonio, que son en definitiva los bienes jurídicos que, por ser relevantes, deben ser tutelados frente a atentados cometidos -dolosamente- por un operador, autorizado o no, del sistema computacional.

b) De la lectura de los informes de la Comisión, se nos aparece "confusa" la concepción que se habría hecho de los bienes jurídicos tutelados.

La presentación de la moción aludió a que había surgido un nuevo bien jurídico: la información, ...en los términos abstractos ya comentados. La idea está repetida en el primer informe de la Comisión de Constitución, Legislación y Justicia de la Cámara de Diputados, al formular una minuta de las ideas matrices o fundamentales del proyecto. También se consigna en la página cinco del segundo informe -en virtud del cual se rechazaron las indicaciones del Ejecutivo-. Sin embargo, al final de la misma página, se señala: que "hubo consenso en el seno de vuestra Comisión de que las indicaciones apuntaban en un sentido diferente, que obedecían a una concepción distinta acerca de los bienes jurídicos a proteger. *Para ella (la Comisión), el sistema informático es un nuevo bien jurídico que se quiere proteger, el cual difícilmente puede asimilarse a otros penalmente protegidos*". Simplemente, no entendemos el criterio de los legisladores sobre el punto; sólo puede ser fruto de la incomprensión conceptual y del

desconocimiento de la razón de ser de la criminalidad informática.

5. Nos parece una errada opción legislar descartando la inserción de un tipo de ilícito informático en una legislación ad-hoc, en la cual primero se formulan los principios esenciales a tutelar y luego se establecen graves sanciones, como las penales (que implican privación de libertad), para cuando ellos no son respetados. Cinco artículos aislados no constituyen una legislación especial y no solucionan el problema de la criminalidad informática.

Menos podría pretenderse su inserción en nuestro Código Penal, pues se desnaturalizaría un cuerpo legal que data de 1874 y que se caracteriza por la no tutela de bienes inmateriales. Consultado durante el debate en Comisión, Viera Gallo declinó pronunciarse, a la espera de las indicaciones del Ejecutivo.

Efectivamente se presentaron -y fueron rechazadas en su totalidad-, pero ellas iban por otro rumbo, porque los tipos propuestos no surgieron en consideración el objeto o bien jurídico "información". El Sr. Presidente de la República presentó indicaciones en las que se optaba por incorporar nuevos tipos dentro de las categorías ya existentes, conservando la penalidad de los mismos: se propuso un delito de sabotaje informático (pero también en consideración al soporte físico), otro de fraude informático (pero reducido a las manipulaciones con fin de lucro) y uno para sancionar los atentados contra la intimidad. Esta opción, la del Ejecutivo, no es tan errada, porque se consideraron hipótesis en que la computación sólo es una específica herramienta de comisión y porque claramente se apuntó a la protección de dos bienes jurídicos: el patrimonio -en cuanto información patrimonial- y la intimidad -en cuanto información nominativa-. Este mismo camino, es el que sigue el ya referido artículo 30 del proyecto elaborado en la pasada Administración, recogido por los diputados Bosselin y Pizarro.

6. Salvo por la ambigüedad o amplitud del artículo primero, no resulta tan claro que el software o los programas computacionales queden amparados por los tipos propuestos. Evidentemente no se sanciona la sustracción fraudulenta o la copia ilegal de programas, ni siquiera "indirectamente", como ha sostenido el diputado Viera Gallo [4]. Ha sido el Presidente de la Asociación Chilena de Software quien ha reconocido cómo su articulado no incide, directamente, sobre el desarrollo local de software. Dando nuevamente muestra de no manejar a cabalidad la temática, el propio diputado ha declarado públicamente, en un seminario realizado en Santiago casi a fines de 1991 [5], que con su moción buscaba sancionar el denominado "pirateo de

[4] Véase la página 3 de la Revista Computerworld, número 8, del 12 al 26 de agosto de este año.

[5] La afirmación la hizo en el Simposium "Informática y Legislación", realizado en Santiago los días 5 y 6 de diciembre de 1991, el que fue auspiciado por la Asociación de distribuidores de Software. La idea fue publicada en el Diario La Tercera del día 9 del mismo mes.

software", situación que en Chile está regulada en el artículo 80 letra b de la Ley de Propiedad Intelectual, Nº 17.336, claramente desde marzo de 1990.

7. Si la presentación de la moción señala que el artículo 1 alude a los atentados contra el software o programas computacionales, nos parece errado, ambiguo o demasiado amplio el uso, en la norma, de la expresión *"funcionamiento de un sistema de tratamiento automatizado de información"*.

Al parecer la expresión habría sido tomada del Código Penal francés, modificado en 1988 [6]; pero allí no se alude a los programas. El primer informe del debate en Comisión, en su página 11, señala que la forma como está propuesto el proyecto tiene su antecedente en la legislación francesa, que tendría ocho artículos sobre el tema. Esto es errado. En Francia existe, desde 1978, una ley de protección de datos fundamental y señera, sobre la informática, los ficheros y las libertades, en la que se tipifican delitos propiamente informáticos. La modificación de 1988 -al Código Penal- fue un complemento de la primera ley y, para entenderla, no puede ser sacada de su contexto (hay que considerar lo que el informe de la Comisión llama, descartándolas, "ideas afines"); porque se introdujo un Capítulo III, en el Título II del Libro III, sobre los crímenes y delitos contra los particulares; el Capítulo I alude a los ilícitos contra las personas, el II a los que se cometen contra los propietarios y el nuevo Capítulo III se titula "de ciertas infracciones en materia informática", ...pero siempre contra los particulares.

Ocurre que, como el funcionamiento de un sistema informático depende de elementos físicos y lógicos (no sólo de los programas), perfectamente puede interpretarse el tipo, en el sentido de que también se considera como objeto material del delito al soporte tecnológico informático (hardware), y resulta que la apropiación -hurto o robo- o la destrucción -daños o incendio- del mismo son perfectamente captables por los tipos penales vigentes. Ocurre también que el "funcionamiento" del sistema se puede inutilizar, obstaculizar o impedir con la sola introducción de un "clip" por la unidad de diskette. El reparo es también válido para el artículo 2, porque la interferencia de, v.gr. una red de transmisión de datos, es perfectamente subsumible por el tipo propuesto.

El punto no queda claro luego del debate en Comisión. La primera nota a pie de página del informe, señala que la moción "no se refiere a los soportes o elementos físicos del sistema, esto es, al hardware o equipos, sino al software, esto es, a los programas y sistemas de programación, al equipo o soporte lógico y también a los datos almacenados"; ¡pero esta afirmación se contradice o es desvirtuada por la página 14 del mismo informe!, cuando se señala que "el proyecto, en general, busca proteger los activos informáticos (hardware y software) ante agresiones, dar seguridad al pro-

[6] Un análisis de la situación de lege data del ordenamiento jurídico francés, puede consultarse en nuestro libro Chile, la Protección Penal de la Intimidad y el Delito Informático, pp. 136 ss.

cesamiento de datos (instalaciones de computadoras, redes de comunicaciones, información, bases de datos) y minimizar los riesgos asociados con él, relativos a la calidad, confiabilidad, oportunidad y confidencialidad de la información procesada".

C. Observaciones de forma o de técnica legislativa.

1. En los tipos alternativos elaborados había que exigir un dolo específico. No se utilizaban elementos subjetivos, con lo cual, conforme a la regla del inciso segundo del artículo 1º del Código Penal, legalmente todas las conductas propuestas se presumían dolosas. ¿Y qué ocurría con las culposas, que estaban quedando sin sanción?; ¿sería conveniente acaso consagrar una hipótesis de cuasi-delito informático, para sancionar la negligencia de aquellos que generalmente son especialistas o personal calificado, ...o deben ser penadas en sede de responsabilidad civil?. La doctrina tiende, tímidamente, a acoger la segunda opción.

El punto fue solucionado en parte durante el debate en Comisión, ya que se incorporó en los artículos 1º y 3º la expresión "maliciosamente".

2. Había reiteración de hipótesis iguales (inciso segundo del artículo 1 y artículo 4) cuando se aludía a los datos contenidos en un sistema informático, asignándole penas distintas. Durante el debate en Comisión se derogó el propuesto artículo 4.

3. Había una reiterada alusión a conductas "indebidas" o "sin derecho" - elementos de antijuridicidad o justificación- sin que se establecieran, o al menos se haya pretendido establecer en un cuerpo legal ad-hoc, cuáles son los actos que debidamente debe realizar, por ejemplo, el responsable del sistema (en que casos se le permite revelar información). Luego del debate en Comisión sólo se mantuvo la expresión en el artículo 2º.

4. Como no se específica, y nada se dijo a este respecto durante el debate, procesalmente debe entenderse que se trata de delitos de acción penal pública o pesquisables de oficio, pudiendo denunciarlos cualquier persona. Porque lo que se busca tutelar es la especial y específica naturaleza de un determinado tipo de información, existe absoluta unanimidad en el Derecho Comparado en consagrarlos como delitos de acción penal mixta, ...que sólo pueden ser denunciados por requerimiento del ofendido o su representante legal.

5. Por ser muy casuística la regulación, surgen importantes lagunas de punibilidad, como es el caso del "hurto de software" o copia ilegal de programas informáticos no constitutiva de pirateo (es decir, hecha sin fines de venta o comercialización posterior) y el hurto de uso de equipos computacionales, los ilícitos operados en la etapa de la recogida de datos (que afectan a la información destinada a ser procesada).

6. Simplemente una constatación: a nivel de terminología, verbos rectores, elementos de antijuridicidad, consideración de la finalidad de lucro y penalidad, se nota una gran coincidencia con los tipos desarrollados por las Comisiones que abordaron el tema durante la pasada Administración, cuyo proyecto, ahora, pasamos a analizar.

IV. Moción de los diputados Bosselin y Pizarro M.

Analicemos la moción contenida en el Boletín Nº 452-07, presentada a la Honorable Cámara de Diputados el 6 de agosto de 1991, por los parlamentarios señores Hernán BOSSELIN C. y Sergio PIZARRO M. En ella se recoge un proyecto de ley elaborado durante la pasada administración, por una comisión ad-hoc del Ministerio de Justicia del Sr. Hugo Rosende, sobre protección del tratamiento automatizado de datos personales y criminalidad informática.

No puede sino elogiarse la actitud de los diputados que han presentado la moción en comento, quienes, en atención a su interés, han retomado un proyecto de ley ya formulado, buscando abrir cauce a un amplio y profundo debate que culmine en dar lugar a una nueva legislación, colocando así nuestras instituciones jurídicas a la altura de los tiempos modernos. Con inteligencia, los parlamentarios Bosselin y Pizarro han dejado de lado la tradicional costumbre de sólo criticar y hacer tabla rasa de lo elaborado por un gobierno anterior, reconociendo su importancia y demostrando, por ende, que en Chile no estamos "a fojas cero" en lo que a las investigaciones el Derecho Informático respecta.

En el transcurso de la tramitación de la moción del diputado Viera Gallo, más arriba analizada, nos han llamado la atención dos hechos.

En primer lugar, las continuas alusiones a este proyecto de ley, para criticarlo y, a nuestro juicio infundadamente, dejarlo de lado. En efecto, al presentar la moción Viera Gallo la califica como una normativa muy ambiciosa y compleja; en declaraciones a la prensa la ha tildado de general y nacionalista; y al concurrir al debate en Comisión señaló que abarcaba el tema de la informática en su globalidad (tarea imposible e innecesaria) y que su alto grado de complejidad se debía a la inclusión de materias que iban desde la protección de la privacidad hasta la propiedad intelectual sobre los software; ésta última afirmación es absolutamente errada, porque, como puede constatarse al tenor de la moción de Bosselin y Pizarro, nunca se pretendió normar en un mismo cuerpo legal los temas aludidos. Existió, en el seno de las comisiones ad-hoc del Ministerio de Justicia de la pasada Administración, la inquietud por abordar en forma específica la regulación legal de los programas computacionales; y esta idea fructificó, porque fue modificada en varios artículos la Ley de Propiedad Intelectual, en marzo de 1990.

En segundo lugar, nos ha extrañado el que distinguidos abogados que participaron en su gestación -como don Hernando Morales Ríos- publiquen trabajos o realicen informes sin pretender reivindicar una idea de lege ferenda sumamente importante y positiva, no obstante los errores de que, creemos, adolece.

Para el análisis del texto normativo en comento, puede considerarse una cierta evolución prelegislativa. Ello, porque con anterioridad el proyecto ahora recogido se redactó un texto que, aproximadamente a comienzos de 1986, fue sometido a consideración de varias entidades (gremiales, universitarias, estatales, empresariales, etc.) y porque con posterioridad se constituyó una Comisión Revisora, la que introdujo algunos cambios de importancia.

Se trata de una ley de protección de datos, similar a las existentes en el Derecho Comparado, en la que se consagran derechos para los titulares de la información, mecanismos procesales de reclamo ante los tribunales civiles, normas sobre el valor probatorio de los medios computacionales y, sobre todo, en la que se tipifican delitos propiamente informáticos.

1. *A nuestro parecer, dos son los contenidos fundamentales del proyecto de ley recogido por los diputados Bosselin y Pizarro M.: la regulación del tratamiento automatizado de información nominativa y la criminalidad informática.* El artículo 1º se extiende en la descripción de los datos amparados por el proyecto (ámbito de aplicación), aludiendo específicamente a los datos personales, los de familia y los concernientes a los derechos y deberes garantizados por la Constitución Política. Un informe técnico, de marzo de 1987, señaló que el proyecto en estudio se refería a la recolección y difusión informática de datos personales, es decir, datos que permiten la identificación del sujeto al que se refieren, quedando los demás al margen de esta legislación. Despejando toda duda interpretativa, consignaba que era la aplicación de la informática la que hacía necesaria la promulgación de una ley que cautelara y protegiera la vida privada de las personas.

2. *Creemos que el proyecto adolece de graves errores de fondo,* los que demuestran como, en la práctica, se tendió a favorecer a los responsables y administradores de los bancos de datos, en desmedro de los titulares de la información, de aquellos a quienes concierne; así:

a) No se aplica a los bancos de datos de la Administración estatal, suprimiéndose la posibilidad de que rijan normas protectoras allí donde precisamente los riesgos de atentados a las libertades son, por su naturaleza, los más graves. En efecto, en conformidad al artículo 5º, los archivos de datos creados como resultado de la aplicación de leyes particulares (v.gr. leyes orgánicas de entes estatales o complementarias) se rigen por las disposiciones de las mismas. Desde un principio, esto nos llevó a concluir en que los bancos de datos que fuesen manejados por el sector estatal iban a quedar marginados de la normativa propuesta y regulados por sus propias -y

particulares o especiales- leyes orgánicas.

Si el proyecto busca la protección de la intimidad y, en consecuencia, el derecho a tutelarla debe primar sobre otros, no alcanzamos a entender los motivos o fundamentos de esta opción prelegislativa, en virtud de la cual los organismos de la Administración del Estado no quedan regulados por la normativa propuesta. Se está descuidando la protección de la privacidad en el ámbito de las relaciones entre los particulares y el Estado.

Si bien es cierto que el artículo 12 del proyecto señala que la ley se aplica también a los archivos de datos personales pertenecientes o administrados por organismos estatales, esta norma sólo alude o se formula en consideración al problema de la difusión de los datos, ya que se consagra en el párrafo correspondiente a esta materia, mas no junto a las restantes disposiciones generales. Pero además, la norma expresamente excepciona del ámbito de aplicación de la ley a los archivos de datos personales contemplados en el artículo 5º -los creados como resultado de la aplicación de leyes particulares- en quanto pertenecieren o fueren administrados por organismos de la Administración del Estado.

Con posterioridad una Comisión Revisora señalaría, expresamente, que las disposiciones del proyecto no le eran aplicables a entes estatales.

b) No se contempla la existencia de un órgano específico de control y fiscalización, para autorizar la creación de bancos de datos nominativos, llevar un registro nacional de los mismos, fiscalizar el cumplimiento de los deberes y obligaciones establecidos en la ley e imponer sanciones administrativas en caso de su inobservancia.

c) Se concibe a la libertad informática desde la perspectiva de los administradores o propietarios de los bancos de datos, quienes detentan la información, sin considerar un procedimiento previo de autorización o registro, lo que, según el informe técnico de marzo de 1987, habría contravenido "los principios libertarios del Supremo Gobierno" de la época e impuesto "la necesidad de complicados y gravosos sistemas de control". Señala el propuesto artículo 4º, que toda persona, natural o jurídica, tendrá derecho a utilizar y servirse de los procedimientos con que cuenta la informática para recolectar, procesar, transmitir y difundir datos, en la forma prevista por la ley.

d) En lo referente a la recolección de datos, extrañamente se elimina la obligación de dar a conocer la finalidad de la misma (artículo 21 del "primer proyecto"). No soluciona el punto el propuesto artículo 8º, que sólo exige informar quienes son las personas destinatarias de la información.

e) En materia de derecho de acceso se obliga al responsable de un archivo a informar (sobre qué datos se registran y la fuente de la cual se obtuvieron), "a lo menos

una vez al año", a las personas respecto de las cuales se posee información, gratuitamente y observando algunas formalidades. Ya no se habla de la facultad de solicitar en cualquier momento una certificación o acreditación (lo que implica un mecanismo de consulta permanente)..., con lo cual habría que someterse al criterio de los administradores, existiendo el riesgo de eventuales indefensiones. Creemos que es conveniente que los responsables o detentadores de archivos de datos nominativos soporten una mayor carga administrativa y financiera que, por cierto, se verá compensada por los beneficios que obtendrán.

f) No se define o establece una distinción entre qué especie de información nominativa es parte de la esfera social de una persona, cuál de la esfera íntima o privada y cuál, por ser "sensible", requeriría de especial protección o, eventualmente, de ser excluida de procesamiento. Y el artículo 19 Nº 4 de la Constitución no señala cuáles son las informaciones propias de la vida privada: simplemente la consagra en términos genéricos, entregando por ende su configuración a la ley.

3. Sin lugar a dudas que el mayor logro lo constituyó el haber insertado en una ley de protección de datos un específico tipo de delito informático, en que el objeto material afectado es el soporte lógico del sistema, ...la información (datos y, necesariamente, los programas) destinada a ser procesada, durante su procesamiento o contenida en un sistema computacional.

a) El artículo 30 alude a los delitos "computacionales". Supone la comisión con medios informáticos de los delitos contemplados en la legislación penal, agravándose su penalidad (agravante especial). Esta figura, que tácita o indirectamente modifica el Código Penal, estimamos que se presenta como un complemento importante al delito tipificado en el artículo 31, por cuanto evita posibles dudas o vacíos de interpretación y amplía la protección penal de los bienes jurídicos que eventualmente pueden verse afectados por la criminalidad informática.

Esta hipótesis cubre a los delitos que pueden cometerse con prescindencia de medios computacionales y que actualmente están tipificados. Precisamente por utilizarse aquellos, se aumenta la pena. Y la estimamos un complemento importante, porque cubre los atentados a datos -objeto "material" del tipo- de naturaleza distinta a los nominativos, v.gr. estadísticos y patrimoniales, que en cuanto datos, en cuanto información estadística o patrimonial no son subsumidos por los tipos vigentes de delitos contra el patrimonio. Pensemos en la hipótesis -tan común- de un hurto de valores a través de transferir electrónicamente fondos; se afectan directamente datos o información patrimonial (asientos contables electrónicos) y, por ende, en definitiva al objeto o bien jurídico patrimonio o propiedad.

b) El artículo 31 es el más importante, por cuanto tipifica en forma amplia un delito específico o propiamente informático, señalando:

"Comete delito informático el que maliciosamente y sin derecho o autorización realice cualquier acto con la finalidad de obtener acceso, de apoderarse, de destruir o inutilizar, transformar o desfigurar la información contenida o destinada a ser procesada, en todo o en parte, en un sistema automatizado de tratamiento de la misma; o con la finalidad de impedir u obstaculizar el normal procesamiento de los datos contenidos en un sistema automatizado; o con la finalidad de revelar o transmitir indebidamente información. El culpable de este delito será sancionado con la pena de presidio menor en su grado medio a presidio mayor en su grado mínimo, según la extensión o cuantía del daño causado".

c) El artículo 32 introduce otro tipo penal, el que consideramos bastante cuestionable. La norma señala:

"Igualmente comete delito informático el que organice o utilice un sistema de tratamiento automatizado de información con un propósito ilícito. El culpable de este delito sufrirá las penas del artículo 293 del Código Penal."

V. Consideraciones finales y proposición de un esquema de proyecto de ley.

1. Frente a la existencia de sistemas informáticos con información nominativa, nos parece que necesariamente deben considerarse cuatro ámbitos o mecanismos de tutela: constitucionales, civiles, administrativos y penales, a los que brevemente pasaremos revista.

a) La garantía constitucional del artículo 19 Nº 4 de la Constitución de 1980 está amparada por el recurso de protección, en cuya virtud la víctima de actos u omisiones arbitrarios o ilegales, que le ocasionen privación, perturbación o amenaza en el legítimo ejercicio de su derecho al respeto y protección de la vida privada, puede accionar directa y judicialmente. Sin embargo, y salvo error u omisión, hasta esta fecha sólo se ha entablado un recurso de protección, contra la empresa Dicom S.A. y en relación directa con el artículo 19 Nº 4, ante la Ilustre Corte de Apelaciones de Concepción, la que por cierto no se pronunció sobre el resguardo de la intimidad sino que sobre la honra u honor del recurrente, afectada porque se le hacía aparecer como una persona que no cumplía sus obligaciones comerciales [7].

b) Del derecho civil, tiene plena aplicación el ámbito de la responsabilidad, contractual y sobre todo extracontractual; ella se traduce en la necesidad de indemnizar a la víctima los perjuicios que se le causen, por conductas dolosas y negligentes o culpables en el ámbito de un sistema informático.

---

[7] Para mayores antecedentes véase el artículo de Patricio Muñoz Navarro, en la Revista "Vigencia" de marzo de 1991, pp. 21 y ss.

La aplicación de esta responsabilidad permite, residual y recurrentemente, que todo aquel ilícito que escape a la sanción penal, por caer fuera de un tipo preciso, pueda ser castigado. Actualmente, la responsabilidad civil es una vía jurídica válida para la protección del derecho a la vida privada, en todos aquellos países que no tienen previstos en sus legislaciones tipos penales que cubran los más peligrosos atentados modernos en contra de la intimidad.

c) En una ley de protección de datos debe implementarse una tutela administrativa, v.gr., exigiéndose requisitos de autorización o registro para la creación y administración de bancos de datos nominativos -privados y públicos-, creándose un órgano ad-hoc que fiscalice la actividad y consagrándose sanciones -como la cancelación de la autorización de funcionamiento o la eliminación del registro-.

d) Por último, frente a conductas en que dolosamente se atente contra el contenido de información de un sistema informático -no sólo nominativo-, existe casi total unanimidad, en la moderna doctrina del Derecho Informático, en que la tutela requerida pasa por la tipificación de hipótesis de delitos informáticos, también insertos en una ley de protección de datos:

- Este es un ámbito en que pueden manipularse datos -fraude informático-, en que puede hurtarse información accediendo sin autorización a un sistema -espionaje informático-, en que ella puede destruirse -sabotaje informático- y en que pueden usarse bancos de datos sin autorización.

- Valorativamente, la intimidad, la información nominativa, es el más relevante de los bienes jurídicos afectados por la criminalidad informática. En Chile, algunos abogados que incluso participaron en la revisión del proyecto comentado en el acápite IV de este ensayo, descartan la tutela penal de la intimidad -vía delitos informáticos- y consideran de mayor relevancia al patrimonio, ...porque los perjuicios económicos suelen ser considerables. No obstante ser importante la criminalidad patrimonial informática, se trata de una opción que no podemos, por formación y convicción, compartir. Cuando se viola computacionalmente una garantía de rango constitucional, un derecho primordial para la dignidad, libertad y seguridad de las personas, deben poder aplicarse las sanciones más drásticas que contempla un ordenamiento jurídico, es decir, las penales, que implican privación de libertad; y éstas deben tipificarse.

- Tampoco existe discusión doctrinaria alguna sobre si los atentados contra la intimidad deben ser ilícitos civiles o penales. Hay quienes señalan que las conductas negligentes o culposas debieran ser sancionadas en sede de responsabilidad civil, descartándose la tipificación de cuasidelitos informáticos. Pero no sabemos de nadie, después de seis años de investigación en Chile y en el extranjero, que afirme que las conductas dolosas no deban sancionarse penalmente: para efectos del resarcimiento por la intromisión dolosa en la intimidad de una persona, se requiere que el hecho sea

constitutivo de delito; así, "la configuración del delito informático como una figura punible distinta, es la única solución que permitirá resolver el problema desde el punto de vista del hecho ilícito".

- No puede pretenderse que la tutela otorgada por los actuales tipos del Código Penal sea suficiente, por cuanto no cabe su aplicación analógica, porque es prácticamente mínima la protección de bienes jurídicos inmateriales, por la intangibilidad del objeto material afectado (información, datos, impulsos eléctricos, "bits") y porque al ser promulgado -hace más de 100 años- era imposible considerar la criminalidad informática, a la que no subsumen.

2. Frente a las consecuencias políticas, sociales, jurídicas y económicas del acelerado desarrollo que, particularmente en Chile, han experimentado la informática y las telecomunicaciones; teniendo en vista las soluciones del Derecho Comparado; y retomando las consideraciones más arriba formuladas, ...en un plano de lege ferenda creemos que una ley de protección de datos -no sólo nominativos-, para ser global y efectiva, debe tener el siguiente contenido y características:

a) Debe existir una parte dogmática, que contenga los conceptos básicos y principios fundamentales (como el derecho de acceso directo para el interesado, la autodeterminación informativa, la libertad informática, la confidencialidad de los datos o el secreto informático, etc); que fije su ámbito de aplicación; que distinga entre las especies de información tuteladas y entre la naturaleza privada o pública del banco; que defina qué datos, por su sensibilidad, deben ser especialmente tutelados o eventualmente excluidos de registro; que regule la recolección, procesamiento, almacenamiento y distribución o difusión de la información; que establezca derechos, obligaciones y responsabilidades para los titulares de los datos y sobre todo para el administrador responsable del sistema -por ejemplo, definiendo expresamente en qué casos se le permite revelarlos-.

En cuanto a los bancos de datos "públicos" o administrados por organismos de la Administración del Estado, tema por cierto delicado, creemos que sus requisitos de constitución deben ser más rígidos (exigiéndose autorización y no mero registro, a diferencia de los bancos de datos privados); que entre ellos debería prohibirse la existencia de bancos de datos integrados (que relacionan entre sí archivos y pueden elaborar perfiles de personalidad), salvo que el órgano de control y registro lo autorice; que por su naturaleza, algunas entidades -como Carabineros, Investigaciones y las FF.AA., que velan por la seguridad pública y la defensa nacional- deberían poseer bancos de datos "de acceso restringido", cuyo control no pueda ser ejercido directamente por los titulares de los datos sino que indirectamente, por el órgano ad-hoc o los tribunales que estén investigando un eventual reclamo o ilícito.

b) Debe existir una parte orgánica, que cree un órgano específico de control y fiscalización (v.gr. una superintendencia, una oficina de inspección de datos, una

comisión nacional de informática y libertades, un "encargado nacional para el secreto informático", una comisión de privacidad, etc.), el que deberá autorizar la creación de bancos de datos nominativos, llevar un registro nacional de los mismos, fiscalizar el cumplimiento de los deberes y obligaciones establecidos en la ley e imponer sanciones administrativas en caso de su inobservancia.

c) Deben considerarse aspectos procesales, como instancias de reclamo, primero administrativas ante el órgano ad-hoc y luego judiciales.

d) Por último, y sólo al final, debe existir una parte represiva o sancionadora, para conductas "indebidas", "no autorizadas" o "sin derecho" y para el uso abusivo de la información o de los atentados contra ella, con sanciones sólo administrativas (v.gr. cancelación de la autorización de funcionamiento, eliminación del registro, multas) y penales (tipificación de delitos informáticos para las conductas indebidas y dolosas o maliciosas), quedando las sanciones civiles entregadas a las reglas generales del derecho.

CAMARA DE DIPUTADOS
CHILE

BOLETIN Nº 412-07

MOCION

PROYECTO DE LEY SOBRE DELITO INFORMATICO

Honorable Cámara de Diputados

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

Nadie discute en la actualidad los grandes beneficios que la introducción de las referidas tecnología ha producido, en términos de un mejor aprovechamiento de energías y recursos. Sin embargo, la creciente importancia que ha adquirido la informática ha hecho patente la vulnerabilidad de las sociedades y de las organizaciones que las utilizan. Son muchos los abusos que, recurriendo a los avances de la ciencia de la información, pueden cometerse. No cuesta gran esfuerzo imaginar el daño que puede causarse a enormes cantidades de personas, si la información contenida en un banco de datos, por ejemplo el de una A.F.P., fuera distorsionada, adulterada o destruida por la acción de un operador malintencionado o que busque *algún tipo de enriquecimiento ilícito* para sí o para terceros. Tampoco resulta difícil suponer los desvastadores efectos que tendría la interferencia a la transmisión de los datos con que debe alimentarse un sistema automatizado de información, o lo que significaría la revelación de los datos que contenga, *fuera de los casos en que tal acción estuviera permitida o expresamente autorizada por la ley*. De ahí que la doctrina penal contemporánea emplee la expresión *"delito masivo"* para referirse a los atentados contra la información acumulada en archivos computacionales o bancos de datos, al tener en cuenta la gran cantidad de personas que pueda ser afectados por ello.

El proyecto de ley que presento a la consideración de esta H. Cámara tiene por finalidad *proteger este nuevo bien jurídico que ha surgido* con el uso de las modernas tecnologías computaciones; la calidad, pureza e idoneidad de *la información en cuanto tal*, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan. Aquélla, por el actual desarrollo tecnológico de la sociedad, merece ser protegida mediante la creación de figuras delictuales nuevas, que pongan de relieve su importancia. *Nos hacemos eco de la tendencia existente en el derecho comparado contemporáneo y de las recomendaciones de organismos internacionales especializados en el tema*. La protección de un sistema de información automatizado se realiza mediante la creación de figuras penales especiales, que evitan la necesidad de hacer interpretaciones extensivas de las tradicionales normas penales, para incluir conductas indebidas en contra los sistemas automatizados de tratamiento de la información, *tanto en lo referente a su soporte lógico o programas de funcionamiento como en lo relativo a los datos que manejan*. Es el camino que han seguido países como Estados Unidos de Norteamérica, Francia, Alemania, Austria, Suiza, entre otros. A la misma conclusión han *llegado los escasos estudios realizados por juristas nacionales*. Estos, después de un exhaustivo análisis de los tipos tradicionales, tales como el hurto, la apropiación indebida, la estafa, los delitos de daños, han constatado que la protección de la información y de los soportes lógicos de los sistemas automatizados no se logra adecuadamente. Sobre el particular cabe señalar que la necesidad de crear la figura del delito informático ha estado presente en nuestro país desde hace algún tiempo. Prueba de ello es la existencia de *al menos dos anteproyectos de ley* que lo establecían como parte de un conjunto de normas destinadas a regular la actividad informática. Sin embargo, precisamente *por haber sido incluido en una normativa muy ambiciosa y compleja* no logró traducirse en ley.

El artículo 1º contempla la figura del *sabotaje al funcionamiento del sistema*, es decir, a sus programas o soportes lógicos. El inciso segundo, siguiendo la tendencia de la doctrina contemporánea, establece una causal de agravamiento de la responsabilidad, cuando como resultado del daño a los programas se produce, además, el de los datos contenidos en el sistema.

El artículo 2º establece la figura del *espionaje a un sistema automatizado*. El artículo 3º sanciona la *revelación de información* contenida en uno de estos sistemas en forma indebida, estableciéndose una agravante para la persona que siendo responsable del sistema lo haga abusando de la confianza depositada en él. El artículo 4º se refiere a la *protección de los datos contenidos* en estos sistemas. En él se tipifica un conjunto de conductas que los expertos están contestes en considerarlas de extrema peligrosidad, por lo que se las sanciona con las penas más drásticas que este proyecto contempla. Por último, el artículo 5º establece una agravante de responsabilidad cuando quien realiza cualquiera de las conductas tipificadas en las disposiciones anteriores lo hagan con el *ánimo de enriquecerse* personalmente él o a un tercero.

Por las anteriores consideraciones expuestas vengo en someter a la consideración de esta H. Cámara el siguiente:

PROYECTO DE LEY

Artículo 1º.- El que indebidamente destruya, inutilice, obstaculice, impida o modifique el funcionamiento de un sistema automatizado de tratamiento de información sufrirá la pena de presidio menor en su grado máximo.

Si como consecuencia de estas conductas se afectaran los datos contenidos en el sistema, en algunas de las formas señaladas en el artículo cuarto, la pena será la indicada en éste aumentada en un grado.

Artículo 2º.- El que sin derecho intercepte, interfiera, o acceda a un sistema automatizado de tratamiento de información será castigado con presidio menor en su grado medio.

Artículo 3º.- El que revele, transmita o se apodere indebidamente de la información contenida en un sistema automatizado de tratamiento de la misma incurrirá en la pena de presidio mayor en su grado mínimo.

Si quien realiza estas conductas es el responsable del sistema la pena se incrementará en un grado.

Artículo 4º.- El que indebidamente introduzca, transforme, desfigure, altere, dañe o destruya los datos contenidos en un sistema automatizado de tratamiento de información será castigado con presidio mayor en su grado medio.

Artículo 5º.- Si las conductas de los artículos anteriores son efectuadas con ánimo de lucro, la pena se aumentará en un grado.

JOSE ANTONIO VIERA-GALLO QUESNEY
Diputado

CAMARA DE DIPUTADOS
CHILE

BOLETIN Nº 458-07

MOCION

PROYECTO DE LEY SOBRE RECOLECCION, PROCESAMIENTO, CUSTODIA, TRANSMISION Y DIFUSION DE DATOS PERSONALES, DE FAMILIA Y CONCERNIENTES A LOS DERECHOS Y DEBERES GARANTIZADOS POR LA CONSTITUCION

Honorable Cámara:

Como es sabido la informática deja sentir su incontenible influjo en prácticamente todas las áreas del conocimiento humano, dentro de las cuales el derecho no puede ser la excepción, dando lugar, en términos instrumentales, a la llamada informática jurídica.

Hace algunos años, por la Comisión Decreto exento, Ministerio de Justicia número 118, de 15-09-86, se elaboró un anteproyecto de ley sobre materias de informática, el cual nos permitimos someter a la consideración de la Cámara de Diputados, por la trascendencia de las materias en él contenidas, sin perjuicio que durante su tramitación, como corresponde a todo proceso legislativo, sea perfeccionado con los aportes de los parlamentarios y sectores interesados en la informática.

Por la importancia que tienen para la fundamentación de este proyecto reproducimos los comentarios de Julio Tellez Valdés, Derecho Informático, Universidad Nacional Autónoma de México sobre la protección jurídica de los datos personales.

PROTECCION JURIDICA DE LOS DATOS PERSONALES

A. Nociones Generales.

Como se ha dejado asentado, la informática no es un fenómeno exclusivamente tecnológico con implicaciones estrictamente positivas. Las computadoras, al permitir un manejo rápido y eficiente de grandes volúmenes de información, facilitan la concentración automática de datos referidos a las personas, constituyéndose así en un verdadero factor de poder.

1. Recopilación de datos personales.

No es sino propiamente en la década de los setenta cuando comienzan a surgir numerosos archivos con informaciones de tipo personal, con un conjunto mínimo de datos como filiación, fecha y lugar de nacimiento, domicilio, estado civil, etcétera, hasta otro tipo de datos con caracteres aún más distintivos como raza, religión inclinaciones políticas, ingresos, cuentas bancarias, historia clínica, etcétera. Dichos datos, al ser recopilados en diferentes centros de acopio como lo son los registros censales, civiles, parroquiales, médicos, académicos, deportivos, culturales, administrativos, fiscales, bancarios,

laborales, etcétera, ya no por medios exclusivamente manuales sino con el apoyo de medios automatizados, provocan una gran concentración, sistematización e instantánea disponibilidad de ese tipo de información para diferentes fines.

2. Destinación e implicaciones.

Este tipo de datos no son vulnerables per se, sino según la destinación de que puedan ser objeto, pudiendo ser variada; de esta forma, dichas informaciones pueden ser empleadas para fines publicitarios, comerciales, fiscales, policiacos, etcétera, convirtiéndose de esta manera en un instrumento de opresión y mercantilismo. La variedad de los supuestos posibles de indefensión frente al problema provoca que los individuos estén a merced de un sinnúmeros de situaciones que alteren sus derechos fundamentales en sociedad provocados por discriminaciones, manipulaciones, persecuciones, presiones, asedios, etcétera, todo ello al margen de un control jurídico adecuado.

B. Nociones Particulares.

Ya desde 1968 en el seno de la Asamblea de los Derechos Humanos auspiciada por la ONU se mostraba una honda preocupación por la manera en que la ciencia y la tecnología podrían alterar los derechos del individuo, empezando a denotar la necesaria emanación de un régimen jurídico que pudiera afrontar cabalmente este género de situaciones.

1. Figuras Jurídicas aplicables.

Por cuanto toca a nuestra problemática en cuestión, son variadas las figuras de índole jurídico bajo las cuales se ha estudiado a intentado regular dicha cuestión.

Así, tenemos que figuran tales como los derechos humanos, derechos personales, derechos patrimoniales, libertades públicas y privadas en el caso de Francia, derecho de la privacidad en el caso de los paises anglosajones, derecho a la intimidad y el honor de las personas como en España, o aún las garantías individuales y sociales como pudiera ser el caso en nuestro país, todas ellas, como eventual protección, han tendido hacia una sujeción apropiada en cuanto a la concentración y destinación de los datos de carácter personal.

2. Diferentes tipos de archivos.

Estos pueden ser, dependiendo de su contenido: archivos públicos (aquellos manejados por el Estado), archivos privados (aquellos manejados por empresas privadas), manuales (si son procesados en forma manual), automáticos (sí son procesados en forma automática), sobre personas físicas (sean residentes o no de un determinado país) o personas morales.

Cabe hacer mención que a nivel positivo no todos estos archivos estarán sujetos a una regulación jurídica.

3. Principales derechos y excepciones.

Es evidente que si se habla de una regulación jurídica ésta engendra a su vez determinados derechos y excepciones. Este problema, por su misma singularidad, motiva asimismo derechos muy especiales entre los que podemos contar:

a) Derecho de acceso.

Es aquel que permite a los interesados conocer las instituciones y el tipo de información que dispongan sobre su persona.

b) Derecho de rectificación.

Complementario al anterior, dicho derecho permite solicitar al interesado una modificación en los términos de alteración o ampliación, o una supresión o cancelación de aquellos datos que, referidos a su persona, considere como inexactos o irrelevantes.

c) Derecho de uso conforme al fin.

Este consiste en que el interesado puede exigir que su información nominativa sea destinada para los objetivos por los cuales se proveyó, es decir, si era de índole administrativo, que no trasciende a niveles más allá de los planteados en un principio.

d) Derecho para la prohibición de interconexión de archivos.

Ahora, bien, cabe señalar que el incumplimiento a estos derechos puede generar diferentes sanciones de índole civil, administrativa o incluso penal, dependiendo de las circunstancias.

Por cuanto concierne a las excepciones a dichos derechos fundamentadas en el equilibrio del Estado y su poder coercitivo y los integrantes de la sociedad, tenemos a aquellas derivadas con motivo de la seguridad del Estado tanto en lo interno como en lo externo, así como las relativas a intereses monetarios, persecución de delitos, motivos de salud, etcétera.

C. Panorama Internacional.

En función del innegable carácter económico inherente a este problema es entonces que hemos considerado conveniente presentar la situación internacional de hecho y de derecho en torno al mismo, estructurada en tres grupos de países bien definidos de acuerdo al régimen económico prevaleciente, a saber; países desarrollados, socialistas y en desarrollo, para presentar finalmente una semblanza del único acuerdo existente a la época, en materia de protección de datos personales: el Convenio de Estrasburgo.

1. Países desarrollados.

En este grupo de países tenemos a aquellos en los que existe una consigna a nivel constitucional alusiva a este respecto como es el caso de Portugal, España, Austria, Holanda y Suiza.

Por otra parte, tenemos, dentro de este grupo, a aquellos países que cuentan con una ley de carácter general que contiene un conjunto de disposiciones alusivas al problema como es el caso de Estados Unidos, con EE.UU. su Privacy Act o Ley de la Privacidad del 31 de Diciembre de 1974, bajo las consideraciones de una protección a la vida privada, siendo los tribunales federales el órgano jurisdiccional competente con sanciones de tipo penal. Cabe mencionar que dicha ley, para los efectos de este problema, se halla complementada por otras disposiciones.

Asimismo, con un ordenamiento general con disposiciones particulares tenemos a Canadá con su Human Rights Act o Ley de Derechos Humanos del 14 de Junio de 1977 inspirada en la ley norteamericana, y en cuyo capítulo IV aborda especificamente los problemas derivados de la informatización respecto a los derechos humanos, existiendo una autoridad encargada de velar el cumplimiento de dicha ley, como es el caso del comisario para la protección de la vida privada nombrado por el minis-

tro de justicia.

Por otro lado, tenemos a aquellos países que dentro de este grupo disponen de una ley que en forma exprofesa regula el fenómeno de la protección de datos personales; tal es el caso de Suecia con su Datalas o Ley de Datos del 11 de Mayo de 1973, primeras regulación a nivel nacional, con un organismo supervisor como es la Data Inspektion Board (DIB), y completamente por la Ley de Información sobre Solvencia de 1973 y la Ley de Trabajo y Cobro de Créditos por cuenta ajena de 1974.

Asimismo tenemos a la República Federal de Alemania (ex RFA) con su Budesdatenschutzegesetz o Ley Federal de Protección de Datos de 27 de Enero, de 1977, con un comisario federal de datos encargado de velar su cumplimiento y complementada por diversos ordenamientos.

Francia, con su Ley relativa a la Informática, Archivos y Libertades del 6 de Enero de 1978 con su Comisión Nacional de Informática y Libertades como órgano especial y autónomo con funciones de control por medio de reglamentos, con derechos a informarse y obligación de informar.

Otros países con disposiciones específicas son: Dinamarca con sus leyes sobre Archivos Públicos y Privados del 8 de Junio de 1978, Noruega con su Ley sobre Datos de Carácter Personal de 9 de Junio de 1978, Australia y su Ley de Protección de Datos del 18 de Octubre de 1978, Luxemburgo y su ley reglamentaria de la utilización de datos nominativos en los tratamientos informáticos del 11 de Abril de 1979, así como las de Islandia del 1º de Enero de 1982 y la Gran Bretaña del 1º de Julio de 1984.

Existen, también, y siempre dentro de este grupo, algunos países que, preocupados por la trascendencia del problema, están cercanos a promulgar una reglamentación jurídica sobre el particular, tal es el caso de Bélgica, Portugal, Holanda, Japón, Italia, Finlandia, Austria y Nueva Zelanda.

2. Países socialistas.

Si bien es cierto que en estos países la informatización avanza por momentos con un ritmo menos pronunciado que los países occidentales, el carácter centralizado de las estructuras políticas y administrativas, aunado al desarrollo informático, provoca en teoría una cierta identidad respecto al problema. Las amenazas sobre el contenido de los derechos cívicos son mal percibidas por los particulares sin disponer del medio de comprobar en su vida cotidiana la eficacia de los sistemas informáticos, pudiendo ser afectados por el manejo inadecuado de la información sobre su persona, aun con implicaciones de carácter comercial.

Sólo ciertos medios son sensibilizados y buscan alimentar un debate más o menos difundido según el país y su grado de pasividad frente a la administración como es el caso de Polonia y Checoslovaquia.

Por otra parte, Hungría en su Código Civil de 1977, en su artículo 83, fracción I, menciona que la informática no debe amenazar en ningún momento los derechos del individuo, disposición sin duda significativa por tratarse de un país localizado detrás de la llamada "Cortina de Hierro".

3. Países en desarrollo.

En este grupo de países, si bien el grado de informatización no llega a ser (salvo el caso de algunas naciones) muy considerables, aun así el problema de la protección jurídica de los datos personales, no deja de estar latente. Sin embargo, cabe mencionar que la preocupación por parte de los organismos internacionales respecto a estos países ha sido mayor en los términos del llamado Flujo de Datos

Transfronterizos que analizaremos posteriormente.

El caso de México no es muy claro, pues aun existiendo consignas a nivel constitucional que garantizan el derecho a la información, derecho de petición o algunos privilegios personales (familia, papeles, posesiones, etcétera), o disposiciones penales sobre violación de correspondencia (artículo 173) y revelación de secretos (artículo 219 y 211), daño moral en materia civil (artículo 1916) e incluso una Ley de Información Estadística y Geográfica de 30 de Diciembre de 1980 y su reglamento de fecha 3 de Noviembre de 1982, y algunos otros ordenamientos, lo cierto es que el problema se puede manifestar sin disponer realmente de una protección jurídica eficaz frente al mismo.

4. Convenio de Estrasburgo.

Este acuerdo internacional de fecha 28 de Enero de 1981 denominado Convención para la Protección de las Personas Respecto al Tratamiento Automatizado de Datos de Carácter Personal y más conocido bajo al rubro del Convenio de Estrasburgo, fue suscrito por ocho países como lo son Australia, República Federal de Alemania, Dinamarca, España Francia, Luxemburgo, Suecia y Turquía, aún no ratificado, y abierto a la firma de todos los países interesados, contiene una serie de disposiciones (27 artículos integrados en 7 capítulos) relativos a objetivos, definiciones, ámbitos de aplicación, obligaciones de las partes derechos, excepciones, sanciones, autoridades, consignas generales y específicas no sólo en materia de protección de datos personales, sino también a nivel del flujo de datos transfronterizos, sin lugar a dudas un cuerpo normativo muy interesante, aunque ciertamente ilimitado a nivel de resolución del problema.

María Claude Mayo, en su libro "Informática Jurídica, Editorial Jurídica de Chile, 1991, expresa:

EL INDIVIDUO

Antes de la existencia del computador los individuos dejaban una multiplicidad de información en todas partes, en cualquier lugar donde se establecía una relación social, comercial o familiar: Nombre, actividad, cédula de identidad, dirección, lugar de trabajo, teléfonos, estado civil, nombre del cónyuge, de sus hijos, ingresos, bienes raíces, etc. Estos datos tenían la cualidad de ser mantenidos y acumulados con diferentes objetivos por las personas con las cuales ese individuo se relacionaba.

La virtud del computador y de esta estructura u organización que se denomina "banco de datos" unidad a la forma de estructurar los datos que se van entregando, ha ido resaltando el hecho que el individuo que entrega esa información, hoy en día, se está exponiendo de algún modo a que los demás entes de la colectividad social tengan la posibilidad de conocer su imagen real o presunta en forma integral en todas sus relaciones familiares, sociales, comerciales, etc., con gran velocidad y certeza mediante la interacción con estos bancos.

Debido al hecho de que estos bancos de datos pueden hoy en día ligarse unos con otros y traspasarse la información, se ha puesto de relieve la situación de que el individuo bajo esta "sociedad informatizada" ha ido perdiendo un bien que hasta este momento no había sentido lesionado: su "privacidad".

En la medida que los datos que se entregan en el medio social se van relacionando con otros, que también han sido entregados privadamente, se van produciendo situaciones tanto favorables como desfavorables para el individuo.

Hoy en día los datos que antes entregábamos y quedaban consignados en fichas de papel se encuentran en prodigiosas memorias capaces de nunca olvidar y siempre estar dispuestas a recordar, que además tiene la virtud de comunicarse con otras de igual capacidad e intercambiar información. Es por ello que hoy el individuo es comparable a un pez al interior de una pecera, cuya vida puede ser observada por quien lo desee y en cualquier momento.

El factor privacidad se puede conceptualizar como el derecho a estar solo, en un espacio propio conocido sólo por aquellos a quienes se lo hemos permitido de un modo libre y natural, derecho a reflexionar sobre uno mismo, por sí mismo, a llegar a conclusiones propias sobre aspectos de nuestras vidas y nuestras familias, sin el conocimiento o la intervención de terceros.

No cabe la menor duda de que, por su trascendencia, la protección de la privacidad es el tema que jurídicamente se debe analizar en primer término.

La regla fundamental de la protección de la privacidad de los datos está configurada por dos extremos que por el bien de la sociedad se desea compatibilizar: el derecho del que gozan los sujetos de la información de tener acceso a sus datos personales y a corregir aquellos que sean erróneos e impertinentes, pero con la limitación que tal prerrogativa no llegue a coartar la libertad de recolección, es decir, sobre bases que no perturben ni entraben el avance de la ciencia y la tecnología y no coarten el principio de libertad informática.

Es por estas consideraciones que nos hemos permitido recoger este interesante proyecto de ley, para así abrir cauce a un amplio y profundo debate que termine para dar lugar a una nueva legislación que, junto con representar un amplio consenso, coloque nuestras instituciones jurídicas a la altura de los tiempos modernos.

TITULO I DE LA LIBERTAD INFORMATICA

PARRAFO PRIMERO: DISPOSICIONES GENERALES

Artículo 1.- La aplicación de la informática a la recolección, procesamiento, custodia, transmisión y difusión de datos personales o de familia o concernientes a los derechos y deberes garantizados a éstos por la Constitución Política de la República, se regulará por las disposiciones de la presente ley, y, subsidiariamente por el ordenamiento positivo vigente, en lo que fuere aplicable. Lo dispuesto en el inciso anterior será aplicable, en lo que sea procedente, a las personas jurídicas, sociedades de hecho y comunidades.

Artículo 2.- Toda persona tiene derecho a que se mantengan en reserva los antecedentes o hechos de su vida privada. Sólo en virtud de la Ley o del consentimiento del interesado podrán hacerse públicos tales antecedentes o hechos.

En el caso de las personas jurídicas, este derecho se refiere a los antecedentes comprendidos en su ámbito de actividades que no estén obligadas a hacer públicas. La publicidad comprende la divulgación y la comunicación de hechos, antecedentes o informaciones.

Artículo 3.- El derecho establecido en el artículo anterior no podrá ser ejercitado para amparar u ocultar la comisión de crímenes o simples delitos.

PARRAFO SEGUNDO: DE LA LIBERTAD INFORMATICA

Artículo 4.- Toda persona natural o jurídica tiene derecho a utilizar y servirse de los procedimientos con que cuenta la informática para recolectar, procesar, transmitir y difundir datos en la forma prevista por la ley.

Artículo 5.- Los archivos de datos que, con cualquier denominación, hayan sido creados como resultado de la aplicación de leyes particulares se regirán por las disposiciones de las mismas.

PARRAFO TERCERO: DE LA RECOLECCION Y PROCESAMIENTO DE DATOS

Artículo 6.- Las informaciones personales o nominativas sólo pueden ser obtenidas o recolectadas por medios lícitos.

Estas informaciones deben ser fieles, exactas, completas, pertinentes y adecuadas al objeto de su recolección.

Artículo 7.- En los casos en que el propósito de la recolección sea estadístico, tanto éstas como los programas y diseños lógicos no podrán incluir ningún elemento que permita la identificación de las personas.

Artículo 8.- En toda recolección de datos que se realice individualmente, a través de encuestas, test u otros instrumentos, se deberá informar del carácter obligatorio o facultativo de las respuestas, de las consecuencias respecto de ellas, y de las personas naturales o jurídicas destinatarias de la información.

Estos instrumentos deberán mencionar las prescripciones aquí establecidas.

Artículo 9.- Todo responsable de un archivo de datos personales deberá establecer procedimientos para la corrección de inexactitudes y la eliminación de información improcedente.

Requerida la corrección o eliminación señalada precedentemente, el responsable de archivo de datos deberá emitir un pronunciamiento e el plazo fatal de diez días, fundando su resolución si fuere negativa. Vencido que sea este término sin que hubiere habido respuesta, se entenderá rechazada la petición, pudiendo el requiriente iniciar las acciones legales que corresponda.

PARRAFO CUARTO: DE LA DIFUSION DE DATOS

Artículo 10.- Se prohibe la comunicación abusiva de datos personales, entendiéndose por tal, la que resulte de cruzar o relacionar datos totales o parciales entregados con un objeto diferente.

Artículo 11.- Los datos personales que se utilicen estadísticos sólo podrán ser difundidos en forma general de modo que no puedan ser atribuídos a personas determinadas.

Artículo 12.- La presente ley se aplicará también a los archivos de datos personales no contemplados en el artículo quinto pertenecientes o administrados por organismos de la administración del Estado.

Artículo 13.- Los archivos de datos referidos en el artículo anterior, podrán transmitir datos de carácter personal sólo en el ejercicio de su actividad u objeto institucional, o con fines estadísticos o de acuerdo al

derecho de conocimiento, establecido en el artículo quince de la presente ley.

Artículo 14.- El incumplimiento de las obligaciones establecidas en los artículos precedentes, da origen por parte del infractor, a la correspondiente responsabilidad civil.

TITULO II DE LOS DERECHOS INDIVIDUALES

PARRAFO PRIMERO: DEL DERECHO DE CONOCIMIENTO Y ACCESO

Artículo 15.- Toda persona natural o jurídica, o sus representantes legales, tiene derecho a saber dónde y qué datos se tienen registrados acerca de ella y las fuentes de información que para ello se han utilizado.

Artículo 16.- El ejercicio del derecho establecido en el artículo precedente implica la obligación del responsable del archivo de datos, de informar en forma gratuita y a lo menos una vez al año a las personas respecto de las cuales posee información, sobre qué datos de éstas registra y la fuente de la cual se obtuvo. Tratándose de datos relativos a la salud, la información sólo podrá ser entregada a requerimiento personal del afectado y a falta de impedimento de éste al cónyuge, sus padres, tutores, curadores o representantes legales.

Artículo 17.- La información que se otorgue de conformidad al artículo precedente, debe ser una transcripción ordenada, íntegra y cabal de los hechos registrados, escrita en idioma castellano. Deberá contener asimismo la fecha de expedición.

PARRAFO SEGUNDO: DEL DERECHO DE CORREGIR

Artículo 18.- Acreditada y fundamentada ante el responsable del archivo de datos la inexactitud de las informaciones contenidas en él, se tendrá derecho a exigir su corrección, debiendo éste emitir un certificado actualizado en los términos señalados en el artículo precedente.

Artículo 19.- En los casos en que proceda la corrección deberá ser comunicada por el responsable del archivo de datos a las entidades a que con anterioridad se transfirió esa información o de las cuales se hubiere obtenido. El cumplimiento de esta obligación corresponderá, en primer término a quien haya suministrado inicialmente la información que se rectifique.

PARRAFO TERCERO: DEL DERECHO DE ELIMINAR DATOS O IMPEDIR SU DIFUSION

Artículo 20.- Toda persona natural o jurídica tiene derecho de exigir que se le excluya de un archivo de datos cuya finalidad sea transmitirlos o difundirlos, a menos que su inclusión tenga su fundamento en una ley o en un acto de voluntad de aquella.

Artículo 21.- Se presume que los datos contenidos en un archivo a los cuales se les da una utilización distinta o diferente de aquella para la cual fueron obtenidos, no ha sido recolectados con la autorización de la persona a la cual se refieren.

PARRAFO CUARTO: DEL DERECHO DE ACTUALIZAR, VERIFICAR Y APERCIBIR

Artículo 22.- Toda persona tiene derecho de exigir la puesta al día de la información que de ella se tenga. Este derecho incluye, asimismo, el de complementarla.

Artículo 23.- Toda persona tiene derecho de solicitar al responsable de un archivo de datos personales, que adopte las medidas necesarias para prevenir o impedir que se puedan conculcar los derechos consagrados en esta ley.

En caso de denegación o retardo en la adopción de las medidas, se podrá acudir ante el juez competente para que sean dictados todos los resguardos conducentes a proteger los derechos consagrados por la ley.

TITULO III DEL PROCEDIMIENTO JUDICIAL

Artículo 24.- El conocimiento y fallo de las causas que tengan su origen en esta ley, se sujetarán al procedimiento sumario establecido en el Título XI del Libro II del Código de Procedimiento Civil, no siendo aplicables en estos procesos lo dispuesto en el artículo 681 del mismo cuerpo legal.

TITULO IV DE LOS MEDIOS DE PRUEBA

Artículo 25.- Se admitirán y apreciarán en toda clase de juicios, en conformidad a las reglas que rigen la prueba documental según la materia de la causa, las pruebas informáticas consistentes en discos, cintas o cualquier clase de archivo magnético o de uno computacional y en la reproducción, por cualquier medio, de su contenido.

La existencia de documentos impresos generados por computador hace presumir que su contenido está o ha estado en un archivo magnético o de uso computacional.

Artículo 26.- Los documentos impresos generados por computador y expendidos por servicios públicos, tendrán valor de instrumentos públicos cuando se conformen a las características que el respectivo reglamento determine.

Artículo 27.- Los documentos emitidos por un archivo de datos hacen prueba en contra de quien los emitió, a menos de probarse que provienen de otro archivo de datos; de otros computadores o equipos accesorios a éstos, distintos a los utilizados por el emisor putativo; o que han sido maliciosamente forjados, en todo o en parte.

Artículo 28.- En las causas en que incidan problemas informáticos y cualquiera fuera el estado de éstas, podrá decretarse la inspección personal del tribunal.

En toda inspección que se decrete, deberá previamente designarse peritos, los cuales se nombrarán conforme a las reglas del párrafo sexto del Título XI del Libro II del Código de Procedimiento Civil. La diligencia se llevará a cabo con la concurrencia de las partes y peritos designados o sólo por el Tribunal y los peritos en ausencia de aquellas, aplicándose en lo demás lo dispuesto en el inciso segundo del artículo 405 y siguientes del mismo código.

Artículo 29.- Cuando se decrete informe de peritos o inspección personal del tribunal, el responsable del archivo de datos deberá permitir el acceso a todos los elementos físicos, magnéticos o de cualquier naturaleza, necesarios para el cabal cumplimiento de la diligencia.

Para los efectos de esta disposición, la palabra acceso empleada en ella significará la acción de conocer y comprender los elementos físicos y de almacenamiento de un archivo de datos y su contenido.

El responsable del archivo estará obligado a señalar, dentro del tercer día hábil, el o los lugares o recintos en que se encuentren dichos elementos.

TITULO V DE LOS DELITOS INFORMATICOS

Artículo 30.- La comisión de los delitos previstos en el Código Penal o en leyes especiales, ejecutados por medios informáticos, tendrá la penalidad que se establece para cada caso, au-mentada en un grado.

Artículo 31.- Comete delito informático el que maliciosamente, y sin derecho o autorización realice cualquier acto con la finalidad de obtener acceso, de apoderarse, de destruir o inutilizar, transformar o desfigurar la información contenida o destinada a ser procesada, en todo o en parte, en un sistema automatizado de tratamiento de la misma; o con la finalidad de impedir u obstaculizar el normal procesamiento de los datos contenidos en un sistema automatizado; o con la finalidad de revelar o transmitir indebidamente información.

El culpable de este delito será sancionado con la pena de presidio menor en su grado medio a presidio mayor en su grado mínimo, según la extensión o cuantía del daño causado.

Artículo 32.- Igualmente comete delito informático el que organice o utilice un sistema de tratamiento automatizado de información con un propósito ilícito. El culpable de este delito sufrirá las penas del artículo 293 del Código penal.

Artículo 33.- La acción penal de los delitos señalados en los artículos precedentes no podrá ser ejercida por el Ministerio Público, ni por otra persona que no fuere la ofendida o su representante legal.

Iniciado el procedimiento, no se suspenderá, sino por las mismas causas porque debe suspenderse el procedimiento en los juicios que se siguen de oficio.

Artículo 34.- La presente ley se aplicará a las actividades y acciones señaladas en el artículo primero aún cuando se efectúe por medios manuales, mecánicos u otros.

Artículo 35.- La presente ley entrará en vigencia 90 días después de la publicación en el Diario Oficial.

SERGIO PIZARRO MACKAY
DIPUTADO

ERNAN BOSSELIN CORREA
DIPUTADO