CRIMINOLOGIA E INFORMATICA

La informática y el derecho a la intimidad

Jorge Zavala Baquerizo

I. Uno de los descubrimientos técnicos que más ha conmovido a la sociedad en los últimos años en casi todas sus relaciones es la Informática, la que tomó a ciertos sectores de la cultura de manera sorpresiva, algunos de los cuales aún no han logrado adaptarse a las nuevas modalidades que ha marcado la Informática. Tal es el caso del Derecho, que ha demorado no poco para reaccionar frente al fenómeno indicado, y lo ha hecho, y lo está haciendo, con mucha cautela y no sin pocas vacilaciones.

No pretendemos hacer un estudio detenido de la influencia que la Informática ha tenido y tiene en el medio social e individual de todos los países, industrializados o no; ni siquiera entraremos al extenso campo de la llamada "Informática Jurídica", sino que trataremos de señalar el impacto que la misma ha tenido y tiene dentro del campo jurídico cuando se presenta como un fenómeno criminal que afecta a singulares derechos del hombre como, la intimidad individual y familiar.

Desde la muy remota época en que el hombre comenzó a tratar de comunicarse con sus semejantes, mediante balbuceos monosilábicos, hasta el presente en que se comunica al mismo tiempo con millones de personas, han transcurrido miles de millones de años, dentro de los cuales ha cruzado por las etapas de la comunicación grabada en piedra a través de las representaciones gráficas, luego con el perfeccionamiento del lenguaje y su expresión en signos y más tarde, luego de la invención del alfabeto, en letras que, posteriormente, fueron capaces de difundirse a través de un nuevo invento que conmocionó la cultura, como fue la imprenta con tipos móviles. Y es necesario reconocer que en este siglo el avance de la comunicación entre los hombres ha provocado un evidente impulso de la cultura y, a la vez, ha ampliado aún más las diferencias tecnológicas

entre los países desarrollados y aquellos a los que se llama peyorativamente subdesarrollados o en vías de desarrollo.

Comenzaremos entregando un concepto que pueda orientar el estudio de la influencia de la Informática en el fenómeno criminal. Nos parece que una noción inteligible sobre lo que debe entenderse por "informática" nos la entrega Vittorio Frosini, quien dice: "La Informática puede definirse globalmente como la tecnología de la información; es decir, no sólo su tratamiento técnico por medio de un instrumento como ocurría ya con las distintas formas de registro mecánico, con los archivos mecanográficos de funcionamiento manual, con los aparatos criptográficos; sino su trasposición a un proceso puramente intelectual de control, de movimiento combinatorio y de traducción a nueva fórmula, que fue desenvuelto por el logicario".

La esencia de la Informática radica en su automatización, en tanto puede reproducirse, corregirse y transmitirse automáticamente. Para este efecto necesita una máquina, cuya "parte material de la computadora, llamada *hardware,* debe distinguirse claramente de la parte meramente lógica del procedimiento de elaboración, de la que se denomina *software,* y que por eso se podría denominar logicario'. Es esta la que da lugar a la denominada inteligencia artificial del *computer,* y que constituye una prótesis electrónica de la inteligencia humana, por medio de la cual se puede identificar, seleccionar y comparar las informaciones recibidas a una velocidad superior a la del pensamiento humano, cuyo proceso se refleja o mejor se reproduce en el logicario" (Frondizi).

El problema de la Informática en relación con la Criminología se lo debe analizar desde dos ángulos diferentes: el de la creación y el del uso, es decir, el amparo penal que debe tener el medio mecánico inventado y que reclama protección; y la mala utilización o abuso de dicho medio que impacta negativamente en las relaciones individuales y sociales en general.

En cuanto al problema relacionado con la protección al invento o creación, se debe recordar que en muchos países se ha pensado que no es necesario darle otra protección penal a la obra creativa que aquella que le conceden las leyes que amparan los derechos de autor, o las referentes al amparo a las marcas de fábrica que, por lo general, contienen tipos penales y, además, ciertas sanciones de carácter civil, particularmente pecuniarias y administrativas.

Estamos hablando, pues, en tanto en cuanto la máquina (computer) u ordenadores, programas, etc., son objeto de acción ilícita. **Desde este** punto de vista pensamos que, en efecto, no se debe pasar más allá de la protección que pueden conceder las vigentes leyes que amparan los derechos de autor, o las de marcas de fábrica, u otras similares, además de la protección penal que ya existe. Pero es necesario dejar constancia que nos estamos refiriendo al derecho que tiene el autor a conservar para sí su creación, esto es, la inspiración que, objetivada, creó el programa, o su contenido, o la máquina, etc. Pero si se tratara de infracciones cometidas sobre la cosa -computer, software, etc.- como hurto o robo, tal conducta entra dentro de la esfera de los delitos comunes.

Pero lo que interesa dentro del enfoque del tema que estamos tratando, es considerar la posible tipificación de un delito que algunos autores, con un poco de ligereza, han denominado "delito informático", y que, aún más, no pocos han planteado la necesidad de crear un "Derecho Penal Infornático", independiente del Derecho Penal común. Pero tales exageraciones no merecen ser consideradas.

Para nosotros lo que existe es un "delito" que se comete a través de la Informática, es decir, que ésta es el medio o instrumento como se puede llegar y afectar la información, en una u otra forma, para con ella provocar un resultado lesivo a intereses importantes de la sociedad o el individuo, como el derecho a la vida íntima, o la seguridad nacional, o la propiedad, etc. Y es desde este punto de vista que nosotros hemos asumido el tema propuesto por el Seminario Internacional al que concurrimos.

Es un hecho indiscutible que la tecnología de la información se ha universalizado en forma tal que afecta la vida del ser humano, individual o socialmente considerado, a extremos tales que tememos que pueda llegar un momento en que el hombre no se sirva de la máquina sino que se convierta en un sirviente de ella.

El "tecnocrimen" es, pues, la manifestación objetiva de conductas delictivas que utilizan la Informática para consumar delitos y otras conductas irregulares que, no estando tipificadas como delitos, provocan daños de gran peligrosidad en el sistema económico y de seguridad humanos. En efecto, aceptamos que ciertos delitos que actualmente constan en las leyes penales pueden cometerse a través de la Informática, pero hay gran número de conductas a las que difícilmente se las puede

"tipificar" en alguna de las previsiones legales penales que hoy existen, pese a que lesionan importantes bienes jurídicos que merecen la protección del Estado.

II. El fenómeno criminal, como se sabe, se integra por la realidad jurídica (delito); la realidad individual (delincuente); y la realidad social (delincuencia). Las tres realidades antes mencionadas constituyen el soporte del fenómeno criminal, al cual todos los Estados combaten, con más o menos relativo éxito, pero que muchas veces dicho fenómeno rebasa las fuerzas sociales de seguridad.

Dentro del mundo de la Informática, por lo menos hasta el momento, los delitos que se cometen a través de ella, sólo pueden ser inspirados y consumados por un número más o menos reducido de agentes, esto es, por los técnicos que conocen el manejo de los ordenadores, etc. y que, por ende, están en capacidad de actuar con eficiencia y que, como sucede muchas veces, tienen el conocimiento y la inteligencia para no dejar huellas o vestigios de su accionar ilícito o inmoral. Es desde este punto de vista que se puede hablar de la tecnocriminalidad que, hasta el momento, la integran personas que actúan solitariamente; pero que, en no pocas ocasiones, ha sido ya manejada por el crimen organizado, cuyos integrantes consideran de menor riesgo "asaltar" un banco a través de la Informática, que entrando en la entidad financiera al estilo de los asaltantes del viejo Oeste americano. En la misma forma, los terroristas y las organizaciones de espionaje, sea individual, industrial o estatal, consideran de mayor efectividad y de menor riesgo el uso de la técnica informática para consumar sus "delitos", que los antiguos sistemas de persecución individual, o de relación directa entre el terrorista, o el espía, con la persona o cosa sobre la que deben actuar.

Y una de las principales características del tecnocrimen es que el delito puede ser ejecutado a distancia, es decir, pasando incluso las fronteras internacionales, mediante el uso ilícito de la técnica de la información.

Dentro de los límites de esta conferencia no nos es posible entrar al estudio particularizado de todas y cada una de las conductas que podrían constituir delitos cometidos a través de la Informática, pero queremos dedicar el tiempo que se nos ha señalado como límite para esta exposición, tratando de un tema especial que nos inquieta profundamente, cual es el relacionado con la protección al derecho que tiene toda persona

a la vida íntima y a la de su familia, que está reconocido universalmente como uno de los derechos humanos que merece especial protección.

III. Nuestra Constitución Política, en el art. 19, N° 3, expresa que el Estado garantiza "el derecho a la honra, a la buena reputación y a la intimidad personal y familiar". Por su parte, en él Código Penal -Capítulo V del Título II del Libro Segundo- se tipifican ciertas conductas que dicen relación con la publicidad de secretos, de "actuaciones y procedimientos" no destinados a la publicidad, así como exige el secreto profesional.

Es indudable que las anteriores previsiones jurídicas le confieren al habitante del país la seguridad de que se encuentra protegido en su "intimidad", y que ninguna persona -salvo casos especialmente previstos- puede alterar o menoscabar dicha intimidad. Esta seguridad jurídica se complementa con la criminalización de la conducta que lesiona "la inviolabilidad del domicilio" de algún habitante de la Nación, pues se entiende que el "domicilio", es decir, la residencia de la persona, es la sede del "hogar", en donde se supone la "intimidad" encuentra su mayor seguridad.

El derecho a la intimidad fue un enunciado que surgió en el año 1891 con motivo de un procedimiento penal instaurado por Samuel D. Warren y Louis D. Brandes, luego de que el primero de los nombrados fuera objeto en diversos diarios de notas sensacionalistas relacionadas con su vida privada. Con motivo de tal procedimiento, Warren y Brandes escribieron un opúsculo que titularon "The Right to Privacy", en donde decían que "el individuo debía tener una completa protección de su persona y propiedades es un principio tan viejo como el 'common law'; pero se ha visto necesario de tiempo en tiempo, definir la exacta naturaleza y alcance de tal protección, Cambios políticos, sociales y económicos conllevan al reconocimiento de nuevos derechos, y el 'common law', en su eterna juventud, crece para satisfacer las demandas de la sociedad... Gradualmente se ha ido ensanchando el alcance de estos derechos, y ahora el derecho a la vida ha llegado a significar el derecho a disfrutar la vida -el derecho a ser dejado en paz-, el derecho a la libertad asegura el ejercicio de amplios privilegios civiles; y el término 'propiedad' ha llegado a comprender toda forma de posesión, tanto tangible, como intangible".

Como se observa, los autores del folleto mencionado partían del derecho de propiedad para concluir asegurando el derecho a la privacidad, el derecho a estar solo (to be alone). Pero es indudable que los citados autores fueron intuitivos cuando hablaron de los peligros que amenazaban la privacidad, esto es, en frases originales de "the right to privacy": "recientes inventos y métodos de negocios llaman la atención sobre el próximo paso que debe tomarse para la protección de la persona, y para asegurar al individuo lo que el Juez Cooley denominó 'el derecho a ser dejado en paz'. Fotografías, instantáneas y empresas periodísticas han invadido el sagrado recinto de la vida privada y doméstica, y *numerosos aparatos mecánicos* amenazan hacer buena la predicción de que 'lo que es susurrado en lo cerrado se proclamará desde los tejados'.

Pero los mencionados autores no trataban de enervar el derecho a informar que tenían los periodistas, sino que ellos afirmaban que era necesario diferenciar entre las personas que no se prestan a la observación pública y los que, voluntariamente, por diversas razones, se exponen a ella. "Hay personas -dicen- que pueden razonablemente reclamar como un derecho la protección de la notoriedad que conlleva convertirse en víctimas de la empresa periodística. Hay otros que, en diversos grados, han renunciado al derecho a vivir sin vidas apartadas de la observación pública. Materias que hombres de la primera clase pueden pretender con justicia que les conciernen sólo a ellos, pueden en los de la segunda ser objeto de legítimo interés de sus ciudadanos".

Aceptamos que Warren y Brandes pusieron las bases para delimitar la diferencia que existe entre el ciudadano común y el ciudadano que, por su voluntad, se expone a la observación pública, es decir, entre las personas que actúan dentro del círculo o esfera reducidos, y el hombre público. Estos últimos se exponen voluntariamente a la crítica observación de sus conciudadanos, y los comentarios sobre sus actuaciones no siempre, necesariamente, deben ser favorables, sin que la crítica desfavorable pueda significar la demostración del ánimo de injuriar, o de penetrar en la vida privada de su existencia.

Lo dicho nos lleva a reflexionar sobre uno de los temas más difíciles, cual es el de conocer hasta dónde se entiende la "intimidad personal y familiar", como dice nuestra Constitución Política y hasta dónde comienza la libertad del informante para penetrar en dicha intimidad.

En este punto la Informática ha trastrocado los puntos de vista originales que se mantenían con el fin de limitar la privacidad. Antes la intimidad era un derecho que se caracterizaba por ser excluyente, esto es, que no permitía el ingreso de la acción extraña en el ámbito de la esfera personal. Pero con el desarrollo de la Informática, y con la constitución de los "bancos de datos" o "banco de memoria", el criterio ha dado un giro de ciento ochenta grados, pues actualmente se acepta que **ese** derecho a la privacidad es el derecho que se le concede a las personas para que tengan acceso a los bancos de datos, para controlarlos cuando se hace referencia a la propia persona, y aun para solicitar la rectificación de la información que se considera falsa, o "sensible", y demandar la eliminación de la misma. Se trata, pues, de un derecho que, de negativo (no injerencia en la vida privada) ha pasado a ser positivo (autoridad para intervenir en los bancos de memoria); de oposición a la información sobre la vida privada, íntima, al derecho a controlar la información recogida e ingresada en los bancos de memoria, así como el derecho a que dicha información no sea difundida.

¿Cómo es que se llegó a ese cambio? ¿Qué fue lo que motivó ese nuevo enfoque jurídico sobre la privacidad? La respuesta es de lo más simple e impresionante: Se debió a la Informática. Sólo ella -desarrollada a extremos tales que con ella se registran los datos personales, unas veces con fines sociales, otras con fines utilitarios- pudo haber puesto en peligro el consagrado derecho a la intimidad al "memorizar" todas las referencias de la persona, hasta en sus manifestaciones más recónditas, con el grave peligro de su difusión masiva, de su transferencia para fines que no fueron los que motivaron la captación de los datos individuales.

Antes de continuar con el desarrollo de la presente exposición, es necesario hacer ciertas precisiones, dejando constancia de algunos principios que deben imperar en el tratamiento de la defensa al derecho a la intimidad; así como establecer lo que debe entenderse por el llamado "delito informático".

IV. El desarrollo de la Informática trajo como consecuencia que se pudiera "almacenar" información de manera voluminosa, mediante las computadoras, lo que pone en peligro una serie de derechos debido a la posibilidad de transferir esa información en cualquier momento a terceros.

La recolección de los datos en una computadora estructura el "banco de datos" o "banco de memoria", como también se llama, en donde se acumula un gran volumen de información en un mínimo espacio. El registro, pues, contenido en un banco de datos es la información que se le ha suministrado a la memoria de la computadora, la cual la mantiene por tiempo indefinido, pudiendo tener acceso a ella, no sólo una persona, sino algunas autorizadas, y otras no autorizadas, así como la información puede ser transferida a un número indefinido de otras computadoras.

No se puede dejar de reconocer que el Estado tiene derecho a conocer los datos relacionados con sus habitantes en tanto en cuanto los mismos sirvan rara fines sociales, pues estos datos pertenecen a la sociedad, en tanto el individuo vive en ella y se vale de ella para desarrollar su vida y para tener la máxima protección. Pero los datos personales deben ser diferenciados tomando en consideración los aspectos antes mencionados; y de ello surge la diferencia entre datos "públicos", que pertenecen a la sociedad y de los cuales se puede servir el Estado; y datos privados, esto es, aquellos a los que el pensamiento suizo que elaboró el proyecto destinado a la protección de los bancos de datos, denominó "datos sensibles". Entre los públicos se encuentran los datos referidos al nombre, residencia, número de identidad personal, profesión, estado civil, lugar de trabajo, etc. Entre los segundos, o privados, tenemos la religión, la opinión política, el estado de salud, su posición económica, etc.

De lo dicho se llega, pues, a la conclusión de que las personas, cuyos datos individuales, sin discriminación entre públicos y privados, están dentro de un banco de datos, se encuentran indefensas en cuanto al resguardo de su intimidad y la de su familia, pues el manipuleo de la información puede provocar graves lesiones a los intereses, no sólo del individuo, sino también de toda su familia. Los autores argentinos Carlos Correa, Hilda N. Batto, Susana Czar de Zalduendo y Félix A. Nazar, en su obra conjunta "Derecho Informático", nos recuerdan lo sucedido en su país durante la trágica dictadura militar última que sufrió dicha Nación. Ellos nos dicen: "En épocas recientes de nuestro país, la acumulación de datos personales en un Estado autocrático, privó a los individuos de toda posibilidad de verificar los datos que sobre ellos se poseían. La manipulación de datos sobre convicciones políticas y religiosas, el recurso a informaciones obsoletas (pertenencia en épocas pretéritas a un centro estudiantil o partido político, etc.), fueron con frecuencia la base de acciones represivas y aberrantes violaciones de los derechos humanos".

De lo dicho surge la necesidad que tiene el ciudadano de hoy de controlar la información que, sobre su persona, contienen los diversos bancos de datos, a fin de proteger su intimidad y la de su familia. Y de esta conclusión se hace presente la necesidad de que existan la suficiente legislación que permita el control de los bancos de datos y el derecho a que se supriman los considerados privados, y se rectifiquen los públicos que se consideren obsoletos o equivocados.

Y lo dicho nos obliga a examinar los principios que deben informar toda acción legislativa que tienda a proteger el derecho a la intimidad.

1. Ante todo es necesario que exista el mandato jurídico que establezca cuáles son los datos públicos.), cuáles los privados, a fin de que se permita la formación del banco de datos con los primeros y se sancione la inclusión de los segundos sin consentimiento del interesado. A este principio lo podríamos llamar "principio de respeto a la información sensible").

2. El particular debe tener derecho a saber la naturaleza de la información que se recopila sobre su persona y para ello la Ley le debe conceder la facultad de inspección sobre el banco de datos personales. Este principio se podría denominar "principio de control".

3. Sólo las personas naturales o jurídicas que la Ley autorice están en capacidad de formar banco de datos personales y, por ende, sólo a ellas el ciudadano debe entregar dichos datos, siempre que no sean los sensibles. Este es el principio de "limitación a la información personal".

4. Como consecuencia del principio de control, el ciudadano debe tener el derecho a que se rectifiquen todos aquellos datos que fueren errados y se excluyan los mismos y todos aquellos que hayan perdido actualidad. Es el principio a la verdad actualizada.

5. El Estado debe garantizar que la información contenida en los bancos de datos autorizados sólo pueda ser utilizada para los fines para los cuales fue recopilada, sin que pueda ser transferida a cualquier otro banco de datos sin consentimiento expreso del interesado. Es el principio de seguridad personal.

6. Toda persona natural o jurídica, autorizada o no, que hubiere hecho uso de la información contenida en un banco de datos personal, de manera arbitraria, esto es, para fines distintos para los cuales fuera

autorizada, o hubiera transferido maliciosa o culposamente la referida información deberá pagar al afectado una indemnización civil, sin perjuicio de las sanciones civiles o penales que se hubieren previsto en el respectivo estatuto jurídico a elaborarse. Este es el principio de indemnización civil.

Con los anteriores principios de carácter general se debe elaborar tanto el régimen jurídico civil, como el penal, a fin de que el ciudadano tenga la máxima protección a su vida íntima en esta etapa de la civilización dominada por la informática. Dada la naturaleza de la presente exposición nos limitaremos a examinar la posibilidad de la criminalización de ciertas conductas en cuya ley respectiva se prevea la sanción para quienes ofendan la intimidad individual o familiar.

Lo expuesto nos lleva al examen de lo que se ha dado en llamar "delito informático", o "delito técnico", o "delito automatizado", etc., etc. Como se puede apreciar no existe acuerdo respecto a la denominación del acto que pueda ser previsto como delito cuando se tiene de por medio la técnica de la información.

V. Como se sabe, cuando de la criminalización de una conducta se trata, el legislador procura reunir diversas conductas delictivas bajo un denominador común contenido en un Título al cual lo identifica con el bien jurídico que se pretende proteger. Y uno de los puntos controvertidos en la doctrina es fijar cuál debe ser el bien jurídico que se protege cuando de los hechos lesivos a vitales intereses de la sociedad o el individuo, se trata en relación con la Informática. Para unos el bien jurídico a protegerse es el patrimonio, poniendo énfasis en que la mayor parte de las conductas arbitrarias surgidas a través de la técnica informática, han tenido como finalidad perjudicar económicamente a las empresas o personas. Otros autores han considerado innecesario buscar un bien jurídico especial para describir los tipos penales relacionados con la Informática, pues, según ellos, basta ubicar los indicados tipos en los respectivos títulos comprendidos en el Código Penal, según el resultado de la conducta respectiva. Así, si se trata de la información concentrada en un banco de datos personales, al cual se accede arbitrariamente para alterar la información, o para obtenerla maliciosamente, dicha conducta debería estar comprendida dentro del Título que tipifica los delitos contra las libertades constitucionales, entre las que se comprende la de la intimidad individual y familiar.

Nosotros pensamos que cuando se trata de buscar el bien jurídico que corresponda a la técnica de la información, se está tratando de seguir los caminos ya recorridos sin tomar en consideración un hecho innegable, esto es, que se trata de un fenómeno nuevo, un fenómeno que no existía en el momento en que se redactaron los Códigos Penales vigentes, es decir, la Informática, o técnica de la información. Por otro lado, no se puede soslayar otro hecho innegable: que la maniobra cometida a través de los ordenadores afecta o hace uso de la información contenida en la parte lógica del mismo. Es la "información" la lesionada, .y es a través de esa "información" arbitrariamente obtenida o manejada que se lesionan ciertos intereses penalmente protegidos. No se puede hurtar o robar a través de la Informática: basta leer la descripción típica para concluir que es imposible que se pueda identificar el concepto de cosa -objeto tangible, corpóreo, según nuestro Código Civil- con el de información (incorpóreo, intangible). De allí la necesidad de describir conductas típicas que puedan aprehender la serie de hechos que se presentan en el manejo de las computadoras.

Se debe, pues, tener presente que el objeto de la conducta arbitraria que entra al ordenador ajeno de manera arbitraria, es la información, pero no la cosa tangible, no el bien material en sí, al cual se puede llegar haciendo uso de la información arbitrariamente obtenida. Por lo dicho es que no se puede comprender la conducta irregular ejecutada a través de la Informática, en los tipos penales tradicionales, sin que por lo menos se reformen ampliando dichos tipos, o se configuren otros que puedan aprehender sin tortura alguna las preindicadas conductas. Se exige, pues, el tipo penal que contenga los elementos relacionados con la técnica informática; de lo contrario, por falta de tipicidad, sería imposible proteger penalmente ciertos derechos garantizados por el Estado como fundamentales para el individuo o para la sociedad.

Afinando lo dicho a la protección del derecho a la intimidad, nos parece que cualquier legislación penal que pretenda criminalizar las conductas irregulares cometidas a través de la Informática, debe inspirarse necesariamente en los aspectos siguientes:

1. Ante todo se debe destacar que lo que se pretende proteger es la "información" en general, cualquier clase de información que **se encuentre automatizada, o tenga como sede los bancos de datos.**

2. Partiendo del antes enunciado general, **se debe concretar** metódicamente cuáles son los objetos jurídicos que se pretenden proteger. Si la "información" está referida a las personas en particular, es indudable que se debe proteger la "intimidad", en el sentido que anteriormente lo explicamos. Pero si la "información" contiene manifestaciones económicas, entonces se acepta que la protección está dirigida a la defensa del patrimonio en general; y si la "información" tiene como contenido elementos que inciden en la seguridad nacional, entonces la protección está dirigida a la seguridad del Estado, sea interna, sea externa.

3. Se debe recordar que, en cuanto al objeto material de las infracciones cometidas a través de la Informática, dicho objeto está constituido por elementos intangibles, como es la información, lo que hace muy difícil que la conducta lesiva pueda adecuarse a cualquiera de los tipos que contienen las actuales leyes penales, redactadas antes que el fenómeno informático aprehendiera la mayor parte de las actividades sociales e individuales.

4. Se hace presente que la protección a la información debe extenderse no sólo al producto ya elaborado sino en todas y cada una de las etapas de su conformación, pues, de lo contrario, quedarían sin protección una o más fases de desarrollo o tratamiento, lo que podría ser de graves consecuencias sociales o individuales.

5. Finalmente, al tipificar la conducta que afecte al derecho a la intimidad se debe tener presente la noción que, sobre la misma, nos entrega A.F. Westin, quien expresa que el derecho a la intimidad es "el derecho que tienen los individuos, los grupos, o las instituciones, de determinar por su cuenta, cómo y en qué medida las informaciones que les atañen pueden ser comunicadas a otras personas".

VI. Estamos de acuerdo con Frosini en que la protección de los datos personales que se hayan automatizado electrónicamente debe comprender cuatro fases principales, a saber: "a) la recopilación de datos; b) su procesamiento (comparación, agregación, análisis finalizado); c) el resultado obtenido y puesto a disposición, y d) su transmisión en redes informáticas y su difusión".

La recopilación de datos debe estar limitada, en tanto en cuanto se refieran a los datos públicos, como el derecho a no obtener los datos

privados. Los datos deben ser verdaderos, completos, obtenidos mediante medios lícitos y para fines concretos.

El procesamiento debe garantizar el respeto al secreto de los datos obtenidos, concediendo la respectiva seguridad de que no serán difundidos, ni alterados, ni suprimidos por personas que no hubieren sido autorizadas para su respectivo procesamiento.

En lo que se refiere al resultado del procesamiento, dice Frosini que "ha de ponerse de relieve que es en esta fase en la que la libertad informática toma consistencia como derecho de control sobre los propios datos personales (libertad de informarse)".

Por último, la parte más importante y que merece especial atención por parte de los legisladores, es el momento en que se ponen "los datos en circulación interna, o sea al interior de un circuito de transmisión (como los datos que se transmiten de una oficina pública a otra) o externa, o sea divulgados de cualquier forma y, por tanto, disponibles para ser utilizados con fines distintos de los previstos desde un principio" (Frosini).

De todo lo expuesto se infiere que la tarea de criminalizar las conductas relacionadas con la Informática no es muy simple y que urge la previsión penal para garantizar fundamentales derechos humanos, como el de la intimidad, hoy seriamente amenazados por la Informática abusivamente utilizada.

La protección de los datos y del banco de datos ha tenido su evolución de acuerdo con el avance acelerado de la técnica relacionada con la información y el nuevo concepto sobre el derecho a la intimidad, tal como lo dejamos expuesto anteriormente. En un comienzo se planteó una oposición entre la computadora y la vida íntima, sin espacio intermedio alguno, lo cual, como es de suponerse, trajo como consecuencia un menoscabo y un enfrentamiento entre el derecho a la vida privada y el derecho a informar que reclamaban, especialmente, los dueños de los medios de comunicación social. Frente a este problema se llegó a un acuerdo, más o menos correcto, por el cual se pretendió conciliar los intereses particulares con los sociales.

Con el nuevo criterio sobre lo que debe entenderse el problema inherente al derecho a la vida íntima (no es el derecho a estar solo, sino

el derecho a vigilar la información contenida en los bancos de datos), es necesario que con ese mismo criterio se elaboren las legislaciones que aspiren a proteger el derecho a la vida privada.

En este punto cabe señalar que se han planteado diversas alternativas que dicen relación con la orientación legislativa a seguir. Para ciertos legisladores lo conveniente es dictar normas generales a las cuales se asocien sanciones civiles, administrativas y penales, sin necesidad de constituir un órgano especial para el control de los bancos de datos, pues cualquier desviación sería conocida y juzgada por los órganos jurisdiccionales comunes. Para otros, lo conveniente es dictar las normas generales, pero el control debería estar a cargo de un organismo especial, independiente tanto de la Función Ejecutiva, como de la Judicial; organismo que tendría como titular a un "ombudsman", como en el caso de la vigilancia de los Derechos Humanos.

Pensamos que es necesario diferenciar los campos de acción legislativa, pues, por un lado, se debe asumir la protección de la toma de datos, del procesamiento, registro, transferencia y cualquier otro nivel semejante; y, por otro, se deben prever las conductas injustas que se pueden cometer a través de cada una de esas etapas, conductas que deben estar enlazadas con una pena, en relación con la intensidad de la lesión causada. Dentro de este sistema también se debería considerar la conducta del que hace uso ilegítimo de la información personal contenida en un banco de datos.

Como se observa, es necesario considerar no sólo el aspecto relacionado con los pasos previos al registro de los datos, y sus efectos ulteriores, sino que también se debe legislar en forma precisa sobre el momento, la forma y el lugar como el particular pueda ejercer su derecho al control de la información registrada, esto es, lo que se llama el "derecho de acceso".

Algunos autores piensan que debe existir un órgano de control específico, como lo explican los autores Correa y otros, en su obra conjunta "Derecho Informático", quienes manifiestan: "El derecho de acceso concedido al individuo no sería una garantía suficiente sin la existencia de una estrategia integral que permita controlar la legalidad de la actuación de las entidades públicas y privadas. De allí es que la opinión mayoritaria de la doctrina considerada es que debe existir un órgano de control específico". Estos órganos podrían ser unipersonales, como en

Alemania, o pluripersonales, como en Francia, en donde el control se ejerce bajo la directiva de un organismo que se integra por delegados de las tres funciones: legislativa, ejecutiva y judicial.

Finalmente, es necesario destacar que cualquiera que sea la técnica legislativa que se adopte con fines de protección al derecho que tiene todo hombre para conservar su privacidad y la de su familia, se debe pensar que ese derecho debe conjugarse con el derecho que tiene la sociedad a estar informada, pero sólo en tanto esa información no sea extraída vulnerando la personalidad moral de las personas, para transmitirla, con fines lucrativos o sin ellos. La información, como cierto autor afirmara, puede ser una mercancía en un momento dado, pero la integridad moral de las personas no puede ser contenido de la mercancía, cualquiera que sea el fin a que se la destine.

BIBLIOGRAFIA

ANTOLA, A. y otros. *Diccionario de Informática.*

ANGARITA BARON, Ciro Angarita. *Hacia la Regulación de los Bancos de Datos Personales: Una experiencia colombiana.*

CORREA, Carlos M. y otros. *Derecho Informático.*

FALCONI PEREZ, Miguel A. *Protección Jurídica a los Programas de Computación.*

FROSINI, Vittorio. *Informática y Derecho.*

FROSINI, Vittorio. *La Protección de la Intimidad: De la Libertad Informática al Bien Jurídico Informático.*

ETTORE, Giannantonio. *Transferencias Electrónicas de Fondos* y *Autonomía Privada.*

GUTIERREZ FRANCES, María Luz. *Fraude Informático y Estafa.*

HERRERO-TEJEDOR, Fernando. *Honor, Intimidad y Propia Imagen.*

GIRALDO ANGEL, Jaime. *Informática Jurídica Documental.*

JIJENA LEIVA, Renato Javier. *Chile, la Protección Penal de la Intimidad y el Delito Informático.*

LEDESMA, Julio C. *Derecho Penal Intelectual.*

LOPEZ-MUÑIZ GOÑI, Miguel. *Informática Jurídica Documental.*