

CAPÍTULO CUARTO
DERECHO DE LA INFORMÁTICA

1. Aclaración conceptual	69
2. La protección jurídica de la información personal	74
3. La protección jurídica del <i>software</i>	88
4. El flujo de datos transfrontera	98
5. Los convenios o contratos informáticos	106
6. Los delitos informáticos	114
7. El valor probatorio del documento electromagnético	130

CAPÍTULO CUARTO DERECHO DE LA INFORMÁTICA

1. ACLARACIÓN CONCEPTUAL

Como ha señalado Vittorio Frosini, el binomio informática y derecho indica con claridad la interacción entre dos ciencias, de la cual surge un campo fecundo del saber; por una parte, la computadora se considera un instrumento utilizado por el jurista para crear bancos de datos jurídicos y para facilitar la administración de justicia, y por otra, recurrir a la computadora plantea una serie de problemas que deben ser regulados por la ley.¹¹⁸

Ante esto, en la práctica ha surgido una gran confusión en determinar si la materia debe denominarse derecho informático, si de la relación antes señalada nos encontramos ante dos disciplinas con objetos de estudio diverso como pueden ser la informática jurídica y el derecho de la informática, o bien, si, como se ha configurado desde el 30 de abril de 1980 en que el Consejo de Europa recomendó que la nomenclatura utilizada fuera “derecho e informática” en la que se incluyeran las dos disciplinas mencionadas, estamos utilizando una verdadera acepción para identificar la materia de estudio.

Hoy día nos encontramos con que se conceptualiza bajo un mismo elemento integrador el derecho informático y el derecho de la informática, lo cual es un error; por lo que, para definir posiciones, la nuestra es determinar que un elemento de estudio

118 Frosini, Vittorio, *Informática y derecho*, Colombia, Temis, 1988, p. 135.

es la informática jurídica, otro, el derecho de la informática, y que ambos se catalogan bajo la relación "derecho e informática".

Lo referente al campo de la informática jurídica ha sido analizado en los anteriores capítulos, por lo que, a partir del presente, nos corresponde delimitar los elementos integradores de esta nueva disciplina conocida como derecho de la informática.

Lo primero que diremos al respecto es que, por la propia integración terminológica, estamos en presencia de información automatizada, por lo que, al conjugarla con el derecho, lo primero que tenemos que determinar es precisamente algo jurídico, normativo y regulador de los efectos en el uso (activo o pasivo) de una computadora.

Pero, antes de iniciar, es conveniente determinar si puede ser objeto de estudio metodológico como rama autónoma en el campo jurídico.

Bajo esta vertiente, señalaremos los puntos negativos y positivos de tal presunta existencia.

Elementos negativos o que pueden determinar que no exista el derecho de la informática.

a) El derecho de la informática no puede entenderse como un cuerpo normativo con naturaleza propia e independiente, por lo que no se le da validez a la existencia a esta disciplina como autónoma o científica, sobre todo porque sus derivaciones pueden darse en el campo del derecho público, del derecho privado y hasta del derecho social y, por tal, supuestamente no goza de autonomía propia; es decir, no se circunscribe propiamente al derecho público, privado o en el social, como sí se da en otras disciplinas.

b) Todo cuerpo normativo desde su perspectiva de disciplina debe respaldarse de normas sustantivas como por normas adjetivas, o bien, reglas propias reguladoras del ser, hacer, o no hacer, como de reglas propias para la solución de sus controversias. Si, como vamos a ver más adelante, en nuestro país es casi inexistente la localización de normas sustantivas que regulen la materia, también nos encontramos con un vacío formal de normas adjetivas.

vas. De ahí que sea prudente resaltar que el encuentro que sufran, por un lado, el avance de la tecnología y, por el otro, el derecho deberán ser resueltas por el aparato jurídico propiamente hablando y no por las reglas informáticas de tal relación; esto es, el derecho no debe supeditarse a la informática; por tal motivo, el derecho de la informática como tal no existe.

c) La norma jurídica tiene origen en el desarrollo y convivencia de individuos en una sociedad tales individuos o gobernados plantean una serie de hechos que el derecho regula, por lo que el avance normativo depende propiamente del individuo y no del avance tecnológico. De esta interpretación se afirma que, en una relación que puede derivar en lo jurídico, el hecho va primero que el derecho; así, la sociedad no puede estar supeditada al derecho, sino el derecho a la sociedad, y ante esto, el derecho de la informática no puede existir como tal, ni pueden dársele valores autónomos.

Estas tres corrientes también pueden señalarse desde un punto positivo en los siguientes términos:

a) Determinar que, por el hecho de pertenecer o no estrictamente a un objeto de estudio del derecho, no por eso pierde su propia naturaleza de observación como fenómeno de estudio. Si su existencia deriva de tres naturalezas distintas, finalmente emana del propio derecho. Tan no es errada esta posición que existen negocios jurídicos que no solamente se circunscriben en una clasificación de derecho público, sino también en una integración de normas de derecho privado, y no por eso la disciplina pierde carácter científico.

b) No todo objeto jurídico de estudio guarda normas sustantivas y adjetivas; pero, suponiendo que éste fuera el caso, nuestro propio sistema jurídico resuelve el problema determinando bajo uno de sus principios generales de derecho que, a pesar de la inexistencia de normas jurídicas que contemplen el supuesto planteado, el juzgador tiene la obligación de emitir una resolución; esto es, los propios valores jurídicos y normativos tienen existencia procesalmente hablando, a pesar de no haber norma adjetiva

expresa, lo que quiere decir que una norma adjetiva no está supeditada a la norma sustantiva.

c) La afirmación de que el hecho va primero que el derecho no es válida en nuestro sistema jurídico, según lo consideramos nosotros. Es cierto que las normas jurídicas están supeditadas a la convivencia social o de los gobernados, pero la regla a esta afirmación admite excepciones planteadas por el propio derecho, por lo que ambos objetos interactúan, ya sea que la sociedad se supedite al derecho o el derecho a la sociedad, ya que lo único que limita al derecho es el propio derecho.¹¹⁹ Por tales argumentos, el derecho de la informática puede abarcar un campo de estudio, por lo que la clasificación tradicional en público, social y privado no restringe científicamente esta disciplina, ya que guarda su objeto de estudio particularizado y consecuentemente su propia metodología.

A unado a lo anterior, es conveniente retomar lo que ha señalado Enrique M. Falcón¹²⁰ al hablar de la autonomía de una rama del derecho; en este caso, del derecho de la informática.

La autonomía no implica que se separe o desentienda de la ciencia a la cual pertenece y de la cual depende, sino que aborde los problemas con método e instrucciones propios. En el concepto tradicional, la autonomía de una rama jurídica se asienta en cuatro pilares:

- En el campo normativo (legislación específica);
- En el campo docente (estudio particularizado de la materia);
- En el campo científico (investigadores y doctrinarios que aborden los problemas específicos de la materia); y
- En el campo institucional (por tener instituciones propias que no se encuentren en otras áreas del derecho).

Ante estos cuestionamientos o afirmaciones, ya han aparecido libros que contienen la normativa y comentarios respecto a esta nueva disciplina del derecho, y ante tales, se confirma día con día

¹¹⁹ Recordemos lo que afirmamos en el capítulo tercero al hablar de la modelística jurídica de Losano.

¹²⁰ Citado por Carrascosa López, Valentín, "El derecho informático como asignatura para juristas e informáticos", *Revista de Informática y Derecho*, Universidad Nacional de Educación a Distancia, Centro Regional Mérida, s. f. e., p. 6.

que ésta emerge con la suficiente autonomía y contenidos aptos para ser estudiados por abogados y estudiosos del derecho, y esto es lo que trataremos de dilucidar en los siguientes apartados del presente capítulo.

El derecho de la informática ha sido considerado por Carras-cosa L ópez como “el conjunto de normas que regulan las acciones, procesos, productos y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones” .¹²¹

Sin definir conceptos, otros¹²² han señalado que la informática como objeto de regulación jurídica ha dado origen al llamado derecho de la informática.

Por otro lado, Julio T éllez ha afirmado que “es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática” .¹²³

Para Emilio Suñé,¹²⁴ “es el conjunto de normas reguladoras del objeto informática o de problemas directamente relacionados con la misma” .

Definiciones se pueden señalar muchas. Desde nuestra perspectiva, podemos conceptualizar el derecho de la informática como el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática o los problemas que se deriven de la misma en las que exista algún bien que es o deba ser tutelado jurídicamente por las propias normas.

En realidad, es cuestionable todavía hoy día si en verdad existe esta disciplina como tal, por lo que una gran mayoría de estudiosos de la materia han preferido analizar algunos campos en los que, aplicando la informática, se podrían relacionar los resultados con el campo del derecho, y así han preferido mejor estudiar los puntos siguientes, los cuales nos servirán de base para la conformación de nuestro estudio:

a) La protección jurídica de la información personal;

¹²¹ *Ibidem*, p. 5.

¹²² Fix Fierro, Héctor, *Informática y documentación jurídica*, p. 53.

¹²³ T éllez, Julio, *Derecho informático*, p. 58.

¹²⁴ Suñé, Emilio, “Introducción a la informática jurídica y al derecho de la informática”, p. 77.

- b) La protección jurídica del *software*;
- c) El flujo de datos transfrontera;
- d) Los convenios o contratos informáticos;
- e) Los delitos informáticos;
- f) El valor probatorio de los documentos electromagnéticos.

Un punto es importante mencionar antes de iniciar con el análisis de cada una de las materias de estudio antes señaladas, y es precisamente en la determinación que en cada una de éstas se da entre la información como concepto relación, como la información como concepto jurídico.

Una solución ya anunciada desde este momento sería implantar una reforma a fondo y congruente del artículo 6o. constitucional, ya que, como se ha precisado, siempre vamos a estar en presencia de la información automatizada pendiente de regular por las normas jurídicas.

2. LA PROTECCIÓN JURÍDICA DE LA INFORMACIÓN PERSONAL

Hoy día, es mucho más frecuente encontrarnos ante la posibilidad de que algunos de nuestros datos más particulares o personales tengan que ser “almacenados” o respaldados en fuentes o bienes informáticos; es decir, en soportes automáticos de información.

Existe el mandato constitucional de que todo ciudadano mexicano debe registrar cierto tipo de información ante el órgano electoral encargado de elaborar las credenciales de identificación oficial ciudadana electoral, mejor conocidas como credenciales electorales; por otro lado, en la actividad diaria y ante la posibilidad de efectuar cierto tipo de contratos privados como el de apertura de cuentas bancarias, entre otros, es necesario también aportar ante órganos privados cierta información personal para determinar qué tipo de régimen de cuentas bancarias es conveniente contratar.

Es decir, ante el avance tecnológico y las posibles masificaciones en el manejo de información, tanto entes públicos como privados han visto la necesidad de modificar sus medios de

archivar tal información para lo cual han recurrido a las computadoras.

Pero este fenómeno que, a simple vista, puede resultar cotidiano es necesario vislumbrarlo o cuestionarlo como una posible o presumible inmiscusión en la esfera privada o íntima de las personas y, ante esto, es necesario también establecer si las normas jurídicas deben determinar estos alcances.

En efecto, ante las condiciones actuales de desarrollo tecnológico, las posibilidades de captar, relacionar, transmitir y almacenar información personal son prácticamente ilimitadas. Por eso, es urgente establecer los mecanismos jurídicos que nos permitan impedir la informatización de los aspectos de nuestra vida cuyo conocimiento deseemos reservar, o bien, es necesario articular la forma de comprobar qué datos o informaciones existen sobre nosotros mismos en registros públicos o privados y determinar los cauces legales para corregir la inexacta información, completar la insuficiente o cancelar la que no debe figurar en ellos. A simismo, es preciso saber a quiénes se puede transmitir esa información personal.

Sin embargo, ante estas expectativas, ¿cómo podemos conceptualizar estas esferas jurídicas de protección personal íntima o privada?

El derecho a la intimidad se construye a partir de la noción de intimidad, *privacy*, *riservatezza* o *vie privée* y se encamina, fundamentalmente, a dotar a las personas de cobertura jurídica frente al peligro que supone la informatización de sus datos personales. Es pues, como lo señala Pablo Lucas Murillo, una respuesta ligada a exigencias concretas propias de la forma en que se desenvuelve la convivencia en nuestros días.¹²⁵

Este derecho no se reduce a tutelar las que podríamos considerar informaciones sensibles ni a las relativas a los aspectos más recónditos de la vida de un individuo; al contrario, este derecho se extiende a datos de apariencia, en principio inocua y que, en

¹²⁵ Lucas Murillo, Pablo, *El derecho a la autodeterminación informativa*, Madrid, Tecnos, 1990, p. 25.

modo alguno, se sitúan en esa esfera privada en sentido estricto que cada uno reserva exclusivamente para sí.

En algunos ordenamientos se ha interpretado el concepto de intimidad de una forma amplia, centrada especialmente en la voluntad de cada individuo afectado. De esta manera, el derecho a la intimidad vedaría, en principio, toda intromisión en aquellas esferas de la vida que el titular se reserva para sí. Esto quiere decir, por lo que respecta a la recogida y utilización de información que se refiere a la persona, que ésta tiene, en virtud del derecho a que nos referimos, la facultad de permitir o no y de controlar el uso que de aquélla se haga.¹²⁶

Si el derecho a la intimidad incluye la facultad de vedar la recogida y utilización de información personal, así como el control sobre esta última, cuando se consienta o se realice por mandato legal, entonces no habrá excesiva dificultad de incluir dentro del contenido de tal derecho la tutela frente al uso de la informática.

La doctrina discute si la intimidad puede ser considerada como un derecho subjetivo. A este respecto, Raúl González Salas¹²⁷ ha considerado la opinión de quienes la niegan y quienes no. Respecto a la primera postura, se señala que el titular de los derechos fundamentales no se puede desvincular de sí mismo, por ejemplo, la vida, la integridad física, la libertad, el honor y la intimidad; de tal manera que tales derechos no son facultades que se deriven de la norma objetiva, sino atributos que integran la propia entidad personal del sujeto. Por el contrario, quienes consideran que los derechos de la personalidad sí son derechos subjetivos señalan que lo son puesto que los derechos fundamentales cumplen una doble dimensión: tanto de derechos objetivos de los ciudadanos, como de elementos esenciales del ordenamiento objetivo de la comunidad nacional.

En algunos estudios doctrinales, se ha cuestionado la similitud en alcances jurídicos de los derechos de la intimidad con aquellos

¹²⁶ *Ibidem*, p. 26.

¹²⁷ González Salas, Raúl, "El bien jurídico: intimidad", *El Foro*, Órgano de la Barra Mexicana, México, Colegio de Abogados, octava época, t. IV, núm. 2, 1991, pp. 67 y ss.

derechos que derivan de la vida privada. Sobre este particular, se ha afirmado que la intimidad es aquel ámbito de la vida de la persona que se sitúa por completo en la interioridad, fuera del alcance de nadie y, por tanto, ajeno a toda exteriorización y relación, mientras que la vida privada es aquélla que se desenvuelve a la vista de pocos, o de otra persona y, en una acepción más amplia, el conjunto de actos que se realizan o piensan para conocimiento de las personas cercanas.¹²⁸

La intimidad se distingue de la vida o esfera privada, entre otras razones, porque pierde la condición de íntimo aquello que uno o pocos conocen, por tanto, se destruye cuando se divulga. Constituye una instancia absoluta, a diferencia de lo público y lo privado, que se limitan dialécticamente entre sí. Por esta causa, la intimidad constituye un ámbito que no puede ser objeto de difusión mediante mensajes informativos, toda vez que difusión equivale siempre, en este caso, a destrucción. Sin embargo, la vida privada o, mejor dicho, determinados aspectos suyos pueden revestir de un considerable grado de interés público que aconseje e incluso exija su difusión, ya sea en razón de las personas que los protagonizan, ya sea de las acciones o eventos de que se trate.

A hora bien, y tratando de entrar en materia, podemos señalar, apoyándonos en lo antes dicho, que, si se distingue entre ambos conceptos, podemos percibir lo siguiente: no pertenece a la intimidad lo que se contiene en archivos y registros públicos, puesto que de hecho ya ha trascendido, y consecuentemente puede ser conocido. Sin embargo, el hecho de que la legislación de diversos países establezca límites al acceso de dichos archivos y a la difusión de los datos obtenidos en ellos implica reconocer que no todo el contenido de los archivos públicos es difundible, por más que tampoco sea íntimo. Ello porque gran parte de esa información se refiere a ámbitos que pueden todavía considerarse vida privada de las personas, habida cuenta de que su conocimien-

128 Serna, Pedro, "Derechos fundamentales: el mito de los conflictos. Reflexiones teóricas a partir de un supuesto jurisprudencial sobre intimidad e información", *Suplemento Humana Iura de Derechos Humanos, Persona y Derecho*, Pamplona, 1994, vol. 4, pp. 215 y ss.

to tiene interés sólo bajo cierto aspecto, en determinadas circunstancias y para ciertas personas que a veces pueden ser únicamente funcionarios del Estado.

Ante esto, el mismo Pedro Serna ha señalado que, en un sentido fáctico, prejurídico, se llama público a lo que de hecho ha sido difundido, en consecuencia, muchos datos contenidos en este tipo de archivos son privados, y deben seguir siéndolo en la medida en que la generalidad de las personas carece de interés legítimo para conocerlos y, por tanto, tampoco tiene derecho a ello. Si se tiene en cuenta que el titular primigenio del derecho a la información es el público, mal podrá existir en estos casos un derecho del informador en difundir aquellos datos.¹²⁹

Ahora bien, en el derecho interno de Los Estados Unidos de América, se hace la distinción entre cuatro categorías de posibles violaciones al derecho a la vida privada o íntima:

a) La injerencia en la intimidad del individuo o *in intrusion on plaintiff's privacy*.

b) La divulgación al público de hechos concretos de la vida privada o *public disclosure of private facts*.

c) La presentación de un individuo al público en general bajo una falsa luz, o *putting the plaintiff in a false light in the public eye*.

d) La apropiación de ciertos elementos de la personalidad del individuo con fines de lucro, o *appropriation of some elements of the plaintiff's personality for the defendant's advantage*. Estos elementos pueden ser el nombre, la imagen, la voz, la conducta, etcétera.¹³⁰

Para estos efectos, hemos considerado entonces acercarnos un poco más a los elementos jurídicos de protección al hablar del derecho a la intimidad.

¹²⁹ *Ibidem*, p. 217.

¹³⁰ Gómez-Robledo Verduzco, Alonso, "El derecho a la intimidad y el derecho a la libertad de expresión: derechos humanos fundamentales", *Ars Iuris*, Revista del Instituto de Documentación e Investigación Jurídica de la Facultad de Derecho de la Universidad Panamericana, vol. 14, 1995, p. 81.

Primero debemos señalar que el vocablo inglés *privacy* no ha sido homologado en nuestro diccionario con la voz correspondiente que sería la de “privacidad”. En el sistema anglosajón, se considera que la *privacy* configura una esfera de la libertad, en la cual la persona ostenta unas facultades de exclusión para preservar sus posibilidades de autorrealización en todos los órdenes de la intimidad; asume el significado de garantía dirigido a preservar el ejercicio virtual de las libertades. Dicho concepto se clasifica en diferentes aspectos o formas, según se expresa la intimidad. Se divide en principio en tres órdenes:¹³¹

1. La *privacy* de la esfera íntima. Ésta comprende principalmente los hechos o circunstancias que pertenecen a la esfera de la libertad de la autoderminación de la personalidad. Se denomina el *habeas mentem* o “libertad genérica de la persona”. Ejemplo de estos hechos o circunstancias que pertenecen a esta esfera:

- Los secretos documentales y domésticos;
- La inviolabilidad del domicilio;
- El derecho a la libertad sexual y a la contracepción;
- El derecho a la planificación familiar.

2. La *privacy* de la esfera política. Esta esfera se inserta en la salvaguarda de las garantías y libertades institucionales como son:

- El derecho de asociación;
- La libertad religiosa o de conciencia;
- El derecho a la sindicalización.

3. La *privacy* de la “libertad personal”. Comprende esta esfera, como las dos anteriores, la protección de la libertad genérica de la persona *habeas mentem*, pero en su forma más directa; es decir, en relación al mismo cuerpo de la persona. Se desprenden de ella como objetos de tutela o de protección de la intimidad los relativos a las informaciones sobre:

- Las operaciones o pruebas médicas;
- La sustracción de sangre;
- El derecho a la confidencialidad y sigilo de las relaciones profesionales (abogados y médicos);

131 Cfr. González Salas, Raúl, “El bien jurídico: intimidad”, pp. 70 y ss.

- La presunción de inocencia;
- El derecho al silencio.

A demás de estas facetas que le dan contenido al bien jurídico de la intimidad, constituye también el *habeas data* (de la cual profundizaremos posteriormente), y la garantía que consiste en proteger la intimidad expresada en la informática.

La protección de los datos computarizados en esta sociedad moderna caracterizada por su avanzada tecnología que implica proteger algunos datos que se desea que no sean del dominio público, como por ejemplo:

- Los estados de cuenta bancarios;
- Las salidas del dinero al exterior;
- El monto del pago de los impuestos, etcétera.

La efectiva protección de la intimidad en la sociedad moderna dependerá no solamente de la protección jurídica de la esfera de la libertad personal, sino también de la regulación del manejo y de la circulación de los datos personales informatizados que de los ciudadanos se haga.

Uno de los elementos más importantes que deben ser tomados en cuenta en la elaboración de trabajos como el que hoy se lleva a cabo, sobre todo, al encontrarnos con un importante número de afirmaciones respecto a las diferencias entre intimidad y vida privada, es determinar sobre todo cuál es el bien jurídicamente protegido en estas relaciones.

En España por ejemplo, y siguiendo información jurídica comparada, se ha planteado que la famosa sentencia del Tribunal Constitucional Federal Alemán de 15 de diciembre de 1983 configuró el llamado "derecho a la autodeterminación informativa" (*Informationelle Selbstbestimmungsrecht*) en orden al tratamiento automatizado de datos personales. Para dicho tribunal, e interpretando el contenido de un artículo de norma jurídica reguladora del derecho a la intimidad, la facultad del individuo (respecto a esta materia) deriva de la idea de autodeterminación, de decidir

básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida.¹³²

Pablo Lucas Murillo considera que el derecho a la intimidad normalmente implica el poder jurídico de rechazar intromisiones ilegítimas en la esfera protegida, y correlativamente, determinar libremente y dentro de ella la propia conducta. Es un típico derecho de defensa. A su juicio, sin embargo,

la técnica de la protección de datos es más complicada. De un lado, combina poderes del individuo frente a terceros (limitaciones, prohibiciones) con diversas garantías instrumentales. De otro lado, los datos que se protegen no tienen porqué ser íntimos, basta con que sean personales, aun cuando parezcan inocuos. De aquí que el ámbito de esta protección sea más amplio que el propio derecho a la intimidad.¹³³

Sobre estas premisas, Lucas Murillo afirma que

en orden a proteger los datos personales frente a la informática conviene abandonar la referencia de la intimidad y enunciar un nuevo derecho (el derecho a la autodeterminación informativa), que tendría como objeto preservar la información individual (íntima y no íntima) frente a su utilización incontrolada arrancando, precisamente, donde termina el entendimiento convencional del derecho a la vida privada.¹³⁴

Conforme a Carlos Ruiz, estas diferencias explicarían que ciertos autores adjetiven la intimidad, distinguiendo la intimidad física o clásica (libertad frente a toda intromisión sobre uno mismo, su casa, su familia, comunicaciones o relaciones) de la intimidad informativa (derecho a determinar cómo y en qué medida se puede comunicar a otros información sobre uno mismo).¹³⁵

El avance en el manejo y uso de las denominadas nuevas tecnologías de la comunicación han puesto en entredicho las

¹³² Ruiz Miguel, Carlos, "Protección de los datos personales automatizados", *Revista de Estudios Políticos* (Nueva Época), Madrid, Centro de Estudios Constitucionales, núm. 84, abril-junio de 1994, p. 237.

¹³³ Lucas Murillo, Pablo, *El derecho a la autodeterminación informativa*, pp. 117 y ss.

¹³⁴ *Ibidem*, p. 120.

¹³⁵ Ruiz Miguel, Carlos, "Protección de los datos personales automatizados", pp. 241 y ss.

valoraciones de derechos fundamentales como el de la intimidad o vida privada. Hoy día nos encontramos con una gran pugna de regulación entre aquéllo que puede comunicarse y aquéllo que en cierta forma puede afectar privilegios personales. Ante esto, es preciso que en un primer aspecto se determine por el poder público qué es aquéllo que sí puede decirse de algo o de alguien para no confundir la variedad de interpretaciones que sobre un concepto fundamental podemos aportar una gran generalidad de personas.

A teniendo a estas cuestiones, y sobre todo a aquéllas que derivan del avance tecnológico, los legisladores europeos del oeste fueron los primeros en considerar los efectos sociojurídicos provocados por la informatización en la sociedad. Con base en esto, países como Francia, Suecia, Alemania, Noruega, Austria y Dinamarca elaboraron, en la década de 1970, los primeros instrumentos legislativos que protegieron al individuo frente al mal uso de su información con apoyos informáticos.

A hora bien, conforme al contenido general de las disposiciones normativas sobre el uso y manejo de la información personal, podemos señalar de tales disposiciones, junto con Marcia Muñoz de Alba,¹³⁶ las siguientes características:

a) El derecho a la autodeterminación informativa es la capacidad que goza toda persona a preservar su identidad controlando la revelación y el uso de los datos que le concierne. Se delimita, junto a este derecho, otro de protección frente a la ilimitada capacidad de archivarlos, relacionarlos y transmitirlos por los medios informáticos, también denominado libertad informática.

Destacan en este sentido la consagración constitucional de este derecho como una garantía individual que han hecho las Constituciones española, portuguesa, colombiana y peruana, entre otras, que, en términos generales, determinan:

Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre; el Estado debe respetarlos y hacerlos respetar. De igual modo,

¹³⁶ Muñoz de Alba, Marcia, "La protección de la persona frente a las tecnologías de la comunicación", *Texturas guerrerenses*, Fundación Académica Guerrerense, año 1, núm. 3, enero-febrero de 1996, pp. 8 y ss.

tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Para efectos tributarios o judiciales y para casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.¹³⁷

Por su parte, el dispositivo peruano indica, dentro del capítulo de derechos fundamentales de la persona que se integran entre otros en el artículo 2o., que toda persona tiene derecho a que en los servicios informáticos, computarizados o no, públicos o privados, no se suministren informaciones que afecten la intimidad personal y familiar.

En la práctica, vemos como este derecho o libertad informática ha tomado varias vertientes: así, tenemos que se excluye del manejo libre de información cierto tipo de datos que reconocen ser de contenido más íntimo a la que denominan información sensible; es decir, aquella información de carácter personal, relevante al origen racial, las opiniones públicas, las convicciones religiosas y otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, que no pueden ser tratados automáticamente a menos que el derecho interno prevea las garantías determinadas. En el mismo sentido, se encuentra la información de tipo personal concerniente a las infracciones penales.¹³⁸

Ahora bien, sobre el tipo de información que puede ser insertada en bancos de información, la libertad informativa toma las siguientes vertientes:

¹³⁷ Entre otros, artículo 15 de la Constitución colombiana.

¹³⁸ *Cf.* artículo 6o. de la Convención para la Protección de Personas sobre el Tratamiento de Información de Carácter Personal, firmada en Estrasburgo el 28 de enero de 1981.

a) Derecho de información: en el sentido de tener el individuo la posibilidad de conocer la existencia de algún banco de datos o fichero de información personal;

b) Derecho de acceso a la información personal: como la aptitud que tiene el sujeto de conocer el contenido de aquellos bancos de datos automatizados cuyo objeto es el manejo o almacenamiento de información personal;

c) Derecho de actualización: gracias al cual el individuo puede exigir la corrección de ciertos datos;

d) Derecho de confidencialidad: el cual concede al sujeto la posibilidad de exigir que la información que proporciona permanezca ajena al conocimiento de terceros;

e) Derecho de exclusión: que, por la naturaleza de la información, puede el individuo cancelar o borrar o solicitar la destrucción de información denominada como sensible.

A hora bien, ¿cómo es que ha sido consagrada esta libertad informativa o este derecho a la autodeterminación informativa? Al respecto, las legislaciones han tomado dos vías principalmente:

Protección de la información personal por la vía administrativa

Países como Francia (Comisión Nacional Informática y Libertades); Dinamarca (Agencia de Protección de Datos); España (Agencia de Protección de Datos) tienen destinadas la tutela y vigilancia de sus disposiciones normativas sobre el manejo, uso y difusión de la información personal a entidades administrativas con funciones inspectoras, sancionadoras y de información a los interesados.

Protección de la información personal vía procesal

En Colombia, Brasil y Perú aparece el llamado *habeas data* como una nueva instancia procesal destinada a la defensa del ciudadano frente al abuso de poder informático en los registros o bancos de datos de entidades públicas o privadas.

De esta manera, el *habeas data*, figura procesal destinada a proteger la libertad informática, opera en rigor como una modalidad del amparo, aunque con finalidades específicas.

Para tomar un ejemplo de los fines y objetivos de esta institución procesal, algunos pronunciamientos jurisprudenciales en Colombia, que a manera de reseña aplica, desarrollan o reiteran algunos valores y principios:

a) La prevalencia de la categoría del ser sobre el haber, con todas sus consecuencias;

b) La prevalencia del derecho a la intimidad sobre el derecho a la información como exigencia de la dignidad humana;

c) La persona es la única legitimada para permitir la divulgación de datos concernientes a su vida privada;

d) La dignidad humana es el supremo principio de la Constitución de 1991;

e) Los procesos tecnológicos no pueden comprometer los derechos y libertades humanas;

f) Los bancos de datos adquieren particular relevancia en el moderno derecho constitucional informático por cuanto pueden amenazar o vulnerar derechos fundamentales tales como la intimidad, la personalidad, la honra y el buen nombre;

g) Los datos tienen por su naturaleza misma una vigencia limitada en el tiempo, el cual impone a los responsables o administradores de bancos de datos la obligación ineludible de una permanente actualización a fin de no poner en circulación perfiles de “personas virtuales” que afecten negativamente a sus titulares, vale decir, a las personas reales so pretexto de mantener “registros históricos o de satisfacer el principio de integridad de la información”;

h) El dato económico personal no puede circular sin que previamente se garantice a sus titulares los derechos reconocidos por la Constitución Política. Además, la entidad financiera que los recibe no se convierte por ello en propietaria exclusiva de los mismos y, en consecuencia, debe respetar los intereses jurídicos del titular concernido;

i) La dignidad humana prevalece sobre la probidad comercial;

j) La veracidad no puede deruir sin motivo legítimo la muralla jurídica de la intimidad;

k) En razón de su dignidad humana, el deudor moroso puede esperar que en el manejo de sus antecedentes se le depare cuando menos el mismo tratamiento que recibe el infractor de la ley penal;

l) La protección del crédito no puede lograrse en desmedro de las exigencias de la libertad personal, particularmente en aquellos casos en los

cuales el deudor no tenga antecedentes penales o contravencionales (en los términos del artículo 248 de la Constitución).¹³⁹

Respecto al caso de Perú, la Constitución Política de 1993 incluye como garantía constitucional la acción de *habeas data* en el inciso 3 del artículo 200, en cuanto que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refieren el artículo 2o., incisos 5o., 6o., y 7o. de la Constitución.¹⁴⁰

Conforme al profesor peruano Julio Núñez Ponce,¹⁴¹ la acción de *habeas data*, tal como lo establece la norma constitucional, constituye un cauce procesal al que puede acudir una persona por el hecho u omisión que vulnere o amenace los derechos de intimidad, información, rectificación de información inexacta, honor, buena reputación, voz e imagen de acuerdo a lo que establezca la ley y en concordancia con los incisos del artículo 2o. de la Constitución.

Al señalar la norma constitucional que procede contra el hecho u omisión que vulnere o amenace estos derechos, está permitido que esta garantía constitucional pueda regularse jurídicamente incluyendo tanto el *habeas data* preventivo como el *habeas data* correctivo. En el primero de ellos pueden incluirse procedimientos y facultades como el de conocimiento y acceso a las bases de datos computarizadas y sistemas informáticos que contengan datos personales con el fin de prevenir la amenaza de vulneración de los derechos protegidos.

¹³⁹ Angarita Barón, Ciro, "Colombia: El *habeas data* en la Constitución de 1991", *Informática e Diritto*, Florencia, vol. 20, núm. 1, 1994.

¹⁴⁰ El inciso 5 es relativo al derecho de petición de información del ciudadano a cualquier entidad pública; además, el secreto bancario y la reserva tributaria pueden levantarse con la autorización del juez, fiscal de la nación o de una comisión investigadora del Congreso. El inciso 7 nos habla del derecho que tienen al honor, a la buena reputación, a la intimidad personal y familiar, a la voz e imagen propias, incluso dice: "toda persona afectada por afirmaciones inexactas o agravada en cualquier medio de comunicación social tiene derecho a que éste se rectifiquen en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de la ley".

¹⁴¹ Núñez Ponce, Julio, "La acción de *habeas data*: su aplicación en un contexto jurídico informático", *Aequitas, Revista Jurídica del Poder Judicial del Estado de Sinaloa*, Culiacán, Sinaloa, núm. 22, diciembre de 1994, pp. 23 y ss.

En el *habeas data* correctivo se pueden incluir las facultades de rectificación y modificación de la información que vulnere los derechos protegidos.

Con base en esta disposición constitucional peruana, para el ejercicio y aplicación de la acción de *habeas data*, se publicó la ley 26,301 con fecha 3 de mayo de 1994 y vigente desde el 4 de mayo del mismo año.

En el caso de México, no contamos con una norma jurídica que expresa y de manera directa reconozca los mencionados derechos a la intimidad, o bien, de la vida privada.

Sin embargo, lo que sí resulta importante señalar es que la nueva Ley Federal del Derecho de Autor, publicada en el *Diario Oficial de la Federación* el día 24 de diciembre de 1996, que entró en vigor el 24 de marzo de 1997, establece en sus artículos 107, 108, 109 y 110 algunas disposiciones respecto a los datos o informaciones contenidas en bancos de datos (término que no es definido por tal ley).

De estas disposiciones y para el tema que nos ocupa, resulta importante transcribir el artículo 109:

Artículo 109. El acceso a información de carácter privado relativa a las personas contenida en las bases de datos a que se refiere el artículo anterior [el artículo 108 habla de las bases de datos que no sean originales], así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.

Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

El gran problema que nosotros encontramos en esto es que el manejo propio de la particularidad de los datos o informaciones personales no es equilibrado en cuanto los sujetos ahí establecidos (se habla de excepciones en cuanto las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, lo cual nos lleva a cuestionar los métodos o técnicas de investigación empleados por tales autoridades).

3. LA PROTECCIÓN JURÍDICA DEL *SOFTWARE*

La protección de la propiedad intelectual en el mercado mundial ha tomado creciente significación en los recientes años. Los propietarios de tecnología del mundo desarrollado, particularmente los estadounidenses, han presionado recientemente para obtener un régimen legal de propiedad intelectual fuerte y relativamente uniforme, como piedra de toque para obtener un tratamiento equitativo en el sistema global del comercio que emerge.

Por otro lado, la posibilidad de incorporar a la protección jurídica estos programas de cómputo en el ámbito del derecho, específicamente en el de la propiedad intelectual y particularmente en las normas autorales, viene dictada por consideraciones de oportunidad, dada la dimensión económica de los intereses en juego entre los que cabe destacar: la posible preservación de la industria nacional frente a una fuerte concurrencia extranjera, la protección de un producto cuya elaboración requiere un gran esfuerzo de inversión, investigación y posterior difusión y, sobre todo, la evidente necesidad de una armonización internacional de reglamentaciones.

En la práctica jurídica internacional, la evolución de la materia no es pacífica. Se puede comprobar como, en un principio, los programas de computadoras fueron objeto de protección a través de diversas fórmulas como el secreto industrial, las cláusulas de confidencialidad en los contratos y la competencia desleal, pero pronto se puso de manifiesto su insuficiencia, y los medios profesionales interesados solicitaron una regulación que les asegurara la propiedad y la protección derivada de la misma.

Llegados a este punto, surgen ásperas controversias doctrinales entre los partidarios de una protección a través del derecho de patentes y los que abogan por una protección por la vía de los derechos autorales, aunque esta última corriente es la que consigue prevalecer.

En nuestro país, la Ley de Fomento y Protección de la Propiedad Industrial, publicada en el *Diario Oficial de la Federación* el 27 de junio de 1991, y modificada en su denominación

el 29 de julio de 1994 por la de Ley de Propiedad Industrial, establece que los programas de cómputo no son considerados como invenciones y, por tanto, no son susceptibles de protección por la vía de patentes.

A hora bien, continuando con el esquema de protección comparada, la definición de parámetros internacionales de protección mínima para el *software* ha sido, sin duda, uno de los objetivos importantes de algunos países como los integrantes del GATT. Si bien es cierto, y como ya lo hemos señalado, en la última década numerosos países desarrollados y en desarrollo han adoptado el derecho de autor como forma principal de protección; diversos problemas, como lo señala Carlos M. Correa,¹⁴² no han encontrado una solución plena, particularmente en la perspectiva de la industria de *software* con una vasta acción internacional. Entre estos problemas tenemos:¹⁴³

- No todos los países han resuelto definitivamente la cuestión del régimen legal aplicable al *software*;
- A un en países en donde la aplicación del derecho de autor ha sido admitida en principio, existen dificultades de *enforcement*, debido a la naturaleza de los procesos judiciales o a la escasa significación de las penas. La piratería, más controlada hoy que hace diez años, no ha dejado sin embargo de constituir un fenómeno extendido, incluso en países industrializados.
- Diferencias de aplicación normativa o de “entendimientos” claros en cuanto la determinación de dónde empieza y concluye la protección jurídica de un esfuerzo intelectual en un programa de cómputo.
- Las diferencias de interpretación sobre el alcance de los derechos se han manifestado incluso en el sistema judicial de Los Estados Unidos de América.

142 Correa, Carlos M., “El derecho informático en el proyecto de acuerdo Trip’s de la rieda de Uruguay”, *Derecho, Revista de la Facultad de Derecho*, Lima, Pontificia Universidad Católica del Perú, núm. 47, diciembre de 1993, pp. 290 y ss.

143 *Idem*.

En cuanto a la situación de los países miembros de la Comunidad Europea, de los doce Estados miembros, el Reino Unido, Alemania, Francia y España tienen leyes específicas que dan protección al derecho de autor para programas de computadora.

Los otros ocho países disponen de la protección del derecho de autor con una variedad de medios, inclusive la jurisprudencia, enunciaciones públicas y el silencio estratégico. Esta sección examina los grados variados de protección de propiedad entre los Estados miembros de la Comunidad Europea en vísperas de la armonización.¹⁴⁴

En 1988, el Reino Unido hizo una modificación sustancial a sus leyes sobre derechos de autor y, en efecto, reemplazaron la propiedad reformada sobre el derecho de autor de *software* de computadora del año 1985. Una ley de 1988 incluye los programas de computadora en la definición de “obras literarias”, igual que la legislación reemplazada.

Aunque la ley de derechos de autor de Alemania incluya “programas para procesamiento de datos” en su lista de obras protegidas, la Corte Suprema de ese país ha limitado específicamente la protección completa sólo a esos programas que sean “creaciones intelectuales personales”. Específicamente, sólo un programa de computadora creado mediante la “aplicación de capacidad sobre promedio de programación” es susceptible de protección del derecho de autor.

Francia también ha promulgado legislación que da protección al autor para programas de computadora, pero la jurisprudencia francesa ha rechazado el requerimiento alemán de “aplicación de capacidad sobre promedio de programación” en su creación. Conjuntamente, la jurisprudencia francesa y la legislación respetan la protección del derecho de autor para programas originales que demuestran una “contribución intelectual del programador”.

¹⁴⁴ Connors, Daniel J. y Westphal, Antje, “La directiva de la Comunidad Europea sobre la protección legal de programas de computadora, una comparación entre el derecho europeo y el derecho estadounidense de la propiedad intelectual”, *Comparative Juridical Review*, Coral Gables, Florida, Rainforth Foundation, vol. 29, 1992, pp. 125 y ss.

España también adoptó la legislación sobre la protección del derecho de autor de programas de computadora después de asociarse a la Comunidad Europea.¹⁴⁵

La jurisprudencia holandesa interpreta sus leyes de derecho de autor para proteger “cifra de objeto”. Sin embargo, un programa debe considerarse una “creación” por un perito para considerarse como objeto de protección de la ley holandesa del derecho de autor.

Aunque la jurisprudencia italiana dispone de la protección de *software*, “el racional fundamental para hacerlo no parece claro”. Es interesante observar que el Código italiano de Derecho de Autor completamente omite el *software* en su cobertura.

Grecia y Portugal no han impuesto vigorosamente sus leyes de derecho de autor. Se ha observado que Grecia parece renuente en proteger al *software* bajo sus leyes de derecho de autor, sin embargo, “oficialmente el régimen nuevo se compromete a la reforma de las leyes del derecho de autor”.

Simultáneamente, a pesar de la carencia de decisiones oficiales de los tribunales de Bélgica y Luxemburgo, “no es realista esperar que alguno de los dos vayan lejos de las leyes de Francia, Alemania u Holanda”.

Aunque no hay ningún fallo sobre el punto, las delegaciones irlandesas y danesas en la reunión del año de 1985 de la World Intellectual Property Organization sobre la protección del derecho de autor de *software* confirmaron que las leyes de derecho de autor de las dos naciones protegen programas de computadora.¹⁴⁶

En nuestro país, como ya lo señalábamos, se da la protección de los programas de cómputo a través de las normas autorales y no bajo las leyes en materia de propiedad industrial.

Recientemente ha sido publicada una nueva Ley Federal, Reglamentaria del Artículo 28 Constitucional, que viene a señalar los nuevos cauces normativos en materia autorales.

¹⁴⁵ *Idem.*

¹⁴⁶ *Idem.*

Esta nueva ley viene a complementar e innovar la reglamentación respecto a los programas de cómputo, que, si bien ya eran regulados por la anterior ley autoral de 1956, no se constituían en formación y estructuración como con el actual capítulo IV del título IV de la Ley Federal.

En efecto, esta Ley Federal del Derecho de Autor, publicada en el *Diario Oficial de la Federación* con fecha 24 de diciembre de 1996 cuya entrada en vigor se dio noventa días posteriores a su publicación, establece bajo un capítulo en particular aquellas regulaciones respecto a “los programas de computación y las bases de datos”.

En virtud de lo importante que para nosotros representa lo señalado en esta nueva ley, pasamos a transcribir algunos de los artículos más representativos respecto al tema que nos ocupa:

Artículo 11. El derecho de autor es el reconocimiento que hace el Estado en favor de todo creador de obras literarias y artísticas previstas en el artículo 13 de esta Ley, en virtud del cual otorga su protección para que el autor goce de prerrogativas y privilegios exclusivos de carácter personal y patrimonial. Los primeros integran el llamado derecho moral y los segundos, el patrimonial.

Artículo 12. Autor es la persona física que ha creado una obra literaria y artística.

Artículo 13. Los derechos de autor a que se refiere esta Ley se reconocen respecto de las obras de las siguientes ramas:

I. Literaria;

II. Musical, con o sin letra;

III. Dramática;

IV. Danza;

V. Pictórica o de dibujo;

VI. Escultórica y de carácter plástico;

VII. Caricatura e historieta;

VIII. Arquitectónica;

IX. Cinematográfica y demás obras audiovisuales;

X. Programas de radio y televisión;

XI. Programas de cómputo;

XII. Fotográfica;

XIII. Obras de arte aplicado que incluyen el diseño gráfico o textil, y

XIV. De compilación, integrada por las colecciones de obras, tales como las enciclopedias, las antologías, y de obras u otros elementos como las bases de datos, siempre que dichas colecciones, por su selección o la disposición de su contenido o materias, constituyan una creación intelectual.

Las demás obras que por analogía puedan considerarse obras literarias o artísticas se incluirán en la rama que les sea más afín a su naturaleza.

A r tículo 14. No son objeto de la protección como derecho de autor a que se refiere esta Ley:

I. Las ideas en sí mismas, las fórmulas, soluciones, conceptos, métodos, sistemas, principios, descubrimientos, procesos e invenciones de cualquier tipo;

II. El aprovechamiento industrial o comercial de las ideas contenidas en las obras;

III. Los esquemas, planes o reglas para realizar actos mentales, juegos o negocios;

IV. Las letras, los dígitos o los colores aislados, a menos que su estilización sea tal que las conviertan en dibujos originales,

V. Los nombres y títulos o frases aislados;

VI. Los simples formatos o formularios en blanco para ser llenados con cualquier tipo de información, así como sus instructivos;

VII. Las reproducciones o imitaciones, sin autorización, de escudos, banderas o emblemas de cualquier país, estado, municipio o división política equivalente, ni las denominaciones, siglas, símbolos o emblemas de organizaciones internacionales, gubernamentales, no gubernamentales, o de cualquier otra organización reconocida oficialmente, así como la designación verbal de los mismos;

VIII. Los textos legislativos, reglamentarios, administrativos o judiciales, así como sus traducciones oficiales. En caso de ser publicados, deberán apegarse al texto oficial y no conferirán derecho exclusivo de edición;

Sin embargo, serán objeto de protección las concordancias, interpretaciones, estudios comparativos, anotaciones, comentarios y demás trabajos similares que entrañen, por parte de su autor, la creación de una obra original;

IX. El contenido informativo de las noticias, pero sí su forma de expresión, y

X. La información de uso común tal como los refranes, dichos, leyendas, hechos, calendarios y las escalas métricas.

De los programas de computación y las bases de datos

A r tículo 101. Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

A r tículo 102. Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.

A r tículo 103. Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste.

Como excepción a lo previsto por el artículo 33 de la presente Ley, el plazo de la cesión de derechos en materia de programas de computación no está sujeto a limitación alguna.

A r tículo 104. Como excepción a lo previsto en el artículo 27 fracción IV, el titular de los derechos de autor sobre un programa de computación o sobre una base de datos conservará, aún después de la venta de ejemplares de los mismos, el derecho de autorizar o prohibir el arrendamiento de dichos ejemplares. Este precepto no se aplicará cuando el ejemplar del programa de computación no constituya en sí mismo un objeto esencial de la licencia de uso.

A r tículo 105. El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando:

I. Sea indispensable para la utilización del programa, o

II. Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación.

A r tículo 106. El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir:

I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma;

II. La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;

III. Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler, y

IV. La de compilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.

A r tículo 107. Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos.

A r tículo 108. Las bases de datos que no sean originales quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de 5 años.

A r tículo 109. El acceso a información de carácter privado relativa a las personas contenida en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.

Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

Artículo 110. El titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir:

I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma;

II. Su traducción, adaptación, reordenación y cualquier otra modificación;

III. La distribución del original o copias de la base de datos;

IV. La comunicación al público, y

V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

Artículo 111. Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por esta Ley en los elementos primigenios que contengan.

Artículo 112. Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior.

Artículo 113. Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta Ley.

Artículo 114. La transmisión de obras protegidas por esta Ley mediante cable, ondas radioeléctricas, satélite u otras similares, deberán adecuarse, en lo conducente, a la legislación mexicana y respetar en todo caso y en todo tiempo las disposiciones sobre la materia.

Artículo 231. Constituyen infracciones en materia de comercio las siguientes conductas cuando sean realizadas con fines de lucro directo o indirecto:

[...]

V. Importar, vender, arrendar o realizar cualquier acto que permita tener un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

El camino respecto a una regulación efectiva en materia de protección jurídica de los programas de cómputo ha sido sinuoso y nada fácil. Las compañías productoras de *software* han invertido importantes recursos económicos y humanos para salvaguardar sus derechos, que no han resultado tan eficiente como se esperaba.

Sobre este particular, ya se han planteado una serie de innovaciones jurídicas que se tratan de fundamentar, en materia del *copyright* o derechos de autor, en una nueva filosofía normativa muy *sui generis* respecto a la protección de este tipo de productos (al respecto recordemos que tanto el mercado de producción como de destino final es muy amplio en el mundo).

Una de estas voces en el ambiente del *copyright* mundial es precisamente la que deriva de la Organización Mundial de la Propiedad Intelectual (OMPI) que, retomando propuestas al respecto de la Comunidad Europea, han señalado una nueva normativa del “derecho *sui generis*” de la propiedad intelectual en derechos autorales en materia de programas de cómputo, pero sobre todo, en los problemas de derecho de autor de la distribución electrónica de documentos.¹⁴⁷

Respecto a los aspectos esenciales del derecho *sui generis* para una efectiva protección, la Comunidad Europea y el O M P I señalan que debe circunscribirse en:

- Un nuevo derecho que se aplicará a todas las bases de datos publicadas que envuelvan inversiones de talento y dinero, no solamente a las bases de datos que sean por sí mismas creaciones intelectuales originales.
- El nuevo derecho se aplicará a todas las bases de datos publicadas, esté o no su contenido protegido bajo derecho de autor.
- El nuevo derecho tendrá una adecuada duración (cincuenta años desde la primera publicación, renovables en razón de cambios sustanciales en el contenido: cambios que pueden evidenciarse por una acumulación de cambios no sustanciales, en su caso).
- El nuevo derecho no estará sujeto a excepciones que lo transformen en inaplicable. La publicación de bases de datos

¹⁴⁷ Clark, Charles, “El ambiente del *copyright* para la infraestructura global de información”, *Derecho de la Alta Tecnología*, Buenos Aires, año VIII, núm. 86, octubre de 1995, pp. 3 y ss.

se dirige a proporcionar un fácil y preciso acceso a pequeñas (y a veces no tan pequeñas) porciones de informaciones extraídas de la masa crítica. Excepciones tales como las fundadas en partes insustanciales, usos leales para investigación o uso privado, privilegios de biblioteca, meramente replican la función del editor y evaden las condiciones de uso impuestas al usuario para asegurar su pago por ese uso. El derecho, en consecuencia, impone controlar el acceso de cada ítem individual componente de la base de datos.

- El nuevo derecho se aplicará tanto a los usuarios comerciales como a los no comerciales. Los usuarios de una base de datos son los clientes potenciales: pueden muchas veces ser miembros del público u otros usuarios “sin fines de lucro” que pueden legítimamente ser requeridos (muchas veces vía sistemas de administración de derecho de autor) a pagar precios justos por los valiosos elementos que están actualizando. El derecho en consecuencia necesita cubrir: a) Usuarios finales (miembros del público e instituciones); b) Usuarios comerciales, que utilicen materiales contenidos en bases de datos; c) Usuarios comerciales o no comerciales que busquen reproducir los materiales para el consumo de otros, se propongan o no venderlos.
- El nuevo derecho no deberá estar sujeto a licencias compulsorias o a disposiciones sobre retribución equitativa, salvo (quizá) que la base de datos haya sido publicada por una autoridad pública para mejorar el acceso a la información pública.
- Finalmente, existe un creciente consenso de que los Estados deberían operar este derecho sobre las bases del trato nacional y no de la reciprocidad, no obstante que el trato nacional no constituya un requerimiento de la Convención de Berna (desde que el derecho *sui generis* no constituiría un derecho de autor, sino una forma de derecho vecino).¹⁴⁸

Como se puede observar, la necesidad de términos amplios es no dar lugar a excepciones a los derechos de autor o derechos vecinos (incluyendo el derecho *sui generis*) respecto de actos que constituyen una explotación primaria.

4. EL FLUJO DE DATOS TRANSFRONTERA

En el año de 1994, específicamente en el mes de mayo, entre los días 16 al 20, se celebró en la ciudad de Bariloche, Argentina, el IV Congreso Iberoamericano de Informática y Derecho. Este evento se vio enmarcado por una importante participación de Horacio Godoy quien, entre otras afirmaciones, manejó el concepto de “espacio informático”.

Al respecto, señaló en su ponencia que el espacio informático está constituido por una infraestructura electrónica cuyos componentes son las bases de datos múltiples, las redes de transmisión de datos y los sistemas de información y de consulta. Miles de bases de datos conteniendo información de todos los rincones de la tierra, ligados en red y en red de redes, en continua expansión y en uso permanente. Esta infraestructura tecnológica es el sostén electrónico de la “infraestructura” que alimenta el proceso de toma de decisiones.

Continuó diciendo, entonces, que el espacio informático es en consecuencia el conjunto integrado por las tecnologías electrónicas mencionadas y el conjunto de información que alimenta las actividades, transacciones, comunicaciones, negocios, contratos, órdenes, instrucciones, maniobras, transferencias, transmisión de información, de datos, de conocimientos, delitos, fraudes, promesas, mentiras, buenos consejos, controles, investigaciones científicas, etcétera, realizados a través de las redes de transmisión de datos y de telecomunicaciones, y de las redes de redes, en el mundo entero, en tiempo real.

Para Godoy, las dos notas fundamentales del espacio informático son, en primer lugar, la escala global en cuanto que el espacio informático llega tan lejos como llegan las redes de transmisión

de datos; en segundo lugar, la velocidad de la transmisión de datos se realiza en tiempo real.

Continuó señalando este autor argentino que ésta es la nueva realidad, éste es nuestro mundo actual con un enorme potencial de futuro que acentuará el proceso de globalización, con muchas dificultades, con muchos conflictos. Pero éste es un mundo de escala global y de "tiempo real" que no alcanzamos a percibir en su complejidad total y, que por lo tanto, no logramos comprender. Y todo este fenómeno es, precisamente, derivado del denominado flujo de datos transfrontera.

Según el Consejo Económico de la Organización de las Naciones Unidas, el Flujo de Datos Transfronterizos (FDT) es la circulación de datos e información a través de las fronteras nacionales para su procesamiento, almacenamiento y recuperación.¹⁴⁹

Conforme a Carlos Correa, la transmisión de datos a través de las fronteras da origen a una nueva problemática jurídica, con repercusiones en el derecho privado y público. La convergencia de la informática y las telecomunicaciones (o "telemática") aumenta notablemente la facilidad con que pueden entrar y salir los datos de un país, sin posibilidad efectiva de controlarlos.

Las fronteras físicas se diluyen así bajo el avance tecnológico, y ponen en entredicho el ejercicio de la soberanía política de los Estados.¹⁵⁰

Conforme a este mismo autor, los flujos internacionales de datos, tal como se entiende generalmente esta noción, pueden ser clasificados, entre otros, según criterios que atiendan a las formas de su transmisión, su función técnico-económica y la naturaleza de la relación existente entre el emisor y el receptor.

A sí, señala que, de acuerdo a los medios de transmisión, el FDT puede ser electrónico o no electrónico (discos, cintas magnéticas); con base en los tipos de información, pueden ser científico-técnica, económica y social, educativa y cultural, comercial y financiera, administrativa, seguridad y sobre las personas; según

149 Citado por Téllez Valdez, Julio, *Derecho informático*, p. 77.

150 Correa, Carlos *et al.*, *Derecho informático*, Buenos Aires, Depalma, 1987, p. 305.

la función técnica-económica, se clasifican en comunicaciones personales y comerciales, transferencia de *software*, acceso a bancos de datos y en procesamiento de datos; y de conformidad a la naturaleza de la relación, se consideran las redes cerradas, venta de servicios (acceso a bancos de datos, procesamiento de datos), venta o licencia de *software* y en transacciones intrafirma.¹⁵¹

El capítulo XIII del Tratado Trilateral de Libre Comercio de América del Norte (TLC)¹⁵² contiene disposiciones alusivas al tema del flujo transfronterizo de datos, en los siguientes términos:

El capítulo señalado se refiere a las medida que adopte o mantenga una parte, relacionadas con:

- El acceso y el uso de redes o servicios públicos de telecomunicaciones por personas de otra parte;
- El acceso y uso que dichas personas harán cuando operen redes privadas;
- La prestación de servicios mejorados o de valor agregado por personas de otra parte, en territorio de la primera o a través de sus fronteras;
- La normalización respecto de la conexión de equipo terminal u otro equipo a las redes públicas de telecomunicaciones.

El artículo 1,302 señala que cada una de las partes garantiza que personas de otra parte tengan acceso y puedan hacer uso de cualquier red o servicio público de telecomunicaciones ofrecidos en su territorio o de manera transfronteriza, en términos razonables y no discriminatorios, para la conducción de sus negocios.

Para ello, cada una de las partes garantizará que las personas de otra parte puedan usar las redes o los servicios de telecomunicaciones para transmitir la información en su territorio o a través de sus fronteras, incluso para las comunicaciones internas de las empresas, y para el acceso a la información contenida en bases de

¹⁵¹ *Ibidem*, p. 306.

¹⁵² *Diario Oficial de la Federación*, 20 de septiembre de 1993, en vigor a partir del 1o. de enero de 1994.

datos o almacenada en otra forma por una máquina en territorio de cualquier parte.

Es importante destacar que, a pesar de pretender eliminar barreras innecesarias en el comercio de bienes y servicios, incluido el flujo transfronterizo de datos e información, el TLC establece con toda claridad que ninguna disposición se interpretará en el sentido de impedir a ninguna parte adoptar o aplicar cualquier medida necesaria para:

- A asegurar la confidencialidad y la seguridad de los mensajes, o
- Proteger la intimidad de los suscriptores de redes o de servicios públicos de telecomunicaciones.

Cada parte garantizará que no se impongan más condiciones al acceso de redes o servicios públicos de telecomunicaciones y a su uso que las necesarias para salvaguardar las responsabilidades del servicio público o proteger la integridad técnica de las redes o los servicios públicos de telecomunicaciones.

Por lo que hace a los llamados “servicios mejorados” o “servicios de valor agregado”,¹⁵³ el TLC señala que cada parte garantizará:

a) Que los procedimientos que adopte o mantenga para otorgar licencias, permisos, registros o notificaciones referentes a la prestación de servicios mejorados sea transparente y no discriminatorio;

b) Que el trámite de las solicitudes se resuelva de manera expedita;

c) Que la información requerida para tales trámites se limite a lo necesario para acreditar que el solicitante tenga solvencia

¹⁵³ Servicios mejorados son los servicios de telecomunicaciones que emplean sistemas de procesamiento computarizado que:

- a) A ctúan sobre el formato, contenido, código, protocolo o aspectos similares de la información transmitida al usuario;
- b) Proporcionan al cliente información adicional, diferente o reestructurada, o
- c) Implican la interacción del usuario con información almacenada.

financiera o que los servicios o el equipo cumplan con las normas o reglamentaciones técnicas aplicables de la parte.

Ninguna parte exigirá a un prestador de servicios mejorados:

- a) Que preste esos servicios al público en general;
- b) Que justifique sus tarifas de acuerdo a sus costos;
- c) Que registre una tarifa, a menos que se trate de corregir una práctica considerada como contraria a las componentes o de un monopolio, que compita de manera ventajosa con personas de otra parte;
- d) Que interconecte sus redes con cualquier cliente o red en particular, o
- e) Que satisfaga una norma o reglamentación técnica específica para una interconexión distinta a la que regula la interconexión con una red pública de telecomunicaciones.

Las disposiciones del TLC no se aplican: a ninguna medida que una parte adopte o mantenga en relación con la radiodifusión o la distribución por cable de programación de radio o televisión, salvo el caso en que las medidas adoptadas por una de las partes sea para garantizar que las personas que operen estaciones de radiodifusión y sistemas de cable tengan acceso y uso continuo de las redes y de los servicios públicos de telecomunicaciones.

Una manifestación importante en este “nuevo” mundo de las telecomunicaciones, de la telemática o teleinformática y que podemos interrelacionar con el FDT es precisamente el *internet*.

El *internet* es una red o conjunto de redes de computadoras interconectadas entre sí a nivel mundial para la comunicación de datos. *Internet* está presente en más de ochenta países y se compone de alrededor de dos millones de computadoras, sus usuarios, más de veinte millones forman parte de todo tipo de instituciones, ya sea de investigación, docencia, gubernamentales o comerciales. Ésta es la red de computadoras más grande del mundo, con un crecimiento exponencial sin precedentes.

Para comunicarse entre sí, las computadoras necesitan “hablar” un mismo lenguaje (protocolo). En la red *internet* el protocolo utilizado se denomina TCP/IP (*Transport Control Pro-*

tol/Internet Protocol). Por tanto, para conectar una computadora a *internet*, además de la conexión física, se requiere que el protocolo TCP/IP esté instalado en dicha computadora. A diferencia de otros protocolos de comunicación, existen implementaciones de TCP/IP para prácticamente todas las marcas y modelos de computadoras, lo que explica su aceptación y utilización en todo el mundo.¹⁵⁴

Para “navegar” por *internet*, se utilizan varios programas entre los que destacan: el *Mail*, para enviar y recibir mensajes de correo electrónico; *Telnet*, para establecer sesiones interactivas en otras computadoras; *Archie*, para localizar información disponible en la red; *FTP*, para transferir archivos desde y hacia otras computadoras.

Desde el punto de vista jurídico, existen algunas cuestiones que es necesario determinar para una posible regulación jurídica de este gran fenómeno de comunicación e intercambio de información.

El primer cuestionamiento es en relación al propietario o administrador de la red de redes (*internet*). Ante esto, lo más que se llega a afirmar al respecto es que “nadie” es el propietario, gestor u operador de *internet*, ni siquiera para establecer reglas o normas de utilización. Su funcionamiento se basa en una amplia colaboración técnica y administrativa entre las redes diseminadas por todo el planeta. Ante esto, si se desconoce a un sujeto tan importante, ¿puede existir regulación jurídica al respecto?

Ahora bien, y ya que lo que se intercambia en este tipo de soportes es información, ¿quién es el titular de los derechos autorales de toda esa información que “puede ir de un lado al otro”?

Sobre el particular, podemos decir que los derechos de propiedad de la información difieren de los derechos de propiedad sobre propiedades tangibles.¹⁵⁵ La diferencia en el objeto de la protección

¹⁵⁴ Esta información ha sido obtenida de la Dirección General de Servicios de Cómputo Académico de la UNAM.

¹⁵⁵ Al respecto también se han pronunciado, entre otros, Nimmer, Raymond T., y K rauthaus, Patricia Ann, “El *copyright* en las autopistas de la información”, *Derecho de la Alta Tecnología*, Buenos Aires, año VII, núm. 80, abril de 1995, Buenos Aires, pp. 2 y ss.

es cuestionar qué es lo que se protege y con qué fines. Los bienes intangibles no pueden ser poseídos, pero pueden ser replicados en copias o memorias. A diferencia de los bienes tangibles, los intangibles pueden ser “conocidos” por muchas personas al mismo tiempo, exactamente en la misma forma.

Por cierto que, en este punto, la diferencia entre información y bienes físicos resulta crítica. Una vez conocida por otra persona, la información no puede ser controlada o restringida, excepto mediante un derecho de propiedad legalmente estipulado u obligaciones contractuales.¹⁵⁶

Y a hemos señalado con anterioridad algunos aspectos que la mayoría de los países regulan como lo referente a la protección del *software* a través de las normas autorales, ahora bien, ¿esta información que se distribuye por todo el mundo a través de las autopistas de la “información” en el denominado “espacio informático” puede regularse como tal?

Es necesario señalar que el modelo analítico básico en el derecho referente a la propiedad sobre la información consiste en condiciones específicas que dan nacimiento a derechos de propiedad definidos y específicos. Tanto las precondiciones como los derechos resultantes deben ser adaptados para balancear los intereses de los propietarios y de las terceras partes que desean usar la información. Las normas autorales realizan sus distinciones sobre la base de puntos como la expresión creativa, la limitación de derechos, el dominio público y frecuentemente subordina una facultad autoral a la posibilidad de usos privados y personales por una tercera parte. Otras instituciones jurídicas usan diferentes lenguajes y parámetros. A medida que examinamos nuevos sistemas de información, la base en la que se realiza el balance político permanece enfocado en antiguos sistemas de transferencia y uso comercial de la información.

Pero ante esto, ¿qué derechos podrían crearse sobre los bienes informacionales?; es decir, ante la ausencia de un órgano supra-

nacional regulador o aplicador de políticas tan subjetivas y dispersas, ¿quién podría conformar una unidad jurídica?

Debemos partir primero de considerar que los derechos que derivan de la "información" han sido ya reconocidos en casi todo el mundo como aquéllos que devienen de las normas autorales; sin embargo, y como ha señalado la doctrina nacional e internacional,¹⁵⁷ existen proporciones jurídicas en el valor de la información; esto es, no solamente las reglas jurídicas autorales protegen la información como tal o a los valores que derivan de ella, como son los políticos, sociales, económicos, por señalar algunos. Esto significa que otro cuerpo o conjunto de leyes protegen la propia información, y así tenemos normas de derecho penal, civil, laboral, intelectual, entre otros, por lo que, con base en esto, señalamos que distintas regulaciones estatales y otras instituciones jurídicas tienen una gran influencia sobre el desarrollo de diversos derechos que influyen sobre la información (de ahí que para nosotros sea muy importante que el artículo 6o. constitucional en nuestro país eleve su significación práctica, pero sobre todo jurídica).

A hora bien, un propietario de información teóricamente podría ejercitar todos los derechos que derivan de la información para hacerla respetar como "suya" ante todo el mundo; sin embargo, también resulta ésta una afirmación inimaginable en cuanto el sentido que en sí conlleva.¹⁵⁸

A sí, se necesita decir que, por su alcance relativo y no comprensivo, definir derechos de propiedad sobre la información involucra diseñar un balance entre los intereses de un propietario, de terceras partes en competencia y de intereses públicos y muchas veces, también, privados. Pero aunque éste fuera el caso, los procesos de balance circunstancial en la fundamentación o "nacimiento" de las propias instituciones jurídicas se hacen general-

157 Baste leer simplemente algunos autores que se citan en la bibliografía del presente estudio.

158 Por ejemplo, las normas jurídicas mexicanas raramente crean derechos que puedan ejercitarse contra todo el mundo.

mente mediante un análisis casuístico específico; esto es, cada sociedad elabora su propio derecho con base en sus circunstancias.

Con todo esto, ¿es conveniente considerarse optimista ante una posible regulación jurídica de lo “no regulable”?

Cada quien puede emitir sus propias conclusiones, no obstante, y ante el conflicto jurídico que esto representa, nosotros planteamos lo siguiente:

El primer paso necesario es regular el acceso “calificado”, por un lado, a lo informativo y, por otro, regular el acceso al usuario desde un punto de vista local o nacional. Por “calificado” entendemos una legislación lo bastante consensada en nuestro país que permita y respete las autorregulaciones (no hablamos de censura), y conformes a una serie de principios y valores públicos “locales”.

Si la norma jurídica mexicana permite que cierta información sea susceptible de manejarse por vía intrafrontera, entonces podrá ser distribuida transfrontera. Con esto, a raíz de una regulación local, se protege el interés internacional a través de una norma jurídica local; es decir, la norma jurídica nacional velará por el cumplimiento de los esquemas de protección jurídica de la información nacional en correlación con la comunidad internacional y viceversa. Consideramos que lo mismo sucedería en cuanto al orden y control local de acceso de usuarios.

5. LOS CONVENIOS O CONTRATOS INFORMÁTICOS

Nuestro actual Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal reconoce la máxima importancia del contrato, al erigir los principios generales de los contratos nada menos que en las normas generales aplicables a toda clase de convenios y de actos jurídicos.¹⁵⁹

Dicha disposición normativa distingue entre convenio y contrato, pues considera a éste la especie y a aquél, el género. A sí, señala el artículo 1,792 que el convenio es el acuerdo de dos o

¹⁵⁹ *Cfr.* artículo 1,859.

más personas para crear, transferir, modificar o extinguir obligaciones; mientras que el artículo 1,793 determina que los contratos son los convenios que producen o transfieren las obligaciones y derechos.

No puede decirse que la voluntad de las partes no juega ningún papel en el nacimiento y fijación del contenido de las obligaciones del contrato, pues el contrato obliga a las partes a lo que expresamente hubieran pactado (*vid.* artículo 1,796), y lo que es más, por mero efecto del contrato se lleva a cabo la transmisión de la propiedad, sin necesidad de tradición (artículo 2,014). A simismo, cuando se trata de fijar el alcance y los efectos de un contrato, se busca ante todo descubrir la intención de los contratantes, como lo señala el artículo 1,851.

Por otro lado, y para el tema que nos ocupa, es necesario señalar que nuestro Código Civil, en sus artículos 1,832 y 2,014, así como en el 1,839 y 1,858, consagra la libertad contractual por lo que hace a la forma, y por lo que toca al fondo del contrato.

Como señala Ramón Sánchez Medal,

existe libertad contractual en cuanto a la forma, ya que hoy día existe la regla general de la consensualidad o ausencia de formas obligatorias en la formación de los contratos, si bien se advierte un renacimiento del formalismo en nuestros días [...] sin embargo este nuevo formalismo en numerosos contratos se ve debilitado con la admisión por nuestro derecho civil de la acción *pro forma* para revestir de las formalidades legales a aquellos contratos que se hubieren celebrado son observarlas, de conformidad con los artículo 1,833 y 2,232.¹⁶⁰

Este mismo autor señala también que existe libertad contractual en cuanto al fondo, porque pueden insertarse en los contratos las cláusulas y condiciones que las partes libremente convengan y pueden celebrarse figuras de contratos distintos de los expresamente reglamentados, sin perjuicio de que existan limitaciones: unas de carácter general y otras de índole particular a la libertad

¹⁶⁰ Sánchez Medal, Ramón, *De los contratos civiles*, 8a. ed., México, Porrúa, 1986, pp. 11 y ss.

contractual, esto con base en los artículos 1,839 y 1,858 del Código Civil.¹⁶¹

Por último, baste simplemente señalar que nuestro Código Civil reconoce la existencia y regulación de los contratos nominados o típicos como de los contratos innominados o atípicos.

A hora bien, esto que hemos pretendido señalar en un principio nos servirá de referencia para determinar la naturaleza de los denominados doctrinalmente como “contratos informáticos”, no sin antes efectuar una referencia a los mismos.

Carlos Ghersi define los contratos informáticos como “aquéllos que establecen relaciones jurídicas respecto de prestaciones consistentes en transferir la propiedad o el uso y goce de bienes, o prestar servicios, ambos informáticos”.¹⁶²

Téllez señala que “el contrato informático es como todo acuerdo de partes en virtud del cual se crean, conservan, modifican o extinguen obligaciones relativas a los sistemas, subsistemas o elementos destinados al tratamiento sistematizado de la información”.¹⁶³

En cuanto a los elementos esenciales del contrato y respecto al consentimiento, se entiende por tal el acuerdo de voluntades entre las partes llámese generalmente proveedor, distribuidor o diseñador como el usuario, cliente o adquirente, para crear y transmitir derechos y obligaciones.

Respecto al objeto del contrato, independientemente de lo que señalamos más adelante, se entiende por tal la operación jurídica por la cual se crean, modifican, transmiten o extinguen relaciones obligacionales sobre bienes y servicios informáticos.¹⁶⁴

Los bienes y servicios antes señalados se integran generalmente en un sistema, que es el conjunto de elementos materiales e inmateriales, ordenados e interdependientes, vinculados por un objetivo común. El sistema integrador de los contratos informáticos se encuentra constituido de la forma siguiente:

¹⁶¹ *Idem*.

¹⁶² Ghersi, Carlos Alberto, *Contratos civiles y comerciales*, 2a. ed., Buenos Aires, Depalma, 1992, t. II, p. 306.

¹⁶³ Téllez, Julio, *Contratos informáticos*, México, UNAM, 1989, p. 17.

¹⁶⁴ Ghersi, Carlos Alberto, *Contratos civiles y comerciales*, p. 307.

a) El soporte físico o material, se refiere a las herramientas o máquinas; es decir, lo que técnicamente recibe el nombre de *hardware*;

b) El soporte lógico o inmaterial, constituido por aquello que hace posible el funcionamiento del sistema, no puede ser apreciado físicamente, siendo éste el caso de los programas conocidos con el nombre de *software*;

c) El elemento humano;

d) La documentación inherente a los bienes o servicios;

e) La asistencia técnica.

Se considera que el objeto de los contratos informáticos es generalmente múltiple. El decreto real belga del 27 de abril de 1977 ofrece una definición abarcante. Su artículo 2o. establece tres órdenes de bienes y servicios: a) los equipos (unidades centrales y periféricas, terminales, etcétera); b) los programas (de sistemas operativos y de aplicación), y c) prestaciones relativas al desarrollo y a la explotación de sistemas de información, así como toda investigación o actividad en relación con el tratamiento de la información.¹⁶⁵

El contrato informático puede clasificarse en diversos tipos según Carlos Correa:¹⁶⁶

1. Conforme a la materia del acto que se celebre, los contratos informáticos pueden corresponder a:

a) Equipamiento: unidades centrales de procesamiento; periféricos para la entrada y salida, o el almacenamiento de datos; equipos para comunicaciones, etcétera;

b) *Software*: *software* de base y aplicativo;

c) Servicios: de análisis y diseño de sistemas; programación, adecuación de locales e instalación, capacitación; mantenimiento (de equipos, de *software*), etcétera;

2. También pueden clasificarse según el negocio jurídico que se celebre, así se propone la siguiente clasificación:

165 Citado por Correa, Carlos M. *et al.*, *Derecho informático*, p. 153.

166 *Ibidem*, p. 154.

a) El contrato de venta: de equipo informático como de programas o *software*;

b) El contrato de *leasing*: las relaciones jurídicas se establecen entre el fabricante de material informático, la entidad financiera de *leasing*, y el usuario: entre el fabricante y la entidad financiera de *leasing* hay una compraventa, la entidad de *leasing* no utiliza el material y lo alquila al usuario juntamente con un compromiso de venta;

c) El contrato de locación: de equipo o de programas;

d) El contrato de horas-máquina: éste es un contrato de cesión de uso en el cual el usuario sólo opera la máquina durante una cantidad determinada de horas-máquina;

e) El contrato de mantenimiento;

f) El contrato de prestaciones intelectuales, el cual comprende los estudios previos, el pliego de condiciones, la formación del personal o el contrato llave en mano;

g) El contrato de prestación de servicios.

Los denominados contratos informáticos asumen con frecuencia la modalidad de contratos de adhesión, sobre todo porque se prescinde de toda discusión precontractual entre las partes, y se reducen a la aceptación total por una de ellas de las condiciones propuestas unilateralmente por la otra.

A sí, es común que los principales proveedores de material informático procuren establecer el vínculo contractual sobre la base de contratos preimpresos, conteniendo éstos cláusulas generales y especiales a que debe sujetarse el vínculo, sin mayor posibilidad para el cliente de discutir sus condiciones. De esta manera, la situación se agrava en los contratos informáticos, ya que por una parte el cliente ignora las características técnicas e informáticas de lo que está comprando, mientras que el proveedor frecuentemente recurre a diversas tácticas para vender su producto.

La mayor representación jurídica que tenemos en este tipo de contratos se da en la compraventa de equipo informático, ya sea *hardware* o *software*.

Ante esto, es importante señalar que el tipo de contrato que regulará esta operación es la de una verdadera compraventa, por lo que se necesitará cumplir con los mandamientos que al respecto dicta el Código Civil.

Independientemente de lo anterior, es necesario indicar que dada la naturaleza del objeto del contrato como de los bienes sujetos al mismo, se ha determinado que los contratos informáticos, independientemente de la verdadera naturaleza contractual de la que deriven, deberán cumplir con el señalamiento de ciertas obligaciones del proveedor como algunas obligaciones también por parte del adquirente.

De esta forma, se debe pretender que dentro de las obligaciones primordiales del proveedor estén: las de brindar información al adquirente; entregar el equipo; capacitar en el uso del equipo; otorgar garantías al cliente; así como otorgar las diversas patentes o licencias de uso, tanto del *hardware* como del *software*.

Respecto a las obligaciones del adquirente, se entienden las de pagar el precio; respetar las advertencias del proveedor; capacitarse en cuanto al manejo del equipo; colocar el equipo en lugares aptos para un uso congruente a la naturaleza del soporte informático entre otras.

A simismo, Daniel Altmark señala que existen cuatro momentos de la relación contractual y de la operación informática que se da entre las partes: a) el periodo precontractual; b) la conclusión del contrato; c) su ejecución, y d) las diferentes formas de extinción.

A pesar de todo lo anterior, mucho se ha discutido sobre la naturaleza de este tipo de acuerdos, que conlleva a afirmar que los contratos informáticos derivan de verdaderos contratos típicos o pueden clasificarse como contratos atípicos.

En favor de la ubicación de derivación de contratos típicos se argumenta en el sentido de que, cualquiera que sea el objeto de las prestaciones, siempre se estará en presencia de contratos nominados; es decir, de una compraventa, una prestación de servicios profesionales, un arrendamiento financiero, etcétera. Ahora bien, se dice que el contrato informático será atípico sólo

si lo es el negocio contractual que genera las obligaciones de las partes, o bien en las características “novedosas” que presenta su objeto.

Con base en nuestro Código Civil y siguiendo a Ramón Sánchez Medal,¹⁶⁷ a los contratos que menciona y cuyo contenido disciplina el legislador se les llama contratos nominados o típicos y a los que no reglamenta, aunque algunos de ellos simplemente los mencione, se les llama contratos innominados o atípicos.

Conforme a los artículos 1,796, 1,832, 1,839 y 1,858, en una y otra especie de contratos el legislador reconoce a las partes la libertad contractual.

Respecto a los contratos innominados o atípicos, no existen normas legales que disciplinen su contenido, el cual puede llenarse o modelarse libremente por voluntad de las partes, en ejercicio de la mencionada libertad contractual, lo que en algunos casos representa un gran problema llenar las lagunas dejadas por las estipulaciones omisas de las partes, por no existir en el caso normas supletorias o dispositivas a propósito de esos contratos.

Se ha determinado que existen en nuestra contratación civil algunas figuras afines que en apariencia pueden considerarse innominados o atípicos, pero que en la realidad no dejan de ser nominados o típicos. Además, el contrato innominado o atípico no es simplemente el contrato que carece de nombre propio, dado que hay contratos que no dejan de ser innominados o atípicos por el solo hecho de ser mencionados por el legislador o por tener ya en doctrina un nombre propio.

Tampoco deben confundirse los contratos innominados o atípicos con los contratos múltiples o uniones de contratos, en que no hay un contrato único con efectos complejos, sino en realidad se trata de la coexistencia de dos o más contratos diferentes.

La doctrina ha dividido los contratos innominados o atípicos en dos grandes grupos:

a) Contratos innominados en sentido estricto o puros, que comprenden tanto los contratos que tienen un contenido comple-

¹⁶⁷ Sánchez Medal, Ramón, *De los contratos civiles*, pp. 521 y ss.

tamente extraño a los tipos legales, como los contratos que tienen un contenido sólo parcialmente extraño a los tipos legales, y

b) Contratos mixtos o complejos, en los que todos los elementos de su contenido son de tipos legales, pero en combinaciones diversas.

Para las dos clases de contratos innominados, nuestro legislador, en el artículo 1,858 del Código Civil, establece que debe acudirse a los principios generales del contrato y a las estipulaciones expresas de las partes, reconociendo en esta forma la validez de la autodisciplina en el contrato innominado.

Pero, a falta de una norma de la teoría general del contrato o de una estipulación expresa, se plantea el problema de qué normas deben aplicarse. Sobre el particular, en el contrato innominado puro cabe la aplicación analógica, a través de las normas del contrato típico con el que el contrato innominado puro tenga más analogía. Respecto al contrato mixto, propiamente no hay aplicación analógica sino más bien aplicación directa; o sea, la aplicación de las normas de los distintos contratos típicos a que correspondan los contratos combinados en el contrato mixto.

Conforme al artículo 1,858 de nuestro Código Civil, se estima que el procedimiento más aceptable es el de la analogía: la aplicación de las normas del contrato típico con el que dicho contrato mixto tenga más analogía.

Por tal se señala que, para circunscribir la jerarquía de criterios que establece nuestra ley, primero se debe recurrir a las reglas generales de los contratos enunciados en la teoría general del contrato; después, a las estipulaciones expresas de las partes, en acatamiento a la libertad contractual; y finalmente, a las normas del contrato nominado o reglamentado por la ley con el que se tenga más analogía.

Por estas consideraciones, nosotros somos de la idea de que en nuestro derecho positivo mexicano, los llamados contratos informáticos, al no ser típicos porque expresamente nuestro legislador no los regula como tales, no se pueden limitar en los contratos innominados o atípicos, ya que en materia de aplicación o

interpretación de estos se debe estar al principio de analogía o de aplicación de normas de los diversos contratos típicos.

A sí estaremos en presencia de verdaderos contratos como el de compraventa, permuta, donación, mutuo, arrendamiento financiero, entre otros, en cuyo objeto o fin se encuentren soportes informáticos, y a sea *hardware* o *software*, pero esto, según nuestra opinión, no da la característica de contrato innominado.

6. LOS DELITOS INFORMÁTICOS

Para poder determinar la posible existencia de los delitos informáticos, es necesario determinar que se debe recurrir precisamente a las dos materias que integran la relación de la que hemos venido hablando en el transcurso del presente estudio como son la informática y el derecho, en la cual cada una aporta su horizonte de proyección.

Respecto a la informática, necesitamos recurrir a ella para conocer cuáles son las conductas que la comunidad científica tecnológica considera que deben protegerse por el derecho, mientras que el derecho debe indagar qué es el delito para posteriormente cuestionar si la utilización masiva de las computadoras y la telemática pueden cambiar la naturaleza y alcance de la ley penal.

La teoría del delito nos dice que el delito es la conducta típica, antijurídica y culpable a la que se asocia una pena como consecuencia. Afirmada la existencia del delito, procede la consecuencia o aplicación de la pena.

Sabemos que, entre una gran cantidad de conductas posibles, sólo algunas son prohibidas por el legislador. Para poder distinguir las conductas que son delitos de aquéllas que no lo son, acudimos a los dispositivos legales que describen las conductas prohibidas. No habrá delito, pues, cuando la conducta de un hombre que utiliza las computadoras y/o su tecnología no se adecua a alguno de esos tipos penales.

Cuando queremos averiguar qué es delito informático, necesariamente debemos buscar la respuesta en la parte especial del

Código Penal, pero aquí surgen algunas posibles interrogantes: ¿en el federal, en el local, en las leyes penales especiales?

La legislación penal en México está compuesta por el Código Penal en Materia Federal en todo el país y en Materia Común en el Distrito Federal, además de las normas penales que como apéndices se encuentran dispersas en leyes, sobre todo administrativas federales, y los ordenamientos estatales que reproducen la situación antes prevista.

Las estadísticas sobre tipos penales varían.¹⁶⁸ Al efectuar un análisis documental legislativo respecto a este problema, podemos afirmar que, con excepción del estado de Sinaloa, que será comentado con posterioridad, en nuestro país, ya sea a nivel federal o local, los delitos informáticos, como tales, no existen, ya que los mismos no se encuentran tipificados.

Lo dicho con anterioridad nos obliga a consultar la doctrina nacional y extranjera para conocer las diversas conductas a las que se les da el nombre de delitos informáticos y, posteriormente, examinar si se adecuan o no a los tipos previstos en las leyes penales vigentes.

Sin embargo, y antes de entrar al fondo de este asunto, es necesario hacer referencia a la aparición en nuestro panorama de otra ciencia: la criminología, inclusión que a nuestro parecer explicará parte de la confusión respecto a la existencia o no de los denominados delitos informáticos.

El saber criminológico (así lo denominan algunos autores para soslayar la discusión sobre si es ciencia o no) se consideró alguna vez auxiliar del derecho penal, y pretendía explicar las causas de la conducta delictiva; para ello recurría a los tipos penales.

En la búsqueda de su autonomía afirmó como su objeto de estudio la conducta "antisocial" como categoría diferente a la penal. A sí, intentó ampliar su horizonte científico y desprenderse del derecho penal. A partir de ese momento, sus investigaciones

¹⁶⁸ Cfr., entre otros, García Domínguez, Miguel Ángel, *Los delitos especiales federales*, México, Trillas, 1987; A costa Romero, Miguel y López Betancourt, Eduardo, *Delitos especiales*, México, Porrúa, 1989.

iban más allá, no importando si las acciones se consideraban o no delito. Por ello, se define la criminología como una ciencia sintética, causal explicativa, natural y cultural de las conductas antisociales.¹⁶⁹

Los aportes de los criminólogos han sido muchos, gracias a ellos se detectaron graves situaciones como olvido a las víctimas, los crímenes de los poderosos, los abusos de poder; se enfatizó el papel selectivo del sistema penal como filtro de vulnerables, entramos a conocer delitos denominados como electrónicos y otros como informáticos, etcétera (como puede observarse, es difícil que no recurran a términos jurídico-penales como lo es crimen o delito).

La desventaja la encontramos en la confusión en llamar “delito” o “crimen” a lo que posiblemente sólo sea una conducta indebida, ilícita o ilegal, y que en el campo de la informática podría ser considerada digna de protección penal en el futuro. Bajo esta perspectiva, debemos considerar que para los criminalistas algo puede ser crimen, delito, ilícito cuando no necesariamente está tipificado en la legislación nacional.

Con esta aclaración, analizaremos lo que se ha dicho respecto a los delitos informáticos.

María de la Luz Lima define el delito por computadora como cualquier acto ilícito penal en el que las computadoras, su técnica y funciones desempeñan un papel ya sea como método, medio o fin.

Otras definiciones citadas por dicha autora, son:

- A quélllos en que se utiliza una computadora como instrumento u ocupación criminal.
- Delito en el campo de la información: cualquier acción ilegal en el que la computadora es el instrumento u objeto del delito (Tiedemann).
- A lgunos autores prefieren hablar de abuso de computadoras. Señalan que son aquellos actos asociados con la tecnología

169 Rodríguez Manzanera, Luis, *Criminología*, México, Porrúa, 1979, p. 10 y ss.

de la computadora en el cual una víctima ha sufrido una pérdida y el autor intencionalmente ha obtenido una ganancia (Parker).

Retomando la primera definición de delito por computadora, Lima menciona ejemplos de delitos clasificados según el papel de la computadora, y así no habla: como método, y cataloga el fraude, robo, robo de servicios no autorizados; como medio: se refiere al acceso no autorizado para extorsionar con la información, y como fin: al señalar la destrucción de programas, daños a la memoria, entre otros.¹⁷⁰

Como podemos determinar, de las anteriores definiciones no se desprende un delito con naturaleza propia, sino que puede ser cualquiera cometido por medio de la computadora o teniendo a ésta por objeto. Parker, citado por Lima, limita a las figuras patrimoniales y, con más propiedad, los llama abusos.

Sin embargo y recurriendo a otras descripciones de conductas informáticas, encontramos que algunas rebasan la posibilidad de adecuarse a los tipos penales.

A sí, la definición que sobre delito informático presenta la Organización para la Cooperación Económica y el Desarrollo señala que será cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automático de datos y/o transmisión de datos.¹⁷¹ Más extensa es la siguiente:

cometerá delito informático la persona que maliciosamente use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información. También comete este tipo de delito el que maliciosamente y a sabiendas y sin autorización intercepta, interfiere, recibe, usa, altera, daña o destruye una computadora, un sistema o red de computadoras o los datos contenidos en la misma, en la base, sistema o red.¹⁷²

¹⁷⁰ *Idem*.

¹⁷¹ Correa, Carlos *et al.*, *Derecho informático*, pp. 295 y 296.

¹⁷² Proyecto de ley informática del Ministerio de Justicia de Chile, abril de 1986.

La clasificación que transcribimos a continuación, elaborada por Uhlrich Sieber,¹⁷³ explicita aún más la variedad de formas de acción que pueden revestir los abusos en el uso de las computadoras:

a) Fraude por manipulaciones de un computador contra un sistema de procesamiento de datos, que incluye cambio de datos o informaciones para obtener un beneficio económico. Estos delitos pueden afectar datos que representan activos (depósitos monetarios, créditos, etcétera), o bien objetos materiales (manejo de inventario).

Sus formas pueden darse a través de la introducción de datos falsos, modificación de resultados, cambio en los programas de computación.

b) Espionaje informático y robo de *software*.

c) Sabotaje informático, que se puede referir a los datos o a los programas, o al equipamiento en sí.

d) Robo de servicios.

e) Acceso no autorizado a sistemas de procesamientos de datos; y

f) Ofensas tradicionales en los negocios asistidos por computadora.

En el mes de septiembre de 1994 se celebró en Río de Janeiro, Brasil, el XV Congreso Internacional de Derecho Penal,¹⁷⁴ evento en el cual se dedicó un espacio al tema de los "delitos informáticos y otros delitos correlativos contra la tecnología informática".

A partir de una serie de consideraciones como la aceptación del hecho de la proliferación de la tecnología informática y el surgimiento de una sociedad informatizada; que una serie de actividades antisociales están corrompiendo dicha tecnología y afectando a individuos y sectores sociales; que la interconexión de redes trasciende las fronteras nacionales de países desarrollados y en vías; que la actividad informática es de interés para todos los Estados y tomando en cuenta los estudios multidisciplinarios de organismos no gubernamentales e intergubernamentales, se propusieron recomendaciones que abarcan seis puntos:

I. Medidas no penales; II. Derecho penal sustantivo; III. Cuestiones específicas a la protección de la intimidad; IV. Derecho procesal; V. Cooperación internacional, y VI. Tareas futuras.

¹⁷³ Citado por Correa, Carlos *et al.*, *Derecho informático*, p. 296.

¹⁷⁴ *Criminalia*, Academia Mexicana de Ciencias Penales, México, Porrúa, año LV, núm. 2, mayo-agosto de 1994, pp. 133-160.

Este XV Congreso fue de suma importancia, ya que recogió los avances que hasta ese momento se habían logrado por parte de la OCDE (Organización para la Cooperación Económica y el Desarrollo), el Consejo Europeo, las Comunidades Europeas, la Mancomunidad Británica, las Naciones Unidas, Interpol y la Cámara de Comercio Internacional. Por tal, presentamos el siguiente resumen de lo que nosotros consideramos relevante:

En medidas de prevención no penales, el aspecto primordial gira en recordar que el derecho penal debe ser una última medida cuando han fallado o fueron insuficientes las sanciones civiles o administrativas. Se deben implantar, en primer lugar, medidas de seguridad por parte de los usuarios; dictar medidas disciplinarias en la industria del proceso de datos dentro de una práctica de patrones profesionales; elaborar políticas de usos informáticos por parte de los gobiernos; promocionar la cooperación ente las víctimas, el entrenamiento y educación del personal en los sistemas de investigación, prosecución y judiciales.

En cuanto al derecho penal sustantivo, se mencionó que, agotadas las posibilidades no penales, sería necesario considerar la adopción de nuevas leyes penales o reforma de las existentes, toda vez que hay o puede haber un bien jurídico afectado que debería tutelarse a través del derecho.¹⁷⁵

Este congreso, igual que parte de la doctrina, considera que los bienes jurídicos afectados por las conductas "informáticas" pueden ser los patrimoniales o los orientados hacia la intimidad (nosotros no estamos de acuerdo al respecto, por lo que más adelante daremos nuestro punto de vista).

Se recomienda limitar la responsabilidad penal a los actos dolosos.

Transcribimos *in extenso* la lista de actos que el Consejo de Europa elaboró en 1989 y que el Congreso hizo suyo con la finalidad de respetar la terminología informática utilizada.

175 Ante esto, nosotros solamente afirmamos que algunas conductas "informáticas" pueden adecuarse a los tipos existentes en la legislación, pero es posible que el *modus operandi* escape a las formas tradicionales o que se requieran nuevos tipos para proteger intereses no tutelados hasta ahora.

A ctos que el Consejo Europeo considera que deban ser criminalizados:

A) Fraude en el campo de la informática

A portes de datos, alteración, tachaduras o supresión de datos computarizados o programas de informática, o cualquier otra interferencia durante el proceso de datos, provocando como resultado pérdidas económicas o pase de la propiedad a otra persona, con el objeto de obtener ganancia financiera ilegal para sí o para terceros (anteproyecto alternativo: con el propósito de usurpar ilícitamente la propiedad en dicha persona).

B) Falsificación en materia informática

El aporte de datos, alteración, tachadura o supresión de datos computarizados, o programas informáticos, o cualquier otra interferencia durante el proceso de datos, realizada de tal forma o bajo condiciones tales que constituyan un delito de falsificación, cuando sea cometido en conexión a un objeto tradicional de tal delito.

C) Daños causados a datos computarizados o programas informáticos

Tachadura, daños, deterioro o supresión de datos computarizados o programas de informática sin derecho a hacerlo.

D) Sabotaje informático

El aporte, alteración, tachadura o supresión de datos computarizados, o programas informáticos, o interferencia en sistemas informáticos con la intención de obstaculizar el funcionamiento de un sistema informático o de telecomunicaciones.

E) Acceso no autorizado

Acceso sin autorización a un sistema informático o red, infringiendo medidas de seguridad.

F) Intercepción sin autorización

La intercepción, efectuada sin autorización, utilizando medios técnicos de comunicaciones transmitidas, recibidas o vehiculadas dentro del ámbito de un sistema o red de informática.

G) Reproducción no autorizada de un programa informático protegido

La reproducción, distribución o comunicación al público no autorizada de un programa de informática protegido por la ley.

Las directrices del Consejo Europeo también identifican, en una "lista optativa", la siguientes áreas adicionales que también podrían considerarse criminales cuando sean cometidas intencionalmente:

A) Alteración de datos computarizados o programa informático.

B) Espionaje informático.

La adquisición, por medios improprios, o la revelación, transferencia o uso de una marca registrada o secreto comercial sin autorización o cualquier

otra justificación legal, con la intención ya sea de causar pérdida financiera a la persona titular del secreto o a obtener una ventaja financiera ilícita para sí o para terceros.

C) Uso no autorizado de una computadora.

El uso autorizado del sistema o red informática, que se realice: (i) mediante la aceptación de un relev ante riesgo de pérdida causado a la persona habilitada al uso del sistema o de daño al sistema o a su funcionamiento; o (ii) con la intención de causar perjuicio a la persona habilitada al uso del sistema, o daño al sistema o a su funcionamiento; o (iii) causar pérdida al titular del derecho al uso del sistema, o daño al sistema en sí o a su funcionamiento.

D) Uso no autorizado de un programa informático protegido por ley que ha sido reproducido sin derecho a hacerlo, premeditadamente, ya sea para lograr una utilidad financiera ilícita para sí o para tercero, o para causar daño o perjudicar al titular del derecho.

Otras posibles conductas punibles: Tráfico de claves informáticas obtenidas por medios contrarios a la ley; otras informaciones sobre medios de acceso no autorizado a los sistemas; y distribución de virus informáticos.

Sobre el tercer punto de la agenda, se propuso que, en el área de la intimidad, las disposiciones penales deben utilizarse particularmente:

- En casos graves, especialmente aquéllos que involucran datos altamente sensibles o información confidencial tradicionalmente protegida por la ley;
- Encontrarse definida clara y precisamente, y no a través del uso de cláusulas vagas o generales;
- Establecer la diferencia entre los niveles de gravedad de las infracciones y respetar las exigencias de la culpabilidad;
- Restringirse primordialmente a actos internacionales, y
- Permitir que las autoridades de enjuiciamiento tomen en cuenta, en lo que atañe a algunos tipos de delitos, la voluntad de la víctima en cuanto al ejercicio de la acción penal.

Ante esto, parece que resulta imperioso nivelar los derechos a la información personal con el derecho de libre circulación de informaciones dentro de la sociedad, así como la dificultad de decidir cuándo se debe proteger penalmente dicha información personal.

Con relación al derecho procesal, se habló de un equilibrio entre los poderes otorgados a las autoridades investigadoras y

judiciales (que se consideró que debían ampliarse) y el respeto a los derechos humanos. Todo ello dentro de la legalidad y las normas del debido proceso. Punto igualmente polémico fue la carencia de normas sobre admisibilidad y confiabilidad de la prueba, cuando se intenta durante los procesos recurrir a registros computarizados.

La cooperación internacional, dada la movilidad de datos a través de redes transnacionales, es un elemento esencial en la prevención y penalización de las conductas informáticas. Para ello sería necesario armonizar en lo posible la legislación sustantiva, establecer la competencia o jurisdicción aplicable en relaciones internacionales y la celebración de tratados para el combate a los denominados “delitos informáticos”.

La comunidad académica y científica, conjuntamente con los gobiernos, deben comprometerse a realizar más investigaciones sobre el delito de la tecnología informática, especialmente sobre:

- Incidencia de los delitos informáticos;
- Extensión de las pérdidas;
- Métodos de perpetración, y
- Características de los infractores.

Desde un punto de vista general, se ha señalado que algunas de las características fundamentales que presentan este tipo de acciones que se encuadran bajo un delito informático:

a) Son conductas criminógenas de cuello blanco, en tanto que sólo determinado número de personas con ciertos conocimientos, en este caso técnico, pueden llegar a cometerlas.

b) Son acciones ocupacionales en cuanto que muchas veces se realizan cuando el sujeto se haya trabajando.

c) Son acciones de oportunidad en cuanto que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

d) Provocan serias pérdidas económicas.

e) Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a cometerse.

f) Son muchos los casos y pocas las denuncias, debido a la misma falta de contemplación por parte del derecho.

g) Presentan dificultades para su comprobación por su propio carácter técnico.

h) Ofrecen facilidades para su comisión a los menores de edad.

i) Por el momento siguen siendo ilícitos manifiestamente impunes ante la ley.

A hora bien, de acuerdo a los fines que se persiguen con las conductas delictivas en los medios informáticos, se presentan dos puntos de vista en cuanto los delitos informáticos:

a) Delitos con medios informáticos, que son aquéllos en los que se piensa en la computadora como herramienta o medio de comisión del hecho punible, y

b) Delitos contra medios informáticos, que son aquéllos que se refieren a la lesión del contenido de información de un sistema que será objeto de tratamiento automatizado, que está siendo procesado o ya fue almacenado y cómo los datos y programas pueden ser afectados por el delito. Éstos son cometidos con medios informáticos, pero puede ocurrir que los instrumentos para efectuarlos no estén vinculados a la computadora, por ejemplo, cuando acercamos un imán y se destruye la información de un disco o de una cinta magnética.

Por su parte, Juan Diego Castro Fernández¹⁷⁶ señala los delitos informáticos que se adecuan a figuras tipificadas en el Código Penal positivo, indicando los bienes jurídicamente afectados, entre otros, determina los siguientes:

I. Delitos contra las personas

Esto lo encontramos en la medicina moderna ya que cuenta con las computadoras entre sus instrumentos de diagnóstico clínico, por lo que es posible a nivel de "mal praxis" el uso indebido de la computadora lo cual representa responsabilidad para el médico, por dolo o por culpa, teniendo frente a nosotros desde un homicidio simple, culposo o lesiones simples o culposas.

II. Delitos contra el honor

¹⁷⁶ Castro Fernández, Juan Diego, *Juristas y computadoras*, Costa Rica, 1992, pp. 25 y ss.

Los encontramos con respecto a la dignidad, decoro, honra, reputación de cada persona, las cuales trata de salvaguardar siempre. Se considera que el honor se afecta al incluirse información falsa de carácter injurioso en un archivo electrónico, que al darse a conocer cause un perjuicio al honor de la persona, o bien, que en registros electrónicos se conserve información falsa de alguna persona.

III. Delitos contra la propiedad

De alguna manera se puede decir que la mayoría de los delitos informáticos afectan primordialmente un bien propiedad de alguien.

Por otro lado, es conveniente señalar también las modalidades de la criminalidad mediante computadoras.

Las principales conductas que conforman la acción delictiva son las siguientes:

- Manipulación. También llamada fraude informático, estas pueden afectar tanto a la fase de suministro o alimentación de datos, como a la salida y a su procesamiento, así tenemos la manipulación en el programa o consola.

Ejemplo: Si se accesa a través de la red telefónica mediante una terminal que opera a distancia, el autor puede efectuar la manipulación desde su casa, con su propia terminal, sin necesidad de introducirse personalmente en la empresa perjudicada. La acción y efecto se verifica por separado, lo cual dificulta el descubrimiento del hecho, esto es uno de los grandes problemas y por lo cual las cifras negras de estos ilícitos cada día son mayores.

- Espionaje. Es la actividad de obtener sin autorización datos o programas o divulgar los obtenidos legítimamente.

En el ámbito del procesamiento de datos, el espionaje económico se ve favorecido por el hecho de que las informaciones se encuentran archivadas en un espacio mínimo y pueden ser transferidas sin problema alguno a otro soporte. Además, dentro del uso indebido de datos, figura siempre el llamado hurto de *software*; es decir, el empleo indebido de programas de computación, los cuales requieren mucho esfuerzo y dedicación, afectándose también comercialmente por el mal uso que algunas personas les dan al realizar la llamada piratería.

- Sabotaje. Son las conductas que persiguen la destrucción o incapacidad de los sistemas informáticos o de algún elemento que la compone (*hardware* y *software*), así tenemos el sabotaje al procesamiento de datos; este resulta favorecido por la gran concentración de información en un mínimo espacio.

- Hurto de tiempo. Esta conducta la encontramos en la utilización indebida de las computadoras por parte de empleados o de extraños, la cual puede producir pérdidas considerables, especialmente en los sistemas de procesamiento de datos a distancia, al efectuarse accesos con números de cuenta o *accounts* ajenos.

La criminalidad mediante computadoras opera a menudo sobre objetos intangibles, tales como activos en los bancos, secretos comerciales, marcas y otros. Ante esto, la norma penal sólo logra

abarcar aquellos comportamientos en forma parcial y más bien casual.

Dentro de los principales métodos con que operan algunos “delincuentes informáticos”, están:¹⁷⁷

a) Datos engañosos. Es la manipulación de datos antes o durante su entrada a la computadora.

b) Caballo de Troya. Es la introducción de un conjunto de sentencias en la codificación de un programa para realizar una función no autorizada. Es el método más común de sabotaje.

c) Técnica de salami. Es la sustracción de pequeñas cantidades de activos de numerosas procedencias, es un redondeo de cuentas.

d) *Superzapping*. Es el uso no autorizado de programas de acceso universal.

e) Puertas con trampa. Utilización de interrupciones en la lógica de un programa en la fase de desarrollo para su depuración y uso posterior de éstas con fines delictivos.

f) Bombas lógicas. Programa que se ejecuta en un momento específico o periódicamente cuando se cumplen determinadas condiciones; es decir, rutinas *a posteriori*.

g) Recogida de residuos. Es la obtención de información “residual” impresa en papel o cinta magnética en memoria después de la ejecución de un trabajo, en la tercera o cuarta cinta magnética.

h) Filtración de datos. Sustracción de datos o copias de datos de un sistema; es decir, duplicar una cinta magnética.

i) Trasiego de personas. Lograr el acceso a áreas controladas, por medios electrónicos o mecánicos.

j) Pinchar líneas de teleproceso. Es la intervención de las líneas de comunicación para acceder o manipular los datos que son transmitidos.

¹⁷⁷ Esta clasificación fue realizada por Donn B. Parker y recogida en Jordán Flórez, Fernando, *La informática, el Estado y el derecho*, citado por Callegari, Nidia, “Delitos informáticos y legislación”, *Revista de la Universidad Pontificia Bolivariana*, Medellín, Facultad de Derecho y Ciencias Políticas, núm. 70, julio-septiembre de 1985, pp. 115 y ss.

k) Simulación. En ésta, se utiliza el ordenador como instrumento para planificar y controlar un delito utilizando técnicas de simulación y modelo.

En el caso de México, se ha empezado a tratar de manera muy precaria este asunto de los denominados delitos informáticos. El único Código Penal que tipifica una conducta ilícita derivada por el avance tecnológico es el del estado de Sinaloa que, en su artículo 217, establece que:

Comete delito informático, la persona que dolosamente y sin derecho:

I.- Use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o

II.- Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadoras o los datos contenidos en la misma, en la base, sistema o red.

Al responsable del delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días de multa.

Con el análisis de este numeral, nos damos cuenta de que se trata de una copia del proyecto de Ley Informática del Ministerio de Justicia de Chile (*supra*), además de que se encuentra clasificado dentro del título correspondiente a los delitos patrimoniales, por lo cual, desde su colocación estructural en el Código se está limitando, ya que el objeto protegido no sólo es el patrimonio de las personas, sino en la manera en que se encuentra tipificado, también protege la intimidad, la seguridad del Estado y la información, pero de manera particular.

En dicho ordenamiento punitivo, lo que se tipifica es un verdadero fraude que se comete a través de medios o soportes informáticos, éstos se usan como instrumentos para alterar esquemas con el fin de obtener dinero y no se emplean como fin en sí mismo, como ilícito informático propiamente dicho. En este artículo se establece, al igual que en el fraude, el hecho de obtener un lucro indebido; por lo tanto, la única diferencia entre fraude y delito informático, según este artículo, es el empleo de sistemas computacionales. Ante esto, resulta erróneo establecer que siem-

pre se tendrá el propósito de obtener un lucro, ya que en muchas ocasiones se realizan tales conductas por gusto o reto intelectual. Este precepto tampoco delimita contextualmente, lo que implica “diseñar, ejecutar o alterar esquemas” sin contemplar el solo hecho de ingresar al sistema o red, sin llegar a crear ningún artificio, sino únicamente entrar como “visitante”.

De esta manera, llegamos a la conclusión de que, aun y cuando se encuentre tipificado en el Código Penal del estado de Sinaloa, no es un delito informático, ya que si bien es cierto que cumple con el elemento tipicidad, también es cierto que no satisface el resto de los elementos formales y materiales. Por lo tanto, desde un punto de vista de la técnica penal, sí es delito para el estado de Sinaloa por estar establecido en su ordenamiento punitivo, pero desde la perspectiva de la técnica informática no llega a plasmar plenamente su descripción.

Otra de las críticas que presenta la denominación en mención es que la llamen “delitos informáticos” por considerar que se trata de una conducta ilícita. El problema radica en no identificar y justificar plenamente, desde la perspectiva normativa, el bien jurídicamente tutelado, ya que la justificación de todas las normas penales radica en la protección de bienes pertenecientes a los individuos y en consecuencia a la sociedad.

Tampoco se establece de manera clara cuál es el sujeto activo y cuál el pasivo, provocando con tal ausencia diversas discusiones como el hecho de cuestionarse si el actor es el dueño de la máquina, o bien, quien haga uso de ella.

Otra carencia es no identificar la naturaleza del ilícito; es decir, si se trata de un delito continuado, permanente o instantáneo, tampoco señala si se acepta la tentativa en estos delitos.

Todos estos aspectos son consideraciones importantes en materia penal; sin embargo, y aun cuando se pretende establecer como delito, no se desentrañan todos los elementos constitutivos del mismo, por tal razón es necesario crear un tipo delictivo que cumpla con todos los requisitos técnicos que regulen el abuso en la informática, debido a que existe la convicción de que lo no penado no está prohibido.

Ante estas consideraciones, podemos señalar que los tipos penales tradicionales resultan inadecuados para encuadrar las nuevas formas delictivas ya que se trata de ilícitos distintos, y aun cuando la doctrina trata de reinterpretar los tipos existentes analizando las figuras punitivas ya creadas para intentar subsumir en ellas los ilícitos informáticos, nosotros consideramos esta actitud como incorrecta, ya que el bien jurídico protegido es distinto en cada uno de ellos.

Somos de la opinión de que en un esquema primario debemos identificar plenamente el bien jurídicamente tutelado. No podemos decir que lo que se tutela es la intimidad o la protección de información personal, porque no sólo se protegen estos, sino también aquéllos que derivan de la seguridad nacional, o datos en materia de seguridad pública o en seguridad industrial, por lo cual no podemos tomar una parte como el todo, sino al todo con todas sus partes.

Ante esta afirmación, consideramos que el bien jurídicamente tutelado en los ilícitos informáticos es la información, debiendo comprender en ésta la que se deriva tanto de un lenguaje natural como del informático.

En efecto, el sistema informático está compuesto por el *hardware* (parte física) y por el *software* (parte lógica); en las configuraciones más usuales, la parte física se compone de teclado, monitor, unidades de lectura o para la grabación magnética de la información, dispositivos de salida, entre otros. La parte lógica incluye el sistema operativo que controla el funcionamiento de todos los elementos del sistema y permite realizar las operaciones básicas (arranque, control de periféricos, grabación, recuperación e impresión de datos, comunicaciones, etcétera), y los programas o aplicaciones específicas que contienen las instrucciones necesarias para que la computadora lleve a cabo una determinada tarea. El soporte lógico no puede quedar reducido al conjunto de instrucciones que gobiernan el funcionamiento de un sistema (algoritmos), sino que también comprende otros elementos, entre los que destacan los lenguajes de algo nivel (Basic, Cobol,

etcétera), en los que se expresan tales instrumentos (código fuente), que luego serán traducidos a lenguaje máquina (código objeto) para su asignación a partes de memoria.

Si bien es cierto que cada uno de estos elementos puede ser objeto de un comportamiento punible, también es cierto que algunas de estas conductas recaen en tipos penales como pueden ser el de piratería informática (que las normas autorales-penales sancionan), o bien en delitos de propiedad ajena, robo, etcétera.

Por lo tanto, afirmamos que el bien jurídicamente tutelado propiamente en los ilícitos informáticos llamados más adelante como delitos informáticos es la información, ya que, por las características de las posibles conductas ilícitas en los supuestos mencionados en el transcurso del presente apartado, lo que se protege es la información contenida en bancos y bases de datos, redes de computadoras, o simples computadoras personales.

A hora bien, toda conducta implica una acción u omisión, los delitos informáticos necesariamente deben requerir de una actuación, de la voluntad del sujeto para que se pueda producir el resultado. Por tal, consideramos que no cabe la omisión en estos delitos.

Respecto a los delitos informáticos, únicamente se admite el dolo, ya que el sujeto al accesar, destruir, alterar información lo hace con pleno conocimiento y conciencia de la conducta que está ejecutándose por ser un delito de resultado. También admiten la tentativa.

En cuanto a los sujetos, el activo siempre deberá ser una persona física, ya que es la única que puede ejecutar las acciones, y el pasivo será el titular de la información, pudiendo ser tanto una persona física como moral. Respecto a los sujetos, no es necesaria una inteligencia superior en el autor, ni se requieren elevados conocimientos técnicos, sino que se trata de comportamientos capaces de ser desarrollados por cualquier individuo mínimamente introducido en el manejo de computadoras así como por aquéllos que tengan avanzados conocimientos técnicos.

Como medios de comisión del delito, se dan tanto en la entrada como en el procesamiento de la información. Por entrada enten-

demos el solo acceso a la red, base de datos o soporte lógico, y por procesamiento, el alterar, divulgar, borrar, manipular, suprimir, falsificar, inutilizar, dañar o cualquier otro que pretenda dar mal uso de la información.

Como podemos notar, pueden existir conductas en las que verdaderamente se cometan conductas ilícitas informáticas como tales; sin embargo, en este tema todavía hay mucho por decir y saber tipificar.

7. EL VALOR PROBATORIO DEL DOCUMENTO ELECTROMAGNÉTICO

Como lo señalan Héctor Fix-Zamudio y José Ovalle Favela,

cuatro son los sistemas que utilizan los ordenamientos procesales mexicanos para determinar cuáles son los medios de prueba admisibles en los respectivos procesos: a) En primer lugar, el que consiste en precisar en forma limitativa, los medios de prueba que la Ley reconoce, como lo hacen el Código Federal de Procedimientos Civiles y el Código de Comercio; b) En segundo término, el que consiste en enumerar en forma enunciativa algunos de los medios de prueba admisibles y dejar abierta la posibilidad para que el juzgador admita cualquier otro medio de prueba diferente de los enunciados, como lo hacen la Ley Federal del Trabajo y el Código de Procedimientos Penales del Distrito Federal; c) En tercer lugar, el que consiste en señalar que es admisible cualquier medio de prueba, sin enunciarlos, pero excluyendo expresamente alguno de ellos, como la confesión de las autoridades, tal como lo hacen el Código Fiscal de la Federación, la Ley del Tribunal de lo Contencioso Administrativo del Distrito Federal y la Ley de Amparo; d) En fin, el sistema que se limita a señalar que es admisible cualquier medio de prueba —sin hacer ninguna enunciación ni exclusión— como ocurre en el Código de Procedimientos Civiles del Distrito Federal y en el Código Federal de Procedimientos Penales.

Con todo, tantos los ordenamientos que formulan la enumeración en forma limitativa como los que lo hacen en forma meramente enunciativa, coinciden generalmente en señalar los siguientes medios de prueba: a) Confesión; b) Documentos (públicos y privados); c) Dictámenes periciales; d) Inspección judicial; e) Declaraciones de terceros (testimonios); f) Fotografías, copias fotostáticas, notas taquigráficas y, en general, “ todos los elementos aportados por los descubrimientos de la ciencia”, y g) Presunciones.¹⁷⁸

¹⁷⁸ Fix-Zamudio, Héctor y Ovalle Favela, José, “Derecho procesal”, *El Derecho en México, una visión de conjunto*, México, UNAM, Instituto de Investigaciones Jurídicas, 1991, t. III, pp. 1,285 y ss.

Es aceptable, desde un punto de vista general, que el derecho a la prueba va unido al derecho fundamental a la defensa; esto es, aquél que dice que tiene un derecho, necesariamente tiene el deber de probarlo ante un juez y mediante un procedimiento determinado. Si no se puede probar un derecho, consecuentemente no existirá tal.

Siguiendo a Carlos Barriuso Ruiz,

las relaciones legales actuales de medios probatorios, no recogen expresamente las técnicas electrónicas, ello no obsta para que podamos invocar y aportar estos elementos probatorios en los juicios en base a [sic] los fundamentos jurídicos de pertinencia, indefensión, adecuación real y social, principio de contradicción, etcétera, ya que nada lo impide, pero recomendando disponer en ellos de señas de identidad y autoría y no violar ningún precepto en su obtención.¹⁷⁹

Ante esto, continúa señalando este autor,

la actual tecnología ofrece la posibilidad de poder individualizar los registros y dotarles de señas de identidad, nada impediría pues, dotar a los dispositivos que producen registros, eléctricos, ópticos, magnéticos y físicos de un carácter, logotipo, número, clave, etcétera que sea exclusivo, y con más dificultades de violación que la firma autógrafa, como por ejemplo la denominada identificación "Biométrica" que partiendo de la huella digital permite el acceso o registro en el sistema, pero impide reconstruir la huella desde ningún sistema, con lo que se preserva la intimidad y se impide la falsificación y manipulación.¹⁸⁰

Consideramos que, en la actualidad, la problemática de la prueba reside en el hecho de que generalmente es asimilada a una prueba escrita (aunque claro, es necesario determinar bajo qué procedimiento nos encontramos). Ante esto, es preciso distinguir el concepto de documento, que no debemos restringirlo a la naturaleza del soporte informático ni al escrito como único elemento material, lo que viene a caracterizar al documento informático es su propia desmaterialización o inmaterialización, aunque con ello no deja de ser concreto, visible y perceptible,

179 Barriuso Ruiz, Carlos, *Interacción del derecho y la informática*, p. 229.

180 *Idem*.

pues siempre existirá un soporte material (llámese disco magnético, disco óptico numérico o listado de impresor).

De lo anterior se infiere que los registros o documentos informáticos no constituyen una información escrita en sentido jurídico, pues estos contienen llaves de acceso, pueden modificarse con facilidad y no permiten diferenciar entre una copia y su original, lo que sí permiten los documentos escritos en papel, aunque a veces se entiende que los documentos informáticos sólo constituyen una manera electrónica de escribir.

Frente a las nuevas tecnologías de la información que ofrecen un lenguaje técnico no comprensible, además de la mediación de una máquina que impide la aprehensión directa de la información, existe una desmaterialización de la propia información, lo que trae aparejada la imposibilidad práctica y física de preconstituir una prueba.

Por otro lado, se considera que surge otro problema en razón de la identificación de las partes que intervienen en una comunicación. Para lo anterior existen mecanismos o servicios que permiten confirmar a partir de la apertura de una conexión o en curso de transmisión, la identidad de las partes en una comunicación, de modo que sea imposible a un tercero hacerse pasar por una de tales partes, nos referimos al llamado:

a) Código secreto, que consiste en la combinación de cifras y/o letras que el sujeto digita sobre el teclado del sistema que utiliza; por ejemplo, los números de identificación personal;

b) La criptografía, que consiste en la codificación del texto que se va a transmitir (incluyendo elementos de autenticación) con la ayuda de claves y algoritmos, realmente incomprensible para quien no posee la clave de desciframiento, y

c) El sistema biométrico, que toma como elementos identificatorios los rasgos y características físicas del ser humano y aunque se encuentra en periodo de experimentación, se considera ya como el único instrumento que asegura la función de autenticación.

A partir de la fusión de la informática con las nuevas tecnologías de telecomunicación, surge la transferencia electrónica de datos

informatizados (TEDI) que permite reemplazar el documento papel en las transacciones comerciales a nivel internacional. En el año de 1986, americanos y europeos elaboraron un lenguaje común para la transmisión de datos informatizados en la administración, el comercio y el transporte (TEDIFACT); esta norma-lenguaje permite armonizar y estandarizar los documentos comerciales.¹⁸¹

Consecuencia de estos lenguajes ha sido la desmaterialización de documentos, pues en realidad se intercambian mensajes en lugar de documentos comerciales por escrito; es decir, a partir de la TEDI, se suprimen los documentos escritos que podrían servir de prueba en caso de litigio o controversia; además, los documentos de las TEDI se considera que no son diferentes de los demás documentos producidos por medios informáticos; esto es, generalmente se determina que no tienen ningún valor jurídico en materia probatoria.

Los medios de prueba que admiten hoy en día las nuevas tecnologías de la información se basan en el peritaje, como medio de búsqueda atribuible al juez, con la consiguiente duda de su efectividad si consideramos la probabilidad de que el juez no sea experto en materia informática.

Por otro lado, podemos señalar que, en materia probatoria sobre las nuevas tecnologías en la información, la legislación ha mantenido el principio de la prueba por escrito; es decir, no reconoce valor probatorio a los documentos electromagnéticos. Además, debemos partir de la constante supresión que la informática ha hecho del documento escrito (papel) y de que existe, opuesto al sistema legal de la prueba, la libertad de apreciación del juez como característica fundamental.

La jurisprudencia en algunos países miembros de la Comunidad Europea ha constatado, en el caso de la TEDI, la imposibilidad de constituir un escrito, y considera los registros y documentos de naturaleza informática como un principio de prueba por escrito. A

181 *Cfr.* Carrascosa López, Valentín *et al.*, *El derecho de la prueba y la informática*, Mérida, UNED, Centro Regional de Extremadura, 1991, pp. 17 y ss.

pesar de lo anterior, algunos países les reconocen igual valor probatorio que los documentos escritos; otros hacen depender dicho valor con base en la convención entre las partes, y, en su mayoría, se inclinan por permitir al juez amplia libertad para decidir sobre su valor o no.

Las pruebas que pueden derivar de una relación jurídica en la que intervenga el documento electrónico, y que Miguel Ángel Davara¹⁸² considera que se pueden hacer valer tanto en su ofrecimiento como en su perfeccionamiento, son las siguientes: los propios documentos electrónicos, confesión, inspección personal del juez, peritos, testigos y presunciones. Respecto a ellas señala:

a) Entendemos por documento electrónico, el soporte o el medio donde queda constancia de los datos, del proceso, de los resultados o de las decisiones, de un sistema electrónico, informático o telemático de cualquier tipo. [Davara habla de documento informático en tres aspectos]: 1) los listados en papel “printout”; 2) los que se encuentran en soporte de información electrónico “input”, y 3) el formado mediante el intercambio de mensajes.

b) Por confesión de las partes [prueba que se desahogará], sobre la certeza y veracidad de los documentos generados por procedimientos electrónicos e informáticos aportados y unidos a los autos.

c) Por prueba pericial [la cual se llevará a cabo respecto], del documento generado por procedimiento electrónico e informático, sobre su contenido y autenticidad, que sea de influencia en el pleito; designando el documento electrónico o la cosa que ha de ser objeto de pericia y señalando en qué consistirá la pericia y si han de ser uno o tres los peritos que se nombren para llevarlo a efecto.

Como prueba de autenticidad de algún documento o registro electrónico pueden valer las encriptaciones, codificaciones, claves, o también los registros internos generados por el reloj del sistema, por *reports* [sic] automáticos, configuraciones, etcétera; el experto en ordenadores, facilitará la determinación del objeto de la pericia y su presentación.

d) Por reconocimiento judicial [que, bajo nuestro sistema jurídico sería la inspección judicial, sería en relación] con las instalaciones que han generado el documento electrónico o informático, para determinar la autenticidad del mismo o el proceso de su elaboración, y posibles manipulaciones

e) Por testigos, es decir personas no inhábiles que por cualquier razón, hayan estado presentes en el proceso electrónico o en la generación o manipulación del documento.

f) Las presunciones, tienen el carácter de medio supletorio de prueba.

182 Davara, Miguel Ángel, citado por Barriuso Ruiz, Carlos, *Interacción del derecho y la informática*, pp. 230 y ss.

Respecto a la prueba presuncional, es importante señalar que la recomendación R (81) 20, adoptada por el Comité de Ministros del Consejo de Europa, durante la 341 reunión de delegados de los ministros el 11 de diciembre de 1981 relativa a la armonización de las legislaciones en materia de admisibilidad de las reproducciones de documentos y de registros informáticos, recomienda salvo prueba en contrario, cuya carga la soportará quien los tache de inexactos o falsedad, la presunción de validez de los documentos o registros informáticos y electrónicos, siempre que sean una reproducción y registro fiel y completo de los documentos o registros originales y de su contenido. Con las debidas garantías respecto a la fiabilidad del origen del documento, con su contenido y la seguridad de su almacenamiento, para poder compulsarlos cuando se necesite. Por lo que si la prueba en contrario, acredita completamente que el documento original del que se deduce, está manipulado o no es auténtico, queda desvirtuada la presunción.

También aconseja la recomendación (R81), determinar qué documentos deben conservarse y en qué forma: si por micrografía o por medio del ordenador para su ulterior presentación, estableciendo el modo de compulsar las copias, regular la admisibilidad y cotejo de las pruebas realizadas por procedimientos informáticos y ópticos; normalizando y homologando los documentos informáticos e indicando las transformaciones y tratamiento sufrido, a fin de evitar manipulaciones y garantizar su autenticidad y originalidad, recomendándose la presunción de validez de los documentos electrónicos entendidos como reproducción y registro fiel de los documentos originales y de su contenido, que obren en el sistema informático, residentes o no, o en el almacenamiento interno o externo, estableciendo medidas de seguridad adecuadas para evitar la manipulación y alteración de los registros.¹⁸³

El uso del documento electrónico o electromagnético se va incorporando cada vez más en nuestro uso cotidiano, por lo que

183 *Ibidem*, p. 232.

también se empieza a admitir como soporte válido en soportes electrónicos e informáticos ya sea magnético, óptico o impreso.

En el caso de México, algunas disposiciones legislativas ya empiezan a contemplar estos usos o soportes. En el apéndice se recogen estas normas legales.