DERECHO INFORMÁTICO

DERECHO INFORMÁTICO

Cuarta edición

Julio Téllez Valdés
Instituto de Investigaciones Jurídicas
Universidad Nacional Autónoma de México

MÉXICO • BOGOTÁ • BUENOS AIRES • CARACAS • GUATEMALA •
LISBOA • MADRID • NUEVA YORK • SAN JUAN • SANTIAGO •
AUCKLAND • LONDRES • MILÁN • MONTREAL • NUEVA DELHI •
SAN FRANCISCO • SINGAPUR • SAN LUIS • SIDNEY • TORONTO

Director Higher Education: Miguel Ángel Toledo Castellanos
Director editorial: Ricardo Alejandro del Bosque Alayón
Coordinadora editorial: Marcela I. Rocha Martínez
Editor sponsor: Noé Islas López
Editor de desarrollo: Edmundo Carlos Zúñiga Gutiérrez
Supervisor de producción: Zeferino García García

DERECHO INFORMÁTICO
Cuarta edición

Educación

A Subsidiary of ***The McGraw-Hill*** *Companies, Inc.,*
Prolongación Paseo de la Reforma 1015, Torre A,
Piso 17, Colonia Desarrollo Santa Fe,
Delegación Álvaro Obregón
C.P. 01376, México, D. F.
Miembro de la Cámara Nacional de la Industria Editorial Mexicana, Reg. Núm. 736

ISBN-13: 978-970-10-6964-6
(ISBN de la edición anterior: 970-10-4306-5)

0123456789 **08765432109**

Impreso en México **Printed in Mexico**
Impreso por Impacto en Medios Publicitarios, S.A. de C.V. **Printed by Impacto en Medios Publicitarios, S.A. de C.V.**

The ***McGraw-Hill*** *Companies*

A Dios, a quienes creemos y a quienes dicen no creer en Él.
A mi querida esposa y a mis hijos.
A mis familiares, amigos y enemigos.
A todos los amables lectores.
A los niños del mundo, a quienes tantas veces olvidamos.

Me interesa el futuro porque en él voy a pasar el resto de mi vida.

Nicolás Mancini

Contenido

Acerca del autor

Julio Alejandro Téllez Valdés es licenciado en Derecho por la Universidad La Salle en la Ciudad de México. Recibió el grado de doctor en Derecho informático por la Universidad de Montpelier, Francia. Es profesor de posgrado en materia de Derecho y nuevas tecnologías de la información y comunicación en diversas universidades públicas y privadas a nivel nacional e internacional, multiconferencista a nivel nacional y mundial, e investigador titular de tiempo completo en el Instituto de Investigaciones Jurídicas en el área de Derecho y nuevas tecnologías de la UNAM. Obtuvo una distinción para jóvenes académicos en el área de investigación de ciencias sociales, otorgada por la UNAM.

Asimismo, es vicepresidente de la Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI) e investigador nacional en el Sistema Nacional de Investigadores.

Prólogo a la cuarta edición

Sin pretender generalizar, desafortunadamente es práctica común en algunas editoriales, incluyendo a aquéllas de corte jurídico, que incorporen en sus obras ya editadas algunos elementos mínimos y con ello hablen ya de una "nueva edición".

Si mi amable y fiel lector tiene el cuidado de revisar las tres ediciones anteriores de *Derecho informático*, se dará cuenta de que siempre he pretendido incorporar elementos nuevos, o al menos originales, en cada una de ellas. Pretendo que esta cuarta edición no sea la excepción, por lo que, como es mi costumbre, pongo a su muy respetable consideración el contenido de la misma, siempre susceptible de mejora, esperando poder colmar sus expectativas. Aclaro que en caso de no lograrlo, trabajaré con ahínco mientras Dios me dé vida, para no volver a decepcionarlos.

El autor

Introducción

Han pasado casi 30 años desde la primera vez que hablé en México de la necesidad de vincular al Derecho con la Informática (hoy con las nuevas tecnologías de información y comunicación) como instrumento y como objeto de estudio.

El término *jurismática* ha quedado como un recuerdo perenne en personas como Daniel León García y un servidor para dar paso al **Derecho informático** y, quizás de manera más genérica, al **Derecho de las nuevas tecnologías**.

En esta cuarta edición se mantiene la mística de la obra, con algunas inevitables incorporaciones a nivel de nuevos temas como el *spam*, con cifras actualizadas y documentos fundamentalmente legislativos en el rubro *Anexos*, que vienen a dar cuenta en términos prácticos, para bien o para mal, de la manera en que se están abordando a nivel nacional e internacional las problemáticas derivadas de esta interdisciplina.

No es fácil, mas sí placentero, incursionar en esta materia habida cuenta del incesante dinamismo de la ciencia y las nuevas tecnologías. Es un reto a la vez que una obligación para quienes nos preciamos de ser orgullosos portadores del título de Licenciado en Derecho, motivados siempre por la sociedad a la cual nos debemos.

Actualicémonos entonces, al menos por el momento, en todas estas fascinantes evoluciones que traen consigo estas nuevas tecnologías y asumamos **todos** ese reto de tratar de entenderlas y sobre todo encauzarlas hacia una mejor vida para nosotros y, muy en especial, para las nuevas generaciones que en muchas ocasiones soslayamos.

EL AUTOR

Consideraciones finales

Reitero mi costumbre de hablar de *consideraciones finales* y no tanto de *conclusiones*, ya que la única conclusión válida es la que tengan los apreciables lectores de esta obra.

Hasta aquí, tenemos algunos elementos doctrinarios y faltaría revisar aquéllos de orden fundamentalmente legislativo incluidos a continuación en el rubro *Anexos*.

Es incuestionable cómo las nuevas tecnologías de información y comunicación nos proveen día con día más elementos para buscar un reposicionamiento de la alicaída imagen del Derecho frente a la sociedad y, por otro lado, las problemáticas derivadas por el mal uso de dichas tecnologías y que obligan a una adecuada regulación jurídica.

Nadie dice que estas tecnologías sean elemento imprescindible para que un jurista alcance niveles paradigmáticos, pero considero que están ahí esperándonos y ofreciéndonos la oportunidad de ser mejores y ¿quién si no es un pusilánime o mediocre no aspira a ser mejor en esta vida? Por lo que respecta a la regulación jurídica, este sendero es inevitable para quienes tenemos claro el compromiso con la sociedad, en este caso de la información y comunicación a la cual nos debemos.

Ignoro qué nos depara el futuro, pero lo que sí me queda claro es que no debemos asumir posiciones confortables de "tecnodependencia" o fatalistas de no poder hacer nada; debemos seguir intentando trascender con el ánimo de lograrlo, y si no, al menos no pasar inadvertidos o ignominiosos en nuestro de por sí efímero paso por este mundo.

Gracias por leer esta obra.

EL AUTOR

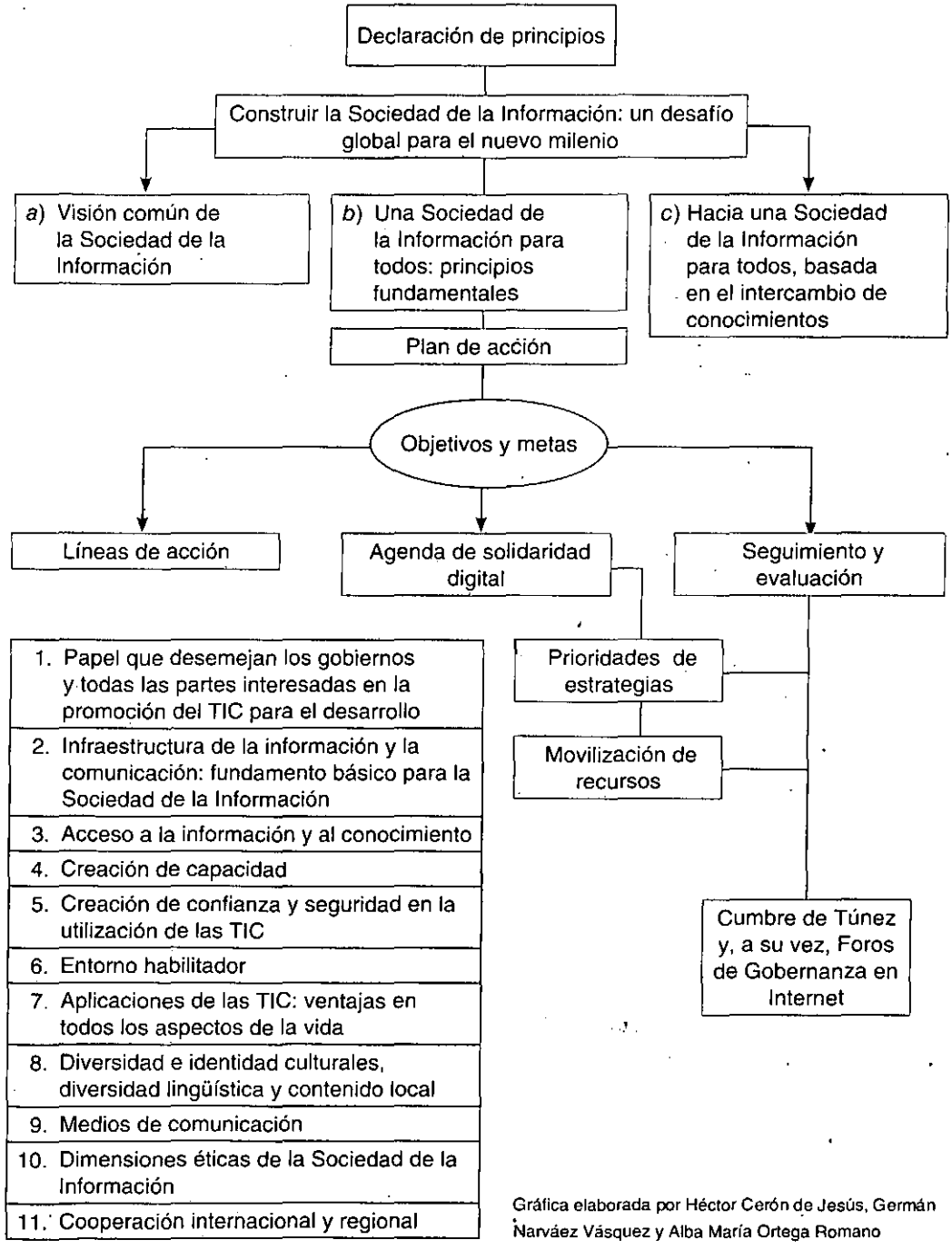
I. Sociedad, tecnología y derecho

SOCIEDAD DE LA INFORMACIÓN Y DEL CONOCIMIENTO

De acuerdo con la ONU, la *revolución* digital en las tecnologías de la información y las comunicaciones (TIC) ha creado una plataforma para el libre flujo de información, ideas y conocimientos en todo el planeta. Internet se ha convertido en un importante recurso, que resulta vital tanto para el mundo desarrollado por su función de herramienta social y comercial, como para el mundo en crecimiento por su función de pasaporte para la participación equitativa y la evolución económica, social y educativa. El objetivo de la Cumbre Mundial de la Sociedad de la Información es garantizar que estos beneficios sean accesibles para todos y fomentar ciertas ventajas específicas en algunos campos, como estrategias, comercio electrónico, gobierno electrónico, salud, educación, alfabetización, diversidad cultural, igualdad de género, desarrollo sustentable y protección del medio ambiente. En la Cumbre de Ginebra, de diciembre de 2003, los líderes mundiales declararon: "Es nuestro deseo y compromiso comunes construir una Sociedad de la Información centrada en la persona, integradora y orientada al desarrollo, en la que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su crecimiento sostenible y en la mejora de su calidad de vida, con base en los propósitos y principios de la *Carta de las Naciones Unidas* respetando y defendiendo plenamente la *Declaración Universal de los Derechos Humanos*."[1]

[1] Cumbre Mundial de la Sociedad de la Información 2003, disponible en línea, URL:http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160|1164, consultada el 29 de mayo de 2008.

Puntos principales derivados de la Cumbre Mundial de la Sociedad de la Información de Ginebra (2003) para este milenio



Gráfica elaborada por Héctor Cerón de Jesús, Germán Narváez Vásquez y Alba María Ortega Romano

Gobernanza en Internet

El Foro de Gobernanza en Internet es convocado desde 2006 por la Organización de las Naciones Unidas en cumplimiento del mandato recibido por los acuerdos surgidos de la Cumbre Mundial de la Sociedad de la Información, realizada en dos fases: la primera en Ginebra en 2003 y la segunda en Túnez en 2005. El Compromiso de Túnez constituye el marco político de la Cumbre de Túnez. En el documento, los gobiernos retiran su apoyo categórico a la Declaración de Principios de Ginebra y al Plan de Acción adoptados en Ginebra.

Los propósitos de este foro se establecen en los párrafos 72 a 79 de la Agenda de Túnez para la Sociedad de la Información. El primer foro se celebró en Atenas en octubre de 2006 y el segundo en noviembre de 2007 en Río de Janeiro, Brasil. El tercero tendrá lugar en Hyderabad, India, del 3 al 6 de diciembre de 2008, y para el cuarto foro en 2009 se tienen las propuestas de Lituania y Azerbaiján.

El Foro de Gobernanza de Internet[2] es una reunión que, de alguna forma, rompe el molde tradicional de Naciones Unidas, ya que se trata de un *nuevo modelo de cooperación internacional* que, como internet, está en constante evolución. Como dice José Soriano, este foro no es un espacio creado para tomar decisiones o para negociar, sino para reunir a personas provenientes de los sectores privado y gubernamental y de la sociedad civil con el fin de favorecer el intercambio de informaciones y compartir buenas prácticas y aprendizajes.

Entre las temáticas más significativas en el Foro de Río de acuerdo con los ejes de la dimensión de desarrollo y la capacitación, se plantearon como prioridades las siguientes:

1. *Acceso*: referido a los problemas especiales de conectividad que enfrentan África y los países menos desarrollados, sin litoral e insulares; los desafíos del acceso en las áreas rurales; el desarrollo de destrezas y capacidades en el uso de la tecnología; las soluciones de acceso de bajo costo; el acceso inalámbrico y móvil; la fiabilidad de infraestructura internacional, políticas de conectividad y costos; la interconexión local y regional y la regulación transfronteriza; el efecto económico del acceso, y temas relacionados con la neutralidad de la red, uno de los más polémicos dado que las empresas de telecomunicaciones obtuvieron un visto favorable del Departamento de Justicia de Estados Unidos para dar un tratamiento diferenciado a los paquetes de información que trafican por internet, lo que despertó las protestas de los defensores de la democratización de las comunicaciones.

[2] Véase http://www.intgovforum.org/ consultada el 27 de mayo de 2008.

En términos generales, la demanda de la sociedad civil en torno al acceso se basa en la creación de un mecanismo internacional de compensaciones que regule la composición de precios para reducir desequilibrios y no dejar a los países que más necesitan conexiones baratas a merced de los poderes que controlan las telecomunicaciones y los recursos de internet.

2. *Recursos críticos de internet*: en este caso lo relativo a infraestructura, administración del sistema de dominios de nombre y protocolos de internet (IP), administración del sistema de servidores raíz, estándares técnicos, interconexión, infraestructura de las telecomunicaciones, incluidas convergencia tecnológica y multilingüístico.
3. *Diversidad*: concerniente a la generación de contenidos locales, el papel de los estándares abiertos en la promoción de la diversidad, políticas públicas y generación de contenidos de parte de los(as) usuarios(as), las comunidades lingüísticas que desarrollan nombres de dominio internacionalizados y contenido multilingüístico, entre otras cuestiones.
4. *Apertura*: involucró discusiones en torno a la libertad de expresión y el rol de los gobiernos en la protección de ese derecho, de la privacidad y su relación con la libertad de expresión, software libre, software propietario y estándares abiertos, los desafíos en cuanto al acceso a información y conocimiento, relaciones entre regulaciones nacionales sobre libertad de expresión y un internet sin fronteras, entre muchos otros puntos.
5. *Seguridad*: amenazas a la seguridad como ciberdelitos, ciberterrorismo, la cooperación internacional en estos temas, seguridad de los recursos de internet, desafíos a la privacidad en un ambiente de seguridad (relativos a la libertad de expresión, privacidad e identidad, privacidad y desarrollo), cuestiones de seguridad relativas a la infancia y protección de niños y niñas del abuso y la explotación en ambientes en línea.

   El tema de la explotación sexual infantil a través de las TIC fue recurrente en varios talleres y las reflexiones de todos los involucrados giraban en torno a la advertencia de que el mundo *online* supone los mismos riesgos y demanda el mismo respeto a los derechos básicos que el *offline*. Ambos mundos están entrelazados, por lo cual no hay que pensar que la virtualidad del mundo en línea es menos riesgosa que, por ejemplo, salir a la calle y subir al auto de un desconocido.
6. *Temas emergentes*: implicaciones políticas de internet móvil y tecnologías inalámbricas, así como las referidas a los contenidos generados por los(as) usuarios(as), entre otros.

Entre las propuestas concretas tenemos la referida a la formación de una Coalición Dinámica sobre Género y Gobernanza de Internet, así como otra presentada por el Consejo de Europa (intergubernamental) y la Aso-

ciación para el Progreso de las Comunicaciones (sociedad civil), relativo a la elaboración de un código para la participación pública en la gobernanza de internet. Se trata de un mecanismo autorregulador para fomentar la participación, el acceso a la información y la transparencia en la gobernanza de internet, que refleja el compromiso del Consejo de Europa con el concepto de valor de servicio público de internet.

Características de la cibernética

Antes de analizar la informática propiamente dicha es menester hacer unas breves alusiones al rubro general de donde se desprende, es decir, la cibernética.

Orígenes

En 1948, un matemático estadounidense, Norbert Wiener, escribió un libro titulado *Cibernética*, y empleó este término para designar a la *nueva ciencia de la comunicación y control entre el hombre y la máquina*.[3]

Friedrich Engels, en su *Dialéctica de la naturaleza*, manifestó que "en los puntos de unión o de contacto, entre las distintas ciencias, es donde se pueden esperar los mejores resultados", es decir, hablaba desde entonces, de la importancia de la interdisciplina.

Nociones y concepto

Si atendemos a la etimología de la palabra, el vocablo *cibernética* tiene su origen en la voz griega *kybernetes* "piloto" y *kybernes*, concepto referido al arte de gobernar. Esta palabra alude a la función del cerebro respecto a las máquinas.

Características de la informática

Una vez desentrañadas las generalidades básicas de la cibernética, procedamos a hacer algunas puntualizaciones en torno a la informática.

Orígenes

El término *informática* surge de la misma inquietud racional del hombre, el cual, ante la continua y creciente necesidad de información para una

[3] Wiener, Norbert, *Cibernética o el control y comunicación en animales y máquinas*, 1a. edición, Barcelona, Tusquets Editores, 1985, págs. 191-193, de 266 páginas.

adecuada toma de decisiones, es impulsado a formular nuevos postulados y diseñar nuevas técnicas que satisfagan dichos propósitos.

Nociones y concepto

La palabra *informática* es un neologismo derivado de los vocablos información y automatización, sugerido por Phillipe Dreyfus en 1962. En sentido general, podemos considerar que la informática es un conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información con miras a una adecuada toma de decisiones.

Características de las computadoras

Habida cuenta de que los instrumentos operativos de la informática son las computadoras se torna necesario, en estas condiciones, exponer los principales rasgos de éstas.

Generaciones

En la llamada *primera generación* de computadoras se utilizaron bulbos de alto vacío como componentes básicos de sus circuitos internos. En consecuencia, eran demasiado voluminosas, consumían mucha energía y producían calor; a pesar de que no fueron tan confiables como se había esperado, eran rápidas pero no lo suficiente y tenían capacidad de almacenamiento interno, aunque limitado.

La *segunda generación* consistió en el uso de transistores que redujeron las deficiencias y mejoraron las ventajas existentes, introduciendo las memorias de ferrita que permitieron reducir el tamaño, con lo cual surgió la segunda generación de computadoras.

En 1963 aparecieron en el mercado las computadoras de la *tercera generación*, en las que encontramos como principal característica el uso de circuitos integrados monolíticos, que aumentaron considerablemente la velocidad de operación, incrementando su confiabilidad y disminuyendo su costo y tamaño.

Posteriormente, la *cuarta generación* existe con la integración a larga escala (LSI, por sus siglas en inglés) y la aparición de microcircuitos integrados en plaquetas de silicio (microchips).[4]

[4] Cabe decir que la quinta generación es o será aquella conformada por las computadoras basadas en la nanotecnología, es decir, la nanocomputadora, que es una computadora con una circuitería tan pequeña que sólo puede verse a través de un microscopio. Las nanocomputadoras pueden ser

Concepto y estructura

1. A nivel operacional podemos conceptuar la computadora como una máquina automatizada de propósito general, integrada por elementos de entrada, procesador central, dispositivo de almacenamiento y elementos de salida.

   a) *Elementos de entrada.* Representan la forma de alimentación e información a la computadora, por medio de datos e instrucciones realizados por equipos periféricos, como pantallas, cintas, discos, etcétera.
   b) *Procesador central.* Dispositivo en el que se ejecutan las operaciones lógico-matemáticas, conocido más comúnmente como unidad central de procesamiento (CPU, por sus siglas en inglés). Su velocidad actualmente se mide en gigahertz.
   c) *Dispositivo de almacenamiento.* Contiene o almacena la información a procesar. Su capacidad se mide actualmente en terabytes.
   d) *Elementos de salida.* Medios en los que se reciben los resultados del proceso efectuado: pantalla, impresora, etcétera.

2. Por otra parte, a nivel estructural la computadora está integrada por los siguientes elementos:

   a) *Hardware.* Constituido por las partes mecánicas, electromecánicas y electrónicas, como la estructura física de las computadoras, encargadas de la captación, almacenamiento y procesamiento de información, así como la obtención de resultados.
   b) *Software.* Constituye la estructura lógica que permite a la computadora la ejecución de las actividades. Actualmente es más importante que el propio hardware.

Lenguajes de programación

Para que las computadoras puedan funcionar en los términos adecuados es necesario emplear los llamados *lenguajes de programación*, aquellos

---

electrónicas (donde la nanolitografía se usa para crear los circuitos microscópicos), bioquímicas u orgánicas (como el caso de las computadoras de ADN) o cuánticas (como en las computadoras cuánticas), etc. Las nanocomputadoras se componen de materiales a nivel molecular y son la promesa de crear computadoras cada vez más pequeñas y rápidas, un concepto muy importante en el mundo de la computación. Las nanocomputadoras, de un tamaño tan diminuto como varias moléculas, aún no son un hecho, pero su construcción está cada vez más cerca. También denominadas nanocomputadoras electrónicas químicamente ensambladas (CAEN, por sus siglas en inglés).

medios que permiten la comunicación entre el hombre y la máquina, es decir, entre la computadora y el usuario.

Entre los principales lenguajes de programación tenemos: Fortran (1957, fórmula traductora), Algol (1958, lenguaje algorítmico), Basic (1958, código de instrucciones simbólicas para principiantes de todo propósito), Cobol (1960, lenguaje orientado a negocios comunes) y posteriormente el Pascal, ADA, PL/I, Cande, APL, Prolog, LISP, Visual Basic, HTML, Javascript, Linux, etcétera.

Características fundamentales del derecho informático

Antecedentes

El derecho informático, como una nueva rama del conocimiento jurídico, es una disciplina en continuo desarrollo, que tiene en su haber (al menos hasta esta fecha) nuevos antecedentes a nivel histórico; empero, podemos decir que las alusiones más específicas sobre esta interrelación existen a partir de 1949 con la obra de Norbert Wiener,[5] en cuyo capítulo 4, dedicado al derecho y las comunicaciones, expresa la influencia que ejerce la cibernética respecto a uno de los fenómenos sociales más significativos: el jurídico. Dicha interrelación se da a través de las comunicaciones, a lo que habría que agregar que si bien estos postulados tienen cerca de 40 años, en la actualidad han adquirido matices que probablemente ni el mismo Wiener hubiera imaginado. Así, esta ciencia de entrelazamiento interdisciplinario sugería una conjunción aparentemente imposible entre los mundos del ser y del deber ser.

Por otra parte, en ese año el juez estadounidense Lee Loevinger publicó un artículo de 38 hojas en la revista *Minnesota Law Review* titulado "The Next Step Forward", en el que menciona que "el próximo paso adelante en el largo camino del progreso del hombre debe ser el de la transición de la teoría general del derecho hacia la jurimetría, que es la investigación científica acerca de los problemas jurídicos..."

Cabe señalar que estas primeras manifestaciones interdisciplinarias ocurrían en los términos instrumentales de las implicaciones informáticas respecto al derecho, los cuales se desarrollaron extraconceptualmente en la década de 1950. A diferencia del estudio de las implicaciones jurídicas motivadas por la informática, en los términos de un derecho informático se considera una serie de implicaciones de orden social, económico, técnico, práctico y evidentemente jurídico, suscitadas por el uso de la informática, como veremos en líneas subsecuentes.

[5] Wiener, Norbert, *Cibernética y sociedad, cap. IV, Derecho y comunicaciones.* FCE, México, 1980.

Concepto y clasificación

Aunque difícil de conceptuar por el variado número de peculiaridades y muy a pesar de los opuestos puntos de vista que pudiera provocar, cabe decir que el derecho informático es una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática).

En función de lo anterior, es notorio que la clasificación del derecho informático obedece a dos vertientes fundamentales: la informática jurídica y el derecho de la informática (considerado por algunos o de manera tangencial y, a mi manera de ver, equivocada, como el derecho informático).

Informática jurídica

Orígenes

La informática, como uno de los fenómenos más significativos de los últimos tiempos (según hemos visto), deja sentir su incontenible influjo en prácticamente todas las áreas del conocimiento humano (ciencias del ser y del deber ser), entre las cuales el derecho no puede ser la excepción y da lugar, en términos instrumentales, a la llamada informática jurídica.

En sentido general, podemos decir que la informática jurídica es el conjunto de aplicaciones de la informática en el ámbito del derecho.

Nacida propiamente en 1959 en Estados Unidos, la informática jurídica ha sufrido cambios afines a la evolución general de la misma informática. Las primeras investigaciones en materia de recuperación de documentos jurídicos en forma automatizada se remontan a los años de la década de 1950, cuando se comienzan a utilizar las computadoras no sólo con fines matemáticos, sino también lingüísticos. Estos esfuerzos fueron realizados en el Health Law Center (HLC) de la Universidad de Pittsburgh, Pensilvania. El entonces director del centro, John Horty, estaba convencido de la necesidad de encontrar medios satisfactorios para tener acceso a la información legal. En 1959, el centro colocó los ordenamientos legales de Pensilvania en cintas magnéticas. El sistema fue posteriormente demostrado, en 1960, ante la American Bar Association (ABA) (Asociación Americana de la Barra de Abogados) en la reunión anual celebrada en Washington, D.C. Ésta fue la primera demostración de un sistema legal automatizado de búsqueda de información.

Nociones y concepto

Si bien es difícil dar una definición de la informática jurídica, como suele suceder con las disciplinas de reciente surgimiento, cabe decir que se tra-

ta, en última instancia, de la utilización de las computadoras en el ámbito jurídico.

En términos generales es válido afirmar que la informática jurídica es "la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como a la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación".

Diferentes denominaciones

La interrelación informática-derecho ha dado lugar a numerosas denominaciones, entre las que destacan, por mencionar sólo algunas de ellas, las siguientes:

a) La primera denominación fue el término *jurimetrics* (en español jurimetría), creado por el juez estadounidense Lee Loevinger en 1949.[6]
b) La segunda fue la de giuscibernética (en español juscibernética), ideada por Mario G. Losano, quien en su libro *Giuscibernética* sostiene que la cibernética aplicada al derecho ayuda no sólo a la depuración cuantitativa de éste, sino también a la cualitativa. En su obra también figura la fundamentación filosófica de la relación del derecho con la informática.[7]

Hay otras denominaciones, como las siguientes:

- *Computers and Law* (países anglosajones).
- *Rechtsinformatique* (antes Elektronische Datervera beitung und Recht en Alemania).
- Jurismática (México).

Con todo, la más conveniente en términos prácticos es, sin duda alguna, la de informática jurídica (*informatique juridique*) y derecho de la informática (*droit de l'informatique*), creadas por los franceses y aglutinadas según mi parecer en una sola disciplina, en este caso el derecho informático.

Evolución

La década de los años 1960 marcó el desarrollo de varios sistemas diversos de los mencionados en los orígenes de la informática jurídica. En 1964 la

[6] Loevinger, L., "The Next Step Forward", en *Minessota Law Review*, vol. XXXIV, 1949, pp. 455-493; y "Science and Predictions and Field of Law", *ibid.*, vol. CLXXVIII, 1961, pp. 255-275.
[7] Losano, M. *Nouvi Siuluppi della Sociologia del Diritto*, 1960, p. 101.

Corporación Americana de Recuperación de Datos comenzó a comercializar sistemas de procesamiento de datos legislativos.

Una siguiente incursión la realizó la Corporación de Investigación Automatizada de la Barra de Ohio (OBAR, por sus siglas en inglés) diferente de las dos primeras experiencias del HLC comentadas ya que fue enfocada hacia los abogados litigantes.

El sistema OBAR comenzó en 1967 cuando la barra del estado de Ohio firmó un contrato con la Corporación de Datos de Dayton, Ohio. Los trabajos de este sistema continuaron en 1970 por medio de la Mead Data Central (CMD), que fue constituida luego de la fusión de Data Corporation con Mead Corporation. En 1973 la Mead Data Central comenzó a comercializar el sistema LEXIS como sucesor del OBAR, hoy día el sistema de informática jurídica más importante y rentable en el mundo.

Clasificación

En sus primeros años, la informática jurídica se presentó en términos de una informática documentaria de carácter jurídico, es decir, creación y recuperación de información que contenía datos principalmente jurídicos (leyes, jurisprudencia y doctrina) o al menos de interés jurídico. Poco a poco empezó a vislumbrarse la idea de que de estos bancos de datos jurídicos se podían obtener no sólo informaciones sino también, mediante programas estudiados expresamente, verdaderos actos jurídicos, como certificaciones, atribuciones de juez competente, sentencias premodeladas. Así, a fines de los años de 1960 nació la llamada informática jurídica de gestión.

Finalmente, al ver que las informaciones y los procedimientos eran fidedignos y permitían lograr buenos resultados, surgió lo que hoy es considerado por algunos tratadistas como los sistemas expertos legales (informática jurídica metadocumentaria).

Desde hace varios años, la informática jurídica ha permitido un mejor conocimiento de los fenómenos jurídicos, por lo que muchos juristas, anteriormente escépticos e indiferentes, han encontrado en la computadora un instrumento eficaz para mejorar sus actividades.

De esta forma, merced a la informatización en el campo del derecho, se han constituido diferentes tipos de archivos (legislativos, de jurisprudencia, doctrinales, bibliográficos, etc.), los cuales representan un potencial informativo insospechado, además de que constituyen un apoyo rápido y eficaz en la realización de actividades de gestión, así como una ayuda en la toma de decisiones en la educación e investigación, por mencionar sólo algunos campos, lo cual representa un hecho sin precedente dentro del ámbito jurídico.

Con base en lo anterior es posible clasificar dicha interdisciplina de la siguiente manera:

a) Informática jurídica documentaria (almacenamiento y recuperación de textos jurídicos).
b) Informática jurídica de control y gestión (desarrollo de actividades jurídico-adjetivas).
c) Sistemas expertos legales o informática jurídica metadocumentaria (apoyo en la decisión, educación, investigación, redacción y previsión del derecho).

Derecho de la informática

Antecedentes y evolución

Como se dijo anteriormente, si bien es cierto que los precursores informáticos nunca imaginaron los alcances que llegarían a tener las computadoras en general o aun en campos tan aparentemente fuera de influencia como el jurídico, hubiera sido todavía más difícil concebir que el derecho llegaría a regular a la informática.

De esa manera, a finales de la década de 1960 y luego de cerca de 10 años de aplicaciones comerciales de las computadoras, empezaron a surgir las primeras inquietudes respecto a las eventuales repercusiones negativas motivadas por el fenómeno informático, las cuales requerían un tratamiento especial.[8]

Nociones y concepto

El derecho de la informática, como instrumento regulador del fenómeno informático en la sociedad, no ha sido estudiado del mismo modo que la informática jurídica, porque se ha dado más importancia a los beneficios que a los eventuales perjuicios que puedan traer consigo las computadoras respecto al derecho y la sociedad en general.

Entre el reducido grupo de tratadistas sobre el derecho de la informática, algunos consideran a éste una categoría propia que obedece a sus reglas, que surge como una inevitable respuesta social al fenómeno infor-

[8] Cabe mencionar que dichas inquietudes surgieron respecto a la influencia que ejercía la tecnología en general. Ya desde la gestación de la Revolución Industrial se dejaban entrever las modificaciones sociales no necesariamente positivas provocadas por las máquinas.

mático, y que por ello es un derecho en el que su existencia precede a su esencia.[9]

Si el punto anterior implica dificultades, qué decir de la conceptualización de este derecho de la informática. Sin duda alguna que esta área, al igual que la informática jurídica, permite una creatividad muy amplia, sin que esto necesariamente trascienda a niveles demasiado imaginativos o especulativos.

De acuerdo con esa tónica, cabe enunciar el siguiente concepto de derecho de la informática: "es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática".

Ahondando un poco sobre este concepto, resulta válido decir que es un *conjunto de leyes* en cuanto que, si bien escasos, existen varios ordenamientos jurídicos nacionales e internacionales con alusión específica al fenómeno informático. *Normas* en virtud de aquellas que integran la llamada política informática, la cual, según se verá posteriormente, presenta diferencias respecto a la legislación informática. *Principios* en función de aquellos postulados emitidos por jueces, magistrados, tratadistas y estudiosos respecto al tema. Por otra parte, se refiere a *hechos* como resultado de un fenómeno aparejado a la informática inimputable al hombre. Por último, se alude a *actos* como resultado de un fenómeno directamente vinculado con la informática y provocado por el hombre.

Fuentes

Para atribuir una eventual autonomía a esta disciplina jurídica es menester hacer alusión, entre otras cosas, a las fuentes de donde emana propiamente este conjunto de conocimientos.

En el nivel interdisciplinario están aquellas provistas por el mismo derecho como es el caso de la legislación, que como se mencionó, es relativamente incipiente al respecto; no obstante, aquí cabría señalar aquellas disposiciones sobre otras áreas caracterizadas por guardar un nexo estrecho en referencia al fenómeno informático, como los ordenamientos en materia constitucional, civil, penal, laboral, fiscal, administrativa, procesal, internacional, etcétera.

Asimismo, en cuanto a la jurisprudencia, doctrina y literatura sobre el particular, existen algunos pronunciamientos, teorías y artículos relacionados con los problemas jurídicos suscitados por la informática.

Por otra parte, en cuanto a las fuentes transdisciplinarias están aquellas provistas por ciencias y técnicas, como la filosofía, la sociología, la economía, la estadística y la comunicación, entre otras, y, desde luego, la informática.

[9] *Véase* Michel Vivant y cols., *Droit de l'informatique*, Lamy, París, 2002.

Política informática

Para un desarrollo informático adecuado es necesario planificar por medio de normas que a su vez conforman una política (en este caso informática) diferente de una legislación en cuanto a que esta última se refiere a aspectos más específicos.

Así, entre esta política informática algunos de los principales puntos contemplados son el adecuado desarrollo de la industria de construcción de equipos de cómputo y de programación; por otra parte, la planeación, difusión y aplicación del fenómeno informático, la contratación gubernamental de bienes y servicios informáticos, la formulación de normas y estándares en materia informática, y el control de importaciones y exportaciones sobre equipos, accesorios y programas de computadoras, etc.; empero, esto no es suficiente para mantener a la informática en los términos idóneos de crecimiento. En México se tienen el Plan Nacional de Desarrollo y los programas sectoriales correspondientes como muestras más evocadoras en donde se sustenta la política informática.

Legislación informática

A diferencia de la política informática, la legislación informática es un conjunto de reglas jurídicas de carácter preventivo y correctivo derivadas del uso (fundamentalmente inadecuado) de la informática, es decir, aquí se trata de una reglamentación de puntos específicos, pero esta circunstancia necesariamente implica las siguientes consideraciones:

a) Si se recurriría a un cuestionamiento de las reglas existentes para determinar si es posible su aplicación análoga frente al problema o si sería necesaria una ampliación en cuanto a su ámbito de cobertura.
b) Esperar la evolución de la jurisprudencia dada la creciente presentación de casos ante los órganos jurisdiccionales en los que se fijen pautas resolutorias o al menos conciliatorias.
c) Crear un cuerpo de nuevas reglas integrándolas a ordenamientos ya existentes, o que den lugar a una nueva ley de carácter específico. A nuestro parecer, esta última es la opción más indicada.

Por otra parte, sea con las consideraciones que fuere el caso, dicha reglamentación deberá contemplar las siguientes problemáticas debidamente identificadas:

Diferentes rubros por regular

a) *Regulación de la información*, ya que la información como un bien requiere un tratamiento jurídico en función de su innegable carácter económico.

b) *Protección de datos personales*, es decir, el atentado a los derechos fundamentales de las personas provocado por el manejo inapropiado de informaciones nominativas.
c) *Regulación jurídica de internet*, con el favorecimiento o restricción de los portales en internet.
d) *Propiedad intelectual e informática*, con los temas referentes a protección de los programas de cómputo y regulación de nombres dominio, ambos derivados de las acciones de "piratería" o "ciberocupación".
e) *Delitos informáticos*, es decir, la comisión de actos ilícitos en los que se tengan a las computadoras como instrumentos o fin.
f) *Contratos informáticos*, en función de esta categoría contractual particular con evidentes repercusiones fundamentalmente económicas.
g) *Comercio electrónico*, nueva forma de comercialización automatizada de bienes y servicios de todo tipo a través de internet. Se incluye el subtema de firma electrónica.
h) *Spam*, entendido como el envío del correo no deseado o no solicitado.
i) *Aspectos laborales de la informática*, como aquellos problemas laborales suscitados por la informatización de actividades: ergonomía y teletrabajo.
j) *Valor probatorio de los documentos electrónicos*, referido a la aceptación y valoración de estos documentos como medio de prueba.

Existen otros tópicos interesantes que a diferencia de los anteriormente señalados no serán motivo de análisis, al menos en esta obra, entre los que destacan la Democracia Electrónica (Voto Electrónico), el régimen jurídico de la videovigilancia, la regulación jurídica de los identificadores de radiofrecuencia (RFID) y las implicaciones legales de la Bioinformática, a reserva de otros tantos que seguramente surgirán en un futuro inmediato.

II. Informática jurídica

INFORMÁTICA JURÍDICA DOCUMENTARIA

Generalidades

La informática jurídica documentaria es el área más antigua de la informática jurídica; sus orígenes suelen asociarse a los trabajos mencionados de John Horty en la Universidad de Pittsburgh, como lo constatamos en el capítulo anterior.

En los sistemas de informática jurídica documentaria se trata de crear un banco de datos jurídicos (o *corpus* jurídico documentario) relativo a cualquiera de las fuentes del derecho (menos la costumbre) a efecto de interrogarlo con base en criterios propios acordes con esa información y su relevancia jurídica.

Al principio, los criterios jurídicos prevalecieron sobre los informáticos. Se tendía a reproducir el criterio de clasificación usado en los repertorios jurídicos como criterio de almacenamiento y recuperación de la información. Esto constituía una clara limitación ya que la máquina ofrecía muchas más posibilidades, y éstas seguían siendo utilizadas en segundo término. Obviamente, el cambio de los sistemas informáticos contribuyó en medida notable a mejorar el uso de los bancos de datos jurídicos.

El rendimiento de un banco de datos de esta naturaleza está en función de la exactitud y extensión de los datos contenidos y de los criterios de búsqueda de los documentos pertinentes. Para una fuente jurídica en evolución, como son la legislación y la jurisprudencia, la actualización se convierte en una innegable necesidad.

Los primeros sistemas de interrogación de bancos de datos jurídicos fueron los *batch*, es decir, aquellos que permitían la búsqueda en los archivos (de texto y de palabras ordenadas alfabéticamente), que indicaban, una vez señalada una palabra, la "dirección" donde estaba almacenada en todos los documentos del archivo, comparando simplemente los archivos.

Utilizar los operadores proposicionales permitía (y permite aún por ser una fase en uso) combinar palabras, a fin de tornar más específico el campo de los documentos buscados.

Así, consultar las palabras "contrato o compraventa" facilita recuperar todos los documentos que contengan las dos palabras, y si se agrega el vocablo "hipoteca (no)" se excluirán todos los documentos del primer conjunto que contienen la palabra "hipoteca".

De los sistemas *batch* se pasó a los sistemas *on-line,* que permiten establecer interrelación a distancia a fin de precisar la pregunta mediante un diálogo entre el usuario y la máquina. Hoy en día, los sistemas de interrogación son lo suficientemente sofisticados para ayudar en forma considerable al interrogador, y se perfila un periodo de transición en el uso de sistemas expertos a efecto de mejorar la calidad de la búsqueda y para hacer "aprender" a la máquina.

Principales características

La finalidad de la informática en un sistema documentario consiste en encontrar lo más rápida y pertinentemente posible la información que ha sido almacenada. El conjunto de esas informaciones constituye el banco de datos o *corpus* (la expresión "base de datos" se reserva por momentos a la designación de subconjuntos del *corpus* total). La interfase almacenamiento-recuperación de información jurídica se manifiesta a través del siguiente proceso:

1. La entrada de documentos (leyes, reglamentos, jurisprudencia, doctrina, acuerdos, etc.) se efectúa bajo una forma codificada comprensible para la máquina. Según la capacidad del sistema, la codificación de textos será más o menos voluminosa. Esta codificación será elemental si la entrada de información es hecha carácter por carácter (letra, cifra, puntuación, etc.). La codificación será más compleja si el texto ha sido condensado previamente de tal modo que sólo contenga sus elementos característicos; cada elemento del texto (palabra o expresión, identificadores, etc.) corresponde a un número de código.
2. La búsqueda de documentos significativos se efectúa de la siguiente manera: la codificación de palabras deseadas, según la combinación escogida, se introduce en la computadora que comparará toda la base documentaria y señalará una concurrencia importante cada vez que la comparación de los códigos pueda combinarse gracias a los operadores *booleanos* (provienen de la lógica de Boole) "y","o" y "salvo", de tal modo que la búsqueda gane en eficacia.

Todos los sistemas prevén la facultad para los usuarios de conocer el número de documentos ligados a cada pregunta a fin de restringir el campo de éste y obtener una información más precisa.

Cabe mencionar que toda búsqueda documentaria deja escapar documentos que pueden ser interesantes o, inversamente, conduce a documentos que no conciernen de manera directa a la cuestión estudiada y que va en función de la misma documentación informatizada. En este caso, las informaciones inútiles constituyen un *ruido* (exceso de información pertinente en una consulta) y las informaciones útiles que no han sido comunicadas son un *silencio* (falta de información pertinente en una consulta).

Esquemas de representación documentaria

El problema principal que se enfrenta en la constitución de un sistema de documentación jurídica automatizado está en función de la naturaleza híbrida del lenguaje jurídico. A diferencia de la mayoría de las otras disciplinas, el derecho no utiliza un lenguaje "científico" al no ser puramente descriptivo o preciso.

De esa forma, el lenguaje jurídico no describe al derecho como objeto, sino en gran medida al derecho mismo; por otra parte, cada uno de los términos empleados no corresponde biunívocamente a una realidad o a un objeto: la ambivalencia estriba en la naturaleza profunda del derecho, a lo cual difícilmente se presenta objeción.

Las palabras que integran los documentos jurídicos no pueden ser consideradas unidades fundamentales con un sentido cada una. Así, cada documento se caracteriza de manera única por las palabras utilizadas (a causa del estilo, de la sintaxis y del vocabulario jurídico) y se emplean esos términos en su sentido más general.

El estilo jurídico recurre con frecuencia a comparaciones o efectos que pueden hacer intervenir una noción análoga en el curso de un texto; pero también puede sugerir una noción o situación sin que el término que señala más habitualmente aparezca en realidad.

Las dificultades inherentes al estilo jurídico presentan dos métodos de almacenamiento de datos documentarios que analizaremos en forma específica.

a) *Método del texto integral* (full text)

Este método consiste en introducir los textos en memoria como son y la computadora los analiza integralmente. Este método es siempre oneroso debido al espacio de memoria; por otra parte, disminuye de manera notoria los riesgos de silencio, pero es altamente generador de ruido.

b) *Método de indización* (key word)
Este método implica el análisis previo del documento para extraer y concretar las características fundamentales (conceptos, circunstancias, elementos de decisión, etc.). Es costoso por la necesidad de contratar a personal calificado, pero disminuye teóricamente los riesgos de ruido.

Cada documento es objeto de un resumen más o menos sintético que recibe el nombre de *abstract*, el cual es un proceso informático-jurídico de tratamiento de información jurídica que tiene por objeto recuperar y presentar universos de información de modo automático, a partir de la elaboración de un soporte derivado en el que se plasman los sintagmas descriptores del soporte documentario de origen, relacionables sintagmáticamente dentro de unidades de ideas, que son estructuradas en forma lógico-deductiva a través del empleo de restrictores de distancia que las hacen concordantes con módulos de interrogación. En función de la lógica de la computadora, en la actualidad se distinguen dos tipos de *abstracts* jurídicos fundamentales: el legislativo y el jurisprudencial.

Cabe expresar que tanto el método del texto integral como el de indización no son antitéticos más que en apariencia: la indización puede en ciertos casos generar un resumen introducido y explotado según los métodos del texto integral; es extraño que un texto sea introducido de manera integral sin ser acompañado de descriptores que realizan una indización en el cuerpo del texto. La oposición entre los dos métodos estaba más marcada en las primeras experiencias, cuando los sistemas eran aún elementales; más recientemente, la naturaleza constitutiva del banco de datos determina la elección de mayor o menor indización (éste conviene más en la jurisprudencia o doctrina, a diferencia del texto integral, considerado más adaptable a los textos legislativos).

La tendencia generalizada para los sistemas importantes es a combinar las ventajas del texto integral (trabajo sobre los documentos jurídicos en sí mismos sin pérdida de información ni interpretación errónea, resultante de la vía de análisis) y aquellas derivadas de la indización, lo cual aumenta la eficacia de la búsqueda, de aquí que se mencione la existencia de un tercer método: el combinado.

Problemas a nivel gramatical

Por otra parte, la sintaxis jurídica presenta dificultades a nivel gramatical que constituyen serios problemas lingüísticos a nivel de ruido (exceso de información) o silencio (falta de información) en una consulta dada para la recuperación de información jurídica. De manera enunciativa y no limitativa, existen los siguientes:

a) *Sinonimias*

Se da cuando una idea se puede expresar con dos o más palabras diferentes, por ejemplo: trabajador, empleado, subordinado u obrero.

Este fenómeno constituye un problema respecto de la recuperación debido a que si se solicita información por la primera palabra y la computadora no provee los documentos que contienen también la segunda o la tercera, la información será parcial, en cuyo caso el problema por resolver es el del silencio informático.

b) *Polisemias u homografías*

Este fenómeno se presenta cuando una palabra (sintagma autónomo) tiene dos o más sentidos. Por ejemplo, el término *autor* puede referirse al creador de un acto jurídico, al autor de una obra literaria o artística o al delincuente en término intelectual o material.

Las polisemias constituyen un problema de ruido informático.

c) *Analogías*

Dicho problema ocurre cuando dos o más palabras, provenientes de distinta raíz, se refieren a ideas parecidas, por ejemplo: mora y retardo o plazo y término.

Este fenómeno constituye un problema por resolver, porque es posible que la información requerida quede incompleta si no se relaciona la palabra mediante la que se interroga con sus análogos. Aquí la cuestión por resolver es la del silencio informático.

d) *Antonimias*

Las antonimias se presentan entre una palabra y otra con sentido opuesto, por ejemplo: constitucional e inconstitucional. Esto es relevante para efectos de recuperación debido a que una palabra precedida o seguida de una negación es sinónimo del sintagma autónomo que sin dicha negación sería su antónimo, por ejemplo: no constitucional = inconstitucional.

De esta manera, a alguien que solicita información por la palabra *inconstitucional* también le interesa recuperar aquella en la que se alude a *no constitucional*.

El problema a que da lugar la antonimia es el silencio informático.

e) *Formas sintácticas*

Dicha formas consisten en la manera como una misma idea se puede expresar a través de diversas relaciones sintagmáticas, por ejemplo:

creación de una empresa
una empresa se creó
una empresa será creada

una empresa creada
una empresa se creará

Los citados son sintagmas equivalentes en caso de una interrogación, por lo que, a efecto de no perder información, es preciso relacionar todas las variaciones de la palabra "creación" que en diferentes redacciones y con un tipo específico de interrogación se puedan dar.

f) Orden de términos
En el caso de modificación del orden de los términos puede haber un cambio en el sentido, por ejemplo:

acción de enriquecimiento ilegítimo
ilegítima acción de enriquecimiento
ilegítimo enriquecimiento en la acción

Esto, sin duda, genera un problema de ruido informático.

Instrumentos lingüísticos

Para resolver los problemas lingüísticos anteriormente expuestos y otros, existen dos instrumentos fundamentales a efecto de lograr una apropiada recuperación de información por ideas, independientemente de la forma en que se expresen; éstos son: el léxico y el *thesaurus*.

El léxico

El léxico consiste en la organización de todas las palabras con contenido informativo,[1] almacenadas en computadora por nociones y subnociones según un criterio morfológico semántico, con la finalidad de resolver los problemas de la sinonimia y ayudarnos a resolver los de homografía o polisemia.

El *thesaurus*

Por su parte, el *thesaurus* pretende servir de medio de apoyo al usuario para resolver los problemas de analogía, antonimia y aislamiento semántico de las palabras polisémicas al momento de la interrogación.

[1] Las palabras carentes de contenido informativo se denominan *palabras nulas*, como para, de, a, etcétera.

Dicho instrumento fundamental se construye a partir de las nociones del léxico y su connotación es distinta de la empleada en los términos de biblioteconomía (lista de descriptores propia de los sistemas de lenguaje cerrado).

Por lo anteriormente expuesto cabe decir que la especificidad marcada del lenguaje jurídico convertiría en inoperante todo sistema documentario si no estuviera integrado a éste y en combinación con los problemas de búsqueda y conversación con los usuarios.

a) *Concepto*

De esa forma, el *thesaurus* se convierte en un léxico jerarquizado que comprende una red de interconexiones, exclusiones, discriminaciones y proximidades semánticas bajo la forma de listas de sustitutivos de contrarios, términos vecinos o genéricos, etc. A cada interrogación del *corpus*, el *thesaurus* orienta la exploración a fin de disminuir automáticamente o en la conversación con el usuario los problemas de ruido y silencio.

b) *Funciones principales*

- Como diccionario analógico en su función de conexión que permite reconocer situaciones y expresiones jurídicas, en las que se toman en cuenta la sintaxis gramatical, se buscan antónimos y se reagrupan sinónimos.
- Como diccionario analítico en su función de discriminación que excluye nociones afines no necesarias o incidentales, así como en las formas no deseadas, al disminuir las figuras polisémicas y sinónimas.
- Como índice en su función de adición de términos que conforman la base de datos o *corpus*.

Los *thesaurus* pueden ser abiertos o cerrados, lo cual depende de que se pueda o no agregar a ellos nuevos elementos.

Principales sistemas en operación

Existen en el mundo varios sistemas en operación a nivel de informática jurídica documentaria. Sin pretender ser exhaustivos, están: Lexis-nexis, italgiure find (de la Suprema Corte de Casación de Italia), IDG (del Instituto para la Documentación Jurídica de Florencia, Italia), Celex (de la Comunidad Europea con sede en Bruselas), Prodasen (de la Cámara de Senadores, Brasil), Credoc (de la Federación Real de Abogados y Notarios, Bélgica, el cual es el más antiguo en Europa).

A nivel nacional existen: el UNAM-IURE (del Instituto de Investigaciones Jurídicas de la UNAM), el de la Suprema Corte de Justicia de la Nación (disponible también en disco compacto, Ius), el de la Cámara de Diputados, el de la Cámara de Senadores, el de Orden Jurídico Nacional de la Segob y a nivel privado Lexis-México, V/Lex,[2] etcétera.

INFORMÁTICA JURÍDICA DE CONTROL Y GESTIÓN

Nociones generales

Aun cuando es el más importante y desarrollado dentro de la informática jurídica, el aspecto documentario no es definitivamente el único. Desde hace tiempo se desarrollan otros sectores en procesos de continua evolución. Uno de ellos es la llamada informática jurídica de control y gestión, que abarca los ámbitos jurídico-administrativo, judicial, registral y despachos de abogados, fundamentalmente.

Dicha área tiene como antecedentes el tratamiento de textos jurídicos mediante el uso de procesadoras de palabra y, por otra parte, las experiencias obtenidas en materia de automatización de registros públicos (en particular de bienes inmuebles).

Su uso en la administración pública

En la administración pública se presenta un crecimiento extraordinario en el volumen y la complejidad de actividades en las dependencias gubernamentales debido, entre otras cosas, al pronunciado desarrollo demográfico, económico y tecnológico. Ello ha obligado a que dicho sector, en sus diferentes niveles (federal, estatal y municipal), esté capacitado para recibir, tramitar, analizar y difundir todo tipo de información jurídica para su correcto funcionamiento.

Mediante la adecuada aplicación de la informática jurídica de control y gestión se puede lograr un mejoramiento sustancial de las estructuras jurídico-administrativas y los sistemas de operación, medida indispensable para que las entidades del sector público, por medio de los poderes Ejecutivo (posteriormente nos referiremos al llamado gobierno digital o electrónico), Legislativo y Judicial, alcancen sus objetivos sociales (justicia y bien común) apoyados en la utilización de la tecnología moderna.

[2] Véase: http://www.juridicas.unam.mx, http://www.ordenjuridico.gob.mx/, http://www.senado.gob.mx/, http://www.cddhcu.gob.mx/, http://www.vlex.com.mx

Sin lugar a dudas, uno de los principales beneficios en esta área, además de la agilización en la tramitación de asuntos jurídico-administrativos, es el descenso de la inercia burocrática y corrupción, lo cual alcanza niveles más significativos en el caso de la administración de la justicia, lo cual permite la impartición de una justicia realmente rápida, expedita, particularizada y sobre todo gratuita, es decir, ajena a la lacerante y enquistada corrupción.

Su uso en los órganos jurisdiccionales

Este tipo de aplicación ha dado lugar a la llamada informática judicial, con un enorme desarrollo en la actualidad. Así, los ejemplos de actividades automatizadas a nivel de la judicatura son numerosos y variados: desde la formulación agendaria de jueces y magistrados hasta la redacción automática de textos jurídicos a manera de sentencias. En el medio hay una enorme cantidad de acciones realizadas en juzgados, tribunales y cortes que han sido objeto de estudio, análisis y automatización. Uno de los ejemplos más simples y concretos lo constituyen la aceptación, registro e indicación de competencia y seguimiento de los expedientes. Una causa nueva que debe ser radicada ante un tribunal pasa previamente por la inscripción automática, la cual le asigna un número y juzgado y verifica si hay o no conexidad en la causa. Por otra parte, las diferentes fases del proceso pueden ser conocidas en cualquier momento, lo cual permite conocer el estado del juicio, así como el lugar donde se encuentra el expediente (con el secretario, actuario, juez, etc.). En un futuro no muy lejano ya no será tan necesaria la "visita" a los tribunales para conocer el estado de los asuntos, ya que todo podrá consultarse vía telemática. Dada la importancia del tema, posteriormente se tratará el aspecto de la ciberjusticia o cibertribunales.

Su uso en despachos y notarías

Este tipo de informática jurídica también ha ganado terreno en otro tipo de profesiones jurídicas como las de los notarios y abogados en aquello que se puede conceptualizar como una "ofimática jurídica" (automatización de oficinas con actividades de índole jurídica). Así, los estudios y aplicaciones en el campo notarial con cerca de 20 años de iniciarse tienen tal funcionalidad que van más allá del simple tratamiento de textos y ofrecen una lista completa de las principales actividades, con una organización, control y seguimiento verdaderamente asombrosos (agenda, estado de asuntos, registros, tarifas, cálculo de impuestos, etc.).

Y qué decir de los despachos de abogados en los cuales se pueden simplificar, mediante el uso de sistemas automatizados, un gran número

de labores propias de dicho entorno (control de asuntos, honorarios, redacción y verificación de escritos, etc.), complemento de las funciones documentarias de orden legislativo, jurisprudencial, doctrinario y bibliográfico, según se analizó anteriormente.

Lo más importante de ello es que dicha modernización facilita a los abogados dedicarse a actividades jurídicas de contenido creativo, crítico e interpretativo tan olvidadas y afines a su profesión, lo que motiva un enriquecimiento del derecho, tan necesario en estos tiempos.

Sistemas expertos legales

Un tipo de aplicación muy especial lo constituye la informática jurídica metadocumentaria, llamada así porque trasciende más allá de la esencia de los fines documentarios propiamente dichos (sin duda alguna constituye el acercamiento más interesante respecto a la difícilmente comprensible iuscibernética). Cabe establecer sus ámbitos principales de injerencia en cinco vertientes bien determinadas: ayuda a la decisión, ayuda a la educación, ayuda a la investigación, ayuda a la previsión y ayuda a la redacción.

Ayuda a la decisión (informática jurídica decisional)

En la actividad de los juristas, la búsqueda del conocimiento jurídico está orientada a resolver cuestiones con consecuencias en la vida política. La informática jurídica ha comenzado a ocuparse también del campo de la decisión, que es, por supuesto, el que más dificultad presenta. No es necesario que el sistema tome la decisión, sino simplemente (como por regla general lo es) ayudar a la decisión que se puede dar en varios planos y niveles.

La cantidad de variables que se requieren para tomar la más mínima decisión hace pensar sobre el carácter limitado que tiene la "decisión automática". Limitada, en el sentido que se puede aplicar (al menos hasta ahora) sólo a sistemas pequeños y en partes "racionalizables", que son dos fuertes limitaciones, pero aun así queda un campo extenso y complejo digno de ser abordado. Nadie pretende saber con exactitud las razones en las cuales se apoya una decisión, sino sólo materializar y sistematizar aquellas "buenas razones" que transforman un juicio jurídico en uno objetivo: por un lado, la kantiana "universalización" y por el otro la fundamentación en una norma vigente.

La teoría de la decisión (desarrollada en otros campos de las ciencias sociales como la economía y la ciencia política) es prácticamente desconocida en la teoría del derecho. Las ventajas que reportaría en el campo jurídico en caso de una adecuada aplicación serían la estructuración del conocimiento y la existencia de una teoría general.

En el área informática, la rama que se ocupa de estos temas recibe el polémico nombre de "inteligencia artificial", manifestada a través de los no menos discutidos "sistemas expertos" como aquellas herramientas que, a partir de ciertas informaciones dadas por un asesor, permiten resolver problemas en un dominio específico mediante la simulación de los razonamientos que los expertos del sistema harían si utilizaran los conocimientos adquiridos.

Se suele esquematizar un sistema experto como un sistema informático que contiene:

a) Una base de conocimientos en forma de banco de datos bien estructurado de forma tal que favorece un cálculo lógico en él.
b) Un sistema cognoscitivo o mecanismo de inferencia que contiene la mayor parte de los esquemas de razonamiento válidos en ese dominio.
c) Una interfase que comunica al usuario con la máquina.

En materia jurídica, la representación del conocimiento en la base del conocimiento presenta problemas de no poca relevancia teórica y con notoria carga de dificultad cuando se trata de representar enunciados de contenido legal.

Las gramáticas que se han propuesto hasta el presente son variadas y en general insuficientes, pero la misma lógica que está por detrás de los enunciados normativos en su parte más específica ha sufrido una crítica acentuada. No existe una solución única ni universalmente aceptada. En cada caso se examina el tipo de objetivo que se quiere alcanzar con el sistema a efecto de adoptar una u otra solución, desde la adaptación del lenguaje natural como el sistema LEGOL hasta las formas más completas de lógica de predicados como permite la utilización del lenguaje de programación PROLOG o LISP. En el medio hay trabajos muy interesantes sobre representación normalizada,[3] así como los referentes a la transformación de las relaciones entre los elementos de la norma en relaciones aritméticas binarias[4] y sobre representaciones de lógica deóntica,[5] la teoría de los conjuntos borrosos (*fuzzy set*), la teoría de los juegos y la modelística.

Cabe mencionar que lo más importante de un sistema experto es hacer funcionar el mecanismo de inferencia que está en las reglas de razonamiento que deben ser incorporadas en forma de condicionales del tipo

---

[3] L. Allen, *Una Guida per i Redattori Giuridici di Testi Normalizzati;* A.A. Martino, C. Ciampi y E. Maretti, *Logica, informática, diritto*, Florencia, Le Monnier, 1979 y *Toward a Normalized Language to Clarity the Sctructure of Legal Discourse;* asimismo, A.A. Martino, *Deontic Logic Computational Linguistics and Legal Information Sistems,* North Holland, Amsterdam, 1982.

[4] M. Sánchez Mazas, *Modelli Aritmetici per Informatica Giuridica;* A.A. Martino, *Deontic Logic Computational Linguistics and Legal Information Sistems,* Amsterdam, North Holland, 1982.

[5] A.A. Martino, "Contributo Lógico Informático all'analisi della legislazione", *Informatica e Diritto.* Le Monnier, Florencia, 1982.

"*sí... entonces*" que constituyen la verdadera revolución informática. El mecanismo de inferencia es un sistema capaz de tomar dos informaciones de la base de conocimientos y obtener una conclusión lógica.

En materia jurídica, la reconstrucción de estas reglas universales de razonamiento jurídico es muy difícil de enunciar y salvaguardar a pesar de algunas excepciones.

El camino para acortar la distancia en el diálogo usuario-máquina constituye el último de los elementos de un sistema experto, y en el ámbito jurídico tiene que ver con la capacidad para obtener reglas de intermediación y sobre todo de control que no hagan "explotar" la máquina con sus enormes números de combinaciones posibles. Las reglas de control más seguras entonces son las tablas de verdad que, no obstante, interfieren con su enorme capacidad de expansión.

Un buen sistema experto debe tener una cualidad rara y crucial: debe aprender. De ser así, cabe pensar en la cantidad de casos que puede analizar y en la extraordinaria "casuística" que está en posibilidad de incorporar.

En el sistema experto es necesario que el problema y el dominio en que se sitúa queden bien definidos, que los conocimientos sean claros y que las reglas de derivación resulten pocas y precisas.

En la actualidad son relativamente pocos los sistemas expertos de índole jurídica en funciones o siquiera en desarrollo; empero, no dudamos de que a la postre esto se va a constituir en la vertiente más significativa de la interrelación derecho-nuevas tecnologías de la información y comunicación (TIC).

Ayuda a la educación

A diferencia de los otros subgrupos enunciados, éste no constituye un conjunto homogéneo de realizaciones, sino un modo de afrontar la informática jurídica para su aplicación en la enseñanza del derecho.

Debido a la rápida evolución de la "sociedad informatizada" es imprescindible estar preparados para ello, de tal manera que no sea una revolución que se "sufra" sino una evolución que se "prepare". Tal realidad, constitutiva de la llamada revolución informática, no puede permanecer ajena al ámbito de los actuales y futuros profesionales del derecho.

En este sentido, si bien el vertiginoso desenvolvimiento de las técnicas informáticas ha determinado la necesidad de implantar en las universidades nuevas asignaturas, especializaciones e incluso carreras, esto no es muy notorio en escuelas y facultades de derecho.[6] A ellas se les impone

[6] Cabe mencionar que desde 1981 se imparte la materia de jurismática, al inicio, en el séptimo y actualmente en el quinto semestre de la licenciatura en derecho en la Universidad La Salle, por lo que es la institución educativa pionera al respecto.

responder al reto de desentrañar y difundir las múltiples aplicaciones que tiene la informática en el mundo del derecho (informática jurídica), a la vez que enfocar sistemáticamente la problemática jurídica ocasionada por el efecto del fenómeno informático (derecho de la informática).

A pesar de lo anterior, el ámbito de conocimiento de la interrelación derecho-nuevas tecnologías de la información y comunicación (TIC) no se detiene ahí, ya que la enseñanza del derecho puede efectuarse de mejor manera mediante el apoyo en soportes informatizados que permiten un acopio heurístico tanto de conocimientos como de experiencias jurídicas que enriquecen la formación de los estudiantes y facilitan la labor de los docentes.

Respecto a esta enseñanza del derecho con la utilización de medios informáticos, cabe decir que recién se está en los albores de las primeras experiencias todavía sin matices específicamente jurídicos, de sistemas de aprendizaje y evolución automatizada del aprendizaje. Empero, es importante resaltar la enorme importancia que revestirá en lo futuro este tipo de desarrollo de orden jurídico-educacional. Lo cierto es que el jurista en general, comienza a estar consciente de que sin conocimientos en materia de computación difícilmente podrá ejercer su profesión en la sociedad informatizada de la que se habla a menudo, y vive a consecuencia de la creciente interconexión de todos los fenómenos sociales. De aquí que sea válido destacar que esto no debe considerarse una mera especialidad, sino una verdadera necesidad.

Ayuda a la investigación

Muchas de las aplicaciones de la informática jurídica son por el momento en esencia empíricas y se han desarrollado sobre bases teóricas relativamente simples. La informática jurídica de investigación o informática jurídica analítica, según denominación del profesor Antonio Anselmo Martino, tiende a descubrir aquellos instrumentos matemáticos que puedan revestir utilidad para incrementar los resultados de realizaciones actuales. Este tipo de investigación es muy complicado y por ahora no ha conducido a resultados espectaculares, tal vez por tratarse de esfuerzos aislados y sin que hayan sido objeto de mucha difusión.

En este tipo de informática jurídica se utilizan las enormes capacidades de la máquina para poner a prueba las hipótesis y teorías jurídicas, o dicho de otro modo, "repensar" el derecho.

Entre las realizaciones de tipo práctico están las de replantear todos los pasos procesales, los cuales se descomponen en orden para la máquina y permiten recrear la racionalidad económica del proyecto en general en cuanto a la aceptabilidad y funcionalidad de cada una de las soluciones

que con el tiempo se han cristalizado en algún sector del derecho hasta hacerlas concebir como "naturales" o "imprescindibles". La reconstrucción paso por paso permite intervenir para hallar la solución más razonable.

Por otra parte, en las realizaciones de tipo teórico creadas para experimentar una teoría o para verificar el funcionamiento de algunas hipótesis, la posibilidad de repensar el derecho se torna obligatoria: en primer lugar para la selección del dato. Separar lo jurídico de lo no jurídico exige una depurada teoría sobre lo primero que permita utilizarla al reconocer los objetos del universo.

Una vez realizada esta primera selección se proponen al teórico todos los problemas relativos a la consideración del derecho vigente (que es el que normalmente interesa al jurista) en el modo más universal y normativo (es decir, objetivo) que sea posible. Los temas relativos a las derogaciones explícitas e implícitas serán más evidentes si se plantean de tal modo que una máquina pueda reconocer dichas situaciones. De esta forma, la expresión "quedan derogados todos los ordenamientos que se opongan a esta ley" adquiere toda su dramática ambigüedad en el momento en que el informático jurídico analítico debe descomponerla para tornarla representable y operativa en un sistema automático.

Toda la gama de soluciones sintácticas de representación del conocimiento jurídico, desde las lógicas deónticas más refinadas hasta los sistemas cercanos al lenguaje ordinario, constituyen una ulterior fuente de reflexión al obtener la parte más representativa o funcional del sistema jurídico y sus formas de representación.

La fase interpretativa de la semántica jurídica constituye, por el momento, el límite más claro y significativo de la posibilidad de aplicación de una computadora en la teoría jurídica. El hecho de que la interpretación como actividad compleja sea difícilmente plasmable en un algoritmo no excluye que algunas tentativas simples puedan realizarse, como las que hacen depender el significado de un término de una regla de uso identificable en alguna autoridad como un tribunal prestigioso o un jurista de renombre, o en los más sofisticados procedimientos ponderados.

Una vez obtenida una interpretación plausible (o posible), la fase más fascinante para repensar de manera científica el derecho consiste en obtener consecuencias a partir de un *corpus* determinado.

Si la configuración del *corpus* constituye una aplicación de notables teorías jurídicas, la obtención de consecuencias, aun de *corpus* ya interpretados, es una parte interesante en la aplicación de teorías jurídicas.

La mayoría de los juristas coinciden en considerar al orden jurídico como un conjunto de enunciados con todas sus consecuencias. Pero determinar las consecuencias de un conjunto de enunciados implica explicar las reglas de derivación necesarias para pasar de los enunciados de base a las consecuencias.

La anterior es la parte más oscura de la actividad jurídica, la de más difícil enunciación, no obstante la larga tradición y la indudable pericia con la cual los juristas la realizan.

Respecto a este punto se plantean problemas de división o especialización de los conocimientos jurídicos; para empezar, la necesaria explicación de los principios o criterios generales y la enunciación de aquellos particulares de una rama o especialización jurídica. La construcción de un sistema experto de derecho administrativo, en estas consideraciones, implicaría, por ejemplo, la inclusión de un principio de facultad por el órgano sólo en caso de permiso expreso y nunca como resultado de la ausencia de prohibiciones del conjunto de normas que regula la materia.[7]

En fin, es de suponer que todos los problemas relativos al significado de un orden de jerarquía entre principios o normas jurídicas (cuestión que nunca ha sido tratada a fondo más allá de los conocidos aforismos *lex posterior derogat, fex specialis derogat*, etc.), para representarlos y utilizarlos en un sistema de informática jurídica de este tipo deben ser susceptibles de enunciación algorítmica, lo cual los juristas están muy lejos de realizar por el momento.

Toda la parte del derecho y la teoría jurídica susceptible de ser enunciada en modo riguroso y paso por paso, así como las relaciones que existen entre los diversos subsistemas de un sistema jurídico son materia teóricamente posible de la informática jurídica de investigación, y se necesitan medios y conocimientos informáticos siempre más sofisticados y, claro está, una formación e información jurídica muy sólidas.

Ayuda a la previsión

La computadora facilita el análisis de bancos de datos multidimensionales que corresponden a una serie de objetos o individuos; no a un carácter sino a una serie de caracteres, de tal modo que se puede derivar el orden de prioridad de factores explicativos de esos datos; de ahí el nombre de análisis factorial dado al conjunto de esos métodos de examen. Dicho análisis ha permitido evolucionar considerablemente los trabajos experimentales basados en la interpretación de observaciones múltiples. Estos métodos de uso común en las ciencias humanas han sido objeto de una singular aplicación en el mundo jurídico.

El derecho es también una ciencia de observación que reposa sobre el registro de experiencias, por ejemplo: todas las decisiones jurisdiccionales concernientes a cierto punto de derecho complejo y que se reparten en

[7] Ésta es una clara derogación del principio general según el cual todo lo que no está prohibido está permitido.

varios grupos siguiendo las soluciones jurídicas tomadas en cuenta por los jueces y magistrados con base en una serie de factores; si el número de factores decisivos es restringido, el jurista que tenga que llevar un nuevo asunto caracterizado por la presencia de esos factores podrá "predecir" el desenlace probable del caso con buenas oportunidades de acierto; si el número de factores es elevado y existen en particular numerosos factores secundarios que han dado lugar a decisiones en apariencia contradictorias, el análisis factorial podrá, bajo reserva de variadas condiciones, convertirse en un instrumento importante para prever *a priori* la clasificación probable del nuevo caso sometido.

La previsión (predicción) de las decisiones judiciales es justamente el dominio de elección de los métodos de análisis de datos jurídicos, en particular en los países anglosajones donde sus técnicas se han desarrollado a causa de la referencia sistemática al precedente (*stare decisis*). Las decisiones de la Suprema Corte de Estados Unidos han sido así objeto de estudios profundos tendientes a medir la validez de esas técnicas en el campo jurídico.

Asimismo, la jurisprudencia en materia penal de ciertos estados ha sido descompuesta según sus métodos para inferir del expediente y los antecedentes personales de los delincuentes la influencia respectiva de diversos factores, como los antecedentes, medio ambiente profesional y familiar, etc., o la severidad de los jueces (duración de la pena, libertad condicional, etc.). De esta forma, más de 400 decisiones han sido analizadas a la luz de una veintena de variables; pensamos que esto no es impensable en países de tradición jurídica romano-germánica como México.

Por otra parte, y también a manera ejemplificativa, cabe destacar que la aplicación del análisis factorial en la jurisprudencia francesa no ha suscitado aún estudios de gran envergadura: la tradición jurídica franco-germánica presenta, en efecto, una inercia marcada al entorno de la cuantificación de procesos decisionales a pesar de la variedad de los sujetos de observación posible. El análisis factorial ha encontrado una mejor adaptación en el marco de los trabajos emprendidos en materia de sociología jurídica o judiciaria, y es utilizado en la investigación de proporciones multidimensionales de previsión de pronunciamientos en Francia.

Ayuda a la redacción

No se trata aquí de la redacción automática de actos repetitivos. La ayuda a la redacción consiste en proveer un apoyo informático permanente al momento de la concepción del texto (en esencia el texto de ley).

Las diferentes proposiciones del texto en vía de elaboración (condiciones, circunstancias, consecuencias de derecho, excepciones, etc.) apa-

recen en la pantalla acorde con una búsqueda no tanto en función de un texto seguido, que desde luego puede obtenerse, sino según una estructuración que corresponde a la lógica interna del texto. Este tipo de aplicación requiere programas más elaborados que aquellos relativos a tratamientos de texto ordinarios. En efecto, ellos deben poner en relieve la estructura lógica del texto considerada para que un simple vistazo permita resaltar las aberraciones, redundancias, lagunas o contradicciones; así, gracias a esta consulta permanente, es posible proceder a todas las correcciones de fondo par ajustar el texto a las intenciones legislativas (por ejemplo, inserción de enmiendas, combinación de textos de origen diferente en caso de ambigüedades parlamentarias) y todas las modificaciones de forma (formato, ortografía, etc.) que faciliten la comprensión del texto. Se pueden utilizar estos programas conjuntamente con un sistema documentario para verificar la coherencia y armonización de la legislación (reenvíos, cláusulas de aprobación o derogación, etcétera).

Los programas más interesantes emprendidos al respecto en Estados Unidos (a diferencia de las instituciones parlamentarias europeas) se basan en el método más simple de presentación estructural del lenguaje jurídico en el que las proporciones del texto son descompuestas e individualizadas y después organizadas usando ciertos signos representativos para los enunciados: y (entre varias condiciones), y (entre varias consecuencias), o (incluso), no (contrario), o (excepto), si (entonces), y sí (solamente).

Este método ha servido en la enseñanza jurídica por computadora conforme a un sistema de interrogación en el cual el estudiante debe reconstruir un texto jurídico aludiendo de modo sucesivo a conjuntos de frases y atribuyendo en cada ocasión el valor de una condición o una consecuencia, así como un coeficiente de importancia. Restituida de esta manera por medio de la experiencia, la estructura material y formal de un texto de ley es evidentemente mejor asimilada, mediante una adecuada valoración del peso semántico de las palabras según la acepción que se le pretenda atribuir.

III. Gobierno electrónico y ciberjusticia

GOBIERNO ELECTRÓNICO

Las nuevas tecnologías de la información y la comunicación (TIC) son una oportunidad y un medio excepcional para transformar de manera estratégica la administración pública en lo que se ha denominado gobierno electrónico.

El gobierno electrónico (e-government) es un concepto de gestión que fusiona el empleo adecuado y acentuado de las tecnologías de la información y comunicación, con modalidades de gestión y administración, como una nueva forma de gobierno.

Un caso interesante es el de Chile, donde este rubro fue elevado a política de Estado,[1] desde 2001. Sus objetivos en cuanto a gestión pública son:

- Aumentar niveles de eficiencia en la gestión pública.
- Disminuir significativamente costos de transacción y coordinación en la interacción entre entes públicos.
- Generar incentivos y prácticas que faciliten modalidades de gestión innovadoras y creativas.
- Agregar mayor valor público como horizonte permanente de las actividades del sector.
- Superar de modo constante los grados de transparencia de esas actividades, en aquello que un servidor conceptualizó como "cibertransparencia".

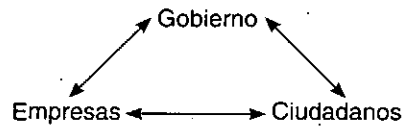
Por otro lado, sus objetivos desde el punto de vista de la ciudadanía son:

[1] Gobierno de Chile, *Instructivo presidencial para el desarrollo del gobierno electrónico No.005*, del 11 de mayo de 2001,. disponible en: http://www.bcn.cl/carpeta_temas/temas_portada.2005-11-14.7329717567/area_2.2005-11-30.2984247872, pdf, consultado en agosto de 2008.

- Acelerar el tránsito hacia una administración centrada en el ciudadano.
- Mejorar la calidad de los servicios que se proveen y las modalidades de provisión.
- Facilitar el cumplimiento de las obligaciones de los ciudadanos.
- Disminuir de manera significativa los costos de transacción entre ciudadanos y agentes públicos.
- Suprimir paulatinamente barreras, ineficiencias e irracionalidad en la interacción entre particulares y sector público.
- Facilitar el escrutinio ciudadano de la información, actividad y calidad de la operación presentes en el sector público.
- Transformar al sector público en facilitador del crecimiento y de distribuciones más equitativas de los niveles de bienestar social.

Un programa de gobierno electrónico es ante todo un proyecto de políticas públicas en el cual se imaginan escenarios, se programan acciones y se actúan relaciones eficientes dentro de la administración y en referencia a los ciudadanos y las empresas.

Definir un modelo ideal permite establecer qué partes son aplicables en qué lugar de la administración, calcular los tiempos, formar el personal y establecer los criterios de control para saber en qué medida y con cuál resultado se cumple la reforma.



Como dice Rodrigo Sandoval Almazán,[2] el debate para definir al gobierno electrónico se centra en la ausencia de límites de su acción, en ser visto como una herramienta para mejorar los trámites y servicios y la posibilidad de gobernar la red y de ser un instrumento que promueva la democracia y los valores democráticos en las sociedades.

En términos generales, el gobierno electrónico se desdobla en los siguientes rubros:

a) *e-administración* (administración electrónica). Este término hace referencia a aquellos mecanismos electrónicos que permiten la presta-

[2] Rodrigo Sandoval Almazán (*Nova Iuris, Revista de Investigación Jurídica*). *El gobierno electrónico en México; los sitios web de los gobiernos estatales.* Año I, número 1, enero de 2005, p. 72.

ción de servicios públicos de la administración, tanto a los ciudadanos como a las empresas.

b) *e-democracia* (democracia electrónica). Son procesos electrónicos o informáticos que permiten la participación ciudadana en la vida política mediante el uso de las TIC, ya sea en forma directa en la toma de decisiones políticas o por medio de sus representantes. Podemos dividir la e-democracia en las categorías de e-participación y voto electrónico, como mecanismos de ayuda de las TIC para desarrollar nuevos medios de participación y establecer una nueva cultura administrativa y de toma de decisión.

c) *e-gobierno* (gobierno electrónico en sentido estricto). Este término es el más general y ambiguo: abarca desde la simple puesta de documentos en la red hasta una integración completa entre ciudadanos y distintos organismos de la administración, así como la participación de aquéllos en la toma de decisiones políticas y, por tanto, engloba los conceptos de e-democracia y e-administración.

Existen diversas clasificaciones, divisiones, fases o etapas de la evolución del gobierno electrónico (ONU, 2005):

La primera etapa corresponde a la disponibilidad de información en línea, que es limitada y básica. La presencia en línea del gobierno electrónico incluye un sitio web oficial.

La segunda etapa es aquella en la que los servicios en línea del gobierno entran de modo interactivo, como información para el pago de impuestos, renovación de licencias, descarga de formularios, etc. Los dirigentes y cargos electos pueden ser contactados vía correo electrónico, fax o teléfono.

En la tercera etapa se halla la presencia transaccional, que permite la interacción entre el ciudadano y el gobierno e incluye las opciones para pagar impuestos, uso de tarjetas de identificación electrónica, actas de nacimiento/pasaportes, renovaciones de licencias de obra y otras.

La cuarta etapa es aquella en la que la prestación de servicios públicos electrónicos supone una transformación e integración de procesos con dos puntos clave: reorganización interna e integración con otras administraciones.

La quinta y última etapa representa el nivel más sofisticado de las iniciativas en línea del gobierno y está caracterizada por una integración de las interacciones con empresas, ciudadanos y otras administraciones. El gobierno estimula la toma de decisiones participadas y está dispuesto a implicar a la sociedad en la red en un diálogo de doble dirección. A través de características interactivas como *blogs,* foros y otros, el gobierno solicita de manera activa opiniones y participación a los ciudadanos y los integra en el proceso interno de toma de decisiones.

DESARROLLO DEL GOBIERNO ELECTRÓNICO POR PAÍS EN 2007

(Los datos de 2006 para efectos de comparación aparecen entre paréntesis)[1]

Lugar	País	Porcentaje sobre 100 puntos	Lugar	País	Porcentaje sobre 100 puntos
1. (1)	Corea del Sur	74.9 (60.3)	2. (3)	Singapur	54.0 (47.5)
3. (2)	Taiwan	51.1 (49.8)	4. (4)	Estados Unidos	49.4 (47.4)
5. (6)	Gran Bretaña	44.3 (42.6)	6. (5)	Canadá	44.1 (43.5)
7. (48)	Portugal	43.8 (31.3)	8. (12)	Australia	43.5 (39.9)
9. (27)	Turquía	43.5 (33.7)	10. (8)	Alemania	42.9 (41.5)
11. (7)	Irlanda	42.4 (41.9)	12. (16)	Suiza	42.3 (36.9)
13. (38)	Brasil	41.1 (32.1)	14. (11)	Dominica	41.0 (40.0)
15. (65)	Bahréin	40.3 (29.6)	16. (32)	Liechtenstein	40.0 (33.0)
17. (40)	Guinea Ecuatorial	40.0 (32.0)	18. (133)	Andorra	39.0 (24.0)
19. (14)	Nueva Zelanda	38.4 (37.6)	20. (35)	Italia	38.0 (32.9)
21. (10)	España	37.7 (40.6)	22. (20)	Hong Kong	37.5 (35.4)
23. (19)	Finlandia	37.3 (35.6)	24. (30)	Ciudad del Vaticano	37.0 (33.5)
25. (36)	Malasia	36.9 (32.7)	26. (15)	Holanda	36.8 (37.4)
27. (46)	República Checa	36.7 (31.7)	28. (106)	Brunéi	36.5 (26.8)
29. (84)	Chipre	36.4 (28.3)	30. (40)	Liberia	36.0 (24.0)
31. (56)	Austria	36.0 (30.6)	32. (17)	Azerbaiyán	36.0 (36.0)
33. (143)	Sierra Leona	36.0 (24.0)	34. (39)	Bután	36.0 (32.0)
35. (175)	Costa Rica	36.0 (20.0)	36. (73)	Eritrea	36.0 (29.0)
37. (166)	Etiopía	36.0 (22.0)	38. (137)	Gabón	36.0 (24.0)

[1] Darrell M. West,, Estudio: Global E-Government 2007, Center for Public Policy Brown University. Disponible en línea en: http://www.insidepolitics.org/egovt07int.pdf, pdf, 23 págs., consultada en mayo de 2008.

Lugar	País	Porcentaje sobre 100 puntos	Lugar	País	Porcentaje sobre 100 puntos
39. (17)	Corea del Norte	36.0 (36.0)	40. (9)	Japón	35.9 (41.5)
41. (28)	Malta	35.8 (33.6)	42. (24)	Qatar	35.6 (34.5)
43. (23)	Francia	35.6 (34.7)	44. (67)	Israel	35.5 (29.4)
45. (88)	Croacia	35.0 (28.0)	46. (51)	Islandia	34.6 (31.1)
47. (77)	India	34.2 (28.7)	48. (54)	Perú	34.0 (30.8)
49. (150)	Zambia	34.0 (23.5)	50. (68)	México	33.9 (29.3)
51. (76)	China (República Popular)	33.7 (28.8)	52. (66)	Emiratos Árabes	33.6 (29.5)
53. (58)	Hungría	33.3 (30.5)	54. (119)	Armenia	33.3 (25.3)
55. (112)	Argentina	33.1 (26.1)	56. (104)	Panamá	33.1 (27.0)
57. (28)	Kazajistán	33.0 (33.6)	58. (50)	Siria	32.8 (31.2)
59. (80)	Colombia	32.8 (28.6)	60. (13)	Suecia	32.7 (38.3)
61. (63)	Polonia	32.7 (30.1)	62. (49)	Serbia y Montenegro	32.4 (31.2)
63. (21)	Noruega	32.4 (35.0)	64. (44)	Dinamarca	32.1 (31.8)
65. (110)	Jamaica	32.1 (26.4)	66. (55)	Luxemburgo	32.1 (30.7)
67. (31)	Libia	32.0 (33.0)	68. (41)	Mónaco	32.0 (32.0)
69. (134)	Bahamas	32.0 (24.0)	70. (116)	San Vicente y Granadinas	32.0 (26.0)
71. (26)	Suazilandia	32.0 (34.0)	72. (97)	Tayikistán	32.0 (28.0)
73. (162)	Botsuana	32.0 (22.0)	74. (89)	Chipre (República Turca)	32.0 (28.0)
75. (90)	Ghana	32.0 (28.0)	76. (190)	Granada	32,0 (16.0)
77. (93)	Guinea-Bissau	32.0 (28.0)	78. (139)	Guyana	32.0 (24.0)
79. (81)	Kuwait	31.9 (28.5)	80. (79)	Líbano	31.5 (28.7)
81. (61)	Egipto	31.3 (30.2)	82. (45)	Eslovenia	31.3 (31.8)
83. (101)	Timor Oriental	31.2 (27.4)	84. (100)	Kenia	31.2 (27.5)

Lugar	País	Porcentaje sobre 100 puntos	Lugar	País	Porcentaje sobre 100 puntos
85. (161)	Belice	31.0 (22.0)	86. (113)	Bulgaria	31.0 (26.0)
87. (155)	Camboya	31.0 (23.2)	88. (34)	Chile	31.0 (32.9)
89. (98)	Arabia Saudita	30.9 (27.9)	90. (126)	Vietnam	30.9 (25.0)
91. (85)	Omán	30.9 (28.1)	92. (82)	Bélgica	30.8 (28.4)
93. (152)	Trinidad y Tobago	30.8 (23.4)	94. (92)	Guatemala	30.8 (28.0)
95. (102)	Irán	30.7 (27.3)	96. (59)	Filipinas	30.5 (30.4)
97. (145)	San Cristóbal y Nieves	30.3 (24.0)	98. (62)	Rumania	30.1 (30.2)
99. (188)	Lesotho	30.0 (16.7)	100. (146)	Surinam	30.0 (24.0)
101. (163)	Cabo Verde	30.0 (22.0)	102. (164)	Islas Cook	30.0 (22.0)
103. (37)	Eslovaquia	29.8 (32.3)	104. (71)	Bosnia-Herzegovina	29.8 (29.1)
105. (148)	Antigua y Barbuda	29.7 (23.7)	106. (74)	Maldivas	29.6 (29.0)
107. (78)	Jordania	29.6 (28.7)	108. (60)	Nepal	29.6 (30.3)
109. (129)	San Marino	29.3 (24.3)	110. (57)	Libia	29.0 (30.6)
111. (53)	Santa Lucía	29.0 (31.0)	112. (183)	Vanuatu	29.0 (20.0)
113. (125)	República del Congo	29.0 (25.0)	114. (83)	Lituania	28.7 (28.3)
115. (22)	Ucrania	28.4 (35.0)	116. (131)	Uruguay	28.4 (24.2)
117. (52)	Nigeria	28.3 (31.1)	118. (169)	Micronesia	28.0 (21.0)
119. (75)	Mongolia	28.0 (29.0)	120. (142)	Mozambique	28.0 (24.0)
121. (180)	Niue	28.0 (20.0)	122. (167)	Samoa	28.0 (22.0)
123. (173)	Barbados	28.0 (20.0)	124. (96)	Sri Lanka	28.0 (28.0)
125. (132)	Albania	28.0 (24.0)	126. (135)	República Democrática del Congo	28.0 (24.0)
127. (107)	Angola	28.0 (26.7)	128. (25)	Estonia	28.0 (34.0)
129. (138)	Gambia	28.0 (24.0)	130. (94)	Haití	28.0 (28.0)
131. (130)	Iraq	28.0 (27.0)	132. (159)	Kirguistán	28.0 (22.4)

Lugar	País	Porcentaje sobre 100 puntos	Lugar	País	Porcentaje sobre 100 puntos
133. (43)	Rusia	27.8 (31.9)	134. (130)	Marruecos	27.8 (24.2)
135. (72)	Pakistán	27.7 (29.1)	136. (70)	Sudáfrica	27.7 (29.2)
137. (99)	Ecuador	27.6 (27.5)	138. (91)	Grecia	27.1 (28.0)
139. (123)	Paraguay	27.0 (25.3)	140. (47)	Georgia	27.0 (31.4)
141. (121)	Fiyi	26.8 (25.3)	142. (107)	Afganistán	26.7 (26.7)
143. (69)	Sudán	26.7 (29.3)	144. (117)	Zimbabue	26.7 (26.0)
145. (109)	Benín	26.7 (26.7)	146. (158)	Uganda	26.2 (22.5)
147. (177)	Madagascar	26.0 (20.0)	148. (64)	Bielorrusia	26.0 (30.0)
149. (165)	República Dominicana	26.0 (22.0)	150. (124)	Senegal	25.7 (25.1)
151. (105)	Uzbekistán	25.7 (27.0)	152. (120)	El Salvador	25.6 (25.3)
153. (115)	Nicaragua	25.2 (26.0)	154. (160)	Yibuti	24.9 (22.1)
155. (149)	Mauricio	24.7 (23.7)	156. (86)	Bangladesh	24.7 (28.0)
157. (118)	Seychelles	24.7 (25.5)	158. (128)	Argelia	24.6 (30.3)
159. (156)	Venezuela	24.3 (23.2)	160. (178)	Malí	24.0 (20.0)
161. (195)	Nauru	24.0 (16.0)	162. (181)	Palaos	24.0 (20.0)
163. (185)	Islas Solomón	24.0 (18.0)	164. (144)	Somalia	24.0 (24.0)
165. (193)	Togo	24.0 (16.0)	166. (87)	Bolivia	24.0 (28.0)
167. (198)	Burundi	24.0 (8.0)	168. (136)	Costa de Marfil	24.0 (24.0)
169. (157)	Cuba	24.0 (22.7)	170. (176)	Indonesia	24.0 (20.0)
171. (171)	Honduras	23.0 (20.8)	172. (153)	Yemen	22.9 (23.4)
173. (172)	Malawi	22.7 (20.7)	174. (197)	Chad	22.7 (9.0)
175. (111)	Túnez	22.4 (26.4)	176. (95)	Laos	22.0 (28.0)
177. (154)	Ruanda	21.9 (23.3)	178. (151)	Tailandia	21.7 (23.4)
179. (168)	Namibia	21.5 (21.4)	180. (184)	Camerún	21.3 (19.0)
181. (33)	Macedonia	20.0 (33.0)	182. (126)	Islas Marshall	20.0 (25.0)
183. (141)	Moldavia	20.0 (24.0)	184. (122)	Myanmar	20.0 (25.3)
185. (179)	Nigeria	20.0 (20.0)	186. (170)	Papúa Nueva Guinea	20.0 (21.0)

Lugar	País	Porcentaje sobre 100 puntos	Lugar	País	Porcentaje sobre 100 puntos
187. (192)	Santo Tomé y Príncipe	20.0 (16.0)	188. (182)	Somalia	20.0 (20.0)
189. (194)	Tonga	20.0 (16.0)	190. (147)	Turkmenistán	20.0 (24.0)
191. (187)	Burkina Faso	20.0 (17.0)	192. (189)	República de África Central	20.0 (16.0)
193. (187)	Tanzania	18.3 (17.5)	194. (114)	Mauritania	18.0 (26.0)
195. (39)	Tuvalu	16.0 (32.0)	196. (174)	Comoras	12.0 (20.0)
197. (191)	Guinea	12.0 (16.0)	198. (195)	Kiribati	8.0 (12.0)

Fuente: Global E-Government 2007, Darrell M. West, Center for Public Policy Brown University.

CIBERJUSTICIA

Cibertribunales

Tienen como propósito servir de mediadores en los litigios derivados del uso de internet (comercio electrónico, propiedad intelectual, protección de la vida privada, etc.). Estos tribunales permiten a las partes interesadas elegir de entre una cantidad de expertos (en ocasiones académicos) aquellos que propondrán soluciones a los conflictos, sustentados en los textos internacionales más avanzados en la materia.

Las innovaciones tecnológicas ofrecen múltiples beneficios y contribuyen al progreso económico de las comunidades y de las organizaciones que las implementan.[4] Pero junto con esto generan situaciones nuevas que podrían ser perjudiciales si no se evalúan, comprenden y corrigen desde un principio. La economía digital se caracteriza por la progresiva integración de los mercados, la internacionalización de los procesos y la interrelación de personas y organizaciones digitales. Estas interrelaciones, en especial las comerciales, son susceptibles de derivar en conflictos que ni los sistemas judiciales nacionales ni los transnacionales tradicionales pueden asimilar porque no están debidamente adecuados a esta nueva realidad.

Son particularmente frecuentes los problemas entre empresas que se interrelacionan en operaciones de comercio exterior en *marketplaces* digi-

[4] A mayor abundamiento ver: Cáceres Nieto Enrique, *Inteligencia artificial aplicada al derecho. Memoria del congreso internacional de culturas y sistemas jurídicos comparados*, Instituto de Investigaciones Jurídicas, UNAM, 2005.

tales (importación-exportación, *joint ventures*, alianzas estratégicas, etc.) o problemas entre *partners* en redes de valor agregado en entornos Electronic Data Interchange (EDI VANS, por sus siglas en inglés). Estos conflictos cada vez se vuelven más comunes en función de las relaciones entre consumidores finales y tiendas virtuales, bancos virtuales y sus clientes u operadores financieros, etcétera.

Por eso los sistemas alternativos de solución de disputas (ADR, por sus siglas en inglés), como el arbitraje, la mediación y la conciliación, presentan claros beneficios y ventajas prácticas en relación con los procesos estatales, en particular para la solución de conflictos dentro de estructuras digitales.

Algunos de sus principales beneficios son:

- Autonomía de la voluntad de las partes.
- Posibilidad de elegir un conciliador o árbitro neutral en otros países.
- Posibilidad de utilizar tecnologías e infraestructuras tecnológicas muy avanzadas (sistemas multiagentes, *webrobots*, *datamining*, etc.).
- Procesos extrajudiciales muy cortos, simples y flexibles (manteniendo todos los derechos de las partes).
- Trabajo y discusión en tiempo real al tratarse de solución *on line* de conflictos.
- No hay posibilidad de prolongar los procesos mediante apelación.
- Costos mucho más bajos.
- Privacidad y confidencialidad durante el proceso y después de él.
- Reducción de la hostilidad emocional entre las partes.
- Posibilidad de que expertos evalúen el caso y dicten el laudo (esto es particularmente importante en casos de comercio electrónico y nuevas tecnologías).
- Posibilidad de que un laudo dictado en un país sea válido en cualquier otro país (tratados internacionales).

Primeras experiencias

Virtual Magistrate. En marzo de 1996 se inauguró el proyecto Virtual Magistrate, un servicio de arbitraje en línea resultante de la colaboración entre el Cyberspace Law Institute (CLI) y el National Center for Automated Information Research (NCAIR). El objetivo primordial del proyecto era estudiar la manera de resolver las diferencias entre un usuario y un operador de redes, o entre usuarios. El ámbito de aplicación del proyecto se limitaba a los conflictos generados por mensajes o ficheros con contenido ilícito.

El procedimiento de *arbitraje* era voluntario y se efectuaba esencialmente por correo electrónico. Conviene precisar que se trataba de un me-

canismo que podría denominarse *arbitraje contractual*, es decir, un mecanismo que, aunque surtía algunos efectos "obligatorios", no tenía efectos ejecutorios con arreglo a las legislaciones y los tratados sobre reconocimiento y ejecución de sentencias arbitrales. El proyecto Virtual Magistrate se prosigue bajo los auspicios de la Universidad Chicago Kent.

On-line Ombuds Office. El proyecto Online Ombuds Office (Oficina de Mediadores en Línea) es una iniciativa del Center for Information Technology and Dispute Resolution de la Universidad de Massachusetts. Desde 1996, este organismo ofrece servicios de mediación para determinados conflictos que se generan en internet, en particular los litigios entre miembros de un grupo de debate, entre competidores, entre proveedores de acceso a internet y sus abonados, así como los relacionados con la propiedad intelectual.

Se han emprendido investigaciones en relación con el uso de textos y gráficas para ayudar a las partes que deciden iniciar un proceso de solución de diferencias. Así, se les envían propuestas de transacción y las partes, con ayuda de gráficos dinámicos y otros instrumentos tecnológicos, tratan de medir la índole, el origen y el grado del agravio y definir con mayor precisión las concesiones recíprocas que deseen. El proyecto se prosigue en la actualidad.

CyberTribunal. El CyberTribunal era un proyecto experimental elaborado por el Centre de Recherche en Droit Publique (CRDP, por sus siglas en francés) de la Universidad de Montreal, en septiembre de 1996. El proyecto apuntaba a determinar si era viable utilizar mecanismos alternativos para resolver conflictos generados en entornos electrónicos.

El ámbito de aplicación del CyberTribunal era mucho más amplio que el del Virtual Magistrate y Online Ombuds Office. Pese a su denominación, es importante aclarar que el CyberTribunal no se erigía en juez. En cambio, trataba de moderar el diálogo entre las partes en el litigio (mediación) y, en su caso, prestar asistencia administrativa y tecnológica en el proceso de adopción de decisiones con base en la voluntad de las partes (arbitraje). El proyecto llegó a su término en diciembre de 1999. El principal artífice del sistema estableció un nuevo proyecto denominado eResolution, que se verá más adelante.

Ejemplos más recientes

SquareTrade. Fundado en otoño de 1999, funciona casi exclusivamente en el sector del comercio electrónico entre consumidores (C2C). La sociedad estadounidense ofrece dos posibles servicios de solución de diferencias: la negociación directa y la mediación. Su asociación con eBay, uno de los más importantes sitios de subastas en el ciberespacio, ha generado rápidamente un importante volumen de casos.

El desarrollo del procedimiento, muy informal, estimula las soluciones amistosas en todas las etapas. En un primer momento, el comprador o el vendedor presentan una queja a SquareTrade, recopilando toda la información pertinente en un formulario electrónico. A continuación se notifica a la contraparte por correo electrónico. Si se presenta una respuesta, SquareTrade permite a las partes el acceso a formularios en un sitio protegido, mediante contraseñas y nombres de usuario. En esta etapa las partes pueden tratar de resolver el litigio en forma amistosa. Si no llegan a un entendimiento, podrán pedir a SquareTrade que designe un mediador, en cuyo caso deberán pagar un honorario bastante modesto. Si en cambio llegan a un arreglo, con o sin ayuda del mediador, la diferencia quedará zanjada y se comunicará a las partes un documento en el que se consigna el acuerdo.

Respecto a la solución en línea de litigios relativos a los nombres de dominio existe *eResolution*. Fundado en el otoño de 1999, inauguró su primer servicio de solución en línea de diferencias el 1 de enero de 2000, cuando recibía la acreditación de la Corporación Internet para Nombres y Números Asignados (ICANN, por sus siglas en inglés) para administrar la solución de conflictos relativos a nombres de dominio, de conformidad con su política. La plataforma tecnológica de eResolution ha permitido resolver de esta manera varios cientos de asuntos con alcance mundial.

El procedimiento de la ICANN allana todas las dificultades relativas a la aplicación o ejecución de las decisiones adoptadas. En efecto, el poseedor del nombre de dominio está vinculado por su contrato de inscripción ante el órgano registrador, el que, con el fin de obtener su acreditación como tal, se compromete a aplicar la política de la ICANN para la solución de litigios sobre nombres de dominio. En virtud de esta política, el órgano registrador ejecuta las decisiones, salvo cuando se interponga un recurso ante los tribunales en un plazo determinado, y procede directamente a la anulación o la transferencia ordenada con arreglo a la política.

El eResolution procedió desde el comienzo a transformar el procedimiento de la ICANN, basado en documentos, en un procedimiento en línea. Gracias a la tecnología establecida por eResolution, las partes, los encargados de la adopción de decisiones y los administradores de los expedientes pueden cumplir todo el trámite en línea. De hecho, todos los intercambios se realizan en un entorno protegido, al que puede accederse con el nombre del usuario y la contraseña.

REQUISITOS FORMALES Y ARBITRAJE EN LÍNEA

A primera vista, la infraestructura jurídica sobre la que se basa el arbitraje internacional puede aceptar sin mayores dificultades la introducción de los medios de comunicación electrónicos. La primera cuestión que se plantea

se refiere a la validez de un acuerdo de arbitraje concluido por medios electrónicos. Se examina aquí el problema relacionado con el respeto de determinadas formalidades impuestas a veces por los textos, en los planos nacional e internacional, en lo tocante a la validez o la prueba de un compromiso o de una cláusula compromisoria. En el plano nacional, en diversas legislaciones nacionales se exige un documento escrito cuando es necesario reconocer los efectos jurídicos de un acuerdo de arbitraje. En el plano internacional, si la Convención de Nueva York se interpreta de manera restrictiva, también se tiene la impresión de que en ella se exige un documento escrito. ¿Qué validez tiene un acuerdo de arbitraje concluido en línea en un contexto de esa naturaleza?

En lo que respecta a las legislaciones nacionales, es evidente que la adaptación de los requisitos formales a las nuevas exigencias del comercio no se podrá realizar en todas partes con la misma facilidad ni la misma rapidez, pero finalmente tendrá lugar. En lo referente a la Convención de Nueva York, se recomienda una interpretación flexible a fin de que la noción de escrito pueda aplicarse a los textos sin soporte material.

La segunda cuestión concierne a la notificación de los documentos. Una vez más, esto constituye un problema bastante insignificante si se considera que es un obstáculo a la informatización de un procedimiento arbitral. En efecto, con el acuerdo de las partes no hay nada que se oponga a la notificación de documentos por medios electrónicos. En cuanto a la prueba del envío y de la recepción en materia de mensajería electrónica, los dispositivos de mensajería interna protegida, que ya se pueden encontrar en los centros serios de solución de litigios en línea, esquivan ese problema de modo satisfactorio. Lo mismo sucede con los problemas de confidencialidad de las comunicaciones.

La tercera cuestión se refiere a la instrucción de la causa. Aquí se puede hacer una distinción entre las audiencias, comprendida la administración de la prueba testimonial o documental por un lado y la cuestión del lugar de arbitraje por otro. En lo que respecta a las audiencias, la videoconferencia ya se utiliza en varios arbitrajes internacionales. Actualmente esa técnica tiende a democratizarse gracias a internet y da lugar a importantes ahorros. De todas formas, cabe recordar que una parte importante del procedimiento arbitral es el intercambio de cartas y documentos entre las partes y los árbitros, que puede realizarse por medios electrónicos.

No se tratarán aquí las modalidades de administración de la prueba por escrito, pero cabe señalar de manera breve que en la mayoría de los sistemas jurídicos las partes disponen de ella con libertad. Se debe recordar también que el problema de la informatización sólo se plantea si se impugna la autenticidad de los documentos, caso que rara vez se presenta. Dejemos a un lado también la cuestión del lugar del procedimiento y mencionemos simplemente la tendencia actual a admitir que se fije un lugar

ficticio para el arbitraje, vale decir un lugar al que ni las partes ni los árbitros deberán trasladarse para llevar a cabo el procedimiento.

La cuarta y última cuestión concierne al dictamen de la sentencia. Si se analiza la cuestión suficientemente a fondo, el problema planteado por el dictamen de la sentencia puede asimilarse en gran medida al mencionado al tratar la cláusula de arbitraje y el compromiso. También hay que señalar una dificultad complementaria: la sentencia debe firmarse. Así como para la convención de arbitraje, se puede esperar que en este caso la armonía de las normas técnicas y la interpretación flexible de los textos existentes servirán para asegurar rápidamente a los operadores respecto a la fuerza ejecutoria de una sentencia sin soporte material. Por otra parte, el arbitraje en línea no espera.

ARBITRAJE Y COMERCIO ELECTRÓNICO

En cuanto a la justicia y su administración, la reflexión sigue el mismo sentido. El arbitraje es la única solución viable para la solución de los litigios planteados por un comercio electrónico forzosamente internacional, y el arbitraje en línea es el único mecanismo que puede garantizar una adecuación entre los costos de la justicia y lo que está en juego en los contratos internacionales que ya no son privativos de los grandes grupos. Como sucede con las normas materiales aplicables a los contratos, las normas consensuales que facilitan la solución de litigios se alejan con rapidez de cualquier tipo de recurso a las normas de procedimiento de un sistema jurídico particular. En menor medida, esas disposiciones para la solución de litigios también tienden a estar determinadas por los usos de la industria en cuestión. Una vez más, si en un futuro el papel de las asociaciones de comerciantes se combina con el de las grandes plazas de mercado electrónicas, cabe pensar que el arbitraje se transformará en jurisdicción de derecho común.

ARBITRAJE DE LOS ASUNTOS DE PROPIEDAD INTELECTUAL

Este arbitraje no se plantea en el marco de los litigios relativos a los nombres de dominio. Aunque habilitado por la administración pública, en este caso el Congreso de Estados Unidos, en lo referente al sistema de direccionamiento internet la ICANN funciona como un agente privado. Se ha señalado que el sistema de solución de diferencias establecido por la ICANN ha sentado precedente y que existe la posibilidad de aplicar ese modelo a otros sectores de la propiedad intelectual. En efecto, estimamos que los mecanismos de arreglo de diferencias en línea podrían ser muy útiles desde el punto de vista jurídico en el caso de los litigios de propie-

dad intelectual que pueden plantear las transacciones informáticas a través de internet. En consecuencia, la cuestión del arbitraje de los asuntos de propiedad intelectual se traslada a los otros sectores.

Al examinar distintas legislaciones se advierte que actualmente la mayoría de los países desarrollados reconocen que, por lo general, los litigios de propiedad intelectual son arbitrables. Pese a ello, recurrir al arbitraje supone la existencia previa de un vínculo contractual entre las partes y la inclusión de una cláusula compromisoria en dicho contrato. Evidentemente, si no existe ese vínculo o una cláusula compromisoria, las partes siempre podrán aceptar de manera voluntaria que su litigio se solucione por arbitraje, incluso si ese medio es más aleatorio. De este modo, los contratos de licencias de propiedad intelectual, los de transferencia de propiedad intelectual y los de investigación o de trabajo, en relación con los que la propiedad intelectual elaboró y desarrolló, pueden estar sujetos a litigios arbitrables. Así, en los entornos electrónicos en los que el contrato parece un marco normativo en particular prometedor, puede entenderse que los litigios de propiedad intelectual fundamentados en contratos se traten mediante mecanismos de arreglo de litigios en línea.

CENTRO DE ARBITRAJE Y MEDIACIÓN DE LA OMPI

Este centro tiene su sede en Ginebra, Suiza, y fue creado en 1994 para ofrecer servicios de arbitraje y mediación en relación con controversias internacionales comerciales entre partes privadas. Los procedimientos que ofrece el centro, diseñados por expertos de renombre en la solución de controversias internacionales, se consideran en especial adecuados para controversias en el campo de la tecnología, el espectáculo y otras en materia de propiedad intelectual a escala mundial.

El centro ha movilizado los recursos necesarios a fin de establecer un marco operativo y jurídico para la administración de controversias relacionadas con internet y el comercio electrónico. Con ello ha logrado, por ejemplo, que se le reconozca como uno de los principales proveedores de servicios de solución de controversias en lo tocante a las controversias que plantean el registro y el uso de los nombres de dominio de internet. Además, también suele consultarse al centro acerca de cuestiones relacionadas con la solución de controversias en materia de propiedad intelectual e internet.

El centro también presta servicios de asesoría en materia de solución de controversias y ha trabajado con distintas organizaciones para desarrollar sistemas de solución de controversias concebidos para satisfacer sus requisitos específicos. Actualmente, el centro presta asistencia al Application Service Provider Industry Consortium, consorcio internacional no

lucrativo formado por más de 400 de las principales empresas mundiales dedicadas a las tecnologías de la información, en la elaboración de un conjunto de mejores prácticas y directrices para prevenir y solucionar las controversias internacionales.

En el desempeño de sus funciones, el centro recibe el apoyo de una comisión consultiva y del Consejo de Arbitraje de la OMPI, ambos integrados por expertos de alto nivel en la solución de controversias que atañen a varios países.

El Centro de la OMPI, al igual que otras instituciones, es miembro de la Federación Internacional de Instituciones de Arbitraje Comercial (IFCAI).

Independiente e imparcial, dicho centro es una dependencia administrativa de la Oficina Internacional de la Organización Mundial de la Propiedad Intelectual (OMPI).

INSTITUTO PARA LA RESOLUCIÓN DE CONFLICTOS (CPR)

Este instituto es una alianza no lucrativa constituida por organismos multinacionales y despachos prestigiosos para ofrecer a empresas e instituciones públicas una alternativa a los costosos procesos judiciales. El CPR está formado por 500 asesores legales de las mayores empresas, socios de los mejores despachos, catedráticos notables e instituciones públicas seleccionadas.

Una de sus maneras de actuar es a través de los llamados paneles de neutralidad, en los que unos 600 abogados nacionales e internacionales, jueces y ejecutivos con formación legal garantizan una neutralidad en todos los niveles (internacional, nacional, regional y específico) sirviendo de mediadores y llevando a cabo otros papeles neutrales.

Desde su fundación en 1979, la misión del CPR ha sido integrar alternativas para la solución de conflictos (ADR) en el marco de departamento legal y práctica jurídica. Para el cumplimiento de esta misión, el CPR está comprometido con una agenda integrada de investigación y desarrollo, educación, abogacía y servicios de solución de conflictos. Además, incluye en su programa extensas publicaciones: libros, videos, modelos de procedimiento de resolución de conflictos y herramientas prácticas en más de 20 áreas tanto sustantivas como procedimentales, así como modelos formales y sus cláusulas correspondientes.

FORO DE ARBITRAJE NACIONAL (NAF)

Este foro fue fundado en 1986 en Minneapolis, Minnesota, y ha sido notable por su neutralidad en la toma de decisiones y la aplicación de leyes

sustantivas para resolver casos de arbitraje. Recientemente el NAF ha sido citado por trabajar con grandes compañías, como bancos, compañías de seguros y fabricantes de computadoras, al requerir a sus clientes a renunciar a sus derechos legales y someterse al *to binding* al arbitraje en caso de controversias. Algunos han acusado al NAF de estar de parte de las grandes compañías que pagan los derechos de arbitraje a fin de conservar en el futuro esos negocios. El NAF obtuvo la aprobación como un proveedor de servicio para la resolución de disputas por ICANN el 23 de diciembre de 1999.

CIBERCORTE EN MICHIGAN

Para tentar a las compañías tecnológicas a que se instalaran en Michigan, Estados Unidos, el gobernador John Engler firmó, a principios de 2002, un decreto para establecer una "cibercorte" independiente, para los casos que tengan que ver con empresas de alta tecnología, en los cuales casi todo se puede resolver vía computadora en lugar de "presencialmente" en tribunales, pretendiendo iniciar actividades en octubre. En este caso, los informes podrían presentarse *on line*; la evidencia, verse en video; los alegatos orales, mediante teleconferencias; las conferencias, vía e-mail. Los abogados no tienen que estar en Michigan. Ni siquiera es necesario que tengan licencia para litigar en ese estado. Las audiencias pueden realizarse en cualquier momento del día, incluso de noche, y los jueces están capacitados para manejar las cuestiones complejas que surjan en disputas tecnológicas.

Se tiene la esperanza de que las empresas tecnológicas se sientan atraídas a "emigrar" a Michigan, de la misma manera que las 500 compañías de Fortune se instalaron en Delaware, donde existe una división de la Suprema Corte de Justicia especialmente habilitada para manejar litigios comerciales. Una de los mayores interrogantes es la jurisdicción de esta corte. Los casos a llevarse ante esta cibercorte implicarían sumas de 25 000 dólares como mínimo y a las partes en litigio se les cobran honorarios más altos que en las cortes regulares.

Por su parte, el estado de Maryland está pensando en una división judicial independiente que pueda seducir a las empresas de alta tecnología. Pero, para algunos abogados y jueces, la idea plantea interrogantes sobre muchas cuestiones, entre ellas el manejo de la evidencia y la capacitación de los jueces. También propone beneficios impositivos para las compañías tecnológicas y el estado ofrece millones de dólares en préstamos destinados a la investigación y el desarrollo de productos en el área de la biotecnología.

DIRECTIVA EUROPEA

El artículo 17 de la Directiva Europea sobre Comercio Electrónico hace referencia a la solución extrajudicial de litigios y dispone en su apartado primero que los Estados miembros velarán por que, en caso de desacuerdo entre un prestador de servicios de la sociedad de la información y el destinatario de aquéllos, su legislación permita utilizar de manera efectiva mecanismos de solución extrajudicial, incluso mediante vías electrónicas adecuadas. Este tipo de mecanismo parece en particular útil para determinados litigios en internet, en especial para los de grandes cantidades y de acuerdo con la envergadura de las partes, que pueden renunciar a emplear los procedimientos judiciales debido a sus costos.

CIBERTRIBUNAL DE LIEJA (BÉLGICA)

Proyecto propuesto a la Fundación Rey Baudouin a finales de 2000, a iniciativa de la barra de abogados de dicha ciudad (programa "Justicia en movimiento") y dentro de los programas pilotos de E-Justice de la Unión Europea, apoyado por el Ministerio de Justicia, que pretende establecer un *cibernexo* entre 800 abogados barristas y los órganos jurisdiccionales (inicialmente está considerada la materia laboral) para intercambiar información entre ambas instancias permitiendo la gestión de litigios por este medio. El proyecto es desarrollado por las facultades de Derecho de Lieja y Namur dentro del rubro de Procedimientos y Nuevas Tecnologías.

EL ESTÁNDAR XML Y SU USO PARA APLICACIONES LEGALES

El término XML significa Extensible Markup Language, y es una especificación derivada del HTML, lenguaje que permite ser leído por cualquier clase de computadora; por ejemplo, un contrato podría contener cláusulas específicas sobre jurisdicción, arbitraje, distribución de responsabilidad, etc., y la computadora podría reconocer en forma automática esta situación, pues esos datos pasan a ser información dadas ciertas circunstancias. Esto no sería posible con un contrato en papel o en lenguaje HTML donde los elementos sólo sirven para marcar atributos del texto (como el tipo o tamaño de la letra). Se trata de un texto plano que, pese a poseer hipervínculos, no contiene significado alguno para la computadora.

Algunas de las principales ventajas son: simplificar la presentación de escritos judiciales, reducir el uso del papel, disminuir los errores de copia y transcripciones y facilitar el acceso, búsqueda y difusión de documentos legales. Su propósito es tener un medio común, con estándares amplia-

mente difundidos, aceptados y establecidos que puedan utilizar todos los actores del proceso judicial.

Se requiere que todos los sistemas informáticos compartan los mismos estándares, que funcionen de la misma manera, en forma compatible, y que estos estándares sean aceptados por todos los usuarios.

ONTOLOGÍAS

Como afirma Edgar Aguilera,[5] el sentido original de la expresión *ontología*, acuñado en el ámbito filosófico, mantiene algunos de sus elementos cuando se emplea en el contexto de la ingeniería del conocimiento. Los elementos que persisten en el uso informático de la expresión son:

a) La función de realizar el análisis de carácter teórico de algún dominio del mundo.
b) El elemento metodológico consistente en la elaboración de un sistema conceptual que identifique las características más generales de un dominio y en la articulación de aquél en términos de las clases de conceptos y de relaciones entre aquellas que pueden establecerse.
c) El análisis del comportamiento lingüístico de los participantes relacionados con el dominio, propio de las investigaciones ontológicas internas.

En relación con *a*), se trata de lo que adolecieron los sistemas expertos en alguna época en general, y los SEJ en sus intentos pioneros. Para que pudiera tener lugar este análisis en el contexto de desarrollo de un SEJ se propuso la estandarización del enfoque basado en modelos. En relación con *b*), podría suponerse que se trata del mismo método, empero, cabe recordar que en el contexto de la realización de una conceptualización se adiciona un grado más de abstracción consistente en la elaboración de un metasistema conceptual que proporciona una interpretación simplificada del dominio, la cual resalta los aspectos que interesa representar al ingeniero del conocimiento. En relación con *c*) es oportuno aclarar que en el caso del desarrollo de un SEJ, sobre todo en el contexto mexicano, debe tenerse en cuenta que en muchas ocasiones las prácticas lingüísticas de los operadores jurídicos ocultan la realización de ciertos procesos cognitivos más sofisticados de lo que puede suponerse si se toma en consideración únicamente el registro de su actividad lingüística.

[5] Aguilera García, Edgar Ramón. *Inteligencia artificial aplicada al derecho*. Instituto de Investigaciones Jurídicas. UNAM. Ciudad Universitaria, DF. México. 2007.

También relacionado con el punto anterior, pero tratándose del análisis del discurso teórico jurídico, la función de la elaboración de una ontología no sólo consiste en extraer de los diversos modelos sus conceptos y relaciones relevantes, sino que además debe considerarse el grado de invulnerabilidad a los contraargumentos que se esgrimen en su contra para estar en condiciones de determinar cuál de aquéllos se asumirá.

Clasificación de las ontologías

El mismo autor,[6] haciendo referencia a Bench-Capon, que se basa en la noción de compromisos ontológicos y en la clasificación que de aquéllos puede hacerse, ofrece la siguiente tipología de las ontologías.

Compromisos ontológicos

Cada ontología imprime a algún fragmento de la realidad cierta estructura mediante un conjunto de conceptos y sus relaciones.

"El conjunto particular de conceptos y relaciones con los que una ontología describe una parte del mundo constituye los compromisos ontológicos de ella." Los compromisos ontológicos pueden clasificarse como sigue.

a) *Compromisos con tareas*. Una ontología hace este tipo de compromisos cuando define entidades y relaciones que expresan una perspectiva del conocimiento del dominio enfocada a tareas. Por esta expresión se entiende la especificación de un objetivo o meta junto con el tipo de información requerida (*input*) y el tipo de conducta deseada (*output*).
b) *Compromisos con métodos*. Una ontología hará este tipo de compromisos si define un grupo de conceptos y relaciones que expresan una perspectiva del conocimiento del dominio enfocada en los métodos, es decir, en la manera en que las tareas deben llevarse a cabo.
c) *Compromisos con el dominio*. Una ontología hará este tipo de compromisos si define un grupo de entidades y relaciones que aportan una estructura general al dominio de aplicación. Por la expresión *dominio* se entiende el fragmento de la realidad que se distingue para ser modelado (las matemáticas, finanzas, medicina, derecho, etc.).

Hecha la distinción del tipo de compromisos ontológicos que pueden hacer las ontologías podemos clasificarlas de la siguiente manera.

[6] *Ibid.*

Clasificación de las ontologías en atención a sus compromisos ontológicos

a) Ontologías que hacen compromisos sustanciales con determinada tarea o grupo de éstas.
b) Ontologías que hacen compromisos sustanciales con un método o grupo de éstos.
c) Ontologías que hacen compromisos sustanciales con la imposición de una estructura particular a un dominio o varios.

Ontologías jurídicas

Restringiéndonos estrictamente al ámbito jurídico, es válida la siguiente clasificación:[7]

Ontologías generales del dominio jurídico: aquellos sistemas conceptuales que aportan una visión abstracta y simplificada acerca de las características generales del derecho y de los procesos cognitivos que pueden llevar a cabo sus operadores en situaciones diversas.

Ontologías de subdominios jurídicos: aquellas que identifican los conceptos fundacionales, y la manera como aquéllos se relacionan, de ciertas áreas específicas de actividad de los operadores jurídicos, por ejemplo, derecho fiscal, penal, civil, administrativo, juicio hipotecario, ordinario, ejecutivo mercantil, etcétera.

Expresión de las ontologías

La expresión de las ontologías varía en un espectro que va desde las más informales articulaciones en lenguaje natural (por ejemplo, esquemas de representación semiformales; redes semánticas) hasta la utilización de lenguajes formales al estilo de los sistemas deductivos axiomáticos de la ciencia, de acuerdo con el contexto de problemas que su implementación pretenda resolver.

En el caso en que la elaboración de la ontología presuponga un ejercicio de conmensurabilidad (*sen do* ampliado), como en el de la unificación de las diversas visiones de un dominio aportadas por científicos provenientes de diversas disciplinas (investigaciones interdisciplinarias), normalmente no es necesaria la expresión formal, pero se recomienda usar esquemas de representación como las redes semánticas.

[7] *Ibid.*

Una red semántica es una jerarquía taxonómica cuya espina dorsal está constituida por un sistema de enlaces de herencia entre los objetos o conceptos de representación, conocidos como *nodos*.

Los nodos se interconectan a través de las llamadas *ligas* (links) que expresan una relación que muestra el esquema X *es un* Y.

Las redes semánticas son el resultado de la observación de que gran parte del conocimiento humano se basa en la adscripción de un subconjunto de elementos como parte de otro más general. Las taxonomías naturales clásicas son un buen ejemplo, por ejemplo, un perro es un canino, un canino es un mamífero, un mamífero es un animal, etcétera.

Ontologías (sistemas conceptuales)
Medios de expresión
Esquemas de representación (redes semánticas)
Lenguajes formales (kif y ontolingua)
Lenguajes naturales (francés, inglés, etc.)

El concepto de *herencia* es fundamental para entender el funcionamiento de las redes semánticas. La expresión *herencia* denota el sistema de razonamiento que lleva a un agente a deducir propiedades de un concepto con base en las propiedades de conceptos más altos en la jerarquía.

Es importante mencionar que los nodos pueden representar clases de individuos (*types*) o instancias particulares de esas clases (*tokens*). Los *tokens* se sitúan en la parte más baja de la jerarquía, mientras que los *types* en una posición superior.

No obstante, cuando se trata de lograr la adecuada y consistente transmisión e intercambio de información entre aplicaciones informáticas que codifican los datos mediante la utilización de diversos esquemas de representación o lenguajes de programación, se recurre a un lenguaje formal a nivel de interfase que facilita la comunicación entre las aplicaciones que interactúan, tales como el formato para el intercambio de conocimientos y la ontolingua.[8]

¿QUÉ ES XML?

XML significa "Extensible Markup Language" (por sus siglas en inglés —lenguaje extensible de marcas—). Es un lenguaje de marca basado en texto. Muy similar a HTML, donde los datos se identifican mediante etiquetas o marcas (ej.: <nombre>)

Las etiquetas en XML revelan el significado de los datos pero no la forma de visualizarlos, como en HTML.

[8] *Ibid.*

Es un conjunto de normas que permiten presentar la información en diferentes vistas y sistemas distintos.

XML proviene de un conjunto de lenguajes de marcas basados en texto, SGML (Standard Generalized Markup Language), donde XML, HTML, etc., son un conjunto de este tipo de lenguajes.

¿Cuál es la funcionalidad de XML?

Se trata de un estándar de creación de documentos. Las utilidades serán independientes de cada empresa y desarrollador.

XML define los mecanismos necesarios para la creación de formatos uniformes de intercambio de datos, y las herramientas adecuadas para la comprobación y validación. Esto lo hace atractivo para el intercambio electrónico de documentos, ya que su medio de transportación puede intercambiarse a través de internet.

Historia de XML

¿Cómo nació XML?

Haciendo un poco de historia cabe remontarse a los años de 1970, cuando los sistemas informáticos eran propiedad de las empresas que los creaban, lo que repercutía en la incompatibilidad de ellos. Por eso la empresa IBM encargó a Charles F. Goldfarb que diseñara un sistema estándar para la creación y edición de documentos que fueran compatibles con cualquier sistema.

Charles Goldfarb trabajó con Ed Mosher y Ray Lorie, por lo cual nació el pionero de los lenguajes de marcas SGML. Se continuó con el desarrollo y entre 1978 y 1986 se creó la norma ISO 8879.

¿Quién ha creado XML?

El Word Wide Web Consortium (W3C)

W3C se creó en 1994 y su fin primordial es servir de apoyo y creación de las distintas técnicas relativas a los estándares utilizados en Internet, entre ellos XML. (*Fuente*: amece.org.mx)

Estructura XML

¿Por qué es importante XML?

- Es texto plano (fácil depuración y escalabilidad)
- Identifica los datos (fácil de utilizar por los programadores)

- Permite aplicar hojas de estilo (XSL) para mostrar su contenido a través de un Browser
- Jerárquico (rápido y fácil de buscar). Empiezan a salir BD especializadas en almacenar contenido XML

La creación de documentos XML tiene que cumplir con un esquema de árbol, donde se inicia con etiquetas comunes, es decir, al crear una etiqueta XML ésta deberá encerrar los datos a mostrar y cerrar con la misma etiqueta de inicio, por ejemplo:

```
<arbol>
<etiqueta>datos a escribir</etiqueta>
```

DTD: las especificaciones para asegurar la validez de un documento se llaman DTD. Esta especificación forma parte del estándar XML y especifica los tipos de elementos que puede incluir un documento y su posición correcta.

- SAX, DOM: especificaciones de programación (API) para acceder a los datos de un documento XML. SAX para acceso mediante eventos y DOM para acceso directo en forma de árbol.
- XML namespaces, para construcción de nombres universales sin posibilidad de colisión.

    - XSL: Estándar que permite formatear y transformar documentos XML

- XQL: XML Query Language

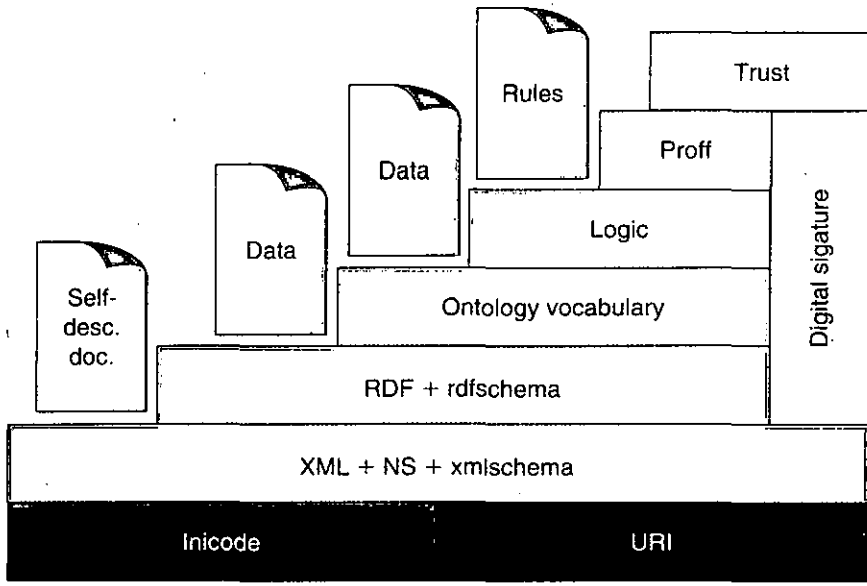
    - XLINK: permite hacer links entre documentos XML

- XSL se refiere a las siglas eXtensible Style Language o lenguaje de estilos extensible.

    - XSL es un lenguaje específico para tratar datos de un documento XML, haciéndose cargo también de su presentación
    - XSL es XML como CSS es a HTML

Según Berners Lee, la web semántica es una "red de datos que pueden ser procesados directa o indirectamente por máquinas". Es decir, una forma de búsqueda, gestión y organización de la información de la red que utiliza propiamente conocimiento en lugar de un mero matching sintáctico. La clave entonces consiste en la representación formal de este conocimiento en lenguajes como el XML, que proporciona una sintaxis para

documentos organizados, pero sin imponer ninguna restricción semántica, que permiten compartir con las computadoras la flexibilidad, intuición y capacidad rápida de asociación de las estructuras conceptuales del lenguaje natural humano.



Fuente: Semantic Web - XML2000 , de Tim Berners-Lee .

Es necesario subrayar que la web semántica no es simplemente una mejor forma de realizar búsquedas, sino que trata de organizar y gestionar el conocimiento (explícito e implícito) contenido en los documentos previamente almacenados y proporciona la interfaz de comunicación necesaria entre el lenguaje natural en que se expresa el usuario y los lenguajes simbólicos de la computadora. La interacción es necesaria para facilitar el aprendizaje y el refinamiento tanto del conocimiento del usuario como del conocimiento almacenado.

De esta forma, a decir de Pompeu Casanova,[9] el vínculo entre lo que el usuario tiene en mente y los objetos informáticos se denomina "ontología". Una ontología es la representación de la estructura de los objetos conceptuales del usuario para compartirlos con la red de computadoras o, en expresión de Studer, Benjamins y Fensel, "la organización conceptual de la red de un modo explícitamente legible para una máquina" (1998).

[9] Pompeu Casanova. *Ontologías jurídicas profesionales.* Sobre "conocer" y "representar" el derecho Instituto de Derecho y Tecnología. Universidad Autónoma de Barcelona. En memoria de Miguel Sánchez Mazas. Madrid, 10-11 de marzo de 2005.

En suma, las ontologías son estructuras conceptuales compartibles, escalables y reutilizables. Otra forma de entenderlas es darse cuenta de que constituyen algo así como la oposición de una escala de dimensión humana a la red de escala libre mediante la que se representa internet. Inciden en la organización del conocimiento y, más allá, en la posibilidad de uso racional de la red.

El derecho —y en particular el ámbito judicial— constituye un ámbito privilegiado de aplicación para la web semántica. Existen ya algunas ontologías jurídicas que han permitido la construcción de prototipos de asistencia, búsqueda y organización documental de la información almacenada en los bancos de datos jurídicos.[10]

Para Casanova,[11] las estructuras jurídicas existentes suelen tener una fuerte relación con los conceptos de la teoría clásica del derecho. Esto significa que entre cualquier ontología de alto nivel (*upper, top ontology*) y la ontología de dominio (*domain specific*) se sitúa un nivel interpretativo intermedio que —al contrario de lo que sucede en la modelización de otros ámbitos— no puede ser obviado. En este nivel se toman las decisiones teóricas básicas sobre los conceptos cuyas relaciones la ontología va a contemplar para efectuar el vínculo con las instancias del nivel inferior y las categorías fundamentales que asumen las ontologías de nivel superior (energía, tiempo, entidad...).

Una ontología jurídica profesional se distingue de una ontología jurídica de otro tipo por el hecho de que los conceptos modelizados se basan en el conocimiento práctico desarrollado por los profesionales del derecho —jueces, fiscales, abogados...— en la realización de las tareas propias de su trabajo diario. Éste es un conocimiento personal, disperso desde el punto de vista organizacional y desigualmente distribuido entre el colectivo. La representación del conocimiento adquirido en una ontología plantea el reto de reconstruirlo de un modo que permita la identificación del vocabulario común, la organización de la estructura de las relaciones entre sus conceptos básicos y la esquematización de las pautas de razonamiento más habituales.

El modo de realizar dichas tareas en las ontologías jurídicas suele consistir en la representación formal intuitiva de los conceptos considerados nucleares (*legal-core ontologies*). Generalmente, estos conceptos se expresan en un lenguaje normativo de derechos, deberes y permisiones.

---

[10] Véase una buena síntesis de las ontologías existentes en A.Valente (2005), Valente, André. "Types and Roles of Legal Ontologies", en Benjamins y cols., *Law and the Semantics Web, op. cit.* pp. 65-76. Los primeros Proyectos Europeos se sitúan en el 5o. Programa Marco (1999-2003). Comprenden e-POWER, CLIME y, de forma especialmente interesante para nosotros, e-COURT (Electronic Court: Judicial IT-based management).

[11] *Ibid.*

Una ontología del conocimiento jurídico profesional empieza con los problemas de la adquisición y representación de este tipo de conocimiento. Es importante darse cuenta de que, a efecto de recuperar información semánticamente enriquecida, no es necesario intentar responder las preguntas de los usuarios mediante el ejercicio de modos de razonamiento jurídicamente análogos. Basta con ofrecer al juez la información estructurada que necesita para tomar la decisión en el momento justo. Pero, para ello, se requiere un conocimiento extenso del entorno de uso, del perfil del usuario y de sus necesidades prácticas. En otras palabras, resulta imprescindible representar el conocimiento profesional del juez en términos que no se confundan con los de la pretensión de conocer el derecho que el juez a su vez conoce. Esta confusión puede llevar a ignorar que un juez en su lugar de trabajo, ante un caso concreto, suele aplicar a su resolución no solamente un conocimiento experto (dogmático, jurisprudencial...), sino también un conocimiento basado en su experiencia anterior de juzgar. Y este segundo tipo de conocimiento contextual es no explícito, tácito y acumulativo.

En la web semántica se manifiesta la necesidad de incrementar la adquisición y representación del conocimiento propuesto por las distintas metodologías existentes para la construcción de ontologías con métodos sociológicos y jurídicos.

Ahí —en cómo se realiza materialmente esto— está la discusión, en absoluto desconocida por los expertos en derecho y computación. No obstante, ahora, con la explosión de internet, la aparición de los servicios web y los nuevos lenguajes de la red, la discusión es más urgente, si cabe decir.

Como dicen Flores, Martín y Arellano,[12] los lenguajes de marcado de texto como el XML pueden ser contemplados como una tecnología complementaria o alternativa a las bases de datos documentales convencionales y presentan ventajas notables sobre éstas para la gestión de colecciones de documentos extensos, con estructura compleja y variable y abundantes referencias cruzadas, como es el caso de los documentos jurídicos. Se exponen experiencias de tratamiento y difusión de documentación jurídica en diversos países, y se usan lenguajes de marcado como SGML, HTML y XML.

Flores, Martín y Arellano mencionan que el mayor interés de la informática jurídica documental radica en su capacidad para, mediante las técnicas anteriormente citadas, tratar de manera adecuada los textos jurídicos y generar productos secundarios que puedan ser interrogados y produzcan los resultados esperados por los juristas. Aparte de otros productos de las

[12] Nogales, J.T.; Martín, B.; Arellano, M.C. *Informática, derecho y documentación. Experiencias y posibilidades de aplicación de los lenguajes de marcado de texto (SGML, HTML y XML) a los documentos jurídicos.* Departamento de Biblioteconomía y Documentación. Universidad Carlos III de Madrid. En: Davara Rodríguez, M.A. (coord.), *Actas del XVI Encuentro sobre Informática y Derecho.* Madrid: Univ. Pontificia de Comillas, 2003. p. 355-374.

tareas del análisis documental (listados de títulos, de materias, de autores, boletines de resúmenes, etc.), el más importante lo constituyen las bases de datos, eje central de la informática jurídica documental. Tal es su importancia, así como el adecuado control de la información contenida en ellas, que, según Silvia de Cartolano, el área documental constituye para el sistema de derecho de cualquier nación uno de los pilares que sostienen su avance y progreso, debido a la capacidad que le proporciona al jurista para la toma de decisiones oportunas.

El desarrollo de las bases de datos jurídicas ha estado marcado por los avances tecnológicos en este campo de la informática. En cualquier caso, tradicionalmente su construcción se ha basado en la abstracción documental de los textos jurídicos, al extraer de ellos la información sustancial y al estructurar ésta en una serie de campos de interés para su recuperación. Con ello se crea una serie de registros que dan soporte a los modelos relacionales o documentales de la base de datos. Al amparo de este *modus operandi* ha surgido en las últimas décadas un gran número de bases de datos jurídicas en todo el mundo.

APLICACIÓN DE LOS LENGUAJES DE MARCADO

Frente a estos modelos convencionales para tratar y difundir la información jurídica surgió en los años de 1980 una corriente crítica, tendiente a usar marcas descriptivas dentro del texto de los documentos, capaces de caracterizar de manera adecuada sus elementos estructurales y semánticos, con lo cual no es necesario someter al documento jurídico original a una fase posterior de abstracción documental, pues éste incorpora *ab initio* tanto el texto propiamente dicho como las marcas que caracterizan su descripción estructural y semántica, al estar preparado para su proceso tanto por el sistema de gestión de bases de datos como por el sistema de edición que haya de darle un formato de presentación en cualquier dispositivo electrónico de salida (pantalla, impresora, dispositivo auditivo, etc.).

Marcado con XML

XML (eXtensible Markup Language, www.w3.org/XML), reducción y adaptación de SGML al espacio de publicación de internet, es un metalenguaje diseñado como recomendación en 1998 por el World Wide Web Consortium (W3C). Permite crear lenguajes o vocabularios de marcado de textos a través del mecanismo de la DTD, que define las estructuras lógicas subyacentes a cada tipo documental tratado y aporta cierta semántica a cada una de las piezas u objetos existentes en dichas estructuras. A su

amparo han surgido otros estándares que lo complementan con diversas capacidades, como XLink (XML Linking Language) para crear enlaces hipertextuales avanzados dentro de los documentos XML, XML Namespaces para integrar diferentes vocabularios, XSL (Extensible Stylesheet Language) para dar a estos documentos un formato de presentación, XML Schema para definir formalmente estructuras documentales y tipos de datos complejos, o RDF (Resource Description Framework) para asignar metainformación a los objetos electrónicos que pueblan la red.

En la nueva web que se pretende construir, definida por J. Bosak y T. Bray a principios de 1999, XML aporta numerosas ventajas: es una tecnología abierta, no propietaria, independiente de plataforma y sistema operativo; es un estándar internacional basado en Unicode; es sencilla de utilizar e implantar; tiene gran potencia para construir vocabularios aplicables a cualquier tipo de documento; se orienta al tratamiento, transmisión o intercambio de todo tipo de documentos o datos; permite reutilizar textos y datos existentes en otros documentos para la elaboración de otros nuevos; y aporta potentes mecanismos para la búsqueda y recuperación de la información.

La comunidad de estudiosos y profesionales del derecho ha vislumbrado su potencial para el tratamiento de la información jurídica y podemos encontrar muchos ejemplos de aplicación de esta tecnología, especialmente en el ámbito judicial. En gran medida, las iniciativas se basan en experiencias adquiridas años atrás en la aplicación de SGML, pero ahora, con la potencialidad de XML para la difusión en internet de los productos desarrollados, su alcance y proyección son mucho mayores.

Algunos de los principales diseñadores e impulsores son el Joint Technology Committee of the Conference of State Court Administrators (COSCA) y el National Association of Court Managers (NACM), que con el nombre de Court XML pretende desarrollar un estándar de XML para tribunales.

Por ende, la mayor parte de los proyectos se han emprendido en Estados Unidos. A escala estatal, podemos destacar el Electronic Court Filing Project (E-CT-Filing, gsulaw.gsu.edu/gsuecp), de la Georgia State University (College of Law, law.gsu.edu, y la Escuela de Negocios J. Marck Robinson, robinson.gsu.edu), dirigido por Winchel "Todd" Vincent, con el objetivo inicial de analizar los diversos sistemas existentes para la mejora de los procesos de gestión e intercambio de documentos electrónicos entre los tribunales de justicia de ese estado, y XMLES el formato de codificación de documentos más destacado.

Este grupo de trabajo se une con otro de la Universidad de Utah, liderado por Brent Israelsen, que venían trabajando en el proyecto Utah Electronic Law & Comerce Partnership (UELCP, www.uelcp.org) para debatir y desarrollar DTD de XML para la edición e intercambio de documentos

jurídicos, y con Gabe Wachob del portal jurídico FindLaw (www.findlaw.com), hoy dedicado a la localización de recursos jurídicos en internet. El nuevo grupo de trabajo, que puso en marcha en 1998 un servicio de listas de correo electrónico, es considerado el promotor de la organización internacional sin ánimo de lucro LegalXML (www.legalxml.org), en la que se integran personas procedentes de todo tipo de instituciones del campo jurídico con el objetivo de diseñar estándares abiertos de aplicación jurídica basados en XML. En el seno del grupo de trabajo, ahora llamado OASIS LegalXML Electronic Court Filing TC, se han elaborado diversos vocabularios relacionados con documentos y formatos de intercambio para las aplicaciones informáticas propias de los tribunales de justicia, como el LegalXML Court Filing 1.1 Proposed Standard), propuesto en julio de 2002 (aunque se está trabajando en la versión 2.0), o el XML Court Document 1.1 Draft Standard, de mayo de 2002. Sin embargo, el Comité Técnico Legal XML dedicado a los documentos legislativos, oasis LegalXML Legislative Documents, Citations, and Messaging TC (http://www.oasisopen.org/committees/tc_home.php?wg_abbrev= legalxmllegislativa) no ofrece ningún estándar en la actualidad.

Por otro lado, dentro del US District Court of New Mexico, Richard Himes trabaja desde 1998 en el Extensible Markup Languague Court Interface (XCI, http://www.oasis-open.org/cover/xcispec19990402.html) como parte fundamental del ACE (Advanced Court Engineering), proyecto de gran envergadura y proyección internacional que pretende alentar el desarrollo e investigación de estándares independientes para los sistemas de edición y transmisión electrónica de documentos judiciales. Asimismo, el estado de California diseñó el Open XML Court Interface (OXCI), con similares características, puesto en marcha en marzo de 2000.

Existen organizaciones supraestatales de Estados Unidos, como el National Center for State Courts (NCSC, www.ncsconline.org), la Conference of State Court Administrator (COSCA, cosca.ncsc.dni.us), la National Association for Court Management (NACM, www.nacmnet.org) y la American Bar Association (ABA, www.abanet.org), que intentan coordinar las iniciativas desarrolladas en los diversos estados con la finalidad de obtener un estándar que sea a la vez común para todos los tribunales de justicia de la nación, pero lo bastante flexibles para adecuarse a variaciones locales.

En Canadá (en especial el gobierno autónomo de Québec) se han lanzado diversas iniciativas y planes estratégicos para el desarrollo tecnológico de sus administraciones públicas, como el *Chantier en ingénierie documentaire*, proyecto conjunto de diferentes ministerios y organismos del gobierno de Québec (Biblioteca Nacional, archivos nacionales y grupo de responsables de gestión documental de dicho gobierno, principalmente) desde 1997, con vistas a establecer directrices generales para la gestión

integral de documentos gubernamentales impresos y electrónicos. Cabe destacar, por la importancia que tiene para nuestra disciplina, que en todos estos proyectos ha participado activamente el *Groupe départemental de Recherche sur les Documents Structurés* (grds.ebsi.umontreal.ca) de la Escuela de Biblioteconomía y Ciencias de la Información de la Universidad de Montreal, dirigido por Yves Marcoux.

En Europa destaca una serie de proyectos enmarcados dentro de las políticas generales de información que diversos países han puesto en marcha en los últimos años. En el Reino Unido se creó en 2000 un plan de modernización de las administraciones públicas, integrando sus sistemas de información con el programa *e-Government Interoperability Framework* (e-GIF, www.e-envoy.gov.uk), que define los requisitos previos esenciales para lograr esta integración tecnológica de los mismos y su disponibilidad para el ciudadano en la web, tomando como base tecnológica XML. Señala tres puntos clave de desarrollo y aplicación de XML al e-GIF: XML y esquemas XML para la integración de los datos; UML, RDF y XML pararon el fin de modelar los datos y el lenguaje descriptivo; y XSL, DOM y XML para la presentación de los datos.

Desde su lanzamiento se han actualizado y concretado progresivamente algunos de sus aspectos más notables, y a la fecha de redacción de este capítulo está en su versión cuarta (de abril de 2002), pero con una actualización posterior de una de las dos partes constituyentes de ella (actualización en octubre de 2002 de su segunda parte, dedicada a los aspectos más técnicos de la aplicación de XML).

En Francia también se busca modernizar sus administraciones públicas; el desarrollo y la aplicación de los estándares XML desempeñan un papel importante. Además de la existencia de diversos foros electrónicos de debate sobre XML, resulta destacable el Club XML de la antigua agencia gubernamental ATICA (actualmente integrada dentro de la Agende pour le Développement de l'Administration Electronique, ADAE, www.adae.pm.gouv.fr), surgido al amparo de las decisiones adoptadas por el Comité Interministériel à la Réforme de l'Etat en octubre de 2000, relativas al desarrollo de un amplio repertorio de esquemas XML de aplicación en las diversas administraciones públicas. Fruto de esta actividad, han arrancado en los últimos años varios proyectos de investigación para el desarrollo de DTD y esquemas XML aplicados a la información electrónica de diversos organismos públicos del Estado. Así, el Consejo Constitucional (www.conseil-constitutionnel.fr) desarrolla un proyecto de investigación aplicada bajo tecnologías XML, aún en fase de experimentación, enmarcado en el proyecto global Service Public d'Accès au Droit (SPAD), que pretende crear un servicio público de acceso al derecho, Legifrance (www.legifrance.gouv.fr), que ponga a disposición de los ciudadanos, gratuitamente a través de internet toda la legislación y jurisprudencia emanada

de los diversos órganos competentes. Asimismo, existe un esquema XML para hacer posible la difusión de documentos jurídicos del Consejo Constitucional a través del futuro servicio SPAD.

El interés creciente que suscita la aplicación de las tecnologías XML a los documentos jurídicos en los países europeos hace que surjan propuestas, proyectos y sitios web en forma continuada. Es el caso del sitio web creado por la Universidad de Ámsterdam en coordinación con el nodo holandés de la organización Lexml (http://law.leiden.edu/xml), MetaLex (www.metalex.nl), conjunto de documentos que dan soporte y explican los esquemas XML desarrollados para el marcado y presentación de documentos legislativos (manual de uso, informes, especificación, hojas de estilo y diversos ejemplos de documentos marcados).

En la Unión Europea, como institución supranacional, podemos encontrar un caso muy representativo de la aplicación de las tecnologías XML al campo de la justicia en el Proyecto GTi (Generic Text interface) a la traducción de los documentos emanados del Tribunal de Justicia de las Comunidades Europeas (incluido, obviamente, el Tribunal de Primera Instancia, www.curia.eu.int). Se está trabajando para cubrir todo el proceso de producción y gestión de los documentos emanados de este tribunal, tanto los internos (la jurisprudencia) como los externos (las diferentes piezas que se integran dentro del procedimiento judicial). Así, el sistema desarrollado proporciona ayuda para la redacción de los documentos, para la inclusión de citas a otras sentencias o normas, para la redacción de los fundamentos jurídicos, para la traducción de todos estos documentos y, finalmente, para la publicación de ellos en diferentes medios electrónicos e impresos. Este complejo entramado tecnológico se sustenta bajo una arquitectura cliente-servidor, en la que XML se emplea como formato para el marcado, el almacenamiento y el intercambio de estos documentos.

IV. Regulación jurídica de la información y de los datos personales

NOCIONES GENERALES

La palabra información (del latín *informare,* que significa poner en forma) es una noción abstracta, no obstante que posee una connotación vinculada con una de nuestras más grandes libertades: la de opinión y expresión de informaciones e ideas por cualquier medio que sea.[1] Por ello, la información se ha considerado un elemento susceptible de ser transmitido por un signo o combinación de signos; empero, para los efectos informáticos que nos ocupa, la entenderemos como un proceso físico-mecánico de transmisión de datos, cuyo dato es el elemento referencial acerca de un hecho. En sentido general, un conjunto de datos constituye una información.

Cualitativamente se ha concebido a la información como el contenido de lo que es objeto de intercambio entre el sujeto y el mundo externo,[2] de tal modo que se presenta un conjunto de datos como elemento de las relaciones del hombre y tendiente a una ordenación; es decir, desde este punto de vista la información constituye un factor de organización. Por otra parte, cuantitativamente, la información es la medida de disminución de incertidumbre del sujeto respecto a los objetos, de aquí que se hable de una entropía en cuanto al nivel de desorganización y desconocimiento del hombre sobre las cosas en un momento dado.

[1] Véase el artículo 19 de la *Declaración Universal de los Derechos del Hombre,* 1948.

[2] Véase Norbert, Wiener, *op. cit.*

NOCIONES PARTICULARES

A raíz de la gran trascendencia que ha adquirido la información, cabe resaltar que autores como R. Hartley destacaban la utilidad de ésta a tal grado de mencionar que la información puede medirse en función de su utilidad (medida Hartley) y que, por lo tanto, "la cantidad de información será proporcional al número de alternativas que se dispongan en un momento dado".[3]

Por otra parte, autores como Claude Shannon, al reformar los aspectos cuantitativos y cualitativos que reviste la información, mencionaban que cuanto mayor y mejor sea la información, menor será el desconocimiento en las personas.[4]

En apoyo de lo anterior, dichas exteriorizaciones han llegado a adquirir una singular relevancia en nuestros días en razón del gran desarrollo que han llegado a alcanzar las computadoras. De esta forma, dichos instrumentos permiten, mediante la integración y disponibilidad de numerosos bancos de información, conseguir uno de los cometidos principales de la informática como lo es la adecuada toma de decisiones.

En ese orden de ideas hay una decisión en los términos de la elección entre dos o más medidas optativas basada en información, con el fin de alcanzar resultados y objetivos previamente establecidos.[5]

Asimismo, existe una toma de decisiones rápida y precisa basada en una variada cantidad de información integrada con elementos dignos de consideración que permitan mayor acercamiento entre la razón y la experiencia en aquello que se consideran las técnicas heurísticas.

En estos términos, la informática y la información están inseparablemente vinculadas por esta "omnipresencia" de las computadoras en el proceso propio de nuestra vida cotidiana, con implicaciones aún más trascendentes de las estrictamente técnicas.[6]

IMPORTANCIA ECONÓMICA DE LA INFORMACIÓN

Por otra parte, la capacidad de almacenamiento, tratamiento, transmisión y sobre todo uso de la información como elemento fundamental para la toma

[3] Dicho postulado, conocido como la teoría de la mediación de la información, fue mencionado por Hartley en su obra *Transmisión de información*, escrita en 1928.

[4] Dicho pronunciamiento lo encontramos en la *teoría de la información*, externada por Shannon en su obra *Teoría matemática de la comunicación*, escrita en 1949.

[5] Herbert Simon menciona la existencia de dos tipos de decisiones: las programables y las no programables. Las primeras de carácter rutinario y repetitivo y las segundas, aquellas que invocan a la intuición y al sentido común.

[6] Sobre éste y puntos anteriores, véase Jean Pierre Chamoux, *L'information Sans Frontiere*, Information et Societé, núm. 8, Francia, París, 1980.

de decisiones con inevitables recubrimientos económicos, por personas e instituciones tanto en el sector público como privado, llegan a ser equiparadas, económicamente hablando, con elementos tales como la energía y las materias primas.[7]

La importancia económica de la información no está puesta en duda y es un verdadero bien susceptible de apoderamiento con un innegable valor patrimonial o contenido económico inherente o intrínseco, que radica en el destino o utilidad de ella. Ahora, más que nunca, en una sociedad dominada por la técnica y el saber, el valor de la información como auténtico centro y vehículo de esa técnica y conocimiento ha alcanzado niveles otrora inimaginables.

RÉGIMEN JURÍDICO APLICABLE

Independientemente del soporte material que le dé origen y que la ofrece en disponibilidad, la información es un bien en sí, inmaterial pero constitutivo de un producto autónomo que por su contenido económico requiere una tutela jurídica en razón de los diferentes derechos y obligaciones que genera, ya sea a nivel de una relación de posesión entre autor y objeto o a nivel de relación de transferencia entre aquel que la emite y aquel que la recibe.

El hecho de que la información sea un producto de la actividad humana sugiere una afirmación en dos sentidos: por un lado, la información es, en principio, susceptible de apropiación desde su origen y, por otro, pertenece originalmente a su autor, es decir, aquel que la pone en disponibilidad para los diferentes fines de que pueda ser objeto y que por esto permite concebir una relación de posesión entre autor e información como un verdadero derecho real.

Si bien existen numerosas informaciones de carácter objetivo referidas a personas y patrimonios, también hay otras en las que se conoce un derecho sobre su creador, como las obras del espíritu. Dichas creaciones gozan de una protección privativa como un derecho de la propiedad intelectual oponible frente a terceros. A este respecto, es innegable que los derechos sobre la información proceden de una operación intelectual de creación o formulación, aun si se utilizan poderosos instrumentos de apoyo como las computadoras.

El anterior esquema describe una tendencia no muy común en cuanto a que la posibilidad de apropiación de la información debe ser motivo de estudio hacia un reconocimiento de derechos específico.

[7] Mac Bride y cols., *Un solo mundo, voces múltiples; comunicación e información en nuestro tiempo* (informe de la Comisión Internacional sobre Problemas de Comunicación), México, UNESCO, IFEC, 1980, p. 54.

Por otra parte, cabe mencionar que una vez "creada" y "apropiada" en los términos expuestos, la información va a conocer cierto número de procesos más o menos complejos, entre los que tenemos los de transformación y explotación, de tal modo que se convierte en materia contractual y reafirma, por tanto, la necesidad de un control jurídico de ella.

En lo que resta de esta obra se explicará por qué es necesario regular jurídicamente este "nuevo bien" llamado información...

PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES

Nociones generales

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

Recopilación de datos personales

En la década de 1970 empezaron a surgir numerosos archivos con informaciones de tipo personal, con un conjunto mínimo de datos, como filiación, fecha y lugar de nacimiento, domicilio, estado civil, etc., hasta otro tipo de datos con caracteres aún más distintivos, como raza, religión, inclinaciones políticas, ingresos, cuentas bancarias, historia clínica, etc. Dichos datos, al ser recopilados en diferentes centros de acopio (como los registros censales, civiles, parroquiales, médicos, académicos, deportivos, culturales, administrativos, fiscales, bancarios, laborales, etc.), ya no por medios exclusivamente manuales sino con el apoyo de medios automatizados, provocan una gran concentración, sistematización e instantánea disponibilidad de ese tipo de información para diferentes fines.

Destinaciones e implicaciones

Este tipo de datos no son vulnerables *per se*, sino según la destinación de que sean objeto y pueden ser variados; de este modo, dichas informaciones pueden emplearse para fines publicitarios, comerciales, fiscales, policíacos, etc., y convertirse de esta manera en un instrumento de opresión y mercantilismo. La variedad de los posibles supuestos de indefensión frente al problema provoca que los individuos estén a merced de un sinnúmero

de situaciones que alteren sus derechos fundamentales en sociedad provocados por discriminaciones, manipulaciones, persecuciones, presiones, asedios, etc., todo ello al margen de un control jurídico adecuado.

Nociones particulares

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

Figuras jurídicas aplicables

En cuanto a nuestra problemática en cuestión, son variadas las figuras de índole jurídica mediante las cuales se ha estudiado e intentado regular dicha cuestión.

Así, figuras como los derechos humanos, derechos personales, derechos patrimoniales, libertades públicas y privadas en el caso de Francia, derecho a la privacidad en el caso de los países anglosajones, derecho a la intimidad y al honor de las personas como en España, o aun las garantías individuales y sociales como en México, todas ellas como eventual protección, han tendido a someter de manera apropiada la concentración y destino de los datos de carácter personal.

Diferentes tipos de archivos

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

Cabe hacer mención que a nivel de derecho positivo, no todos estos archivos están sujetos a una regulación jurídica.

Principales derechos y excepciones

Es evidente que si se habla de una regulación jurídica, ésta genera a su vez determinados derechos y excepciones. Este problema, por su misma

singularidad, motiva asimismo derechos muy especiales, entre los que podemos contar los siguientes:

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

Derecho de rectificación. Complementario al anterior, este derecho permite solicitar al interesado que se modifiquen los términos de alteración o ampliación, o que suprima o cancele aquellos datos que, referidos a su persona, considere inexactos o irrelevantes.

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

Derecho para la prohibición de interconexión de archivos. Ahora bien, cabe señalar que el incumplimiento a estos derechos puede generar diferentes sanciones de índole civil, administrativa o incluso penal, lo cual depende de las circunstancias.

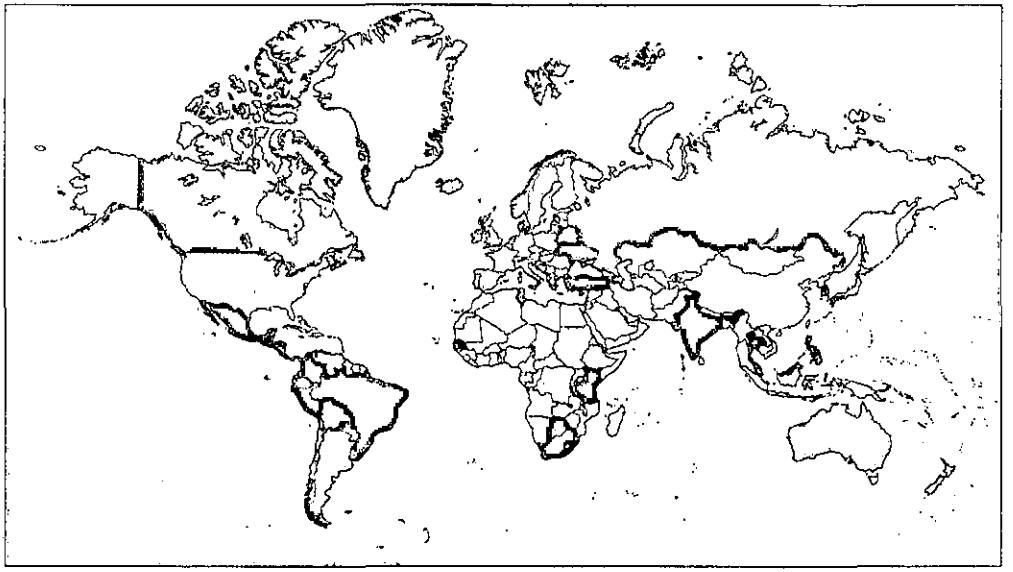
En cuanto a las excepciones a esos derechos fundamentadas en el equilibrio del Estado y su poder coercitivo y los integrantes de la sociedad existen aquellas derivadas con motivo de la seguridad del Estado tanto en lo interno como en lo externo, así como las referentes a intereses monetarios, persecución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

PANORAMA INTERNACIONAL

En función del innegable carácter económico relacionado con este problema es conveniente presentar la situación internacional de hecho y de derecho en torno a él, estructurada en tres grupos de países bien definidos de acuerdo con el régimen jurídico prevaleciente, a saber: quiénes regulan el problema desde la Constitución, quiénes lo hacen por medio de leyes generales y quiénes disponen de una ley particular al respecto.

Autoridades de protección de datos		
Alemania:	**www.datenschutz.de**	**www.bfd.bund.de**
Andorra:	**www.apda.ad**	
Argentina:	**http://www.jus.gov.ar/dnpdp**	
Australia:	**www.privacy.gov.au**	
Austria:	**www.dsk.gv.at**	

I. LEYES DE PROTECCIÓN DE DATOS EN EL MUNDO



- Legislación completa y promulgada de protección de datos
- Esfuerzo pendiente para promulgar la legislación
- Sin legislación

Autoridades de protección de datos	
Bélgica:	**www.privacy.fgov.be**
Bulgaria:	**www.cpdp.bg**
Canadá:	**www.privcom.gc.ca**
Chipre:	**www.dataprotection.gov.cy**
Dinamarca:	**www.datatilsynet.dk**
Eslovaquia:	**www.dataprotection.gov.sk**
Eslovenia:	**www.varuh-rs.si**
Estonia:	**www.dp.gov.ee**
Finlandia:	**www.tietosuoja.fi**
Francia:	**www.cnil.fr**
Grecia:	**www.dpa.gr**
Guernsey:	**www.dataprotection.gov.gg**
Holanda:	**www.cbpweb.nl**
Hungría:	**abiweb.obh.hu/abi**

Autoridades de protección de datos	
Irlanda:	**www.dataprivacy.ie**
Hong Kong:	**www.pco.org.hk**
Islandia:	**www.personuvernd.is**
Italia:	**www.garanteprivacy.it**
Jersey:	**www.dataprotection.gov.je**
Letonia:	**www.dvi.gov.lv**
Liechtenstein:	**www.sds.llv.li**
Lituania:	**www.ada.lt**
Luxemburgo:	**www.cnpd.lu**
Malta:	**www.dataprotection.gov.mt**
Noruega:	**www.datatilsynet.no**
Nueva Zelanda:	**www.privacy.org.nz**
Polonia:	**www.giodo.gov.pl**
Portugal:	**www.cnpd.pt**
Reino Unido:	**www.dataprotection.gov.uk**
República Checa:	**www.uoou.cz**
Rumania:	**www.avp.ro**
Suecia:	**www.datainspektionen.se**
Suiza	**www.edsb.ch**

Estado		Albania	Andorra	Armenia	Austria**	Azerbaiyán
Convención 108	Firmada	09/06/2004			28/01/81	
	Ratificada	14/02/2004			30/03/88	
Constitución nacional		Art. 35, Constitución de 1998		Art. 20, Constitución de 1995	Cláusula constitucional del artículo 1, secciones 1-3, Ley de protección de datos 2000	Art. 32, Constitución de 1995

Estado		Albania	Andorra	Armenia	Austria**	Azerbaiyán
Legislación nacional específica		Ley no. 8517 Acerca de la protección de datos personales			Ley federal respecto a la protección de datos personales. Implementación de la norma 95/46/EC Legislación Länder	Ley de la República de Azerbaiyán "acerca de datos, procesamiento de datos y protección de datos"
Promulgación (entrada en vigor)		22/07/99			17/08/99 1/01/2000)	07.12.99
Amplitud	Procesamiento manual	Sí			Sí	
	Persona no física	No			Sí	
	Sector público o privado	Ambos			Ambos	
Registro o notificación		No			Todos los datos (importantes excepciones)	
Autorización especial para exportación		No			Algunos datos	
Autoridad de protección de datos		Ministerio Público			Comisión de protección de datos	

Estado		Bélgica**	Bosnia y Herzegovina	Bulgaria	Croacia	Chipre
Convención 108	Firmada	07/05/82	02/03/2004	02/06/98	05/06/2003	25/07/86
	Ratificada	28/05/93		18/09/02	21/06/2005	21/02/02
Constitución nacional		Art.22, Constitución de 1970	Art. II, párr. 3 F, Constitución de Bosnia y Herzegovina de 1995	Art. 32, Constitución de 1991	Art. 37, Constitución de 1990 (enmiendas – 1997, 2000)	Art. 15, 1960 Constitución

Estado		Bélgica**	Bosnia y Herzegovina	Bulgaria	Croacia	Chipre
Legislación nacional específica		Ley sobre protección de datos personales Ley de implementación de la norma 95/46/EC Decreto de promulgación de la ley de protección de datos personales	Ley sobre la protección de datos personales	Ley de protección de datos personales	Ley sobre protección de datos personales (2 reglamentos que están como leyes: Reglamento sobre el método de mantenimiento y la forma de los registros en el sistema de archivo de los datos personales (boletín oficial, 105/04, 28 de julio de 2004) y Reglamento sobre el método de almacenamiento y medidas técnicas especiales de protección de categorías especiales de datos personales (boletín oficial, 139/04, 6 de oct. 2004).	Ley de 2001 de procesamiento de datos personales (protección de los individuos)
Promulgación (entrada en vigor)		08/12/92 11/12/98 (01/09/01) 13/02/2001	20/12/2001 (25/01/2002)	21/12/2001 01/01/2002)	01/10/2005	2001
Amplitud	Procesamiento manual	Sí		Sí	Sí	Sí
	Persona no física	No		Sí	No	No
	Sector público o privado	Ambos	Ambos	Ambos	Ambos	Ambos

Estado	Bélgica**	Bosnia y Herzegovina	Bulgaria	Croacia	Chipre
Registro o notificación	Todos los datos		Todos los datos	Todos los datos (importantes excepciones)	Algunos datos
Autorización especial para exportación	Algunos datos	No	Sí	No	Sí
Autoridad de protección de datos	Comisión para la protección de la privacidad	Comisión de protección de datos	Comisión para la protección de datos personales	Agencia de protección de datos personales	Comisionado de protección de datos personales

Estado		República Checa	Dinamarca**	Estonia	Finlandia**	Francia**
Convención 108	Firmada	08/09/00	28/01/81	24/01/00	10/04/91	28/01/81
	Ratificada	09/07/01	23/10/89	14/11/01	02/12/91	24/03/83
Constitución nacional		Art. 10, la Carta de los Derechos y las Libertades Fundamentales de 1992 (mandato constitucional)		Art. 42, Constitución de 1992	Sección 10, Constitución de 1991	
Legislación nacional específica		Ley sobre la protección de los datos personales y sobre las enmiendas de algunas leyes relacionadas	Ley sobre el procesamiento de datos personales	Ley de protección de los datos personales Ley de bases de datos, y Ley de información pública	Ley de datos personales Ley sobre la enmienda de la Ley de datos personales	Ley sobre la informática, los archivos de datos y las libertades
Promulgación (entrada en vigor)		04/04/2000 (01/06/2001)	31/05/00 (01/07/2000)	12/06/96 12/03/97 (19/04/97)	22/04/99 (01/06/99) 24/11/00 (01/12/00)	06/01/1978 06/08/2004

Estado		República Checa	Dinamarca**	Estonia	Finlandia**	Francia**
Amplitud	Procesamiento manual	Sí	Sí	Sí	Sí	Sí
	Persona no física	No	Algunas	No Sí	No	Sí (decisión administrativa de la CNIL 03/07/84)
	Sector público o privado	Ambos	Ambos	Ambos	Ambos	Ambos
Registro o notificación		Todos los datos	Algunos datos	Algunos datos	Algunos datos	Algunos datos
Autorización especial para exportación		Algunos datos	Algunos datos	No	Algunos datos	Algunos datos
Autoridad de protección de datos		Oficina de protección de datos personales	Agencia danesa de protección de datos	Inspectorado de protección de datos	Ombudsman de protección de datos	Comisión nacional para la informatización y la libertad (CNIL)

Estado		Georgia	Alemania**	Grecia**	Hungría	Islandia
Convención 108	Firmada	21/11/01	28/01/81	17/02/83	13/05/93	27/09/82
	Ratificada		19/06/85	11/08/95	08/10/97	25/03/91
Constitución nacional		Arts. 20/41, Constitución de 1995	Art. 10, Constitución de 1943		Art. 59, Constitución de 1949	
Legislación nacional específica			Ley federal de protección de datos (instrumentación de la norma 95/46/EC) Ley de telecomunicaciones Legislación Länder (más...)	Ley no. 2472 sobre protección de los individuos en referencia al procesamiento de datos personales	Ley no. LXIII sobre protección de datos personales y divulgación de datos de interés público	Ley sobre protección de las personas con respecto al procesamiento de datos personales

Estado		Georgia	Alemania**	Grecia**	Hungría	Islandia
Promulgación (entrada en vigor)			01/01/2002	26/03/1997 (10/04/97)	17/11/92 (02/05/93) Capítulo III (02/12/93) Capítulo IV (22/06/93)	01/01/00
Amplitud	Procesamiento manual		Sí	Sí	Sí	Sí
	Persona no física		No	No	No	Sí
	Sector público o privado		Ambos	Ambos	Ambos	Ambos
Registro o notificación			Algunos datos	Todos los datos	Todos los datos	Todos los datos
Autorización especial para exportación			No	Algunos datos	No	Todos los datos
Autoridad de protección			Comisión federal de protección de datos	Autoridad de protección de datos personales	Ombudsman de protección de datos	Autoridad de protección de datos personales

Estado		Irlanda*	Italia**	Letonia	Liechtenstein	Lituania
Convención 108	Firmada	18/12/86	02/02/83	31/10/00	02/03/2004	11/02/00
	Ratificada	25/04/90	29/03/97	30/05/01	11/05/2004	01/06/01
Constitución nacional				Art. 96, Constitución de 1922	-	Art. 22, Constitución de 1992
Legislación nacional específica		Ley de protección de datos Reglamentos de protección de datos, 2001	Código de protección de datos personales Decreto legislativo No. 196/2003	Ley sobre protección de datos personales	Ley de protección de datos 2002 Ordenanza de 9 de julio de 2002, relativa a la ley de protección datos	Ley sobre protección jurídica de los datos personales

Estado		Irlanda*	Italia**	Letonia	Liechtenstein	Lituania
Promulgación (entrada en vigor)		13/07/88 (19/04/89) 19/12/01 (01/04/02)	01/01/2004	23/03/00 (20/04/00)	14/03/02 (08/05/02) 09/07/02 (18/07/02)	17/07/00 (01/01/01)
Amplitud	Procesamiento manual	No	Sí	Sí	Sí	Sí
	Persona no física	No	Sí	No	Sí	No
	Sector público o privado	Ambos	Ambos	Ambos	Sí	Ambos
Registro o notificación		Algunos datos	Algunos datos	Todos los datos	Sí Algunos datos	Algunos datos
Autorización especial para exportación		No	Algunos datos	Algunos datos	Sí	Algunos datos
Autoridad de protección de datos		Protección de datos Comisionado	Garante para la protección de datos personales	Inspección del estado de los datos	Comisionado para la protección de datos	Inspectorado para la protección del estado de los datos

Estado		Luxemburgo*	Malta	Moldavia	Mónaco	Países Bajos**
Convención 108	Firmada	28/01/81	15/01/2003	04/05/1998		21/01/88
	Ratificada	10/02/88	28/02/2003			24/08/93
Constitución nacional		Art. 28, Constitución de 1868	Art. 28, Constitución de 1994	Art. 28, Constitución de 1994	Art. 22, Constitución de 1962	Art. 10, Constitución de 1989
Legislación nacional específica		Ley de protección de las personas relativa al procesamiento de los datos personales (sólo en francés) Proyecto de ley en curso (sólo en francés)	Ley de protección de datos, 2001		Acta relativa al procesamiento de la información nominal de 1998, ordenanza para establecer las modalidades de aplicación de la ley relativa al procesamiento de la información nominal	Ley de protección de datos personales Ley de protección de datos personales (doc)

Estado		Luxemburgo*	Malta	Moldavia	Mónaco	Países Bajos**
Promulgación (entrada en vigor)		02/08/02 (01/12/02)	14/12/2001		23/12/1993	06/07/00 (01/09/01)
Amplitud	Procesamiento manual	Sí	Sí	No		Sí
	Persona no física	Sí	No	No		No
	Sector público o privado	Ambos	Ambos	Ambos		Ambos
Registro o notificación		Todos los datos (con excepciones)	Todos los datos		Todos los datos	Algunos datos
Autorización especial para exportación		Algunos datos	Algunos datos		No	Algunos datos
Autoridad de protección de datos		Comisión nacional para la protección de datos Esch-sur-Alzette	Comisión de protección de datos		Comisión de supervisión de la información personal	Comisión de protección de datos

Estado		Noruega	Polonia	Portugal**	Rumania	Rusia
Convención 108	Firmada	13/03/81	21/04/99	14/05/81	18/03/97	07/11/01
	Ratificada	20/02/84	23/05/02	02/09/93	27/02/02	
Constitución nacional			Art. 51, Constitución de 1997	Art. 35, Constitución de 1976	Art. 26, Constitución de 1991	Art.24, Constitución de 1993
Legislación nacional específica		Ley de datos personales	Ley sobre protección de datos personales	Protección de datos personales (implementación de la directriz 95/46/EC)	Ley sobre la protección de las personas con respecto al procesamiento de datos personales y a la libre circulación de estos datos No. 677/2001 Ley. No. 102/2005 Ley No. 506/2004	

Estado		Noruega	Polonia	Portugal**	Rumania	Rusia
Promulgación (entrada en vigor)		14/04/00 (01/01/01)	29/08/97 (04/98)	28/10/1998 (27/10/98)	12/12/2001	
Amplitud	Procesamiento manual	Sí	Sí	Sí	Sí	
	Persona no física		Sí	No	Sí	
	Sector público o privado	Ambos	Ambos	Ambos	Sí	
Registro o notificación		Todos los datos	Algunos datos	Algunos datos	Sí	
Autorización especial para exportación		Todos los datos	Sí	Algunos datos	Sí	
Autoridad de protección de datos		Inspección de los datos	Inspector general para la protección de datos personales	Comisión nacional de protección de datos	Autoridad nacional para la supervisión del procesamiento de datos personales	

Estado		San Marino	Serbia	Eslovaquia	Eslovenia	España**
Convención 108	Firmada		06/09/2005	14/04/00	23/11/93	28/01/82
	Ratificada		06/09/2005	13/09/00	27/05/94	31/04/84
Constitución nacional			Art. 33, Constitución de 1992	Arts. 19 y 22, Constitución de 1992	Art. 38, Constitución de 1991	Art. 18, Constitución de 1978
Legislación nacional específica		Ley sobre recolección, elaboración y uso de datos personales informatizados	Ley sobre protección de datos personales	Ley sobre protección de datos personales Euro enmienda de la ley 428/2002 COLL. Entró en vigor el 1 de mayo de 2005	Ley de protección de datos personales	Ley orgánica 15/99, relativa a la protección de datos personales
Promulgación (entrada en vigor))		01/03/83 (23/05/95)	12/05/1998	03/02/2005 (01/05/2005)	08/07/99 (07/08/99)	13/12/99 (14/01/00)

Estado		San Marino	Serbia	Eslovaquia	Eslovenia	España**
Amplitud	Procesamiento manual	No	Sí	Sí	Sí	Sí
	Persona no física	Sí		No	No	No
	Sector público o privado	Ambos	Sí	Ambos	Ambos	Ambos
Registro o notificación		Todos los datos		Algunos datos	Todos los datos	Todos los datos
Autorización especial para exportación		Algunos datos		No	Algunos datos	Algunos datos
Autoridad de protección de datos		Garante de la protección de la confidencialidad y los datos personales	-	Oficina de protección de datos personales de la república eslovaca	Comisionado de información	Agencia de protección de datos

Estado		Suecia**	Suiza	"Ex República Yugoslava de Macedonia"	Turquía	Ucrania
Convención 108	Firmada	28/01/81	02/10/97	24/03/2006	28/01/81	29/08/2005
	Ratificada	29/09/82	02/10/97	24/03/2006		
Constitución nacional		Capítulo 2, Art. 3, Constitución de 1989	Art. 13, Constitución de 1999	Art. 18, Constitución de 1992	Art. 20, Constitución de 2001	Art. 32, Constitución de 1996
Legislación nacional específica		Ley de datos personales	Ley federal de protección de datos Ordenanzas: OLPD, OALSP (francés)	Ley sobre la protección de datos personales		
Promulgación (entrada en vigor)		29/04/1998 (24/10/98)	19/06/92 (01/07/93) Ordenanzas adoptadas 14/06/93	25/01/2005		

Estado		Suecia**	Suiza	"Ex República Yugoslava de Macedonia"	Turquía	Ucrania
Amplitud	Procesamiento manual	Sí	Sí	Sí		
	Persona no física	No	Sí	Sí		
	Sector público o privado	Ambos	Ambos	Ambos		
Registro o notificación		Todos los datos	Algunos datos	No		
Autorización especial para exportación		Todos los datos	Algunos datos	Sí		
Autoridad de protección de datos		Directorio de inspección de datos	Comisionado federal de protección de datos e información	Órgano administrativo. Directorado para la protección de datos personales		

Estado		Reino Unido**
Convención 108	Firmada	02/10/97
	Ratificada	02/10/97
Constitución nacional		
Legislación nacional específica		Ley de protección de datos Leyes territoriales: Ley de Jersey Ley de Guernsey Ley de Isle of Man
Promulgación (entrada en vigor)		16/07/98 (01/03/00)
Amplitud	Procesamiento manual	Sí
	Persona no física	No
	Sector público o privado	Ambos
Registro o notificación		Todos los datos

Estado	Reino Unido**
Autorización especial para exportación	Sí
Autoridad de protección de datos	Oficina del comisionado de la información

* Estados miembros de la Unión Europea que todavía tienen que aplicar la directriz 95/46/EC del Parlamento Europeo y del Consejo del 24 de octubre de 1995, relativa a la protección de las personas con respecto al procesamiento de datos personales y a la libre circulación de estos datos, en sus respectivas legislaciones nacionales.

** Estados miembros de la Unión Europea que han aplicado la directriz 95/46/EC del Parlamento Europeo y del Consejo del 24 de octubre de 1995, relativa a la protección de las personas con respecto al procesamiento de datos personales y a la libre circulación de estos datos en sus respectivas legislaciones nacionales.

II. ESTADOS NO MIEMBROS DEL CONSEJO DE EUROPA

A) Estados no miembros que tienen la condición de observador en el Consejo de Europa

Estado		Estado Vaticano	Estados Unidos	Canadá	Japón	México
Convención 108	Firmada					
	Ratificada					
Constitución nacional				Ley Constitucional, de 1982, sección 8		Arts. 6, 16; Constitución de 1917
Legislación nacional específica			1. Ley de privacidad 2. Ley de diferentes sectores en la protección de datos personales: Ley de protección de la privacidad de cable Ley de derecho educativo familiar a la privacidad (FERPA) Ley de privacidad de comunicaciones electrónicas 3. Principios de puerto seguro	Ley de privacidad Ley de protección de la información personal y documentos electrónicos Información adicional	Sector público: Ley para la protección de los datos personales procesados en poder de los órganos administrativos Encargados de hacer cumplir la ordenanza de la Ley para la protección de los datos personales procesados en poder de los órganos administrativos	Ley federal de transparencia y acceso a la información pública gubernamental

Estado		Estado Vaticano	Estados Unidos	Canadá	Japón	México
Promulgación (entrada en vigor))			1. 1974 A) 1984 2. B) 1974 C) 1986 3. 2000	01/07/83 13/04/00 (01/01/01)	16/12/88 01/10/89 (1990,94,96,97)	05/2002
Amplitud	Procesamiento manual			Sí	No	
	Persona no física			Sí		
	Sector público o privado			Ambos	Sector público	
Registro o notificación					Algunos datos	
Autorización especial para exportación						
Autoridad de protección de datos				Comisionado de privacidad Autoridades federales (más...)	Oficina de gestión administrativa Ministerio de administración pública, Asuntos del interior, Correo y Telecomunicaciones	Instituto Federal de Acceso a la Información Pública

Estado		Argentina	Australia	Brasil	Chile
Convención 108	Firmada				
	Ratificada				
Constitución nacional		Arts. 43. 3, Constitución de 1853		Art. 5.x, Constitución de 1988	Arts. 19. 4, Constitución de 1980
Legislación nacional específica		Ley de protección de datos personales	Ley federal de privacidad Ley de enmienda de privacidad (sector privado) Leyes federales	Ley de *habeas data*	Ley sobre protección de datos personales

Estado		Argentina	Australia	Brasil	Chile
Promulgación (entrada en vigor)		04/10/2000	18/10/88 (1989) 21/12/2002	1997	28/08/99
Amplitud	Procesamiento manual	Sí	Sí		Sí
	Persona no física		No		Sí
	Sector público o privado	Ambos	Sector público Sector privado		Ambos
Registro o notificación		Todos los datos			No
Autorización especial para exportación		No			
Autoridad de protección de datos		Comisión independiente con el ministro de justicia	Comisionado de privacidad		

Estado		Israel	Montenegro	Paraguay	Perú
Convención 108	Firmada				
	Ratificada				
Constitución nacional		Sección 7, 1992 Ley fundamental: dignidad humana y libertad		Art. 33, Constitución de 1992	Art. 2, Constitución de 1993 Ley No. 26.301 (regula los aspectos procesales de la acción de *habeas data*)
Legislación nacional específica		Ley No. 5741, relativa a la protección de la intimidad Ley administrativa de protección de datos No. 5746		Ley No. 1682 Regulación de la información privada	
Promulgación (entrada en vigor)		02/1981 1986		28/12/2000	02/05/1994

Estado		Israel	Montenegro	Paraguay	Perú
Amplitud	Procesamiento manual				
	Persona no física				
	Sector público o privado				
Registro o notificación		Algunos datos			
Autorización especial para exportación					
Autoridad de protección de datos		Registro de bases de datos			

Estado		Corea del Sur	Tailandia	Nueva Zelanda
Convención 108	Firmada		06/09/2005	
	Ratificada		06/09/2005	
Constitución nacional		Art. 17, Constitución de 1948	Sección 34, Constitución de 1997	Art. 28, Ley de declaración de derechos de Nueva Zelanda 1990
Legislación nacional específica		Ley sobre la protección de información personal administrada por organismos públicos	Ley de información oficial B. E 2540	Ley de privacidad
Promulgación (entrada en vigor)		07/01/94	1997	17/05/93 (01/07/93)
Amplitud	Procesamiento manual	No		
	Persona no física	No		
	Sector público o privado	Público	Sí	
Registro o notificación				
Autorización especial para exportación		No		No
Autoridad de protección de datos			Oficina de la comisión de información oficial	Comisionado de privacidad

III. OTROS TERRITORIOS

Entidades		Hong Kong	Taiwan
Convención 108	Firmada		
	Ratificada		
Constitución nacional		Art. 30, Constitución de 1990	
Legislación nacional específica		Ordenanza sobre datos personales (privacidad)	Ley de protección de datos personales procesados en computadora
Promulgación (entrada en vigor)		08/1995	11/08/95
Amplitud	Procesamiento manual	No	Sí
	Persona no física	No	No
	Sector público o privado	Ambos	Ambos
Registro o notificación			Todos los datos
Autorización especial para exportación			
Autoridad de protección de datos		Oficina del comisionado de privacidad de datos personales	Ministerio de Justicia

Safe-harbor (puerto-seguro)

A principios de 2000 se llegó a un acuerdo entre las administraciones de Estados Unidos y la Unión Europea (UE) según el cual las empresas estadounidenses que se unieran al programa denominado *Safe-Harbor*, en materia de protección de datos, no se verían sancionadas por la administración de la UE. Dicho acuerdo entró en vigor el 1 de noviembre de 2000.

En este caso, si bien cada país puede tener su propia ley de protección de datos, la Unión Europea tiene una directiva (de obligado cumplimiento), la 95/46 CE, que prohíbe la transferencia de datos personales a un tercer país que no tenga un adecuado sistema de protección de la privacidad. Estados Unidos, por el contrario, no tiene legislación muy amplia concerniente a la materia, por lo que se basa principalmente en la autorregulación.

Las empresas estadounidenses no parecen tener las cosas muy en claro, por lo que se muestran indiferentes por dicho acuerdo, primero tal vez por no estar acostumbradas a plantearse el problema de la privacidad de

la misma manera como se hace en Europa, aun si el acuerdo es bastante "permisivo" con la manipulación de datos desde el punto de vista de las leyes europeas; segundo, porque a las empresas les puede costar bastante dinero adecuar su infraestructura a dicha legalidad, y tercero, porque será difícil para Europa mantener un control sobre lo que se hace realmente con los datos del otro lado del Atlántico.

Para obtener la "exención" europea, las empresas estadounidenses deben suscribirse a programas como el Truste o el *BBB on line* y comprometerse a seguir al menos siete principios cuando utilicen y manejen datos personales de ciudadanos europeos. Por ejemplo, se prevén los derechos a la información, a la rectificación o a ser eliminado de las bases de datos, a ser informado sobre las posibles cesiones de datos a terceros y, finalmente, el derecho a que existan sistemas seguros de acceso a los datos.

PANORAMA NACIONAL

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS

Por reformas publicadas en el *DOF* del 20 de julio de 2007 y el 13 de noviembre de 2007, se establece lo siguiente:

Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.

Para el ejercicio del derecho de acceso a la información, la Federación, los estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

I. Toda la información de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.
II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.
IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustituirán ante órganos u orga-

nismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión.

V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.

VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.

VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.

El 5 de abril de 2006, el entonces senador Antonio García Torres (PRI) presentó iniciativa de adición al artículo 16 de la *Constitución Política de los Estados Unidos Mexicanos* ante la Cámara de Senadores, la cual fue aprobada por 77 votos y cinco abstenciones, turnándose a la Cámara de Diputados. El texto aprobado en la Cámara de Senadores es de la siguiente forma:

Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

Toda persona tiene derecho a la protección de sus datos personales, así como al derecho de acceder a los mismos y, en su caso, obtener su rectificación, cancelación o destrucción en los términos que fijen las leyes.

La ley puede establecer supuestos de excepción a los principios que rigen el tratamiento de datos, por razones de seguridad nacional, de orden público, seguridad, salud o para proteger los derechos de tercero.

La Cámara de Diputados realizó cambios a tal propuesta y la devolvió a la Cámara de Senadores el 20 de septiembre de 2007 en estos nuevos términos:

Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal de procedimiento.

Toda persona tiene derecho a la protección de sus datos personales, así como al derecho de acceder a los mismos, y en su caso, obtener su rectificación, cancelación y manifestar su oposición en los términos que fijen las leyes.

La ley puede establecer supuestos de excepción a los principios que rigen el tratamiento de datos, por razones de seguridad nacional, de orden, seguridad y salud públicos o para proteger los derechos de tercero.

Además, remitió al Senado una propuesta de reforma al artículo 73 constitucional al adicionar lo siguiente:

Artículo 73. El Congreso tiene facultad:

I. a XXIX-N. ...
XXIX-Ñ. Para legislar en materia de protección de datos personales en posesión de particulares.

Hasta el momento en que se escriben estas líneas no se ha discutido acerca de ambas propuestas en la llamada Cámara Alta.

V. *Regulación jurídica del flujo internacional de datos y de internet*

FLUJO DE DATOS TRANSFRONTERIZOS

Origen y concepto

Según el Consejo Económico de la Organización de las Naciones Unidas (ONU), 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".[1]

Este problema consiste en la eventual limitación o favorecimiento de la circulación de datos a través de las fronteras nacionales, lo cual depende de los beneficios o afectaciones que ello pueda traer aparejado a los diferentes países.

En cuanto a los orígenes del problema, cabe decir que éste se deriva de la amalgama surgida entre la informática y las telecomunicaciones; de ahí el vocablo *teleinformática* o telemática, la cual comienza a aparecer en forma a partir de la década de 1960. Esto es un problema con claros antecedentes de índole técnica.

Implicaciones generales

En las economías posindustriales, en las cuales el manejo de información representa hoy en día entre 40 y 50% del valor agregado, es natural que los intercambios internacionales de información estén destinados a

[1] Véase recomendaciones del 23 de septiembre de 1980 en el punto relativo a las definiciones.

desempeñar un papel muy importante. Con base en ello se sustenta en gran medida el adecuado funcionamiento de la economía mundial, en el que la especialización y la interdependencia de los Estados se acentúa aún más.

A pesar de lo anterior, sus implicaciones a menudo no son completadas en la forma más adecuada. Empero, asistimos a un desplazamiento rápido de preocupaciones, de los derechos del hombre concernientes a la soberanía nacional y posteriormente en relación con las incidencias económicas y sociales de intercambios inmateriales entre las naciones.

Cabe distinguir estas implicaciones según dos consideraciones diferentes: unas de carácter positivo y otras de carácter negativo.

a) Implicaciones positivas

Respecto a lo diferentemente externado, no debe soslayarse que el FDT aporta beneficios considerables a las colectividades nacionales, entre los que podemos contar los siguientes:

Favorecimiento de la paz y la democracia. Deben recordarse los vínculos estrechos existentes entre libertad de circulación de información, derechos del hombre y valores fundamentales de la humanidad.[2] La libre comunicación de mensajes y de opiniones es esencial para la democracia y la paz mundial; todo atentado a la libertad de expresión es un peligro para la democracia, por lo cual resulta difícil concebir una paz duradera sin el mínimo de confianza que conlleva el intercambio de hombres e ideas.

Favorecimiento en el progreso técnico y el crecimiento. La cooperación entre los científicos que constituyen una comunidad a escala mundial y la competencia de industriales y empresarios han hecho gala de su aptitud al difundir los conocimientos y técnicas. Todo país que se aislara del potencial de innovación extranjera se condenaría de manera irremisible a vivir un estado de regresión o estancamiento. Por otra parte, la telemática o teleinformática permite asimilar más atinadamente al planeta como un verdadero mercado único de productos y servicios.

Interdependencia económica de las naciones. Hoy en día, ésta es una realidad irreversible. A raíz de la internacionalización de compañías y la especialización de actividades nacionales, toda restricción súbita y deliberada a la continuidad del flujo de datos como existen hasta ahora podría asimilarse a una especie de acta de guerra econó-

[2] Véase al respecto el Acta final de la Conferencia de Helsinki sobre la Cooperación en los Ámbitos Humanitarios, 2a. parte, *Problemas políticos y sociales*, núm. 324, noviembre de 1977, La Doc. Francaise.

mica a la par de un bloqueo o embargo. La inercia que manifiesta la intensidad capitalista de economías industrializadas requiere evidentemente modificaciones de entorno progresivo: es imposible concebir hoy en día a algún país que goce de una independencia total en el plano económico.

b) *Implicaciones negativas*

Así como el desarrollo muy pronunciado de los flujos internacionales de información generada por la revolución tecnológica de la microelectrónica y el progreso de las telecomunicaciones traen consigo una serie de aspectos positivos, paralelamente producen un sinnúmero de cuestiones percibidas al principio según las consideraciones de verdaderos riesgos, entre los que cabe distinguir, reservando los de carácter jurídico para un análisis ulterior, los siguientes:

La *vulnerabilidad social* en términos, por ejemplo, de una eventual "descompostura" de la red telemática con irrupción de los flujos con entorpecimiento en los tratamientos o la alteración de archivos y programas derivados de una falla técnica, catástrofe natural o intervención humana (sabotaje, terrorismo, crisis política, etc.). De esta forma, el país que haya transferido sus datos al extranjero en más de dos ocasiones sería privado de todo argumento de soberanía para definir una solución al problema.

Amenaza a la identidad cultural provocada por la cada vez más frecuente apertura mundial de forjar las culturas nacionales respecto a aquello que ofrecen las culturas importadas. Un verdadero problema reside en las posiciones dominantes y prácticas de los fenómenos de transculturación mediante las llamadas "industrias de la cultura" como el cine, la radio, la televisión, la prensa, las publicaciones, etc., ahora acompañados por los bancos de datos y edición puestos en disponibilidad a través de las redes teleinformáticas.

Dependencia tecnológica exagerada. La evolución de firmas multinacionales ha producido una especialización de producciones y globalización de mercados, al tener a la tecnología y más específicamente a la informática y las telecomunicaciones como una de sus máximas manifestaciones, creándola sólo por momentos para satisfacer una serie de necesidades de los Estados fundamentalmente en desarrollo, lo cual fragmenta sus territorios en actividades planificadas a niveles de resolución supranacionales.

Incidencia económica notoria. El desarrollo y la pérdida de nuevas tecnologías de la información traen consigo una gran cantidad de inversiones económicas, con notorias desproporciones a nivel de los verdaderamente beneficiados y aquellos que ingenuamente consideran

estar en este cuadro. Sin lugar a dudas, esta industria de la información se halla destinada a ser la más predominante dentro de la escala económica mundial, sin que por el momento se vislumbre una corriente contraria al respecto.

Diferentes flujos de información

Según el tipo de datos o información que fluyan a través de la telemática, existe lo siguiente:

a) La información comercial, la cual se manifiesta según una lógica mercantil de distribución (*one-way*) aun si los usos comerciales no están del todo consolidados en este aspecto. Así, se distinguen el flujo de prensa general y especializada; servicios documentarios y bancos de datos, sean de carácter bancario, financiero, industrial, bursátil, comercio de audiovisuales (discos, casetes, películas, programas de televisión), comercio de programas de cómputo y tecnologías, etcétera.

b) La información empresarial, como aquella sustentada en rasgos distintivos, por ejemplo: pedidos, existencias, control de producción, consolidación financiera, gestión del personal, etc., en un cuadro puramente privado en el seno de consorcios empresariales con notorias repercusiones a nivel de dirección, decisión, administración y operación de ellas.

c) La información especial, como aquella que, sin estar necesariamente vinculada con intereses comerciales o empresariales, se convierte en intercambio de conocimientos que permiten un mejor desarrollo de las actividades educativas o de investigación a nivel técnico o científico.

Diferentes clases de redes

Las redes por las que pueden circular dichas informaciones suelen ser muy variadas, lo cual depende del tipo de datos que fluyan en ellas, caracterizadas en su mayoría por innegable importancia, como las siguientes: la red de la Sociedad Internacional de Telecomunicaciones Aeronáuticas (SITA) que permite controlar las telerreservaciones aéreas a nivel mundial, la Red Bancaria de Intercambio de Mensajes Financieros (SWIFT, por sus siglas en inglés) que facilita la comunicación a nivel mundial entre las instituciones bancarias y financieras, la Red de la Policía Internacional (NICS, por sus siglas en inglés) que favorece el intercambio de información referida a

criminales perseguidos por Interpol, etc. Empero, la red más famosa mundialmente en estos momentos es internet, por lo cual se hará referencia a ella después.

Como se deduce, las instituciones beneficiadas por la existencia de este flujo de información son muchas, ya sean de carácter público o privado, lo cual ha producido una dependencia cada vez mayor hacia este fenómeno; con todo, hay una serie de problemáticas jurídicas a las que por momentos no se les da la importancia debida.

PROBLEMÁTICAS JURÍDICAS PARTICULARES

En función de lo que se ha manifestado a lo largo de este capítulo y en el precedente, el flujo de datos transfronterizos trae aparejadas las siguientes problemáticas jurídicas particulares:

Utilización ilícita de datos transmitidos al extranjero. El envío de información a otro país, en el estado actual de derecho, permite a aquélla escapar a la reglamentación a la que pudiera estar sometida en el país de origen. De aquí se pueden derivar atentados graves a las garantías de los ciudadanos o aun a la seguridad de los Estados, lo cual amerita sin duda una solución jurídica.

Tarifas y régimen fiscal aplicables. Si se ha reiterado el contenido económico de la información, es evidente que ésta deberá hallarse sujeta a una cotización económica y más aún si va a ser objeto de exportación, lo cual motiva en su caso un aumento o disminución de las tarifas por aplicar. Y qué decir del gravamen fiscal que deberá imponer el Estado con base en esa cotización, lo cual, a falta de una debida contemplación jurídica, evita la incorporación de cuantiosos y nada despreciables ingresos por dicho concepto a los Estados que exportan y/o reciben información.

Atenta contra la soberanía de los Estados. La teleinformática, al igual que otras manifestaciones tecnológicas, trae consigo una serie de repercusiones que en última instancia inciden en uno de los valores más importantes de toda nación: su soberanía (entendida no sólo en lo político, sino también en lo social, cultural y otros órdenes), lo cual implica tener un control jurídico que evite o al menos limite este tipo de situaciones.

Revestimientos contractuales en torno a la información. Ésta, como un verdadero bien que puede ser objeto de derechos y obligaciones y por tanto materia del contrato en sus diferentes modalidades, motiva una reducción particular de cláusulas afines a su naturaleza que prevean posibles conflictos generados por dichos convenios (jurisdicción competente, etc.), así como los riesgos a que pueda estar sometida y su eventual aseguramiento.

Propiedad intelectual de la información. Es decir, los problemas que pudieran suscitarse en cuanto a la disputa o reivindicación de la propiedad intelectual de la información respecto a la disponibilidad y, por ende, probables beneficios económicos que ello genere, sobre todo por la amplia cobertura o difusión que pudiera tener a través de las redes teleinformáticas.

Seguridad jurídica de las empresas teleinformáticas. Esa información o redes pueden ser motivo de ilícitos ya sea como medios o como objetivos, por lo que una contemplación internacional en términos penales limitaría dichas acciones en forma no sólo correctiva, sino también preventiva.

Organismos gubernamentales y no gubernamentales interesados en el tema

Ante esta situación de notoria trascendencia internacional, son muchos los organismos de esta investidura que se han dado a regular por la vía jurídica el fenómeno provocado por el flujo de datos transfronterizos, a saber:

1. Organización para la Cooperación del Desarrollo Económico (OCDE) interesada en la problemática derivada de la protección y seguridad de datos.
2. Centro de Corporaciones Transnacionales de las Naciones Unidas (UNCTC) interesado en el problema de las tarifas y el régimen fiscal aplicable a este tipo de información.
3. Comisión de Comercio y Desarrollo de las Naciones Unidas (UNCTAD) interesada en la problemática contractual y propiedad de la información.
4. Organización Mundial de la Propiedad Intelectual (OMPI) interesada en el problema de la propiedad de la información y el registro de nombres de dominio, al igual que el ICANN.
5. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) interesada en la trascendencia social, cultural y educativa del FDT.
6. Unión Europea (UE) en cuanto a las implicaciones que pueda traer consigo a los países miembros de la Unión.
7. Organización Mundial del Comercio (OMC) respecto a las tarifas y régimen fiscal aplicable.
8. Organización Internacional de Telecomunicaciones Vía Satélite (INTELSAT) en referencia a los problemas jurídicos por la transmisión de información vía satélite.
9. Unión Internacional de Telecomunicaciones (UIT) respecto a que sean transmitidas por medios que no usen satélites.
10. Banco Mundial, la privacidad y confidencialidad de datos.

Convenio de Estrasburgo

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

REGULACIÓN JURÍDICA DE INTERNET

Origen y evolución de internet[3]

Es casi imposible pelear una guerra efectivamente cuando no hay medios de comunicación entre los centros de mando y las unidades de combate. Por ello, en pleno apogeo de la guerra fría, durante los inicios de los años de 1970, la ARPA (Advanced Research Projects Agency, o Agencia de Investigación de Proyectos Avanzados), una rama científica de las fuerzas armadas estadounidenses, inició el diseño de una red de computadoras que pudiera sobrevivir a cualquier tipo de catástrofe.

Esta red debía tener varias cualidades para ser eficaz. Primero, debía ser redundante, lo cual quiere decir que la información debía encontrar más de una ruta desde su origen hasta su destino, obviando así cualquier "hueco" que pudiera producirse en la red. En segundo lugar, la red debía ser descentralizada; no debía haber un solo centro que fuera fácil de eliminar. En tercer lugar, la red debía ser fácil de implementar al usarse la infraestructura existente. ARPA inició la puesta en práctica de esta red, a la que llamaron ARPAnet.

Al inicio, ARPANet contaba con pocas máquinas, accesadas principalmente por usuarios académicos e investigadores tanto de ARPA como de otros órganos del gobierno de Estados Unidos, como ciertas universidades y la NSF (National Science Foundation, o Fundación Nacional de

[3] Tomado de http://www.infoapuntes.com.ar/Apuntes/historia%20internet.htm

Ciencias). Conforme estos individuos comenzaron a usar de modo más intensivo esta red, su demanda creció exponencialmente.

Diseñadores de Estados Unidos, Inglaterra y Suecia comenzaron a poner en marcha el protocolo IP en todo tipo de computadoras. En esta etapa del desarrollo de internet, su uso era casi exclusivamente para recibir y enviar correo electrónico, por lo que no era necesario tener computadoras poderosas para accesarlo. Como la red había sido diseñada para utilizarla con muchos tipos diferentes de equipos, diversas organizaciones comenzaron a emplear los equipos que tenían disponibles.

Alrededor de 1983 ocurrió una revolución en el mundo de la informática: aparecieron las primeras computadoras personales de oficina. Estas máquinas eran relativamente accesibles a muchos individuos y empresas, y podían ser conectadas entre sí para formar redes de área local y de área extendida.

Muchas compañías y organizaciones comenzaron a construir redes de PC y estaciones de trabajo que utilizaban los protocolos IP de ARPANet para comunicarse internamente. Estas redes se multiplicaron hasta que llegó un punto en que todo el mundo visualizó lo beneficioso que sería tener estas redes dispersas conectadas entre sí.

Una de dichas redes era la NSFNET, la cual puso en práctica cinco centros de supercómputo en universidades importantes durante los finales de los años 1980, a costos elevadísimos. NSF decidió interconectar estos centros de cómputo mediante la tecnología IP de ARPANet con líneas telefónicas. Para evitar los altos costos de las telecomunicaciones telefónicas de larga distancia, NSF diseñó un sistema de direcciones que permitía a los centros de supercómputo conectarse con sus vecinos más cercanos para retransmitir la información.

Esa solución fue extremadamente exitosa, por lo que otras universidades comenzaron a utilizar la red y el costo de su uso empezó a disminuir de manera proporcional. En 1987 el contrato de administración y mantenimiento de la red fue pasado a una compañía llamada Merit Network, Inc., en colaboración con MCI e IBM. Éste fue el inicio del internet comercial. En 1987, internet todavía se empleaba principalmente para enviar y recibir correo electrónico y archivos vía FPT.

En 1993, Tim Berners-Lee, joven científico que trabajaba en el CERN (Laboratorio Europeo de Física de Partículas, en Suiza), diseñó un sistema de hipertexto que permitía a usuarios de redes IP navegar a través de una serie de documentos mediante la activación de enlaces en los documentos. Este método de navegación, mucho más sencillo que los anteriores, era extensible y permitía desplegar imágenes y otros medios en conjunto con los documentos textuales.

El nuevo servicio de internet se llamó World Wide Web y su crecimiento vertiginoso ha impulsado el desarrollo de internet en la segunda mitad de la década de los años 1990.

Para navegar en web es necesario utilizar aplicaciones conocidas como *browsers*. El primer *browser* en tener una verdadera aceptación popular fue Mosaic, ideado en la Universidad de Illinois en Urbana por un joven llamado Marc Andreesen.

Andreesen y un empresario llamado Jim Barksdale fundaron luego una compañía para mercadear una versión comercial de Mosaic, a la que llamaron Netscape. El *browser* Netscape Navigator pronto se convirtió en el navegador estándar de internet, lo cual llevó a sus creadores a la fama y fortuna.

Al realizar el potencial de productos como Navigator y de web en general, la corporación Microsoft lanzó un producto competitivo llamado Internet Explorer. Este navegador, que está interrelacionado profundamente con el sistema operativo Windows, es cada vez más importante.

La WWW; es un conjunto de servicios basados en *hipermedios*, ofrecidos en todo el mundo a través de Internet: se llama WWW (world wide web, o red de alcance o cobertura mundial). No existe un centro que administre esta red de información, sino más bien está constituida por muchos servicios distintos que se conectan entre sí a través de referencias en los distintos documentos, por ejemplo: un documento contenido en una computadora en Canadá puede tener referencias a otro documento en Japón, o a un archivo en Inglaterra o a una imagen en Suecia. Al hablar de hipermedios se alude a información que puede presentarse con distintos medios, como documentación ejecutable, de texto, gráficos, audio, video, animación o imagen.

Historia de internet en México y el proyecto internet 2[4]

Los orígenes de internet en México se remontan a 1987. En 1992 se creó Mexnet, A.C., una organización de instituciones académicas que buscaba en ese momento: promover el desarrollo de internet mexicano, establecer un *backbone* nacional, crear y difundir una cultura de redes y aplicaciones en relación con internet y contar con conexiones a nivel mundial.

Los principales logros en esos días fueron el diseño y operación del primer *backbone* nacional de 64 kbps en asociación con RTN, ahora de 2 mbps, que eran líderes en experimentación de nuevas tecnologías en internet. Actualmente se cuenta con dos salidas internacionales.

Respecto a los orígenes de la www en México, a principios de 1994 existió la iniciativa de Mexnet para desarrollar servicios en la red. Para entonces, el ITESM inició un *home page* experimental, la UDLA desarrolló

[4] Tomado de http://www.isocmex.org,mx/historia.html

su Mosaic y la UDG presentó su Mosaic y diseñó una sección sobre arte y cultura mexicana.

Respecto al Proyecto Internet 2 en México, cabe mencionar que tiene como principal objetivo impulsar el desarrollo de una red de alto desempeño que permita correr aplicaciones que faciliten las tareas de investigación y educación de las universidades y centros participantes. Entre las aplicaciones que se desarrollan se encuentran telemedicina, manipulación remota, bibliotecas digitales, educación a distancia, colaboratorios, almacenamiento distribuido y supercómputo, entre otros.

La Corporación Universitaria para el Desarrollo de Internet (CUDI) es el organismo encargado de promover y coordinar el desarrollo de Internet 2 en México y está formado por las principales universidades y centros de investigación del país: CICESE, IPN, ITESM, LANIA, UANL, UAT, UAM, UDEG, UDLA-P, UNAM, ULSA, UV y UACJ, además de CONACYT y varias compañías de telecomunicaciones, como Telmex, Cabletron Systems, Fore Systems y Nortel Networks.

En ese esfuerzo tan importante para el desarrollo científico y tecnológico del país, la UNAM es el Centro de Operación de la Red Nacional de Internet 2 (NOC -Internet 2 México), cuya responsabilidad reside en asegurar una alta disponibilidad de la red, mediante el rápido reconocimiento de fallas y detección de niveles de degradación de servicio, así como la realización de las tareas de control proactivo y correctivo de fallas en la operación de dicha red, además de participar activamente en la coordinación de pruebas tecnológicas con otros grupos de trabajo.

Intentos de regulación

En internet cambia para el derecho la noción de tiempo y espacio, ya que se pueden realizar enlaces inmediatos a tiempo real, sin importar el lugar del mundo donde se encuentren las partes.[5]

Hay quienes dicen, como M. Burstein: "no hay un lugar en internet", y otros, como Herbert Kronke, la Corte del Distrito de Munich o la Corte del Distrito Sudeste de Nueva York, sostienen que "todos los lugares están en internet". De un modo u otro, todos presentan esta paradoja de un espacio no territorial, no geográfico, que por su sola existencia genera interrogantes y problemas al mundo legal conocido, fuertemente atado a lo geográfico por el concepto de las soberanías.

Internet es una red de redes. Si se intentara dibujarla, seguramente se presentaría con un formato distribuido, reticular, de incontables nodos

[5] Véase Eloy Ruiz Herrero, *Revista Internauta de Práctica Jurídica*, núm. 8 (julio-diciembre de 2001), "El comercio electrónico".

interrelacionados, sin centro, como es de su propia naturaleza. Además, es globalmente accesible y sus mecanismos y protocolos son universales.

Esta red, por medio de proveedores de servicios de internet, conecta a los usuarios entre sí y, aunque aparentemente no existe un *gobierno* ni autoridad central como hoy se conocen, existen agencias internacionales de gobierno de internet que establecen estándares y habilitan el sistema para que funcione (Internet Society, ICANN, WIPO y otras), pero el acatamiento a sus disposiciones es voluntario y depende, en mucho, de la posición que se adopte frente a los principios de autogobierno de internet.

Las fronteras no existen en internet y los Estados tienen serias dificultades para delimitar sus jurisdicciones. Es indudable que el Estado intenta regular unilateralmente, sin contar con la anuencia de las demás entidades, cualquier asunto que sucede en su territorio.

Es indiscutible que, excepto en casos muy concretos, las operaciones comerciales que se realizan por internet tienen un ámbito internacional, pues el elemento extraterritorial se encuentra presente.

Según el profesor Antonio Martino, ha llegado el momento de pensar seriamente en una estandarización jurídica, algo así como un nuevo derecho, un nuevo *ius gentium* para la libre circulación de las personas, las ideas y los bienes. Si esto es así, dicha libre circulación va a provocar un derecho común que deberemos admitir los próximos años.[6]

En trabajos recientes, Lynch, Brenna, Bianchi y Martino consideraron que internet debe estar sujeto a algún tipo de regulación. Brenna, entre las soluciones que propone, ubica lo siguiente: *a*) unificación de reglas legales; *b*) unificación de una ley sustantiva de internet, y *c*) reconocer a internet como jurisdicción propia y asignar disputas a un tribunal internacional de arbitraje de internet o una corte especial exclusiva para estas disputas con una ley sustantiva que rija.[7]

M. Burnstein presenta una serie de alternativas: *a*) una unificación de la elección de reglas legales, *b*) una unificación de una ley sustantiva de internet, y *c*) reconocer a internet como jurisdicción propia y asignar disputas a un tribunal internacional de arbitraje de internet o una corte especial con competencia exclusiva para estas disputas.[8]

Vinton G. Cerf, considerado uno de los creadores de internet, junto con el ingeniero Robert Khan, a partir del protocolo que permitió a todas las computadoras entenderse en un mismo lenguaje, el TCP/IP, afirmaba hace poco tiempo que el problema que surge al legislar es que internet

[6] EcomDer, 2000, *Primer Congreso Internacional por Internet sobre Aspectos Jurídicos del Comercio Electrónico*, Facultad de Derecho, Buenos Aires, Argentina.

[7] *Idem.*

[8] Coloquio internacional en honor de Michel Pelichet, organizado por el Instituto Molengraff de Derecho Privado de la Universidad de Utrecht y la Conferencia de La Haya de Derecho Internacional Privado.

avanza de manera muy rápida y, cuando se aprueba una ley, la tecnología ya ha cambiado.

La Convención de las Naciones Unidas para la venta internacional de bienes de 1980, el UNIDROIT, los Principios de los Contratos Comerciales Internacionales, los Principios del Derecho Contractual Europeo y la Ley Modelo de Comercio Electrónico de UNCITRAL podrían señalarse como pasos en el camino de desplazar la aplicación de los derechos locales, con los inconvenientes que presentan, por un derecho sustantivo de internet de ámbito internacional.

No es aventurado sostener que la actividad informática constituye el vínculo estrecho que otorga el fundamento teórico y la utilidad práctica que justifica concentrar en un mismo subsistema las regulaciones dispersas entre ramas tradicionales del derecho, pues sólo así se podrá juzgar la conveniencia de apartarse de las soluciones previstas en cada una de ellas, es decir, la aparición de un derecho especial frente al común, en aquello conocido como derecho de la informática.

Por lo anterior, se debe considerar la posibilidad de que exista el derecho internacional de la informática como medio adecuado para la regulación de internet, en la que el derecho internacional podría reducirse a un gran sistema de reglas de elección de la ley a aplicar a la resolución de un caso, dadas ciertas circunstancias. Si esto es así, parece lógico plantearse la unificación de estas reglas de elección, sin que ello pase por la unificación del derecho sustantivo.

Sería entonces pensable construir un cuerpo supranacional articulado de reglas de elección aplicables a la determinación de cuál derecho nacional regularía la disputa o conflicto originado en internet.

Por lo pronto, existen dos maneras conocidas de alcanzar un derecho unificado sustantivo para internet: las cortes y los tribunales desarrollan con sus pronunciamientos un derecho común de internet o se realizan acuerdos o tratados internacionales para tal fin.[9]

Ese derecho unificado sustantivo de internet generado a partir de la decisión de las cortes tendría la característica de ser un derecho de *sujeto* específico y no de *lugar* determinado, como el derecho tradicional local y geográfico.

Burnstein propone tomar como modelo la *lex mercatoria* y desarrollar analógicamente este nuevo derecho común. Dicha ley de comercio tuvo origen en una colección de prácticas y costumbres que tenían los viajantes de comercio de la Europa medieval y se transformó en "obligatoria" en todos los países comerciales del mundo civilizado por aquellos tiempos.

Así como los comerciantes desarrollaron y practicaron ese conjunto de usos y costumbres que aceptaron como ley entre ellos, podría pensarse que

[9] Véase http://www.it-cenit.org.ar/Seminario/DerEconDIG2000/material/accleg/accleg.htm

los usuarios de internet pusieran en práctica usos y costumbres del mundo *on line* de la red, a partir del conocimiento que su práctica generalizada fuere acumulando y que tal práctica generase, por su general acatamiento, un derecho común de este espacio que algunos denominan *ciberespacio*.

Cuando un tribunal fuese llamado a intervenir para resolver una disputa de internet, buscaría en este derecho consuetudinario del ciberespacio la colección de costumbres, usos y prácticas aceptadas, desarrolladas por las cortes, con la guía de los usuarios, gobiernos, industria y demás sujetos reconocidos de la red.

Hay un elemento atrayente en esta postura de sostener la creación de un derecho común del ciberespacio: un derecho así conformado se presenta como lo suficientemente flexible para acompañar el rápido devenir del cambio tecnológico, y por ende legal, que es propio del medio. Sin lugar a dudas, el proceso legal convencional es mucho más lento y necesita edificarse a partir de consensos que sólo se alcanzan después de transitar largos procesos de negociación política entre los Estados.[10]

La Decency Act estadounidense

La Ley de la Decencia en las Comunicaciones de Estados Unidos, fue promovida en 1995 por el senador Jim Exon en el marco de la nueva ley de telecomunicaciones de ese país y ratificada como ley federal el 8 de febrero de 1996, lo cual provocó una reacción inmediata en su contra por las asociaciones pro derechos civiles en la Unión Americana. En junio de 1997 fue declarada atentatoria contra la libertad de expresión consagrada en la *Primera Enmienda* y, en consecuencia, inconstitucional por la Suprema Corte de esa nación, porque se formuló de manera muy amplia o general al prohibir el acceso a sitios con material (artículos y órganos sexuales o excretorios) considerados manifiestamente ofensivos e indecentes La ley fue impugnada judicialmente por la American Civil Liberties Union (ACLU, Asociación de Libertades Civiles de Estados Unidos), que sostuvo su inconstitucionalidad por la violación de la libertad de expresión y objetó que su vaguedad le impedía ser aplicada de manera razonable.

Según se exponía en tan criticada ley, cualquier ciudadano que exhibiera en una página web opiniones o imágenes de contenido "indecente" u "ofensivo" y que fueran vistas por un menor de edad, podría ser sancionado con una pena de hasta dos años de prisión.

Algunos de los principales postulados de dicha ley, eran castigar a cualquiera persona "que cree, haga, solicite o inicie en medios de telecomunicación nacionales o extranjeros, cualquier comentario, solicitud, su-

[10] *Idem.*

gerencia, propuesta, imagen u otra comunicación obscena, lujuriosa, sucia o indecente; que pretenda molestar, abusar, amenazar, acosar u hostilizar a otra persona..."

Con todo, según nuestro parecer, lo más rescatable de dicha ley era su artículo 230, que reconocía a Internet como "una herramienta extraordinaria para la educación, cultura, discurso político y actividad intelectual, que se ha desarrollado con un mínimo de regulación gubernamental, por lo que se promoverá su desarrollo y competencia en el mercado libre para beneficio de personas, familias y escuelas...". De acuerdo con nuestro entender, éste es uno de los conceptos más claros y contundentes de lo que debiera ser internet...[11]

Autorregulación de internet

Así surgieron iniciativas provenientes de la misma sociedad civil y de las empresas que marcaron la pauta en internet y que han comenzado a adaptar políticas de "Autocensura", como la mayoría de las compañías que ofrecen portales gratuitos y prohíben la publicación de imágenes pornográficas y grupos de discusión "desalientan" el uso de lenguaje impropio, ambos en términos de su uso, con miras a desarrollar y estructurar la red de modo armónico y equilibrado para que responda a vitales intereses de la comunidad y a las necesidades esenciales del hombre actual.[12]

Con apego a estos principios, uno de los primeros países en introducir códigos deontológico o de buena conducta en la red es Francia con sus "netiquettes" o reglas de etiqueta en la red; asimismo, en Inglaterra se han adoptado mecanismos de autorregulación, en los que se han elaborado códigos de conducta y creado organismos independientes como la Safety Net

[11] Véase noticias y texto de la ley en: http://www.cnn.com/US/9706/26/scotus.cda/index.html. En una parte del fallo, el juez de la Suprema Corte, John Poul Stevens, al confirmar las decisiones previas de inconstitucionalidad de los Tribunales Federales de Filadelfia y de Nueva York, manifestó que... "de acuerdo con la tradición constitucional de nuestro país, en ausencia de prueba en contrario, debemos presumir que la regulación de los contenidos y de la expresión está más cerca de inferir el libre intercambio de las ideas y de promoverlo. El interés en potenciar la libertad de expresión en una sociedad democrática está por encima de los beneficios teóricos e indemostrables de la censura".

Cabe mencionar que uno de los jueces, Stewart R. Dalzell, entendió que internet implica una garantía para el desarrollo libre y autónomo de las comunicaciones entre los ciudadanos normales frente a la presencia de los grandes magnates poseedores de los medios de información. Según este juez, puede considerarse a internet una "conversación mundial sin fin". Por ello, el gobierno no puede arbitrariamente interrumpir esta conversación cívica por medio de normas como la CDA (Communication Decency Act).

Finalmente, los jueces Sandra Day O'Connor y Wiliam Rhenquist, en un voto particular, apoyaron también el carácter inconstitucional de la CDA, excepto en su estricta aplicación en cuanto a la comunicación a los menores, de informaciones o imágenes indecentes u obscenas.

[12] Gabriela Armas y Rafael E. Tobia, *La libertad de expresión en internet*, Universidad Católica Andrés Bello, Escuela de Derecho, Caracas, Venezuela, junio de 2001.

Foundation que mantienen una línea directa en la cual se pueden recibir denuncias de aquellos contenidos, ideologías o actividades que se consideren ilícitos. También se ha hecho común lo que denominamos "programas filtro" o cerrojo, o de selección de contenidos que bloquean el acceso a determinados sitios web y que para nosotros es el mecanismo técnico más adecuado para evitar la existencia de contenidos ilícitos, lo cual limita o impide el acceso a dichos contenidos mas no a otros. De esa forma es plenamente factible permitir la libre circulación de ideas que reclaman la libertad de expresión, pero al mismo tiempo se bloquea el acceso a determinados contenidos expuestos en sitios web, respetándose así la diferencia de criterios, valores y costumbres morales. De esa forma se configuraría una censura (más bien *autocensura*) que no tendría por fuente una restricción o prohibición legal, administrativa o judicial, sino que el control o filtrado se produce a nivel del proveedor que ofrece acceso a la información o a nivel del usuario final en la computadora donde se recibe la información. Esto haría que fuésemos "legisladores digitales" de nuestros actos, sin que por ello tal idea sea romántica. Claro está, no podemos dejar a un lado y de modo absoluto la participación del Estado en la elaboración de políticas y campañas que contribuyan a alcanzar este propósito.

VI. *El derecho a la propiedad intelectual y las nuevas tecnologías de la información y comunicación*

INTRODUCCIÓN

Uno de los problemas más importantes que enfrenta el derecho de la informática es el de la protección jurídica derivada de las nuevas tecnologías de la información y la comunicación (TIC). Entre todas éstas, se destacarán dos de ellas que parecen en especial significativas: la protección de los programas de computación y la de los llamados *nombres dominio.*

PROTECCIÓN JURÍDICA DE LOS PROGRAMAS DE COMPUTACIÓN (SOFTWARE)

Generalidades

Técnicamente, los programas de cómputo se caracterizan sobre todo por ser un medio necesario para ofrecer un conjunto de instrucciones comprensibles por una computadora, a efecto de resolver cierto problema. Los programas se basan en un análisis consistente en determinar ese problema, clasificar los datos y definir las estructuras y los resultados esperados, así como en prever la evolución del problema y los procedimientos de control necesarios.

Una de las definiciones más completas hechas por expertos es la de la Organización Mundial de la Propiedad Intelectual (OMPI), que considera a los programas un conjunto de instrucciones expresadas en un lenguaje natural o formal; así, una vez traducidas y transpuestas en un soporte descifrable por una máquina de tratamiento de datos o por una parte de esta máquina, se pueden efectuar operaciones aritméticas y sobre todo lógicas, en vías de indicar u obtener un resultado particular.

Evolución del problema

La comercialización de las computadoras se inicia en la década de los sesenta. En un principio, 70% del capital destinado al desarrollo de la industria informática se empleaba en el área de componentes físicos (hardware) en tanto que 30% se canalizaba al área de soporte lógico (software).

Posteriormente, la producción de equipos requería menos inversiones; no obstante, la creación de programas se ha tornado más compleja y, por ende, más costosa en virtud de que los programas de cómputo soportan en gran medida el adecuado comportamiento y carácter efectivo de las computadoras. Todo ello, aunado a la falta de una apropiada estandarización de los programas, ha motivado que las cifras se inviertan, por lo que la industria de programación absorbe actualmente 70% de los costos, cantidades difícilmente amortizables, entre otras causas por la falta de un adecuado régimen regulador que impida o limite las continuas actitudes de apoderamiento ilícito en perjuicio de los creadores y usuarios.

Nociones fundamentales

Cabe enunciar que el problema de la protección de los programas no es estrictamente jurídico, sino que denota la presencia de dos elementos fundamentales: el técnico y el económico.

1. *Aspecto técnico*

Los programas de cómputo son el conjunto de procedimientos o reglas que integran el soporte lógico de las máquinas que permiten conseguir el proceso de tratamiento de la información. En la práctica se pueden distinguir los siguientes tipos de programas:

a) Los programas fuente (conocidos también como *sistemas operativos* o *de explotación*), que están ligados al funcionamiento de la máquina y guardan una estrecha relación con las memorias centrales y auxiliares de la computadora a través de dispositivos como los

compiladores, traductores, intérpretes, editores, etc., que permiten el adecuado enlace entre la máquina y los trabajos del usuario.

b) Los programas objeto, que son los realizados para satisfacer las necesidades más variadas de los usuarios, que facilitan el tratamiento de datos definidos de manera concreta y que resultan disociables de la máquina. Algunos de estos programas resuelven las necesidades de un gran número de usuarios y otros responden "sobre medida" a necesidades específicas de determinados usuarios.

c) Los programas de explotación (conocidos también como sistemas operativos), que están vinculados con el funcionamiento de la máquina y que permiten aprovechar al máximo sus posibilidades. Además, guardan estrecha relación con las memorias centrales y auxiliares de la computadora y tienen en cuenta las funciones de enlace de los trabajos de los usuarios.

Aquí es importante distinguir, por una parte, los programas referentes al funcionamiento interno (compiladores, traductores e intérpretes), que traducen el lenguaje simbólico en lenguaje codificado propio de la máquina; y por la otra, monitores, supervisores y editores que controlan el seguimiento de instrucciones, atribuyen los espacios de memorias, los programas de servicio y los estándares (de clasificación), etcétera.

d) Los programas de aplicación, que son los realizados para satisfacer las necesidades más diversas y variadas de los usuarios; permiten el tratamiento de datos definidos concretamente y son "separables" de la máquina. Entre ellos se distinguen los concebidos para satisfacer las necesidades de múltiples usuarios (paquetes de software) de los que "sobre medida" responden a las necesidades del usuario (programas específicos).

2. *Aspecto económico*

En líneas anteriores se ha expresado la importancia económica que reviste actualmente el bien-información. Los programas de cómputo como una de las máximas manifestaciones del producto-información han provocado un apuntalamiento de la industria de programación, lo cual ha provocado que los problemas en torno al software rebasen el ámbito puramente técnico para alcanzar niveles económicos y, por ende, jurídicos.

Principales implicaciones

El indiscutible contenido económico de los programas ha suscitado, entre otras cosas, que dichos bienes se constituyan en objeto de inversiones muy

altas, así como de acciones ilícitas de apoderamiento, lo cual ha urgido la búsqueda de soluciones a dichos problemas, primeramente encuadradas bajo la misma perspectiva técnica y económica. Analicemos entonces estas implicaciones.

Despilfarro

La falta de protección ha causado que las empresas creadoras de software destinen, la mayoría de las veces, considerables sumas de dinero para desarrollar programas similares (si no es que iguales) a los de sus competidores, lo cual redunda en un ofrecimiento desmedido de programas para determinadas áreas en detrimento de otras tantas, así como un alto precio del producto, ambas en menoscabo de los intereses de los usuarios informáticos.

Pillaje

La lucha continua para dominar el mercado de programación en la industria informática por las empresas especializadas y aun por los intereses de los particulares genera un sinnúmero de acciones tendientes al apoderamiento dentro de los "términos" más técnicos posibles, mediante métodos directos o indirectos, sofisticados o no, de mala o aun buena fe por manifestaciones como el robo, espionaje industrial, chantajes físicos o morales, etc., lo cual ha propiciado una búsqueda desesperada de soluciones por los creadores de programas.

Intento de solución: el uso de la criptografía

Esto ha ocurrido de acuerdo con la forma de un resguardo secreto de los programas, así como con dispositivos más sofisticados como la criptografía, códigos casi indescifrables o introducción de instrucciones que impiden el copiado de programas llegando hasta el bloqueo o destrucción total de éstos, todos ellos muy onerosos, a la vez que transitorios, a pesar de su relativa eficacia durante su corta existencia, ya que al estar fundamentados en bases técnicas, es evidente su superación por la misma técnica. De esta forma, el problema queda aún sin solución, por lo que surge la necesidad de interesarse en instituciones aparentemente más resolutorias, como el derecho.

Para comprender esta nueva técnica, cabe mencionar que la criptografía es la ciencia que transcribe las informaciones secretamente, forma incomprensible para toda persona que no sea el usuario o destinatario. El

"decriptaje", a su vez, es la ciencia cuyo objeto reside en el descifrado de las informaciones secretas o codificadas sin el conocimiento previo del código, del método o la clave del código. La criptografía es la amalgama de esas dos ciencias.

Expuesto lo anterior, es conveniente mencionar que la protección deriva de la criptografía normalmente utilizada para prevenir y controlar el abuso y para autenticar las fuentes y las informaciones que pueden estar comprendidas. La criptografía consiste, por tanto, en "criptar" los programas por un sistema de codificación sofisticado que emplea una o varias claves, conjunto de caracteres que transforman un método general o un algoritmo específico en informaciones codificadas, a efecto de que si el competidor pirata o "enemigo" conoce el algoritmo no le sea de provecho, pues deberá conocer también la clave, la cual podrá ser cambiada y representar consecuentemente un nuevo obstáculo para aquel que quiera tener acceso al sistema. Estos métodos son por momentos tan eficaces que el algoritmo codificado puede ser objeto de una publicación o ser conocido sin representar problema alguno.

Las diferencias entre los diversos métodos de criptografía residen en que la transformación no utiliza el procedimiento de operaciones lineales, es decir, de adición o de multiplicación, pero pone en práctica el estudio reciente de las funciones no lineales. Así, la investigación del algoritmo necesario al "decriptaje" es imposible en un periodo razonable, aun con una computadora. La compañía IBM ha concebido y comercializado un sistema de codificación denominado DES, considerado inviolable.

El uso de estos dispositivos, si bien ayuda a limitar la piratería, presenta a su vez el inconveniente de que un programador descontento pueda sabotear el programa luego de que este empleado deje la empresa. Por ello, Donn B. Parker, presidente consultor de sistemas de la compañía SRL International, en Menlo Park, California, habla de los posibles sabotajes a los programas como un verdadero delito informático y preconiza para fines de protección los consejos de seguridad siguientes:

Establecer un código de conducta en el cual se especifique aquello que constituye o no una actividad autorizada, con leyes que permitan la persecución en caso de delito.

Organizar reuniones especiales con el personal que presente problemas con la empresa.

Utilizar "contactos" dispersos en la empresa.

Recurrir a un sistema individual de funciones, de verificación y de balances para vigilar continuamente al personal.

Desarrollar políticas para el personal incorporando datos varios y entrevistas susceptibles de mejorar las relaciones o enviar al empleado a *vacacionar* durante dos semanas para separarlo de los demás y provocar un cambio de actitud más positivo en favor de la empresa.

Enlistar o marcar diferencia con texto normal ya sea inciso, viñetas o puntos.

Empero, lo anterior conforma sólo un paliativo. La protección (técnica) perfecta no existe. Lo cierto es que la protección de los programas no puede resolverse sólo con utilizar estos medios técnicos. Hay que considerar necesariamente al derecho, aun si en primera instancia pueda derivarse una comprobación de insuficiencia.

Régimen jurídico aplicable

A continuación se estudian algunas de las figuras más significativas de aquello que puede conceptuarse como un derecho clásico, por ejemplo: la vía civil (entiéndase también mercantil) o penal frente al problema de la protección jurídica de los programas, incursionando posteriormente en las figuras derivadas del llamado derecho de la propiedad intelectual, como las propiedades industria literaria y artística, para finalizar con una institución jurídica *sui generis* acorde con las circunstancias.

Vía civil

a) Contratos

En los contratos se establece un conjunto de cláusulas alusivas a la seguridad y protección de los programas, en las que se consigna el eventual acceso a éstos por personas no autorizadas, uso inadecuado, modificaciones no pactadas, destrucción de información, etc. Todo ello implica un régimen de confidencialidad y resguardo bajo secreto.

En términos generales, todo contrato referente a un programa (o materia gris) deberá hacer alusión a cláusulas que garanticen la seguridad de los datos y prohibir el acceso a toda persona no autorizada a:

- Obtener informaciones que "pertenezcan" al contratante (ya se trate de copia, duplicación de archivos o "robo" de programa).
- Modificar las informaciones contenidas en un soporte magnético o modificar su programa.
- Destruir informaciones, borrar el contenido de un disco o una banda magnética o escribir en una banda que contenga información.
- Utilizar los recursos de un sistema sin autorización.
- Explotar un programa en el que el uso esté reservado por contrato.
- Todos los agentes y personas que con motivo de la ejecución de un contrato tengan acceso a datos, o a programas que una empresa desee reservar en secreto, deberán comprometerse a llevar un ré-

gimen de confidencialidad en que los responsables estén constreñidos por escrito a destruir o borrar todas las "copias" que les sean dadas con motivo de la ejecución del contrato.

Existe igualmente interés en indicar en el contrato los datos y programas que presentan un carácter "sensible", a fin de que la atención del personal del proveedor se enfoque hacia las consecuencias que tendría la divulgación de esos datos en el exterior de la empresa. Por ello, es muy recomendable asegurarse de que:

- El personal que ejecutará el contrato ha sido notificado del carácter confidencial que presentan los datos y los programas en cuestión.
- El contrato contiene una cláusula de "secreto profesional".
- Estas personas sean objeto de las mismas reglas de disciplina general aplicables al personal especial en materia de seguridad.

Esta protección no ha sido empleada de manera adecuada, por lo que su eficacia ha sido relativa.

b) Competencia desleal

En forma sintética cabe decir que la acción de la competencia desleal es la vía jurídica que permite contrarrestar los actos de competidores que son contrarios a los usos honestos del comercio, y principalmente los que puedan crear una confusión con el establecimiento, los productos o la actividad industrial o comercial de un competidor; los alegatos falsos que tiendan a desacreditar el establecimiento, los productos, o la actividad industrial o comercial de un competidor; las indicaciones o alegatos susceptibles de inducir al público al error sobre la naturaleza, la forma de fabricación o las características de las mercancías, etcétera.

Para que un individuo (o una empresa) pueda ser objeto de una acción en competencia desleal es necesario que cause un perjuicio por el hecho de "sustraer" de modo furtivo un secreto de empresa. Por tanto, la acción en competencia desleal no es normalmente aplicable al encuentro de terceros, que han adquirido el secreto sin haber cometido de forma deliberada un acto contrario a los usos honestos. Por regla general, en cuanto a su naturaleza jurídica, esta acción se identifica con la acción en responsabilidad civil prevista por la ley.

La característica de dicha acción en competencia desleal aplicada en la protección de programas es que no impide la utilización simple del programa a falta de una apropiación desleal y furtiva. Esto no ex-

cluye suponer su utilización a título supletorio de otras acciones para sancionar no tanto la violación de un derecho privativo de la propiedad incorporal (como tal oponible a todos), sino un comportamiento desleal que atente a los intereses comerciales de un competidor, sobre todo en el desvío de su clientela por un riesgo de confusión presuntamente creada, aun si esta función ha sido criticada como atenuación de un derecho privativo, en el que no existe disposición legal o voluntad de las partes.

c) Enriquecimiento sin causa

Se trata de una acción basada en la teoría del enriquecimiento sin causa, calificado en Estados Unidos de *injust enrichment* y que deriva de un principio general de equidad según el cual está prohibido enriquecerse en detrimento de otro.

Para triunfar en una acción basada en la teoría del enriquecimiento sin causa, el demandante debe probar que la utilización de su idea o invención por un tercero ha permitido a éste enriquecerse y que correlativamente ha provocado un empobrecimiento. No obstante, esas pruebas son tan difíciles de aportar en la práctica que el recurso a la teoría en cuestión es invocado de manera esporádica.

Por otra parte, una regulación de tal acción (que queda aun por imaginar) no facilitaría mucho su uso, ya que podría generar graves abusos, en virtud del riesgo latente de ver a particulares o empresas invocar con falsedad un perjuicio (un empobrecimiento) largamente ficticio o al menos muy sobrestimado.

Vía penal

Se ha llegado a considerar que delitos como el robo, el fraude, el abuso de confianza o los llamados secretos comerciales (figura estadounidense) y secretos de fabricación (figura europea) se presentan como medios de solución frente al problema; empero, dichas instancias parecen no estar integradas por elementos tales que permitan atribuir una cabal asimilación.

Así, en el robo se requiere el apoderamiento físico de una cosa mueble, la cual, en términos de la información como un "algo" indiscutiblemente intangible o inmaterial, no configura de manera convincente el supuesto. Por otra parte, en el abuso de confianza se necesita la disposición de una cosa ajena mueble, lo cual representa de la misma forma problemas a nivel de la carga de la prueba. En el fraude se requiere un engaño o aprovechamiento de un error que permita hacerse ilícitamente de alguna cosa (no se especifica de qué tipo) o alcanzar un lucro indebido, lo cual, si bien pudie-

ra aplicarse a final de cuentas por su misma abstracción frente al problema, ofrece serias inconveniencias en la práctica.

Ahora bien, en cuanto a los secretos comerciales y de fabricación (si bien no utilizados en México), implican una divulgación intencional (o aun fortuita) de alguna información, en este caso referida o contenida en un programa de cómputo. Dichas figuras, aunque apropiadas en apariencia (sobre todo porque son castigadas penalmente), revisten asimismo dificultades a nivel probatorio respecto al apoderamiento y difusión de la información.

Propiedad industrial

a) Marcas

La marca es un signo distintivo que permite a su titular (fabricante o comerciante) distinguir sus productos o sus servicios de los de la competencia.

Desde el punto de vista económico, la marca es un signo que tiende a procurar a la clientela, la mercancía o el servicio que busca y paralelamente a la empresa una clientela apegada a la marca. La Organización Mundial de la Protección Intelectual (OMPI) define por marca "un signo visible protegido por un derecho exclusivo concedido en virtud de la ley, que sirve para diferenciar las mercancías de una empresa de las mercancías de otra empresa".

Entre sus principales características están asegurar:

- Al producto un carácter distintivo: esta distinción o carácter distintivo deriva de la esencia de la marca, según la definición expresada.
- La protección del producto a partir de la empresa: la marca protege al titular contra sus competidores, al igual que al público contra los "usurpadores potenciales".
- Una garantía de calidad; además, la calidad del producto lo califica intrínsecamente, pues lo que el comprador busca al adquirir un producto es una calidad determinada, sin que le sea necesario conocer la empresa que lo produce, lo cual reviste un carácter secundario.
- Una indicación de origen, en tanto permite identificar el producto con la empresa.
- Una publicidad. ¿Es necesario señalar el carácter publicitario de las marcas?

Patentes

Entre el llamado derecho de la propiedad industrial resalta la figura de las patentes, surgida a raíz de la Revolución industrial y, por ende, más reciente que las ya analizadas. Se considera que es uno de los métodos más apropiados para resolver el problema.

Toda invención, para ser susceptible de atribuirle una patente, requiere denotar una novedad, actividad inventiva, así como una aplicación industrial. De estos elementos, los dos primeros revisten mayor grado de dificultad en función de la complejidad del llamado *estado de la técnica*, con base en la existencia o no de antecedentes, así como que dicha invención resulte o no evidente.

En el caso de los programas de cómputo se discute en torno a esas anterioridades y evidencia en los términos de que no presentan caracteres suficientes para atribuirles una patente. Algunos autores (y aun plasmado en los ámbitos legislativo y jurisprudencial) consideran que dicha figura no es aplicable, mientras que otros opinan lo contrario, al adquirir fuerza nuevamente esta figura legal, según se aprecia en líneas posteriores.

Propiedad literaria y artística (derechos de autor)

Sin lugar a dudas, el derecho a la propiedad literaria y artística y de manera más específica los *copyright* o derechos de autor se presentan como la figura más aparentemente aplicable frente al problema de la protección de los programas. Si bien los criterios de selección del género, de la forma de expresión, del mérito, la destinación y aun el principio de exclusión de las ideas a proteger no representan mucha dificultad, la situación no es la misma en lo concerniente al principio de la originalidad. Ésta, distinta de la novedad en las patentes en cuanto que una se aprecia en atención a un criterio subjetivo y la otra con base en un criterio objetivo, hace pensar que la mencionada originalidad podría sustentarse en la existencia de un esfuerzo intelectual personalizado por el creador del programa que permite diferenciarlo de entre los demás creadores y programas, aun si éstos están dedicados a la resolución de un mismo problema.

Los autores que han coincidido en aceptar (incluso secundados por disposiciones legislativas y judiciales) a los derechos de autor como la figura más aplicable frente al problema son varios: con todo, se considera que algunas prerrogativas (como el término de duración de los derechos, el ejercicio de los derechos de exposición, la representación pública, la divulgación, el retiro de obra, etc.) no encuentran un acomodo acorde con la naturaleza de los programas de cómputo, provocando que el convencimiento no pueda manifestarse en forma plena.

Situación internacional

a) Situación actual en la Unión Europea

La polémica acerca de las patentes de los programas de computación ha llegado de nuevo al seno de la Unión Europea. Después de meses de discusión, la Dirección General para el Mercado Interno de la Comisión Europea ha publicado su propuesta de directiva europea sobre este asunto, que propone la admisión de las patentes relacionadas con programas informáticos. Dicha propuesta invita a los países miembros de la Unión Europea a armonizar las legislaciones sobre patentes de inventos que requieran un programa informático, con el fin de establecer "un marco jurídico claro y uniforme" en la Unión Europea.

Según la organización Eurolinux, la propuesta de la comisión ignora informes realizados en Francia y Alemania que muestran el efecto negativo de las patentes de software sobre la innovación; además, aseguran que la directiva permite patentar "programas producto". Esto supone de hecho patentar técnicas innovadoras que se implementen con software, incluidos los métodos de negocio.

Tras la consulta efectuada en torno al Libro Verde de 1997 que concierne a la patente comunitaria y el sistema de patentes en Europa, la patentabilidad de las invenciones implementadas en computadora fue uno de los temas declarados prioritarios al inicio de 1999 para que la Comisión Europea adoptase medidas con rapidez. Se consideró que una directiva que armonizara las legislaciones de los Estados miembros sobre esta cuestión eliminaría la ambigüedad y la falta de seguridad jurídica que existen en la actualidad. Por otro lado, se estableció que, simultáneamente con esta acción a nivel comunitario, los Estados contratantes del CPE deberían adoptar las medidas necesarias para modificar la letra *c*) del apartado 2 del artículo 52 del Convenio de Munich, con el fin de suprimir la referencia a los programas de computadora en la lista de invenciones no patentables.

Con base en estudios recientes, se ha llegado a la conclusión de que la patentabilidad de las invenciones relacionadas con programas informáticos ha contribuido al crecimiento de las industrias relacionadas con este ámbito en Estados Unidos, y en particular al de las Pequeñas y Medianas Empresas (PYME) y los creadores de programas informáticos independientes, que se han convertido en empresas importantes. También en Europa los creadores de programas informáticos independientes utilizan cada vez más, aunque en niveles relativamente bajos, las patentes para obtener financiación o conceder licencias. La legislación sobre derechos de autor ha sido la fuente principal de protección que ha permitido el desarrollo de la industria del software.

En la Directiva 91/250/CEE se incluyen preceptos específicos (artículos 5 y 6) que establecen que no se violan los derechos de autor en un programa informático si se realizan actos en determinadas circunstancias que, de otra forma, supondrían una transgresión de éstos. Dichas excepciones incluyen los actos efectuados para estudiar las ideas y los principios implícitos en el programa y la reproducción o traducción del código, siempre que sea indispensable para obtener la información necesaria para la interoperabilidad de un programa creado de forma independiente. Asimismo, se especifica que no podrá impedirse la realización de una copia de seguridad por una persona con derecho a utilizar el programa.

Tales preceptos se justifican y son necesarios en el contexto de la legislación acerca de los derechos de autor, ya que éstos confieren el derecho exclusivo a impedir la realización de copias de una obra protegida. Todos los actos mencionados implican obtener copias y, por tanto, violarían los derechos de autor de la obra si no existieran excepciones. Por otro lado, las legislaciones sobre patentes de los Estados miembros, aunque no están armonizadas totalmente, no se aplican en general a los actos realizados de forma privada y con fines no comerciales, o a los actos efectuados con fines experimentales en relación con el objeto de la invención. Es probable que la realización de una copia de seguridad en el contexto de una explotación autorizada de una patente relativa a un programa de computadora o a la ejecución de un programa tampoco pueda interpretarse como una transgresión de los derechos de autor.

b) La situación jurídica en Estados Unidos y Japón

La diferencia entre Estados Unidos y Europa y entre Estados Unidos y Japón es que en Europa la invención debe aportar una *contribución técnica*. En Japón existe una doctrina que se ha interpretado tradicionalmente de forma similar: la invención debe consistir en una creación muy avanzada de conceptos técnicos mediante la cual se aplique una ley natural. En la Unión Americana, la invención debe situarse simplemente en un ámbito tecnológico y no es necesaria una contribución técnica. El mero hecho de que la invención utilice una computadora o un programa informático la convierte en parte de la tecnología si proporciona también un "resultado tangible, útil y concreto". El hecho de que en el vecino país del norte no se exija que la invención aporte una contribución técnica significa que apenas existen restricciones a la solicitud de una patente de métodos comerciales (aparte de las exigencias de novedad y actividad inventiva).

Cabe agregar, finalmente, que a raíz de la resolución del tribunal federal estadounidense de apelación, del 23 de julio de 1998, en el

caso *State Street Bank & Trust Co. vs. Signature Financial Group, Inc.*, 149 F.3d 1368, las solicitudes de patentes para métodos destinados al ejercicio de actividades económicas han aumentado en forma vertiginosa.

Situación nacional

México ha alcanzado, sin duda alguna, un grado de desarrollo muy prometedor en la industria de programación, lo cual, evidentemente, ha motivado la aparición de considerables controversias en relación con la propiedad de los programas. La *Ley Federal de Propiedad Industrial* no considera invenciones a los programas de cómputo y, por tanto, no son susceptibles de obtener los beneficios de una patente.

Por otro lado, la *Ley Federal del Derecho de Autor* de diciembre de 1996 contiene un capítulo, que incluye los artículos 101 a 114, que regulan en forma específica la protección de los programas y las bases de datos, mediante la obtención de un certificado autoral, expedido por el Instituto Nacional del Derecho de Autor (INDA).

Tendencias actuales de protección

En el largo debate (más de 30 años) en torno al problema de la protección jurídica de los programas, algunos autores opinan que, debido a la complejidad de los programas y a una necesaria regulación bajo las consideraciones de una "reserva privativa", ésta puede ocurrir, tomando los elementos más significativos de las instituciones jurídicas expresadas (en especial en materia de patentes y derechos de autor), a fin de integrarlos en una estructura nueva y específica que constituya un derecho *sui generis* o particular acorde con las condiciones específicas de los programas.

En dicha figura se podrían atemperar requisitos tales como la novedad y la originalidad, así como un apoyo con un sistema de registro (depósito) de carácter internacional a fin de que revista una verdadera trascendencia. A este respecto, son interesantes las apreciaciones formuladas por los comités de expertos de la Organización Mundial de la Propiedad Intelectual (OMPI) en torno al problema, lo cual incluso ha dado lugar a la formulación de las llamadas disposiciones tipo para la protección del soporte lógico.

Sin embargo, cabe hacer notar que el problema puede percibirse de diferente manera, lo cual depende del contexto; por tanto, la solución no puede ser la misma.

La protección por medio de patente y los derechos de autor son aspectos complementarios. Una *patente* protege una invención, dentro de

los límites de las reivindicaciones, que determinan el alcance de la protección concedida. De esta forma, el titular de una patente por una invención implementada en computadora tiene derecho a impedir la utilización por terceros de cualquier programa informático que aplique su invención (tal como se defina en las reivindicaciones). Este principio es aplicable a pesar de que puede haber diversas vías para conseguirlo, utilizando programas cuyos códigos fuente o códigos objeto sean diferentes y de que puedan protegerse a la vez con derechos de autor independientes que no se infrinjan de forma mutua.

Por otro lado, de conformidad con la Directiva 91/250/CEE acerca de la protección jurídica de programas de computadora, sólo se protege mediante *derechos de autor* la expresión del programa de computadora, mientras que las ideas y principios implícitos en los elementos del programa, incluidos los de sus interfaces, no pueden acogerse a aquéllos. El programa de computadora estará protegido si es original en el sentido de que sea una creación intelectual de su autor. En la práctica, esto significa que los derechos de autor seguirán existiendo en cualquier expresión del código fuente o del código objeto de un programa, pero no en las ideas y principios implícitos del código fuente o del código objeto de dicho programa. Los derechos de autor prohíben la copia sustancial del código fuente o del código objeto, pero no impiden las múltiples vías alternativas para expresar las mismas ideas y principios en distintos códigos fuente o códigos objeto.

Asimismo, tampoco protegen contra el desarrollo de un programa idéntico o básicamente idéntico sin el conocimiento de unos derechos de autor existentes. En consecuencia, la protección jurídica puede existir de forma complementaria respecto al mismo programa mediante la legislación tanto sobre patentes como sobre derechos autor. La protección puede ser acumulativa en el sentido de que un acto que implica la explotación de un programa determinado puede vulnerar a la vez los derechos de autor del código del programa y una patente cuyas reivindicaciones incluyan las ideas y principios implícitos.

Informe global de piratería de programas de cómputo

Según el estudio anual concerniente a piratería de software global, elaborado por la Bussiness Software Alliance (BSA) y la International Data Corporation (IDC), se percibe que la piratería de programas de cómputo sigue planteando desafíos a la industria y a la economía global.

A continuación se muestra la lista de los mayores y menores, según dicho estudio:[1]

TABLA 1 Piratería de software en 2007

Alta piratería		Baja piratería	
País	**2007**	**País**	**2007**
Armenia	93%	Estados Unidos	20%
Bangladesh	92%	Luxemburgo	21%
Azerbaiyán	92%	Nueva Zelanda	22%
Moldova	92%	Japón	23%
Zimbabue	91%	Austria	25%
Sri Lanka	90%	Bélgica	25%
Yemen	89%	Dinamarca	25%
Libia	88%	Finlandia	25%
Venezuela	87%	Suecia	25%
Vietnam	85%	Suiza	25%
Iraq	85%	Reino Unido	26%
Indonesia	84%	Alemania	27%
Pakistán	84%	Australia	28%
Algeria	84%	Países Bajos	28%
Camerún	84%	Noruega	29%
Montenegro	83%	Israel	32%
Ucrania	83%	Canadá	33%
China	82%	Sudáfrica	34%
Bolivia	82%	Irlanda	34%
Paraguay	82%	UAE	35%
Botsuana	82%	Singapur	37%
Nigeria	82%	República Checa	39%
Zambia	82%	Taiwán	40%
El Salvador	81%	Reunión	40%
Costa Ivory	81%	Hungría	42%
Kenia	81%	Francia	42%

[1] Estudio elaborado por Bussiness Software Alliance (BSA) y la International Data Corporation (IDC), *Estudio global sobre piratería de software*, disponible en línea http://global.bsa.org/idcglobalstudy2007/studies/2007_global_piracy_study.pdf, [formato pdf], 16 páginas, consultado en mayo de 2008.

TABLA 2 Pérdidas durante 2007 por piratería en software

Países con 250 millones de dólares o más en pérdidas			
País	**2007 ($M)**	**País**	**2007($M)**
Estados Unidos	8 040	Polonia	580
China	6 664	Corea del Sur	549
Rusia	4 123	Países Bajos	502
Francia	2 601	Australia	492
India	2 025	Tailandia	468
Alemania	1 937	Venezuela	464
Reino Unido	1 837	Indonesia	411
Japón	1 791	Ucrania	403
Italia	1 779	Argentina	370
Brasil	1 617	Turquía	365
Canadá	1 071	Suecia	324
España	903	Malasia	311
México	836	Suiza	303
		Sudáfrica	284

TABLA 3 Porcentajes anuales de piratería en América Latina

América Latina	2007	2006	2005	2004	2003
Argentina	74%	75%	77%	75%	71%
Bolivia	82%	82%	83%	80%	78%
Brasil	59%	60%	64%	64%	61%
Chile	66%	68%	66%	64%	63%
Colombia	58%	59%	57%	55%	53%
Costa Rica	61%	64%	66%	67%	68%
República Dominicana	79%	79%	77%	77%	76%
Ecuador	66%	67%	69%	70%	68%
El Salvador	81%	82%	81%	80%	79%
Guatemala	80%	81%	81%	78%	77%
Honduras	74%	75%	75%	75%	73%
México	61%	63%	65%	65%	63%
Nicaragua	80%	80%	80%	80%	79%
Panamá	74%	74%	71%	70%	69%
Paraguay	82%	82%	83%	83%	83%

TABLA 3 Porcentajes anuales de piratería en América Latina

América Latina	2007	2006	2005	2004	2003
Perú	71%	71%	73%	73%	68%
Uruguay	69%	70%	70%	71%	67%
Venezuela	87%	86%	82%	79%	72%
Otros	83%	83%	82%	79%	81%
TOTAL AL	65%	66%	68%	66%	63%

Fuente: Estudio anual 2008 de piratería de software BSA-IDC.

Puntos finales importantes por considerar

a) La realización del mercado interior implica eliminar las restricciones a la libre circulación y las distorsiones de la competencia, así como crear un entorno que sea favorable a la innovación y a las inversiones. En este contexto, la protección de las invenciones por medio de patentes constituye un elemento esencial para que haya éxito en el mercado interior. Una protección efectiva y armonizada de las invenciones implementadas en computadora en los Estados miembros es básica para mantener y fomentar las inversiones en este ámbito.

b) Existen diferencias en la protección de las invenciones implementadas en computadora que otorgan las prácticas administrativas y la jurisprudencia de los Estados miembros. Tales diferencias podrían crear obstáculos al comercio e impedir así el correcto funcionamiento del mercado interior.

c) Esas disparidades se han desarrollado y podrían incrementarse a medida que los Estados miembros adopten nuevas leyes y prácticas administrativas diferentes y que sus interpretaciones jurisprudenciales nacionales se desarrollen de manera diversa.

d) El incremento constante de la difusión y uso de programas de computadora en todos los ámbitos de la tecnología y de su difusión mundial a través de internet constituye un factor crucial de la innovación tecnológica. Así, es necesario garantizar la existencia de un entorno óptimo para los creadores y usuarios de programas informáticos en la comunidad.

e) Las normas jurídicas, según se interpretan en los órganos jurisdiccionales de los Estados miembros, deberían armonizarse y la legislación relacionada con la patentabilidad de las invenciones implementadas en computadora debería ser más transparente. La seguridad jurídica resultante permitirá a las empresas obtener el máximo beneficio de las patentes para las invenciones implementadas en computadora e impulsará la inversión y la innovación.

f) Con arreglo al Convenio sobre la Concesión de Patentes Europeas, firmado en Munich el 5 de octubre de 1973, y las legislaciones sobre patentes de los Estados miembros, no se consideran invenciones y, por tanto, quedan excluidos de la patentabilidad los programas de computadoras, así como los descubrimientos, las teorías científicas, los métodos matemáticos, las creaciones estéticas, los planes, principios y métodos para el ejercicio de actividades intelectuales, para juegos o para actividades económicas, y las formas de presentar informaciones. No obstante, esta excepción se aplica y se justifica sólo en la medida en que la solicitud de patente o la patente se refiera a uno de esos elementos o actividades considerados tales, porque dichos elementos y actividades no pertenecen al campo de la tecnología.

g) De conformidad con la Directiva 91/250/CEE del Consejo, de 14 de mayo de 1991, sobre la protección jurídica de los programas de computadora, cualquier forma de expresión de un programa de computadora original estará protegida por los derechos de autor como obra literaria. No obstante, las ideas y los principios en que se basa cualquiera de los elementos de un programa de computadora no están protegidos por los derechos de autor.

h) Aunque se considera que las invenciones implementadas en computadora pertenecen a un campo de la tecnología, para que entrañen una actividad inventiva, como las invenciones en general, deberán aportar una contribución técnica al estado de la técnica. En consecuencia, si una invención no aporta una contribución técnica al estado de la técnica (por ejemplo, si su contribución específica careciera de carácter técnico), la invención no implicará actividad inventiva, ni podrá ser patentable.

PROTECCIÓN JURÍDICA DE LOS NOMBRES DOMINIO[2]

Generalidades

La historia del sistema de nombres de dominio, DNS (Domain Name System), se remonta a la década de los setenta, cuando cada una de las computadoras conectadas a la red tenía asignada una dirección numérica (de la misma forma que los teléfonos actuales tienen asignado un número telefónico). Para accesar a dichos equipos de cómputo era necesario recordar la dirección numérica de cada uno, ya que el esquema de nombramiento en aquel tiempo era bastante limitado.

[2] Basado en el artículo del M. en C. Óscar Robles, miembro mexicano del ICANN, *¿Qué es el DNS? Aparecido en el Boletín del INEGI*, núm. 1, año 2003, disponible [en línea] http://www.inegi.gob.mx/informática/español/servicios/boletín/2003/bpil-03/nicdns.html.

El DNS, diseñado por Paul Mockapetris, buscaba un objetivo muy simple —desempeñar una función técnica de traducción de nombres de equipos de cómputo a su dirección numérica correspondiente— que fuera conveniente, amigable y fácil de utilizar por los usuarios de internet, es decir, proveer un esquema de interpretación entre los usuarios y las computadoras, sin que los primeros tuvieran la necesidad de recordar las direcciones numéricas de cada uno de los equipos a los que intentaban comunicarse, por ejemplo: 131.178.11.16 o 200.23.1.7, en vez de *www.mty.itesm.mx* y *www.nic.mx*, respectivamente.

La realidad es que este esquema, el DNS, cumplió con su intención y, más que eso, los nombres de dominio no sólo fueron para los usuarios una manera fácil de conectarse a los equipos en la red, sino que además significó una manera simple de representar ideas, productos, servicios, empresas, organismos, etc. El fenómeno del WWW le aplicó una aceleración importante al registro de dominios y pronto vendrían los problemas. A partir de este punto, fue imposible dar marcha atrás a un esquema de nombramiento que empezó por ser técnico y, gracias a la comercialización de internet, acabó generando conflictos con esquemas sociales definidos anteriormente.

Diferentes tipos de TLD (Top Level Domain)

a) Genéricos conocidos como GTLD (Generic Top Level Domain)

Entre los más importantes están los siguientes: .aero, .biz, .com, .coop, .edu, .gov, .info, .int, .mil, .museum, .name, .net, .org y .pro

b) Códigos de país conocidos como CCTLD (Country Code Top Level Domain)

Algunos de los más importantes son los que siguen: .ar–Argentina; .at–Austria; .au–Australia; .be–Bélgica; .bg–Bulgaria; .bo–Bolivia; .br–Brasil; .ca–Canadá; .ch–Suiza; .cl–Chile; .cn–China; .co–Colombia; .cr–Costa Rica; .cu–Cuba; .de–Alemania; .dk–Dinamarca; .ec– Ecuador; .es–España; .fr–Francia; .gt–Guatemala; .hn–Honduras; .il–Israel; .it–Italia; .jp–Japón; .lu–Luxemburgo; .mx–México; .ni–Nicaragua; .nl–Holanda; .no–Noruega; .pa–Panamá; .pe–Perú; .ru–Federación Rusa; .uk–Reino Unido; .us–Estados Unidos; .uy–Uruguay y .ve–Venezuela.

Registro de los nombres dominio

La administración de los GTLD fue un trabajo inicialmente académico, realizado por el Instituto de Investigación de Stanford en Menlo Park (SRI) y conocido como SRI-NIC. Este instituto mantuvo el registro de dominios

bajo los GTLD, con el auspicio del Departamento de Defensa de Estados Unidos, desde mediados de la década de 1980 hasta principios de la de 1990, cuando la National Science Foundation (NSF), del Departamento de Educación, tomó esta responsabilidad, y en marzo de 1992 realizó una licitación para asignar la función del registro de nombres de dominio bajo los GTLD.

El 1 de enero de 1993, tres empresas tenían una parte de la administración del los GTLD, función que luego sería conocida como Internic. La empresa NSI (Network Solutions Inc.) proporcionaba los servicios de registro, AT&T los servicios de directorio y Global Atomics los servicios de educación y capacitación; estas tres actividades serían subsidiadas por la NSF y serían gratuitas para los usuarios.

Actualmente, los registros se realizan en la mayoría de los países por medio de su respectivo NIC (Network Information Center). Este nombre es una herencia del SRI-NIC (Stanford Research Institute Network Information Center), el cual en la década de 1980 desempeñaba funciones de administración y supervisión de algunos recursos de internet (en aquella época Arpanet y NSFNET). Más tarde surgió Internic, que INTERNIC administraba los nombres de dominio genéricos y las direcciones de IP (esto último hasta 1997). Al mismo tiempo existieron las conexiones de otros países a internet, con lo cual era necesario establecer un NIC para cada país.

Así, a finales de 1998 se funda en el estado de California la Internet Corporation for Assigned Names and Numbers (ICANN), organización sin fines de lucro que busca supervisar el funcionamiento técnico de internet con una estructura que representa los intereses de la comunidad de la red, geográfica y técnicamente. Además de este organismo, está la IANA (Internet Assigned Numbers Authority), encargada de atribuir los códigos numéricos a las direcciones electrónicas.

Conflictos entre nombres de dominio idénticos o similares a marcas

Uno de los primeros casos de disputa legal por nombres dominio sustentados en una marca, y quizá el más conocido en su tiempo, fue el del nombre de dominio mcdonalds.com, registrado por el estadounidense Joshua Quittner, con la intención de probar que el sistema de resolución de controversias era inadecuado. Al enterarse de esto, la cadena de restaurantes McDonald's inició un proceso de disputa por la titularidad del nombre de dominio, objetivo que no consiguió con el proceso de resolución de disputas y tuvo que pagar por este dominio a Quittner, quien decidió donar lo recaudado a una institución de beneficencia una vez conseguido su objetivo.

Diferencias fundamentales entre el DNS y el sistema marcario

Nombres de dominio	Marcas
Un nombre de dominio sólo puede tener caracteres numéricos, letras del alfabeto inglés y el guión medio	Una marca puede tener cualquier carácter representable en el alfabeto oficial del país
Los nombres de dominio (todos) son alcanzables o visibles desde cualquier punto en internet, sin importar si son GTLD, CCTLD, abiertos o restringidos	Las marcas están sujetas a una territorialidad, y la marca tiene protección sólo en el país que se registra
La administración de los dominios en el mundo la hacen en 95% instituciones privadas (Cuba, Argentina y otros países son administrados por el gobierno)	La gestión de marcas la hace algún organismo público
El registro de un dominio cuesta en promedio entre 20 y 50 dólares anuales	El registro de una marca en México cuesta 125 dólares por 10 años
Existen 26 millones de nombres dominio ubicados bajo los GTLD y 14 millones bajo las restantes 244 CCTLD	
Debajo de cada TLD puede haber un número indefinido de SLD o subclasificaciones	La clasificación marcaria utiliza 42 códigos
No puede haber dos nombres de dominio idénticos con la misma clasificación	Pueden coexistir nombres de marcas idénticos en la misma clasificación
El criterio de identidad entre dos nombres es estrictamente matemático, comparación letra por letra	El criterio de identidad incluye el concepto de similitud en grado de confusión
La mayoría de los registros de dominios con algún TLD tarda sólo unos minutos	El registro de marcas tarda meses

Paralelamente a lo anterior, se solicita a la Organización Mundial de la Propiedad Intelectual (OMPI) iniciar un procedimiento transparente y balanceado que incluya a todos los grupos de interés relacionados con el registro de dominios para:

a) Desarrollar recomendaciones uniformes destinadas a resolver disputas entre nombres de dominio y marcas registradas.
b) Recomendar un procedimiento para proteger las marcas famosas.
c) Evaluar los efectos para incluir nuevos nombres de dominio genéricos que compitan con .com, .net, .org.
d) Crear la UDRP (Política Uniforme de Resolución de Disputas).

De esta forma, la OMPI inició la primera ronda de consulta sobre nombres de dominio y marcas, en la cual se buscó dar solución a esos tres puntos.

Durante dicho proceso se evaluaron alternativas tanto de prevención como de solución de controversias. Se encontró que establecer un mecanismo de prevención basado en la prohibición del registro de marcas (idénticas o similares en grado de confusión) representaba un trabajo excesivo y que obtendría pocos resultados, sobre todo al considerar lo siguiente:

1. Que el proceso de registro de dominios requiere una respuesta inmediata y que el examen del nombre implica mayores recursos: tiempo y personal (para aplicar un examen similar al registro de marcas y obtener documentación que acredite la titularidad de marcas, representación legal, etcétera).
2. Que hasta la fecha se han presentado casi 4 000 disputas, de casi 40 millones de nombres de dominio bajo los GTLD. Esto indica que sólo 0.01% de dominios presenta una controversia. Aplicar un esquema de prevención perjudicaría a 99.99% de dominios registrados legítimamente.
3. Que el registro de nombres de dominio es un recurso técnico y como tal no representa violación alguna a leyes o reglamentos; el uso de estos nombres podría implicar una falta, pero hasta entonces.

Cuando la OMPI finalizó su trabajo con el informe final, éste fue sometido a estudio de la corporación recién establecida, ICANN. En octubre de 1999, el Consejo Directivo de ICANN aprobó la aplicación de la Política Uniforme de Resolución de Disputas (UDRP) para los dominios registrados bajo los GTLD. Esta política ataca la problemática inicial entre nombres de dominio y marcas registradas, pero sobre todo busca resolver las disputas por la mala fe en el registro y uso del nombre de dominio.

El procedimiento es similar a un arbitraje, desde la perspectiva de que el panelista lleva el caso y emite su resolución atingente; empero, el procedimiento no es considerado un arbitraje formal. Hay tres tipos de resoluciones: cancelar el nombre de dominio en cuestión, transferirlo al solicitante o suspender el procedimiento de resolución sin perjuicio para las partes. El proceso completo tarda entre 45 y 70 días, lo cual representa uno de los mayores beneficios para quien utiliza este procedimiento.

Particularidades

El Registro de Nombres de Dominio bajo el CCTLD .MX es administrado por el Centro de Servicios de Información y Registro en Internet,

NIC-México, del Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Monterrey por delegación de IANA (Internet Assigned Names and Numbers) e ICANN (Internet Corporation for Assigned Names and Numbers), de acuerdo con los principios contenidos en el documento RFC_1591. El arbitraje, la mediación y la conciliación son la expresión concreta de la autonomía de la voluntad de dos sujetos o partes que deciden que sus conflictos sean resueltos por un tercero a fin de minimizar los efectos negativos de un litigio actual o potencial. El laudo arbitral tiene el mismo valor que una sentencia dictada en la vía judicial, pero los tribunales de arbitraje no tienen ningún poder para ejecutarlos. Los laudos son mayoritariamente aceptados por el vencido como una confirmación del empeño de las partes en resolver sus conflictos de intereses de una manera austera y definitiva.[3]

Cuando el laudo no es aceptado y pretende ser incumplido por alguna de las partes, intervienen varias instituciones judiciales de reconocimiento y ejecución forzosa que legitiman la institución arbitral y ponen al laudo en un nivel procesal más favorable, incluso, que una sentencia judicial. Estas instituciones son las de convenios internacionales y las normas locales de reconocimiento y ejecución de laudos.

[3] Por ejemplo, en el Tribunal Arbitral de la Cámara de Comercio Internacional (CCI), en el que el nivel de aceptación voluntaria supera 90%.

VII. Contratos informáticos: riesgos y seguros

GENERALIDADES

La incontenible progresión del fenómeno informático en el entorno social ha propiciado, entre otras cosas, una ascendente comercialización de los bienes y servicios derivados de dicha tecnología, regulados mediante figuras jurídicas recientes como los llamados *contratos informáticos*. Este tipo de contratos, emanados esencialmente del derecho civil contractual, revisten una serie de caracteres específicos muy marcados que dificultan su adecuada negociación en la práctica. Así, esta nueva categoría contractual (tanto en lo técnico como en lo jurídico) amerita un tratamiento pormenorizado, sobre todo en cuanto a las diversas implicaciones hasta hoy desconocidas o conocidas de manera parcialmente tradicional, a fin de contemplar un régimen jurídico efectivamente aplicable.

Por otra parte, también aunados a este género de contratos existe otra serie de aspectos muy acentuados generadores de enormes pérdidas económicas, como son los denominados *riesgos informáticos*, los cuales se vinculan de forma directa a la incertidumbre existente debido a las consecuencias de la posible realización de hechos y actos relacionados con los bienes y servicios informáticos. Dicha problemática (seria y trascendente) justifica un estudio particular a la luz de las medidas preventivas y correctivas inherentes a dichas contingencias por medio de figuras jurídicas acordes con sus matices, como los *seguros informáticos*, ambos rubros englobados en la cada vez más importante área de la seguridad informática.

ANTECEDENTES Y EVOLUCIÓN

Los contratos informáticos surgen ligados a la inminente comercialización de las computadoras. En un principio, éstas se empleaban, según hemos

dicho, en el ámbito científico y militar y después fueron incorporadas al ámbito de los negocios, lo cual originó su rápida comercialización y, por ende, la proliferación de contratos en materia informática, cuya redacción significó una notoria diferencia respecto a lo que podríamos considerar contratos *clásicos* en función de su alta tecnicidad.

En un principio, este tipo de contratos se englobaba en uno solo, lo que provocaba ambigüedad en ellos, pero favorecía la práctica comercial de monopolios en detrimento de la libre concurrencia de los mercados, lo cual incluso generó el seguimiento de un juicio antimonopólico en contra de la compañía IBM con el amparo de las leyes Sherman y Clayton.

Todo lo anterior dio como resultado una diversificación contractual conocida con el anglicismo *unbundling*, consistente en hacer una contratación por separado en referencia a los bienes y servicios informáticos, lo cual trajo como consecuencia la creación de mercados muy diversos; así, surgieron empresas especializadas en cada una de las vertientes informáticas, tanto en la construcción y venta de equipos como en la prestación de servicios como mantenimiento, programación, asistencia técnica, etc. Lo cierto es que dichos contratos han evolucionado paralelamente con el avance tecnológico, mas no a la par del derecho.

PRINCIPALES IMPLICACIONES

Entre las principales implicaciones producidas por tales contratos está el notorio desequilibrio entre las partes causado por el mayor y mejor conocimiento de los elementos fundamentalmente técnicos concernientes al proveedor, aparejado esto a la situación desfavorable de los usuarios, quienes en general se ven obligados a aceptar las condiciones contractuales (cláusulas) impuestas por el proveedor, en razón de sus necesidades de informatización.

Dicha problemática se acentúa por las ambiciones desmedidas de los proveedores, quienes, para rentar o vender equipos y/o programas o prestar servicios, en muchas ocasiones crean necesidades u ofrecen bienes o servicios que en realidad no corresponden a lo requerido.

Para evitar este tipo de situaciones (desequilibrio, alta tecnicidad, oscuridad de las cláusulas, etc.) es conveniente que el usuario se interiorice en los aspectos técnicos elementales apoyándose de preferencia en la opinión de expertos a fin de percibir de manera más adecuada las eventuales implicaciones en dichos contratos.

Por otra parte, la redacción debe estar en términos jurídicos y técnicos debidamente precisados (castellanización, citas de artículos, inclusión de glosarios y anexos, etc.) a efecto de evitar malentendidos y dar más claridad a la relación contractual.

CLASIFICACIÓN DE LOS BIENES, SUMINISTROS, PROGRAMAS Y SERVICIOS INFORMÁTICOS

Según Davara Rodríguez,[1] se consideran bienes informáticos "todos aquellos elementos que forman el sistema —computadora— en cuanto al hardware, ya sea la unidad central de procesamiento —CPU— o sus periféricos, y todos los equipos que tienen una relación directa de uso respecto a ellos y que, en su conjunto, conforman el soporte físico del elemento informático, así como los bienes inmateriales que proporcionan las órdenes, datos, procedimientos e instrucciones, en el tratamiento automático de la información y que, en su conjunto, constituyen el soporte lógico del elemento informático".

Bienes informáticos

El equipo informático está integrado por lo siguiente:

a) *Unidad central de procesamiento*: unidad de memoria (memoria principal y extensión de memoria), unidad aritmética y lógica, unidad de entrada/salida (canal multiplexor, selector, multiplexor de bloques, concentradores, etc.), unidad de control, consola de operación, dispositivos especiales, reloj de tiempo real y de tiempo encendido.

b) *Unidades periféricas*: dispositivos magnéticos (diferentes unidades de disco, de cinta magnética, de tarjetas magnéticas y lectora de tarjetas), dispositivos no magnéticos (lectora de tarjetas, de marcas, de cinta de papel, distintos tipos de impresoras (matriz de puntos, térmicas, inyección de tinta, de monoelemento, de impacto y láser), digitalizadores, convertidores analógicos/digitales, clasificadores de tarjetas, simuladores y adaptadores, estaciones de trabajo, unidades de distribución e incremento de potencia, convertidores de modelos, controlador de entrada/salida, canales de alta, media y baja velocidad), dispositivos de emisión/recepción, terminales de video inteligentes, de entrada/salida, de consulta, de transmisión remota de entrada/salida, de despliegue visual (programable y no programable), terminales portátiles, modulares, demodulares (sincrónicos y asincrónicos), multiplexores (de tiempo, sincrónicos y asincrónicos), multiplexores de carga

[1] Davara Rodríguez, Miguel Ángel, *Derecho informático* Aranzadi [en línea] en http://www.colex-data.es

(sincrónicos y asincrónicos), interfaces (sincrónicas y asincrónicas) y controladores de comunicaciones.

c) *Equipo de transmisión de datos*: *módems* (sincrónicos y asincrónicos), concentradores, multiplicadores (digitales y analógicos), interruptores (digitales y analógicos), líneas de comunicación y eliminadores de ruido, dispositivos de redes (infrarrojo, wifi, bluetooth, etcétera).

d) *Equipo de telecomunicaciones*: teléfono, microondas, terminales remotas y satélites.

Suministros informáticos

a) *Suministros para registro de información*: formas continuas (papel sensible para impresión térmica, de impresión común, papel y formas especiales, papel para impresión de rayos láser, papel para impresión sin papel carbón), formas no continuas (papel y formas especiales para uso manual o mecanizado, suministro de papel perforado, paquetes de discos magnéticos, cartucho de cinta magnética), suministros de micropelícula (fichas).

b) *Suministros de abastecimiento del equipo*: cintas de control de avance de papel, cinta para impresoras de inyección y cinta para marcas magnéticas, tinta para impresoras de inyección.

c) *Suministros auxiliares del equipo*: líquido limpiador de unidades de cinta y discos magnéticos y para graficadores electrostáticos, cortador, teclado, monitor, etc., otros elementos de limpieza (como gasas y alfombras antiestáticas), aire comprimido, etcétera.

d) *Suministros auxiliares para tareas de programación*: carpetas de archivos de programas, de documentación, para formas continuas, reglas especiales de diagramación, formas especiales de codificación, etcétera.

e) Refacciones, partes y accesorios, plumas para graficadores, etcétera.

Servicios informáticos

Según Davara Rodríguez,[2] por servicios informáticos se entienden "todos aquellos que sirven de apoyo y complemento a la actividad informática en una relación de afinidad directa con ella".

[2] *Idem*.

Tipos de contratos referidos a servicios informáticos

a) *Relacionados con recursos humanos*: servicios de reclutamiento y selección, de evaluación y diagnóstico, de capacitación, de entrenamiento y desarrollo de recursos humanos mediante cursos específicos en la materia (captura de datos a nivel técnico, control de datos, operación de equipos, programación, análisis, alta gerencia e informática para ejecutivos, sistemas de información, bancos de datos, comunicaciones, teleproceso, auditoría y seguridad en informática, proceso distribuido, proceso de palabras, administración de centros de cómputo, preparación de estudios de viabilidad para la adquisición de bienes y servicios informáticos) y servicios de localización de personas por medio de radio para atención de emergencia.

b) *De consultoría general*, de planeación, de diseño, de programación, de desarrollo, de implantación y de mantenimiento de sistemas.

c) *De planeación de locales e instalación de equipo de cómputo y auxiliares*: servicio de consultoría en la instalación del equipo de cómputo, servicio de consultoría en la planeación y diseño del centro de cómputo (del edificio y de la sala de cómputo, local e instalación del equipo auxiliar y de apoyo).

d) *De uso de equipos de cómputo por tiempo limitado*: de cómputo de tiempo compartido, de transmisión de datos, y de limpieza y certificación de cintas.

e) *De explotación de programas bajo licencia de uso con o sin cargo*: programas para aplicaciones específicas, de utilería, apoyos auxiliares y complementarios, compiladores, traductores, intérpretes, sistemas operativos, programas utilizados en la conversión de un equipo a otro, paquete del sistema de información integrados. De aplicación científica, de administración de bancos de datos y de control de la productividad y eficiencia de sistemas computarizados.

f) *De consulta de archivos y de banco de datos nacionales e internacionales.*

g) *De estudios de mercadotecnia en informática.*

h) *De documentación técnica en informática*: de consulta de revistas y publicaciones, de preparación de la documentación técnica de los sistemas de información bibliográfica automatizada.

i) *De mantenimiento preventivo, correctivo y de conservación de equipo informático*: de medios magnéticos de equipo de cómputo, de equipo de proceso de palabras, de equipo de redes de teleproceso, de equipo de comunicaciones, y servicios especiales de mantenimiento de equipo informático.

j) *De manejo de datos*: de captura, control y proceso de datos de operación de equipo, de captura de datos, de proceso de datos, de conversión de medios, códigos y formas.

k) *De auditoría y diagnóstico en informática*: auditoría de operación, de sistemas, auditoría administrativa, diagnóstico de relación costo-beneficio de recursos informáticos, diagnóstico de eficiencia y productividad de recursos informáticos.

l) *De desarrollo de estudios de viabilidad para la selección de bienes o servicios informáticos.*

m) *De desarrollo de estudios de factibilidad, inversión y adquisición de bienes y servicios informáticos.*

TELEMÁTICA: UN NUEVO DESARROLLO

La asociación cada vez más estrecha entre las tecnologías de la informática y las telecomunicaciones ha creado aspectos de interés en el análisis de las aplicaciones que ambas tecnologías tienen en la actualidad, fundamentalmente en aquello que se conoce como *redes*.

Esta conjunción informática-telecomunicaciones, comúnmente conocida como *telemática* o *teleinformática*, se encuentra en una etapa de creciente desenvolvimiento, por lo que su importancia como medio de comunicación y herramienta de cálculo y proceso compartido es innegable.

Lo anterior hace que sea imperativo, si se desea una adecuada racionalización de los recursos informáticos, planear su desarrollo armónico, de tal forma que se puedan satisfacer las demandas actuales y potenciales de las dependencias, y coadyuvar a lograr los objetivos económicos y sociales de aquéllos.

El uso intensivo de las redes internacionales de comunicaciones para la transmisión de información, antes o después de su proceso, ha propiciado que su tratamiento no se realice necesariamente en los países donde se origina o donde se utilizan los resultados de tal proceso.

En la actividad, que cada vez adquiere proporciones mayores en cuanto al número de usuarios de centros informáticos ubicados en el extranjero, el valor de los servicios prestados bajo tal modalidad y otros factores, en los últimos años han participado no sólo las empresas prestadoras de servicios o las instituciones públicas o privadas usuarias de ellos, sino también los gobiernos de los países y diversos organismos internacionales involucrados en mayor medida en el análisis de la problemática creada por el uso de redes internacionales de comunicaciones.

En la estructura de los sistemas de redes de teleinformática existen los siguientes componentes vinculados de manera directa con los llamados bienes y servicios informáticos:

- Terminales.
- Concentradores o dispositivos intermedios.

- Transmisión de datos.
- Dispositivos de la red de telecomunicaciones.
- Acopladores o adaptadores de transmisión.
- Software de soporte.

CARACTERES PARTICULARES

Redacción

La existencia de sistemas destinados al tratamiento automatizado de la información es el hecho técnico que fundamenta los llamados *contratos informáticos*, ya que se trata del concepto principal que permite predicar la unidad de la nueva rama frente a la multiplicidad aparente de los fenómenos jurídicos que la integran. La práctica comercial de contratar por separado las prestaciones informáticas no debe hacer perder de vista el enfoque esencial que permite contemplar en su verdadera dimensión a los contratos de bienes y servicios informáticos consistente en tener siempre presente que el objeto de éstos son los sistemas informáticos, subsistemas o elementos en interacción entre sí y con el medio ambiente.

Cuando se contratan por ejemplo bienes informáticos, sea en conjunto o por separado, se debe ser explícito en cuanto a la interacción mencionada, de tal manera que cumplan con la función instrumental para la que fueron diseñados de acuerdo con sus respectivas especificaciones técnicas en el contexto de la finalidad concreta a la cual se destinarán en el sistema informático al que se integrarán como partes componentes.

Por eso cabe afirmar que en la experiencia jurídica, además de la tipicidad legal de algunos contratos como la compraventa, existe también la tipicidad consuetudinaria de los contratos de equipos, soporte lógico, desarrollo de sistemas, etc., ya que se plantea una serie de problemas recurrentes que exigen soluciones repetitivas y adecuadas, es decir, "típicas", que sólo adquieren pleno sentido cuando se les contempla con la perspectiva del sistema informático.

A fin de evitar sorpresas desagradables, los contratos informáticos deben contener en forma explícita y precisa elementos generales como el objeto (creación y transmisión de derechos y obligaciones respecto de los bienes y servicios informáticos), duración y rescisión, precio, facturación y pago, garantías y responsabilidades y disposiciones generales.

Mención especial en este rubro merecen las llamadas *garantías* (obligación inherente a una persona de asegurar a otra el goce de una cosa o derecho, de protegerla contra un daño o de indemnizarla en caso de determinados supuestos). Estas cláusulas señalan la manifestación de compro-

miso sobre todo de los proveedores, aunque en nuestro ámbito contractual, en la mayoría de las ocasiones se trata de cláusulas limitativas de responsabilidad que constituyen verdaderos contratos de adhesión.

Por otra parte, también están las llamadas *responsabilidades*, que determinan el accionar de las garantías, como la obligación de reparar el daño causado al contratante por la falta de ejecución del compromiso adquirido en los contratos informáticos; las responsabilidades más importantes son las referidas a la seguridad material del equipo y aquello concerniente a los daños causados por el material o el personal del proveedor. Lo anterior no exime a los contratantes de convenir otras cosas a manera de disposiciones generales.

Elementos específicos

Es menester que en todo contrato informático sobre bienes y/o servicios se incluyan cláusulas referidas a aspectos tan importantes como las definiciones, control, supervisión y acceso, asistencia y formación, secreto y confidencialidad, además de cláusulas diversas, a saber:

a) *Definiciones*

El ambiente informático en muchas ocasiones se convierte en fuente de ambigüedades en cuanto que su léxico está integrado por numerosos vocablos de orden técnico, a los que comerciantes, juristas y aun los mismos expertos en informática llegan a atribuir contenidos diferentes, lo cual puede traer como consecuencia que los derechos y obligaciones contractuales lleguen a ser diversos de aquellos que las partes pensaron haber suscrito.

Para atenuar dichas eventualidades es conveniente incorporar a los contratos un preámbulo, cláusulas o anexos que precisen o expliquen los términos técnicos fundamentales por medio de definiciones simples, concretas y completas.

b) *Control, supervisión y acceso*

El usuario debe ejercer un estricto control y supervisión en el funcionamiento del equipo informático que adquiera; además, es conveniente un asesoramiento externo de un experto en la materia para que vigile el buen desarrollo de dichas actividades.

Por otra parte, es importante que el usuario dé un buen mantenimiento a su equipo, y si en este proceso intervienen funcionarios del proveedor deberá tener un control discreto sobre ellos a fin de prevenir

una eventual actitud dolosa que pudiera suscitarse, por ejemplo: que los empleados del proveedor pretexten mal funcionamiento del equipo y pretendan hacer creer al usuario una "necesaria" reparación y su consiguiente aumento en el cobro de honorarios o llegando aun al extremo de "robar" los programas creados por el usuario.

c) *Asistencia y formación*

Los contratos de asistencia técnica al usuario de sistemas informáticos son específicos; no obstante, en algunos contratos informáticos se prevé una cláusula especial sobre dicha asistencia técnica, la cual debe ser periódica y oportuna. Este servicio puede ofrecerlo el proveedor o una empresa que se encargue de ello, y queda al usuario la elección según las circunstancias.

En ese sentido, la formación se refiere a la capacitación que el proveedor dé al personal de la empresa del usuario, en especial a quienes se vayan a encargar de manejar el sistema. Es indudable que el éxito que pueda tener la informatización de una empresa radica de manera fundamental en que tenga un buen equipo, eficientes programas de cómputo y personal debidamente capacitado.

d) *Secreto y confidencialidad*

Esto consiste en el carácter confidencial que el proveedor debe dar a la información de su cliente; por el contrario, si realiza o permite su divulgación a un tercero, eventualmente o no competidor, el usuario estará en todo su derecho a demandarlo por la vía civil o en la penal por abuso de confianza. Es esencial que en una empresa informática se sigan estos principios de secrecía y confidencialidad para su buen funcionamiento, seguridad y reputación.

e) *Cláusulas diversas*

Estas cláusulas se refieren a un concepto en especial y las partes convienen en insertarlas en los contratos informáticos. Por ejemplo: la cláusula de no solicitud de personal, en la que el cliente se compromete a no contratar al personal del proveedor para que trabaje con él. Esta cláusula se interpreta como una obligación de no hacer.

Existe otra cláusula que se refiere a la restricción de acceso al equipo y que con frecuencia se utiliza en los contratos de mantenimiento para liberar al proveedor de toda garantía en caso de intervención del usuario o de una tercera persona sobre el equipo informático. Dicha cláusula es limitativa de responsabilidad.

Naturaleza jurídica

Aunque difíciles de encuadrar, se ha considerado que algunas características respecto a la naturaleza jurídica de los contratos informáticos son las siguientes:

a) Son de tipo complejo, pues surgen de una serie de vínculos jurídicos, ya que en ella se pueden encontrar diversos contratos, como compraventa de hardware y de software, *leasing*, licencia de uso de software, alquiler, contrato de servicios y mantenimiento.
b) Es un contrato atípico, pues carece de regulación propia y suele no estar regido por una normatividad legal especial. Empero, en términos generales, se considera que este contrato se sujeta a los contratos tradicionales existentes y a las disposiciones generales establecidas en los códigos civiles.
c) Es un contrato principal, pues no depende de otro contrato que le sea precedente, es decir, tiene "vida propia", pero puede suceder que vaya acompañado de garantía, sea ésta real o personal.
d) Es oneroso, pues cada una de las partes sufre un empobrecimiento, compensado por una ventaja. Además, como sucede con otros contratos, este carácter pecuniario no significa necesariamente que exista equivalencia económica en las prestaciones y casi siempre existe un desequilibrio entre ambos.
e) Es consensual, pero en la práctica se celebra por escrito dada su trascendencia económica y de diferentes derechos y obligaciones que surgen como consecuencia de su nacimiento y normalmente la forma de celebración por adhesión, con cláusulas prerredactadas con los llamados *contratos tipo*.

Asimismo, cabe mencionar que estos contratos son *sui generis* en cuanto que incluyen en sus cláusulas múltiples normas legales de distintas áreas del derecho, como el derecho civil, administrativo, mercantil, de propiedad intelectual, internacional privado, etcétera.

ANÁLISIS ESPECÍFICO DE LOS CONTRATOS SOBRE BIENES INFORMÁTICOS

Según el peruano Willheim David Angermüller,[3] el contrato informático es el acuerdo de voluntades de dos o más partes con el fin de crear vínculos de obligaciones y que busca crear, regular, modificar o extinguir una rela-

[3] Licenciado en derecho egresado de la UNMSM, y de Letras PUC, analista programador y experto en sistemas de comunicación informatizada.

ción jurídica patrimonial, cuya prestación debe estar relacionada en todo o en parte con el proceso informático: un hardware, un software, un servicio informático, datos ofrecidos por las computadoras o servicios informáticos múltiples o complejos.

Dicho autor concibe que todo contrato que tenga por objeto un bien o servicio informático debe ser considerado informático y que a su vez debe ser diferenciado de los contratos que se apoyan en la tecnología informática para facilitar la contratación y que la utilizan como utensilio, en cuyos casos la participación de la informática es la misma que la de una balanza en una compraventa cualquiera que se realice en un mercadillo; en este caso, la balanza facilita el intercambio pero no necesariamente es objeto de transacción. Por ello, se debe establecer la diferencia entre contratos informáticos o contratos cuya finalidad es un bien o servicio informático, y que son objeto de nuestro estudio de aquellos contratos auxiliados por la informática, en los cuales ésta presta su asistencia, y denominados *contratación con asistencia informática*.

Al respecto, Emilio del Peso define al contrato informático como "aquel cuyo objeto sea un bien o un servicio informático —o ambos— o en el que una de las prestaciones de las partes tenga por objeto ese bien o servicio informático".[4]

La contratación sobre bienes informáticos se nutre en muchas ocasiones de diversas formas de contratación tradicional, lo cual crea un modelo contractual complejo no sólo en lo que respecta a su materia u objeto, sino también en cuanto a su estructura.

En muchos aspectos también, el contrato informático resulta similar a un contrato clásico; empero, los tecnicismos que posee y que lo distingue de los modelos contractuales tradicionales, así como la importancia económica y el vertiginoso crecimiento que dichos bienes han tenido tras el desarrollo de las ciencias y las comunicaciones lo vuelven una necesaria e importante fuente de estudio.

Otro aspecto por considerar es que muchos modelos contractuales que se utilizan en materia de bienes informáticos son copias o adaptaciones de los modelos contractuales de otros países —lo cual no es novedad si se considera nuestra legislación— y muchas veces responden a situaciones jurídicas que suceden en lugares distantes, donde mantienen una costumbre social y económica ajena a la realidad mexicana.

En otros casos no la emulación directa de los modelos internacionales, sino el traslado de las cláusulas de contratación que redacta el representante de la firma internacional tiene que adherirse el distribuidor y corres-

[4] Del Peso, Emilio, *Contratos informáticos*, disponible [en línea] http://www.asertel.es/cs/home.htm consultada en mayo de 2008.

ponde al establecimiento de plazos, garantías y particularidades de uso común en el país de origen de la mercadería. Estas cláusulas redactadas de acuerdo con los modelos internacionales se trasladan al comprador final sin mayor modificación. Esto resulta útil al distribuidor local, pues puede trasladar la garantía y demás obligaciones del importador mayorista de manera directa al comprador sin ningún tipo de complicaciones.

Cabe señalar que ninguno de los contratos aquí mencionados es enteramente puro, sino que se interrelaciona con otros, pues todo contrato de hardware presupone usar en alguna medida el software para realizar las pruebas de funcionamiento, del mismo modo que los modelos contractuales sobre el software tienen cierta interrelación con el hardware, además de los servicios y datos, entre otros.

El criterio de clasificación que se utiliza está en función del objeto principal que persigue el contrato, salvo en los contratos informáticos mixtos o complejos, que tienen una igualdad de importancia de los objetos perseguidos. Un ejemplo típico es el contrato mixto de seguridad que presupone la adopción de medidas necesarias tanto en software, hardware y servicios con el objetivo de brindar un servicio de resguardo a los datos, equipos electrónicos, redes computacionales y sistemas de información; sin lugar a dudas, ésta es una combinación de recursos que se ponen en movimiento tras celebrar dicho contrato.

Tal enumeración de ninguna manera quiere limitar la contratación informática dentro de estos contratos; existen otras formas contractuales cuyo uso e importancia pueden considerarse menores, por ejemplo: un comodato o préstamo a título gratuito de un equipo de cómputo por determinado tiempo, práctica que existe con relativa frecuencia, pero que puede ser considerada menos significativa por su trascendencia económica.

1. Contrato de compraventa de hardware

El bien informático es por su naturaleza un bien mueble, por fuerza material para que cumpla con el requisito de ser físicamente aprensible, característica que la informática exige para ser denominado hardware.

Al hacer referencia al hardware no sólo se alude al requisito de materialidad, sino además debe ser fruto del desarrollo de las ciencias y tecnologías de la electrónica, basado en los principios de la lógica matemática y estar orientado a ser un elemento generador de información automática computacional o instrumento que ayude a dicho proceso, requisitos indispensables para hablar del elemento hardware informático.

Dicho hardware es el objeto que el vendedor se obliga a entregar a favor del comprador y este último está obligado a pagar el precio pactado.

2. Contrato de arrendamiento de hardware

En este contrato, el arrendador o locador cede temporalmente un bien informático, una computadora o conjunto de computadoras como regla y/o uno o más suministros, periféricos o repuestos de computadoras como excepción en arrendamiento a favor de un arrendatario, quien se obliga a pagar una renta en contraprestación.

En la práctica este uso se ve obstaculizado por la obsolescencia informática; por ello, las empresas que desean poner en arrendamiento sus equipos son pocas, pues al ser devueltos han sufrido un alto nivel de depreciación que genera costos elevados y poca aceptación de los consumidores. Otro aspecto a tomar en cuenta en este contrato es que el arrendador debe otorgar —si se trata de un equipo de informática completo— también de manera temporal las licencias de uso de los programas instalados en la computadora, pues se parte de dos suposiciones: primero, toda computadora presupone la presencia de por lo menos un software que debe acompañarla y que será la aplicación que se "correrá" en dicho equipo y segundo, sobre ese software existen los derechos patrimoniales y morales de un autor, el cual provee de una licencia de uso que es puesta a la comercialización. De lo anterior se concluye que toda computadora que se encuentre en funcionamiento debe contar por lo menos con una licencia de uso de un sistema operativo; en caso contrario, se estaría frente a la práctica de la piratería informática.

3. El contrato de mantenimiento de hardware

Este contrato se encuentra muy popularizado, pues es común que las grandes instituciones requieran los servicios especializados, permanentes y sobre todo rápidos de las empresas encargadas de mantener y reparar equipos informáticos, cuyos usuarios van desde las grandes corporaciones bancarias que desplazan gran cantidad de recursos humanos para mantener sus equipos en óptimo funcionamiento hasta los hogares que ocasionalmente contratan estos servicios.

En la práctica cabría diferenciar tres tipos de contrato: los *contratos de mantenimiento preventivo*, que se realizan con el objetivo de evitar anomalías en el funcionamiento de los equipos y que no incluyen el servicio de las reparaciones necesarias, los *contratos de mantenimiento correctivo*, que surten sus efectos cuando los componentes del equipo presentan fallas o problemas de funcionamiento, y los *contratos de mantenimiento preventivo-correctivo*, que incluyen la revisión periódica de los equipos a solicitud del cliente de acuerdo con un cronograma y que se realizan con el fin de detectar fallas, además de la reparación de los equipos al presentar problemas de funcionamiento.

Asimismo, en estas dos últimas formas de contrato es factible que las partes puedan determinar libremente si los costos de mantenimiento incluyen o no los costos de los repuestos utilizados.

También es común que el contrato de mantenimiento de hardware se incluya en un contrato de compraventa de equipo, ya que de las cláusulas del contrato pueden emanar derechos de mantenimiento sobre el equipo adquirido que el comprador pudiera ejercer sobre el vendedor y que se suscriben a los términos y condiciones puestos en las cláusulas del servicio de mantenimiento que se hayan consignado en el contrato de compraventa que los haya otorgado.

4. El contrato de *leasing* sobre el hardware

El contrato de *leasing* o arrendamiento financiero se basa en la necesidad del empresario de obtener un crédito —materializado en maquinarias como herramientas de producción— en el cual la garantía está constituida en la propiedad de dichas herramientas. El contrato tiene elementos de la compraventa y del arrendamiento y está destinado a los empresarios que requieren un capital de trabajo para invertirlo en la adquisición de maquinarias. Las entidades bancarias se encargan de comprarlas en las cantidades, marcas y especificaciones dadas por el empresario, de tal modo que la maquinaria sirva para el uso que se le va a dar y compromete al empresario a pagar el crédito al aumentar los impuestos, las primas de seguros y las utilidades del banco a cambio de la entrega en uso durante determinado tiempo, luego del cual el empresario puede optar por la compra del bien a su precio residual del mismo.

FRAUDES EN LA COMERCIALIZACIÓN DE HARDWARE

En este tipo de transacciones puede haber:

- Instalación de sistemas operativos o programas informáticos sin licencia o "piratas".
- Incumplimiento de los términos de licencia OEM.
- Falsificación de marcas o signos distintivos de empresas de reconocido prestigio.
- Manipulación del microprocesador para que simule ser un modelo o velocidad superior.
- Publicidad engañosa.
- Manipulación del *set up* para que aparezca un caché no existente o de menor calidad (*write back*).

- Incompatibilidad de los componentes con los estándares de hardware y sistemas operativos.
- Ausencia de garantía y servicios de posventa.
- Instalación de componentes usados o de muy baja calidad.

DIFERENTES PARTES

A continuación se describen las partes que conforman la relación contractual de índole informática, como los proveedores y los usuarios.

Proveedores

Los proveedores son los fabricantes, distribuidores y vendedores de bienes informáticos, así como los prestadores de servicios informáticos. Sus principales obligaciones son las siguientes:

- Salvaguardar los intereses del cliente y darle consejo e información.
- Cumplir con la entrega de los bienes o con la prestación de sus servicios en los plazos estipulados. El incumplimiento de los términos o plazos permite al cliente establecer una demanda en reclamo de los daños y perjuicios motivados por el retraso o llegar a la rescisión del contrato.
- Realizar la prestación conforme a las especificaciones del contrato.
- Garantizar los vicios ocultos que pudiera tener la prestación realizada.
- Realizar el estudio de viabilidad para el usuario, y actuar en todo momento con probidad y honestidad, así como con una asesoría y apoyo adecuados.

Usuarios

Los usuarios son aquellas entidades (públicas o privadas) o individuos que requieren satisfacer determinadas necesidades por medio de los bienes informáticos. Entre sus principales obligaciones están las siguientes:

- Informarse, documentarse, visitar exposiciones y demostraciones de equipo o de servicios informáticos en general, solicitar folletos explicativos sobre las características y el funcionamiento de los centros de cómputo, así como de los programas existentes.
- Determinar de manera precisa sus necesidades de automatización de tal modo que se establezcan y comuniquen sus objetivos precisos.

- Dar al proveedor información exacta de su empresa, acompañada de documentos, gráficas, proyectos, etcétera.
- Capacitar adecuadamente a su personal para manejar el centro de cómputo (funcionamiento, seguridad, programación, etcétera).
- Obtener una mejor adaptación de su empresa a los imperativos de funcionamiento del material instalado.
- Realizar la elección final entre las ofertas que le presenten los proveedores, considerando los elementos de apreciación de orden financiero y técnico.
- Aceptar y recibir el material o los servicios que ha solicitado.
- Acordar un periodo de prueba a efecto de verificar el funcionamiento del equipo.
- Respetar las directrices propuestas y formuladas por el proveedor sobre el modo de emplear el material o los programas.
- Pagar el precio convenido según las modalidades fijadas entre las partes, salvo si se emitieron reservas luego de recibir el material o servicio.

CLASIFICACIÓN

Genérica

Los principales contratos informáticos asimilables en las categorías jurídico-contractuales son los siguientes: compraventa, arrendamiento, arrendamiento con opción a compra de bienes informáticos, así como la prestación de servicios informáticos. Hablemos de cada uno de ellos:

1. Compraventa

   Se refiere a los equipos y suministros (componentes, accesorios, etc.). Su esencia es similar a la de cualquier contrato de compraventa referido a otros bienes, pero reviste una serie de elementos peculiares que los tornan aún más complejos. En este contrato informático se debe establecer en primer término que el proveedor venderá al usuario el material de acuerdo con los planes de contratación ofrecidos, y ha de incluirse una relación de las máquinas que integren el centro de cómputo materia de la compraventa, indicando asimismo el modelo, descripción, cantidad, precio de compra y cargo mensual de mantenimiento.

   En el contrato se deberá asentar la fecha de entrega del equipo de cómputo, así como el sitio y las condiciones. Los pagos deberán

hacerse de conformidad con el plan de contratación específico establecido en el contrato y ningún cargo comenzará a "surtir efecto" hasta que se haya aceptado el sistema de cómputo y los demás productos amparados por el contrato. Es importante establecer en el contrato el momento en que el usuario adquiere la propiedad; por otra parte, podrá haber un periodo de prueba del equipo que comience desde la fecha de entrega del sistema y termine después de 30 días naturales. Si después de 60 días no se ha alcanzado un nivel de eficacia, el usuario podrá solicitar el reemplazo total del equipo o de la unidad que no funciona.

El proveedor deberá responder por los daños y perjuicios que le cause al usuario en caso de incumplimiento; asimismo, asumirá cualquier responsabilidad para el saneamiento en caso de evicción (es decir, la reivindicación de la propiedad material por terceros). Por ello, en el contrato el proveedor deberá garantizar también el tiempo que se obligue a suministrar al usuario las partes y refacciones necesarias para mantener los equipos en las condiciones adecuadas de funcionamiento. Por otro lado, el proveedor proporcionará por escrito al usuario toda la información técnica necesaria para que éste use adecuadamente el equipo.

Durante el tiempo del contrato y aun después, ambas partes deberán convenir en mantener con discreción cualquier información recibida de la otra parte que haya sido clasificada como confidencial. El proveedor será responsable de las violaciones que se causen en materia de patentes o derechos de autor acerca de los objetos materia del contrato proporcionados al usuario. A este respecto, debe comprometerse al pago de daños y perjuicios.

Las partes deben establecer el plazo durante el cual el usuario puede cancelar temporal o definitivamente el equipo solicitado mediante aviso por escrito. En caso de que el usuario, por así convenir a sus intereses, adquiera equipos de compañías extranjeras, deberá darse cumplimiento a lo establecido en las leyes respectivas. Este contrato informático de compraventa constituye un acuerdo entre las partes y deja sin efecto cualquier negociación, obligación o comunicación (ya sea oral o escrita) hecha con anterioridad a la firma de aquél.

2. Arrendamiento

Al aplicar este contrato en materia informática, existen cláusulas específicas para el arrendamiento de sistemas de cómputo, en cuyo caso se debe incluir en el contrato una relación de las máquinas y los sistemas operativos, indicando su modelo, descripción, cantidad, precio de compra, renta mensual y cargo mensual de mantenimiento. También se deberá estipular la duración del contrato en los términos y con-

diciones acordados con apego a los mecanismos de prórroga que se presenten; asimismo, se deberán definir claramente la fecha, el sitio y las condiciones de entrega del sistema de cómputo.

Una vez que las partes han fijado los precios que regirán las operaciones del contrato, se estipulará el compromiso de no alterar los precios pactados originalmente durante la vigencia de aquél; el pago del precio da derecho al arrendatario a usar en forma ilimitada el sistema de cómputo con sus fases operativas y de programación. El usuario tiene el derecho a solicitar que se estipule en el contrato que el equipo de cómputo se pruebe en las instalaciones del proveedor de acuerdo con ciertos estándares establecidos, así como el arrendador ha de proporcionar documentos, formularios y publicaciones referentes a ese equipo de cómputo. El arrendatario podrá cancelar cualquier unidad de equipo si avisa al arrendador con 30 días de anticipación y podrá dar por terminado el contrato si el proveedor incurre en violación de cualquiera de las cláusulas del aquél.

En el contrato se deberá estipular que el arrendador notificará al usuario con uno o dos años de anticipación, según se haya pactado, su retiro del mercado nacional y mientras esté en el mercado deberá comprometerse a prestar los servicios amparados por el contrato.

En el contrato informático de arrendamiento existen varias cláusulas similares a las que se pactan en un contrato de compraventa, entre ellas que el arrendador deberá mantener en forma confidencial toda documentación que le haya sido facilitada por el arrendatario a fin de realizar el estudio de viabilidad. El proveedor o arrendador será responsable de las violaciones que se causen en materia de patentes o derechos de autor y se comprometerá a indemnizar por daños y perjuicios a un tercero afectado. Por otro lado, el arrendador deberá garantizar que el equipo y sus dispositivos estarán libres de cualquier defecto de materiales o mano de obra y comprometerse a mantener el objeto material del contrato en condiciones satisfactorias de operación, para lo cual habrá de ajustar, reparar o reemplazar las piezas o artículos defectuosos que causen una operación anormal, así como hacerse cargo de la instalación del sistema de cómputo. El proveedor también debe ser responsable de los empleados que envía a las instalaciones del usuario y asumir cualquier responsabilidad para el saneamiento en caso de evicción, así como indemnizar al usuario en caso de actuar de forma dolosa.

3. Arrendamiento con opción a compra

Esta figura es una modalidad del contrato de arrendamiento muy empleado en materia informática y generalmente conocido con el anglicismo *leasing*. Este contrato establece que la opción de compra se

podrá ejercer en cualquier momento después de la fecha de aceptación del sistema de cómputo respecto a todo o parte de él, considerando los porcentajes pactados de las rentas pagadas que se abonarán al precio de compra. Al ser la compra de equipo informático un gasto muy fuerte para las empresas, es común que al principio tomen en arrendamiento el centro de cómputo y lo paguen a plazos hasta adquirir la propiedad de éste. A dicho contrato informático se le aplican las cláusulas del contrato de arrendamiento y las del contrato de compraventa en cuanto a adquisición del equipo.

4. Prestación de servicios

Este contrato se refiere a los trabajos que se realicen sobre determinadas materias. En el derecho civil mexicano, el contrato que más se asemeja a este tipo de contrato informático es el de prestación de servicios profesionales, referente a los servicios que presta un profesional a una persona llamada *cliente*, quien se obliga a pagarle una determinada retribución denominada *honorarios*. En esta figura se requiere que el prestador de servicios tenga una adecuada preparación técnica además de un título profesional, así como capacidad general para contratar. A este respecto, cabe mencionar que se entiende por ejercicio profesional "la realización habitual de todo acto o la prestación de cualquier servicio propio de cada profesión".

Entre las principales características de este contrato están las siguientes: son bilaterales, onerosos, conmutativos y formales o consensuales, según acuerden las partes. Los elementos reales son: el servicio profesional y los honorarios. Conforme el tema que interesa, es menester enunciar que en el llamado contrato de prestación de servicios informáticos hay una categoría concerniente a la utilidad o provecho que se obtiene de la realización de acciones o actos de personas físicas o morales que coadyuven de manera directa o indirecta al manejo de la información, cuya aplicación se relacione con la estructuración y composición de datos. Las partes en este contrato informático se denominan: *a) proveedor*, el cual presta el servicio (prestador) y la mayoría de las veces son empresas de computación, y *b) cliente o usuario* (prestatario), aquel que recibe el servicio y lo retribuye.

Como ejemplo de contratos de servicio informático cabe citar el de explotación de programas, el de consulta de archivos y bancos de datos, el de estudio de mercado en informática, el de documentación técnica, el de mantenimiento correctivo y preventivo de equipo o de sistemas, el de manejo de datos, el de desarrollo de estudios de viabilidad para la selección de bienes y servicios, el de consultoría, el de diseño de sistemas, asistencia técnica, formación, etc. Cabe señalar que la importancia que han adquirido estos contratos es el resultado de la

necesidad cada vez mayor de asesoramiento y servicios informáticos varios que requieren los usuarios.

De acuerdo con el objeto

Por el objeto del contrato existen contratos de hardware, contratos de software, contratos de instalación llave en mano y contratos de servicios auxiliares.

1. Contratos de hardware. En éstos se debe conceptuar como hardware todo aquello que físicamente forme parte del equipo, considerando como tal también los equipos de comunicaciones u otros elementos auxiliares para el funcionamiento del sistema que se va a poner en práctica.
2. Contratos de software. Al analizar una contratación de software hay que diferenciar si se trata de un software de base o de sistema, o de utilidad, de aplicación o de usuario, ya que este último debe responder a necesidades particulares, las del usuario, el que encarga la aplicación, y que deberán quedar claramente especificadas en el contrato. No obstante, el software de base o sistema y el de utilidad responden a características generales, que son las del sistema o las de la utilidad a la cual sirven y es un producto conformado de antemano que no se somete a peticiones o particularidades del usuario.
3. Contratos de instalación llave en mano. En éstos se incluyen el hardware y el software, así como determinados servicios de mantenimiento y de formación del usuario.
4. Contratos de servicios auxiliares. Pueden ser, el mantenimiento de equipos y programas o la formación de las personas que van a utilizar la aplicación respecto a equipos, sistema o aplicaciones.

Por grupos

Clasificación según el español Xavier Ribas:[5]

1. Contratos referidos al hardware
    - De compraventa de hardware
    - De arrendamiento de hardware

[5] Estudio de Xavier Ribas. http://www.asertel.es/es/info.htm

- De *leasing* de hardware
- De mantenimiento de hardware

2. Contratos referidos al software

   - De licencia de uso de software
   - De licencia de uso de código fuente
   - De desarrollo de software
   - De mantenimiento de software
   - De *escrow*

3. Contratos referidos a servicios informáticos

   - De ayuda *hot line*
   - De formación y capacitación de usuarios
   - De acceso a internet
   - De albergue de páginas web (*hosting*)
   - De diseño de páginas web
   - De publicidad en internet (*banners* publicitarios)
   - De consultoría
   - De auditoría informática
   - De transferencia de tecnología o *know-how*
   - De acceso a Boletin Board Service (BBS)
   - De auditoría de seguridad
   - De auditoría de calidad
   - De instalación y actualización periódica de antivirus
   - De certificación de transacciones electrónicas
   - De teletrabajo

4. Contratos relativos a bases de datos

   - De compraventa de base de datos
   - De suministro de información

5. Contratos informáticos mixtos

   - De distribución
   - De concesionario
   - De *outsourcing*
   - De franquicia
   - De llave en mano
   - De gestión de redes
   - De implantación de plan de seguridad
   - De implementación y mantenimiento de intranet
   - De firma digital

Relativos a internet

Clasificación de contratos referidos a internet, según Olivier Hance:[6]

- De proveedor de acceso a internet
- De operador de sistema en internet
- De suministro de información
- De edición en internet
- De "renta" de espacio en línea y servicios relacionados
- De publicidad en línea
- De correduría en línea
- De "renta" en línea de espacio publicitario
- De desarrollo de productos multimedia en línea
- De estudio de mercado en línea
- De distribución en línea
- De desarrollo y mantenimiento de una página web
- De investigación en línea
- De cabildeo y mercadotecnia en línea
- De participantes en un foro en línea
- Para acceso a bases de datos en línea
- Contrato maestro de ventas al menudeo
- De comercio electrónico entre profesionales
- De certificación de autoridad
- De política de uso aceptable

ETAPAS CONTRACTUALES

A fin de establecer un vínculo contractual más adecuado, en detrimento de eventuales dificultades, es conveniente que las partes contratantes estén debidamente compenetradas de los compromisos que pueden contraer. De aquí que en las siguientes líneas vayamos a hacer lo que consideramos una pertinente distinción entre las relaciones precontractuales y las relaciones contractuales propiamente dichas.

Relaciones precontractuales

Estas relaciones se refieren al análisis, estudio y negociación previa a la firma del contrato y se establece por medio de dos figuras fundamentales: el estudio previo o de oportunidad y el de viabilidad.

[6] Oliver Hance, *Leyes y negocios en internet*, McGraw-Hill Interamericana, México.

El *estudio previo de oportunidad* es el análisis que realiza el eventual usuario acerca de sus necesidades mediatas de informatización a efecto de que se evalúen las condiciones fundamentalmente técnicas y económicas que permitan una adecuada oferta de bienes o servicios informáticos por los proveedores. Uno de los inconvenientes de dicho análisis es que el eventual usuario, en función de su evidente desconocimiento, requiere una asistencia técnica que en la práctica sólo podrá brindarle el mismo proveedor, por lo cual queda a expensas de favoritismos comerciales que dificultarían la elección.

Otra figura es la del *estudio de viabilidad*, que es aquel realizado por el proveedor en el cual se precisan las aplicaciones informáticas hacia el eventual usuario, quien para ello deberá responder los cuestionamientos plasmados en el llamado cuaderno de cargos a efecto de permitir que el proveedor formule sus ofrecimientos susceptibles de ser aceptados o rechazados. Las inconveniencias de dicho estudio son la falta de profundidad y objetividad, ya que el eventual usuario en muchas ocasiones no llega a precisar de manera adecuada sus necesidades presentes y futuras y, por otra parte, no realiza ofertas satisfactorias. Desafortunadamente, en nuestro medio no se le han atribuido las consideraciones debidas a estas relaciones por lo que muchas veces hay problemas una vez establecido el vínculo contractual.

Es conveniente señalar que en la etapa contractual, es decir, en la elaboración de los estudios de oportunidad y viabilidad, éstos tendrán importantes aplicaciones para la elección del material o la prestación de servicios de que se trate. Si esto se logra, las subsecuentes etapas contractuales no tendrán problemas generadores de litigio, por lo cual es conveniente analizar cada una de ellas, como se hará a continuación.

De acuerdo con un estudio de oportunidad o de viabilidad hay etapas diferentes y complementarias entre sí, como las siguientes:

1. Una reflexión del usuario sobre la oportunidad y los objetivos de automatización.
2. Un asesoramiento adecuado que, luego del análisis de necesidades, traduzca éstas en una forma apropiada según las consideraciones de un cuaderno de cargos.
3. Dar a conocer el cuaderno de cargos a diversos proveedores a fin de tener varios ofrecimientos y una elección más adecuada para realizar los objetivos definidos.

Estos primeros pasos de una relación precontractual son básicos, pues de ellos se deriva que el usuario haga una adecuada exposición de sus necesidades informáticas y, en consecuencia, una buena elección con base en las diversas ofertas que le hagan los proveedores. Antes de solicitar apoyo

a un asesor externo, es recomendable establecer una reflexión elemental con todas las personas implicadas en ello para recoger los puntos de vista respecto a los objetivos que se pretenden, e inquirir acerca del correcto fundamento de la informatización en un contexto general (tipo de actividad, organigramas, dificultades sociales, balances, disponibilidad, etc.), así como los beneficios susceptibles de generarse mediante la automatización de la empresa.

Se debe establecer el estado real de la empresa a fin de diagnosticar las necesidades reales en materia de informática y clasificarlas por orden prioritario, fijando una gama de objetivos teóricos. Es importante también determinar la trascendencia del cuaderno de cargos dentro de la futura o eventual contratación, así como redactar éste en términos muy claros para que permita incluir respuestas igualmente claras del proveedor y que, si no se cumple el contrato, se facilite el libre acceso a la vía judicial.

Derivado de lo anterior y a partir del contenido del cuaderno de cargos o del estudio de viabilidad, el cliente podrá contar con un elemental conocimiento de causa hacia una acertada elección en el ámbito informático, a pesar de que la elección esté supeditada en última instancia a la efectividad del equipo informático y la adecuada satisfacción de necesidades. Es conveniente, entonces, que el usuario antes de hacer su elección tome en cuenta un conjunto de criterios, como la clase de equipo que va a adquirir, su compatibilidad con los materiales de la empresa, su costo, la efectividad y rapidez, condiciones de la instalación y mantenimiento que se requerirá, las evoluciones posibles del sistema, rentabilidad, etc. En suma, analizar todas las prioridades para hacer una correcta elección. Por desgracia, la política mercantilista de los proveedores consiste en ofrecer las mejores ideas a los clientes y no necesariamente los mejores productos, a la vez que hay un margen de irrealidad entre lo requerido y lo ofrecido.

Relaciones contractuales propiamente dichas

Estas relaciones se refieren al momento en que los contratantes aceptan de manera tácita las condiciones del contrato y externan su voluntad de obligarse a cumplir el sistema mediante su firma. La fecha para la firma del contrato variará de acuerdo con lo que establezcan las partes. A este respecto, cabe señalar que para el proveedor será conveniente realizar esta etapa lo más pronto posible a efecto de asegurar la operación; en cuanto al usuario, tendrá que afrontar una disyuntiva porque si no firma pronto el contrato (en general pactado en dólares), esto causará un alza considerable en el costo previsto de la operación, pues normalmente los proveedores se reservan la facultad de aumentar los precios en función de la variabilidad del tipo de cambio.

Por otro lado, en los momentos anteriores a la firma del contrato puede haber un nuevo equipo o aun una baja de precios en función de la gran variedad oferente, por lo cual la celeridad o prontitud de la firma puede convertirse en un arma de dos filos. Una vez firmado el contrato, es usual que el proveedor determine un plazo de 30 a 60 días para entregar el equipo. Si este plazo no es respetado porque el equipo no ha llegado del extranjero, porque aún no sale de la fábrica o por cualquier otra razón que se alegue, es conveniente que el usuario estipule una cláusula penal en el contrato para prever que se le pague cierta cantidad por la demora o incluso rescindir el contrato con el fin de protegerse.

En consecuencia, puede ocurrir que, una vez entregado el equipo, éste no sea instalado y el proveedor haga saber al usuario, sin justificación válida alguna, que la instalación se realizará con posterioridad, para lo cual es conveniente estipular en el contrato un término máximo razonable para que ésta se lleve a cabo; se estima que 15 días es un plazo de espera razonable. Asimismo, es conveniente para el usuario realizar pagos parciales en caso de adquisición de equipo, para así tener un margen de protección más amplio y que el último pago se haga luego instalar éste.

Una vez hecha la entrega, surge el periodo de prueba del equipo para comprobar su buen funcionamiento y su adaptación al sistema del usuario. En este sentido, la aceptación del equipo será de carácter parcial en tanto no se vea que funciona en perfectas condiciones.

ANEXOS

Entre los anexos tipo, que ayudan a describir el objeto y que siempre deben figurar en un contrato informático destacan:

- Especificaciones del sistema por contratar.
- Especificaciones de los programas por desarrollar.
- Pruebas de aceptación.
- Resultados a obtener y que, en algún caso, formarán el objeto del contrato.
- Análisis.

PROBLEMÁTICA FUNDAMENTAL

Dicha problemática consiste en el desequilibrio notorio existente entre las partes en razón de que, en general, el proveedor de bienes o servicios se vale de sus conocimientos técnicos sobre la materia, y el correlativo desconocimiento del usuario, para imponer sus condiciones mediante una redacción contractual con términos muy técnicos en detrimento de los ele-

mentos jurídicos, los cuales, en la mayoría de las ocasiones, son aceptados por los usuarios en razón de sus necesidades informáticas y su falta de adecuada asesoría técnica, lo cual convierte a éstos en verdaderos contratos de adhesión.

En razón de lo anterior, tales contratos manifiestan una gran cantidad de lagunas jurídicas, las cuales, a su vez, son fuente de controversias y conflictos en cuanto a la falta de precisión en caracteres tan importantes como las garantías, responsabilidades, reparación del sistema, pago de daños y perjuicios, etc. De esta forma, se percibe que los contratos informáticos ameritan un tratamiento pormenorizado, sobre todo en cuanto a las diversas implicaciones hasta hoy desconocidas por el derecho tradicional a efecto de contemplar un régimen jurídico regulador efectivamente aplicable.

RIESGOS INFORMÁTICOS

Generalidades

La acepción *riesgo informático* es un concepto nuevo en la terminología jurídica sin existir, por tanto, una definición específica. El *riesgo* se refiere a la incertidumbre o probabilidad de que ocurra o se realice una eventualidad, la cual puede estar prevista; en este sentido, es válido decir que el riesgo es la contingencia de un daño. En función de lo anterior, cabe aseverar que los riesgos informáticos se refieren a la incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos como los equipos informáticos, periféricos, instalaciones, proyectos, programas de cómputo, archivos, información, datos confidenciales, responsabilidad civil que éstos ocasionan frente a terceros por la prestación de un servicio informático, etcétera.

En nuestro medio, los riesgos informáticos no constituyen una figura jurídica especial, aunque se pueden aplicar en su tratamiento ordenamientos como las leyes en materia de seguros; empero, lo que motiva y justifica señalar los riesgos informáticos como un fenómeno jurídico especial es la complejidad de los problemas que presentan en la práctica. Por otra parte, es conveniente enunciar que la forma de apreciar un riesgo de esta índole resulta muy distinto del tratamiento que se da a los riesgos comúnmente conocidos en el mercado de seguros. De esta manera, el concepto de riesgo informático es una noción tan extensa que se desarrolla al parejo de la tecnología y es objeto de estudio del llamado derecho informático con el rubro de los contratos informáticos.

Prevención de riesgos

La prevención contra los riesgos diversos tiene como finalidad la protección de las personas, equipos y trabajos vinculados con la actividad informática.

En la protección se distinguen tres niveles básicos:

a) *La protección amplia*, la cual debe ser eficaz y concierne a los locales de procesamiento y sus anexos. En algunos casos también los locales de disposición de las informaciones de entrada y los de almacenamiento y archivo disfrutan de esta protección.
b) *La protección media*, cuyos efectos deben ser compensadores y complementarios. Se instala en los locales de control y de disposición de resultados.
c) *La protección restringida*, en función del grado seleccionado de vulnerabilidad. Es conveniente para los locales de gestión y para los de análisis y programación.

Dichas protecciones, independientemente del nivel de que se traten, reclaman decisiones directivas en lo que concierne a:

- Implantación de locales y equipos.
- Selección de medios de protección, alarmas. evacuación y servicio.
- Circulación de las personas y los medios de control.
- Circulación de informaciones y control de esta circulación.

Previsión de medios de reinicio de operaciones después de un siniestro

La selección de los medios de protección distingue a las personas, equipos y trabajos, pues impone los de alarma, evacuación y servicios, además de la circulación de personas, información y medios de control correspondientes. De esta manera, cabe decir que la seguridad es un todo que no se puede fraccionar y que está sometida a un reglamento general que describe, entre otros aspectos, los siguientes:

- La lista de los objetos en cuestión, su valor, su vulnerabilidad y las consecuencias de su deterioro.
- La lista de los medios de prevención, alarma, servicio y recuperación. Los criterios de repartición de los equipos y trabajos entre los diferentes niveles de protección.
- Las consignas generales de puesta en operación de las protecciones y acciones.

- Las pérdidas posibles de explotación y los costos correspondientes.
- Los controles de aplicación de los reglamentos.

Clasificación de riesgos informáticos

Con base en lo antes señalado, se pueden distinguir cuatro categorías de riesgos agrupados de la siguiente manera:

a) Respecto a los equipos
b) En cuanto a los programas
c) En relación con las personas
d) En referencia a los trabajos

A continuación se explica cada uno de estos grupos:

Riesgos provenientes del equipo

En este tipo de riesgos se pueden mencionar los que siguen:

- Pérdida o cambio de mensajes durante el proceso de transmisión.
- Desastres e interrupciones (sean temporales o prolongadas) en la capacidad de funcionamiento del equipo o sus líneas. Éstos pueden ser causados por fuego, inundaciones, terremotos, disturbios, terrorismo, pérdida de energía eléctrica, fallas en el sistema de aire acondicionado, etc. (sean fenómenos de la naturaleza o del hombre).
- Falta de facilidad de respaldo al equipo, líneas de comunicación y personal en el seno de la empresa.
- Fallas del equipo, las cuales pueden provocar la aparición de datos erróneos, omisiones, pérdida de información y problemas similares.

Cabe mencionar que la protección respecto a estos riesgos se ha centrado de manera tradicional en la lucha contra dos elementos muy nocivos para los equipos, como el agua y el fuego, cuyo especial control debe ser completo y muy diversificado y consiste sobre todo en la instalación de sistemas de detección apropiados, medios de extinción automáticos, así como los accesorios de lucha contra los riesgos.

Así, los sistemas de detección apropiados son los relativos al incéndio, distinguiéndose los de tipo gas-humo, instalados en la sala de máquinas bajo el piso falso, en el cielo falso, al igual que en los conductos de aire acondicionado. En este sentido, los sistemas de alarma son visuales y /o audibles. En cuanto a los medios de extinción automática, se puede utilizar el CO_2, el agua o la espuma de gran expansión, complementados por

los medios portátiles de primera intervención, cuyos materiales son de la misma naturaleza.

Riesgos provenientes de los programas

Entre este tipo de riesgos se pueden mencionar los siguientes:

- Fraude o desfalco mediante la afectación de los activos de la empresa (incluida información), por persona no autorizada y en su proyecto, que puede ser un empleado en la compañía o una persona ajena a ésta.
- Robo de programas, que podrá ocurrir mediante el apoderamiento físico o por medio del copiado ilícito de éstos.
- Falta de posibilidad de recuperación y reinicio del proceso o comunicación de datos.
- Modificaciones no autorizadas, ya sean de carácter temporal o permanente o aun las realizadas por personal normalmente autorizado, ya sea por dolo o por imprudencia.
- Alteración de secuencias. Al no contar con medios para rastrear la información en el proceso de datos, éste se puede alterar o perder de manera indebida, lo cual provoca, entre otras cosas, complejidad y pérdida de tiempo al tratar de rehacer los movimientos en proceso.
- Deficiente validación de datos-programa. Esto es, la edición de datos, la comprobación de cálculos y las acciones específicas que el sistema pueda generar y cualquier otra función relacionada con la entrada o salida controlada por programa puede no estar debidamente planteada, lo cual puede hacer que continúe el proceso con base en datos erróneos.
- Falta de comprobación intermedia. Es decir, la falta de un control debido a los diferentes pasos del proceso puede provocar no estar en condiciones de saber si se procesan bien o no los datos o si no se ha perdido la integridad de la información durante el proceso.

Riesgos relacionados con los trabajos

Entre este tipo de riesgos tenemos los siguientes:

- Riesgos en los proyectos informáticos. Realizar un examen estadístico al respecto pone en relieve la frecuencia de perjuicios y problemas para las empresas o clientes, dada la inejecución o deficiencias en cuanto a la realización de este tipo de proyectos.
- Riesgos contra los datos. Éstos son los provocados por la destrucción voluntaria o involuntaria de los soportes que contienen la información,

como las cintas, discos, etc., lo cual genera la desaparición o distorsión de datos. En cuanto a esto, también existe la divulgación intencional o imprudencial de datos confidenciales, así como otro tipo de manifestaciones caracterizadas por su alto grado de repercusión económica, datos relacionados con una persona o un asunto de la empresa. Estas acciones se relacionan con el control del flujo, proceso y archivo de la información.

- Provocación accidental o intencionada de errores y omisiones durante el proceso informático, que puede constituir información incompleta o inexacta, mal funcionamiento del equipo o cualquier otra irregularidad que afecte los archivos de la empresa, o falta de control de documentos negociables; esto es, el manejo indiscriminado de documentos negociables (cheques en el banco, pagarés, letras de cambio, etc.) puede provocar su extravío o mal uso.
- Acceso indebido a los sistemas. El acceso no autorizado a los sistemas en desarrollo y en operación expone a la empresa a otra serie de riesgos, como fraude, robo, sabotaje, chantaje, etcétera.
- Acceso indebido a las instalaciones. Similar a lo anterior, el acceso no controlado al equipo o a las terminales representa una posibilidad muy amplia de alteración o conocimiento de información confidencial.

Cabe mencionar que la protección contra riesgos debidos a agentes físicos obliga durante la construcción de los locales de procesamiento a evitar exposiciones a las radiaciones magnéticas o electromagnéticas. Esta protección se relaciona también con las concernientes a los riesgos debidos a los agentes químicos para que se apliquen de manera íntegra las consignas de protección del personal y las máquinas. Los trabajos también están expuestos a riesgos derivados de los errores en la concepción de las aplicaciones, la redacción de programas, la captación de información, la preparación de procesamientos, la explotación de programas, el funcionamiento de la biblioteca de los soportes magnéticos, la edición, formato y difusión de soportes, así como la actualización y mantenimiento de la información.

Estos errores, cuyo costo de reparación puede afectar fuertemente el presupuesto del servicio informático, podrán evitarse si el proceso de gestión informática se controla con firmeza durante la ejecución de los procesamientos; de esta forma, la instalación, el mantenimiento y el control de este proceso requiere una formalización total. De la distensión al realizar el proceso de gestión informática pueden surgir ciertos riesgos debidos a posiciones de deshonestidad, venganza o idealismo. Estas actitudes son difíciles de detectar, por lo que es necesario tomar las precauciones debidas desde la concepción del plan de funcionamiento del servicio informático.

La gama de ilícitos es muy extensa e incluyen riesgos de todo tipo y aun sin relación aparente. Listarlos en forma íntegra resulta difícil, pero se pueden mencionar los siguientes:

- Huelga con ocupación de los locales, con los consecuentes riesgos de destrucción o alteración de la información fundamental.
- Destrucción de los soportes de información por agentes físico-químicos no detectables de inmediato, como limaduras de hierro, cenizas de cigarro, imanes permanentes, etcétera.
- Alteración o sustracción de datos.
- Espionaje industrial.
- Robo de fondos, de tiempo-máquina y de programas.
- Falta de respeto voluntario de las consignas de protección.

Los disturbios son un hecho social y la prevención contra ese riesgo radica en el reforzamiento de los medios materiales de cierre de locales, el uso de buenas cerraduras, barras de hierro en las ventanas, así como cristales tríplex para las aberturas que dan al exterior. La huelga es también un riesgo social; el peligro no reside en el personal informático que está consciente de sus responsabilidades, sino en los elementos externos incontrolables e incontrolados, de manera que la seguridad de la información debe preverse en la gestión informática.

La destrucción por agentes físico-químicos podrá evitarse con la prohibición de DESI: se prohíbe que circulen personas extrañas en los locales cuyas prioridades de protección hayan sido definidas previamente. Los robos, las alteraciones y el espionaje industrial plantean el problema deontológico de las profesiones informáticas. A este respecto, algunos acuerdos interprofesionales tácitos u oficiales pueden constituir un freno eficaz.

El incumplimiento de las consignas de seguridad es también un hecho ético. Seguramente un conjunto de sanciones y una información preventiva de motivación limitarían este riesgo. Por último, los disturbios, las huelgas y/o la destrucción de los soportes de información son irregularidades que ameritan una protección física, mientras que las otras acciones (que se pueden calificar de morales) podrán limitarse o incluso hacerse desaparecer si se estudian a fondo los procesos de gestión informática.

Riesgos respecto de las personas

Dichos riegos están vinculados con la protección contra los otros riesgos e incluyen de manera simultánea una acción de sensibilización, formación y control.

La *acción de sensibilización* es informativa y presenta al personal los diferentes peligros a los cuales hay que enfrentarse y los medios que están

a su disposición para combatirlos; por ello, todo el personal, cualquiera que sea su posición jerárquica, debe conocer a la perfección el reglamento de las consignas de seguridad.

Cada quien debe ser advertido de sus responsabilidades en materia de seguridad respecto a sus colegas, equipos y trabajos. El personal de explotación (y en menor grado el de estudios y programación) debe tener conocimiento de los comandos manuales de alarma y de las condiciones de seguridad de los equipos, trabajos y programas, así como de las consignas a respetar en caso de siniestro), como los siguientes:

a) Operación de los medios de alarma.
b) Instalación de los primeros dispositivos de servicio y combate.
c) Modalidades de evacuación de los locales para las personas.
d) Consignas de guardia durante las horas de cierre de los locales: rondas, consignas de protección de primera urgencia (80% de los siniestros se declaran durante las horas de cierre).

La *acción de formación* implica para todo el personal la obligación de conocer el reglamento de seguridad y sujetarse a él, la selección de equipos de primera intervención, cuyos miembros tengan como objetivo combatir los siniestros, así como la formación de este personal en el uso de los medios de prevención y de servicio. Esta formación debe ser tanto teórica como práctica e incluir la disposición de las consignas de seguridad, eventualmente la constitución de un grupo de bomberos voluntarios que reciban una formación avanzada, así como la ejecución de ejercicios de alerta, operación de los medios de servicio y combate, al igual que la de ejercicios de evacuación mediante fuegos simulados. Una mención muy especial concierne a los accidentes de las personas y/o la electrocución, para los cuales se colocan letreros, además de otros implementos.

La *acción de control* comprueba la permanencia de la sensibilización y formación, de tal modo que asegure un firme conocimiento de las consignas y efectúe su actualización inmediata en el caso de modificaciones debidas a mutaciones y /o transformaciones.

Metodología de análisis y evaluación

Una de las técnicas nuevas para definir estos riesgos y proponer medidas de prevención consiste en revisar los recursos y activos de la empresa manejados por sistemas de información con el propósito de determinar su susceptibilidad de riesgos. Como resultado de ellos, un análisis proporcionará una relación de activos, clasificados en orden a la probabilidad de que ocurra una pérdida o daño; de su lectura se deriva una orientación de

esfuerzos de prevención con base en el costo de los bienes o activos y su vulnerabilidad.

Por lo que respecta a una metodología, ésta se puede desarrollar con apoyo en los siguientes pasos:

a) Revisar las medidas de seguridad existentes, lo cual implica que también sean identificados los activos protegidos.
b) Determinar el valor de los activos por proteger. Esto se hará en función del costo de pérdida y reposición de los activos si éstos fuesen destruidos, robados o deteriorados hasta dejarlos sin uso. A este respecto, cabe mencionar que como regla práctica no se consideran en la evaluación destrucciones parciales. Por otra parte, se pueden preparar cuestionarios que sirvan de base para una evaluación. En este caso, la decisión final se tomará según la recopilación de las respuestas a dichos cuestionarios.
c) Identificar los riesgos a que están expuestos.
d) Estimar la probabilidad de que ocurran. Este aspecto es el más subjetivo, pues depende de muchos factores para determinarla.
e) Cuantificar las pérdidas ocasionadas. Se recomienda formular una matriz de activos valuados contra riesgos probables.
f) Determinar los requerimientos de seguridad y recomendar las medidas de prevención consecuentes. Ésta es la parte más importante para la empresa, ya que de ella depende la reducción de riesgos.

De acuerdo con lo anterior, se estará en condiciones de elaborar un programa preventivo de riesgo. Para reducir los riesgos de mal funcionamiento del equipo informático, la temperatura del local se debe mantener uniforme y con un constante sistema de ventilación y aire acondicionado que pase por los cables de las máquinas al igual que por conductos de aspiración adecuados.

La empresa debe controlar la fuente eléctrica de la planta a fin de proteger el ambiente electromagnético e interrumpir la alimentación eléctrica cuando sea necesario. Debe haber una estrecha vigilancia en los locales informáticos que prevea rondas de vigilantes, así como una adecuada instalación de alarmas y medios de supervisión. Por otro lado, se deben proteger los locales informáticos contra fugas de agua importantes para disminuir los riesgos de inundación; por ello, es conveniente pasar por debajo del suelo los conductos y tuberías que llevan el agua y tomar toda clase de medidas de seguridad contra este riesgo que puede inutilizar el centro de cómputo. Asimismo, se debe contar con extintores de alto poder y detectores de agua, ya sean lineales (bandas lineales que se deslizan a los lugares de más probable aparición de agua) como las tuberías, o de niveles, llamados hidrómetros, que vigilan si hay agua en un punto bajo.

Los locales informáticos deben ser áreas restringidas con operativos de seguridad y custodios que limiten el acceso al local a fin de evitar cualquier tipo de daño o siniestro por un tercero. Cuando la empresa informática es muy grande, se pide que haya vigilancia automática por medio de video o televigilancia para detectar intrusiones, sabotaje o cambios de frecuencia, para lo cual se usan señales de luz infrarroja; debe haber también cerraduras con bandas de ondas. Los aseguradores deben llevar a cabo exámenes previos del equipo y todos sus componentes, de tal modo que certifiquen su buen funcionamiento y calidad.

Cabe destacar que lo antes expuesto es deseable, pero por desgracia, debido a la alta competencia existente, las compañías de seguros afrontan los riesgos sin llevar a cabo un detallado análisis y sin exigir de manera adecuada las medidas de seguridad necesarias, lo que trae como consecuencia una alta tasa de siniestros en el área informática.

En cuanto a los archivos y datos informáticos

Una vez que los programas han pasado las pruebas de validez se archivan en la computadora durante el proceso de extraer los datos para crear el programa o cuando éste se evalúa y luego se archiva, y pueden ser objeto de daños de diversa índole, como modificarse o alterarse los programas, lo cual trae consigo graves problemas y perjuicios; en consecuencia, la compañía aseguradora debe exigir la adopción de estrictas medidas de seguridad respecto a este tipo de riesgos. Consideramos que las medidas de seguridad más importantes aquí son: tener un control periódico del número de impulsiones de cada programa, llevando a cabo una comparación constante de códigos; asimismo, cuando hay sistemas de programas repartidos, prever el número de ellos a partir del sitio central para evitar la subderivación de programas, evitando que un mismo programador haga la entrada y salida de otro programa. Por otra parte, no se debe permitir que las terminales periféricas estén reconfiguradas como consola central, pero deben trabajar dos operadores juntos cuando haya cambio de valor de parámetros en la memoria.

El desvío de datos confidenciales tiene implicaciones muy severas en el ámbito del seguro, por lo cual la compañía aseguradora debe exigir que haya un estricto control de instrucciones que permitan analizar los archivos de los clientes, es decir, que tenga lugar dentro de eficaces medidas de seguridad con el control del sistema de operación. Asimismo, se deben criptar o cifrar los elementos clave de cada programa para que sólo tengan acceso a él los técnicos capacitados y encargados de ello.

Se pide también poner cuidado en borrar del sistema todas las "memorias" luego que se transmitió el programa al usuario. Se debe prever la

protección de los parámetros conservados en la memoria después de fallas en el sistema a fin de que no se vaya a hacer mal uso de esos datos; esta previsión debe tomarse en cuenta cuando se pasa un programa a otro sistema y quedan parámetros en la memoria del sistema anterior.

Se debe instalar un dispositivo de alarma muy especial cuando haya tentativas de conexión al sistema por terceros. También se ha de tener mucho cuidado en los sistemas de tiempo compartido de máquinas en cuanto al archivo de información por medio de claves y códigos para que no se presente la piratería de datos. Por otro lado, se debe vigilar que un programa no invada el desarrollo de otro.

En cuanto a los archivos informáticos, es importante proteger el acceso a los listados que versen acerca de la configuración y el procedimiento de aquéllos, vigilar que los sistemas de control de acceso a los archivos sean eficaces a fin de reducir los riesgos de intrusión, sabotaje, utilización indebida de los datos y programas contenidos en discos, así como el robo físico o de la información que contienen. Asimismo, debe haber consignas de seguridad muy estrechas para las salas de archivo y registros; por otra parte, cuando haya daños provocados por agua en los archivos, paralelo al aviso a la compañía de seguros del siniestro se debe realizar una copia de los documentos registrados en los archivos a fin de prever una oxidación de los medios magnéticos mojados. En Estados Unidos, las compañías de seguros exigen al asegurado un estricto control del centro de cómputo en cuanto a errores; degradación de la información, pérdida de confidencialidad y fraude.

Para prevenir los errores se pide un control de captura por duplicidad, tomando en cuenta su fecha de captura. Existe un manual de procedimientos y tratamiento de errores para prevenir los fraudes en los programas, y se exige un tratamiento de control sistemático estrechamente vigilado, así como la instauración de un procedimiento de acceso por código, clave y número de secuencia del mensaje; los códigos de habilitación deben guardarse en un lugar seguro. También se debe llevar un procedimiento de criptaje antes de la transmisión, para lo cual se requieren operadores y técnicos altamente capacitados. El asegurador debe dar a conocer toda la documentación, catálogos, manuales, contratos y garantías que dé el proveedor al asegurado.

En algunos países (como Francia) existe un controlador, quien se encarga, entre otras cosas, de evaluar los proyectos y verificar los programas, estructura e instalación de archivos y acceso a la información. Tal labor es muy importante antes de que la aseguradora tome un riesgo. El objetivo de esta persona es atenuar los riesgos hasta los límites de lo accidental o de lo imprevisible y que, cuando ocurra un siniestro, inspeccione y ajuste y, en caso de salvamento, se encargue de ellos a nombre y cuenta de la aseguradora.

Las prevenciones de todo tipo limitan los riesgos, pero no los evitan: por ello, es necesario instalar un plan de reinicio de actividades después de un siniestro, así como los medios de indemnización correspondientes.

El plan de reinicio de actividades debe incluir el establecimiento y actualización de una lista de centros informáticos periféricos que, ocupados de manera similar, puedan permitir la ejecución de los procesamientos. La lista de estos centros podrá completarse si se conocen las adaptaciones del software empleado en las configuraciones de apoyo, las horas disponibles en los equipos de estos centros y la adaptación de la planeación de la empresa a esos horarios, el volumen y la disposición de los locales que podrían obtenerse en préstamo, personal del que podría disponerse, tarifas de renta, así como de las cláusulas de los seguros.

Después de un siniestro hay que reemplazar los equipos parcial o totalmente destruidos y reconstituir las herramientas de trabajo (software, archivos, etc.). El plazo de reemplazo de los equipos debe ser objeto de una cláusula específica en el contrato de compra o de renta suscrito con el proveedor. La reconstitución de las herramientas de trabajo debe permitir la construcción de los programas y los archivos de todos los niveles. Sin las debidas precauciones, esta reconstrucción resulta difícil y por momentos imposible, por lo cual es indispensable duplicar los archivos y almacenar los duplicados en locales alejados del centro de procesamiento; empero, se requieren elementos aún más consolidados, según veremos a continuación, como erogar una prima, resarcir un daño o pagar una suma de dinero al verificarse la eventualidad prevista en el contrato.

LOS SEGUROS

A continuación se analizan los elementos generales del contrato de seguro, los cuales se encuentran señalados en la definición que da la ley.

Elementos personales

El asegurador

El asegurador es la persona que debe pagar la indemnización al ocurrir el siniestro; actúa como intermediario entre las diversas economías aseguradas para distribuir el daño sufrido por los afectados. En el derecho mexicano, el carácter empresarial del seguro es característica esencial del contrato; por tanto, sólo pueden ser aseguradores las empresas organizadas en la forma que la ley dispone.

El maestro César Vivante expresa que una empresa aseguradora es aquella que asume profesionalmente los riesgos ajenos, trata de reunir con

las contribuciones de los asegurados un fondo capaz de proporcionar los capitales prometidos a esos asegurados al vencimiento de las promesas, y extrae de los asegurados todo su capital industrial y éstos encuentran la mejor garantía de sus derechos en la integridad del fondo que ellos han suministrado.

El asegurado

El asegurado contrata con el asegurador y se compromete a pagar determinada cantidad a cambio de la prestación que recibirá llegado el caso y que resuelve la necesidad económica que crea la producción del riesgo. El asegurado puede atender la constitución de la relación contractual, el interés asegurado y el destino de las obligaciones del asegurador. La figura subjetiva constitutiva de la relación es la persona a cuyo nombre se celebra el contrato de seguro (contrayente); su consentimiento y capacidad son relevantes; sobre ella recaen por lo general las obligaciones del contrato y le corresponden ciertas facultades de disposición de la relación. Por otra parte, la figura subjetiva relativa al interés es la persona sobre cuyo ámbito patrimonial recae el riesgo y que, por ende, necesita el seguro: es la persona titular del interés asegurado.

El beneficiario

El beneficiario es la persona a quien se abona el dinero o se prestan los servicios que constituyen el contenido de la obligación del asegurador, pero no tiene un derecho propio sino derivado, no independiente sino sujeto a las contingencias del contrato por el asegurado.

Los destinatarios de la prestación del asegurador son aquellos a cuyo favor se ha estipulado el seguro: en el seguro de daños, generalmente el titular del interés asegurado; en el seguro de vida, en especial para el caso de muerte, un tercero. El beneficiario, como tal, no es el sujeto del contrato, sino un tercero, en quien (en consecuencia) al principio tampoco recaen obligaciones, pero le corresponde el derecho a la prestación del asegurador. Al beneficiario corresponde el derecho a la indemnización mediante el patrimonio del beneficiario; por transmisión intervivos (cesión); causa; o en cuanto titulares de intereses concurrentes (acreedores), que pasan de la cosa a la indemnización o de intereses coincidentes (copropietarios).

Elementos formales

A continuación incursionaremos en los elementos derivados en cuanto a la forma en el contrato de seguro. En el derecho mexicano, la redacción

por escrito del contrato de seguro constituye un requisito *ad probationem* (para fines de prueba), ya sea en documento público o privado, o se admite expresamente la confesional; la perfección del contrato es consensual y no puede sujetarse a la condición suspensiva que la entrega de la póliza de cualquier otro documento en que conste la aceptación, ni a la condición del pago de la prima.

Es conveniente citar una idea que esboza el maestro Ruiz Rueda, quien menciona que, aunque el contrato de seguro es uno de los contratos de adhesión más característicos, no por ello bastaría que una persona acudiera a una sociedad aseguradora para manifestar su aceptación de las condiciones de cualquier tipo de seguro con el fin de que éste se perfeccione, porque un contrato es en esencia un acuerdo de voluntades acerca de un objeto materia de él.

Las condiciones generales del contrato de seguro permanecen inmutables para dar uniformidad a todas las operaciones que se hagan en cuanto a aquél, pero existen condiciones particulares que abarcan riesgos especiales y que son objeto de negociaciones entre las partes porque determinan la extensión del riesgo que se cubre, la suma asegurada, la prima que corresponde de acuerdo con la tarifa aplicada, sus exclusiones, etcétera.

Por lo anterior, el futuro asegurado debe llenar un formulario de propuesta que contenga los requisitos establecidos en el artículo 7 de la *Ley del Contrato de Seguro* con el fin de manifestar su voluntad de celebrar un contrato definitivo de seguro. Para que el contrato se perfeccione bastará que el asegurador declare que acepta lisa y llanamente la oferta, no sin antes haber analizado el riesgo a cubrir. Es frecuente que el contrato de seguro se celebre con la intervención de agentes de seguros, quienes explican las operaciones al cliente y le proporcionan los formularios.

El contrato de seguro se celebra por correspondencia la mayoría de las veces; a su vez, la empresa aseguradora necesita recabar la información relativa a las circunstancias y los hechos importantes para apreciar la magnitud del riesgo; además, pide la mayor parte de la documentación por correo y cuando así se requiere envía técnicos especializados para que decidan si se acepta o se rechaza el riesgo.

Desde que se perfecciona el contrato de seguro entra en vigor para ambas partes y obliga a los contratantes a cumplir lo expresamente pactado y a las consecuencias que dicho acuerdo de voluntades origine. La forma no puede considerarse. En relación con el contrato de seguro, no puede considerarse que la forma sea un elemento de validez.

Elementos reales

En el presente tema es oportuno resaltar este tipo de elementos denle el contrato de seguro.

Objetos asegurables

Se aseguran los intereses que tienen relación con determinados objeto o personas, es decir, se aseguran los intereses que existen sobre las personas y sobre toda clase de cosas. Es indispensable que los contratantes designen la cosa o persona respecto de la cual existe el interés asegurado. Cosas asegurables por haber un interés en ellas son todas las corporales (responsabilidad, crédito, cambio y seguro de seguros). Para asegurarse, las personas han de reunir condiciones de capacidad. Pueden asegurarse varios intereses sobre una cosa y también uno o varios intereses sobre varias cosas consideradas como unidad, por ejemplo: el seguro de personas (seguro de grupo).

La póliza

Las leyes en materia de seguros imponen a las empresas aseguradoras la obligación de redactar y entregar al contratante del seguro una póliza en la que consten los derechos y obligaciones de las partes. La póliza debe contener, entre otros, los siguientes elementos:

- Los nombres, domicilios de los contratantes y firma de la empresa aseguradora.
- La designación de la cosa o de la persona asegurada.
- La naturaleza de los riesgos garantizados.
- El momento a partir del cual se garantizan el riesgo y la duración de esta garantía.
- El monto de la garantía.
- La cuota o prima del seguro.
- Las demás cláusulas que deban figurar en la póliza de acuerdo con las disposiciones legales, así como las convenidas lícitamente por los contratantes.

La compañía de seguros tiene la obligación de expedir, a solicitud y por cuenta del asegurado, copia o duplicado de la póliza. El valor de la póliza es en esencia comprobatorio.

Existe otro documento que expide el asegurador para servir de prueba por cualquier modificación que se haga al contrato; en Estados Unidos se conoce como *endorsement* y en México se llama *endoso*. En él consta cualquier cláusula adicional que contenga la póliza de seguro.

Las leyes de seguros establecen que las pólizas de seguro pueden ser nominativas, a la orden o al portador. Que una póliza pueda endosarse o transmitirse la garantía del asegurador junto con los bienes expuestos al riesgo asegurado ha causado el problema de su naturaleza jurídica (concretamente de si es o no título de crédito).

En el derecho mexicano no es posible considerar que la póliza de seguro pueda tener el carácter de título de crédito, porque está configurada como documento comprobatorio del contrato de seguro. Por tanto, la póliza es no sólo un documento de los que la doctrina llama declarativos, sino también una prueba testimonial porque representa una declaración de verdad escrita. Los títulos de crédito son una especie particular de documentos constitutivos, y si en derecho la póliza de seguro (según la *Ley de Seguros*) sólo es un documento probatorio y no constitutivo, no se puede considerar que es un título de crédito.

La prima

La prima es la principal obligación del asegurado y constituye un elemento esencial del contrato. Se calcula en función del tiempo de exposición al riesgo que tiene la suma asegurada y de la gravedad e intensidad de él. El artículo 34 de la *Ley del Contrato de Seguro* llama *periodo de seguro* el lapso para el cual resulta calculada la unidad de la prima.

Ese lapso es casi siempre de un año. Es importante mencionar el principio de indivisibilidad de la prima, pues ésta se debe calcular íntegra. "Salvo estipulación en contrario, la prima convenida para el periodo en curso se adeudará en su totalidad, aun cuando la empresa aseguradora haya cubierto el riesgo sólo durante una parte de ese tiempo."

El deudor de la prima es el contratante del seguro, pero la obligación se extiende al tercero por cuya cuenta se contrata. El beneficiario del seguro se convierte en deudor de la prima cuando el siniestro se produzca. La ley autoriza a las partes que intervienen en este contrato a pactar el pago de la firma anual en forma fraccionada. Como el contrato de seguro es consensual, su vigencia no puede condicionarse al pago de la prima inicial. La ley concede 30 días como plazo para el pago de la prima. Si no se realiza, se extinguirá el contrato al sobrevenir la condición resolutoria legal. La ley lo señala así:

En el seguro de cosas gravadas con privilegios, hipotecas o prendas, los acreedores privilegiados hipotecarios o prendarios se subrogarán de pleno derecho en la indemnización hasta el importe de crédito garantizado por tales gravámenes. Sin embargo, el pago hecho a otra persona será válido cuando se haga sin oposición de los acreedores y en la póliza no aparezca mencionada la hipoteca, prenda o privilegio, ni estos gravámenes se hayan comunicado a la empresa aseguradora.

Los siniestros

El riesgo (amenaza de daño) es universal o general, pero el siniestro (la realización del daño temido) es particular. "Siniestro es la realización del

riesgo que amenazaba a una persona." A este respecto Fanelli añade que "si el riesgo es el evento que actualiza la responsabilidad del asegurador, mientras no se realicen todas las condiciones de hecho capaces de convertir en actual la obligación del asegurador, no puede hablarse de que haya un siniestro".

La garantía o el riesgo asumido por el asegurador se limita por la ley o convencionalmente por las partes en relación con muchos factores (como el tiempo) o por el objeto del riesgo, porque se garantiza contra el riesgo que amenaza a una persona o una cosa determinada. También existe la limitación territorial, la cual consiste en que el asegurador garantiza sólo cuando el evento afecte a personas o cosas que se encuentren en determinados lugares; otra limitación es por la naturaleza del riesgo o cuando el evento se realiza en determinadas circunstancias.

El asegurado tiene el deber de informar a la empresa aseguradora que se ha producido el siniestro en los términos establecidos. Cabe decir que muchas veces al denunciar el siniestro no es posible que el asegurado dé toda la información; empero, las leyes disponen que es obligación del asegurado proporcionar a la compañía de seguros toda la información y documentos de los hechos relacionados con el siniestro para que ésta analice cuidadosamente e indemnice al siniestrado.

El siniestro fortuito es típicamente el destinado a ser cubierto por el seguro, pero con la extensión del principio de la responsabilidad. La ley previene que la empresa aseguradora responderá del siniestro aun cuando éste haya sido causado por culpa del asegurado, y sólo se admite en el contrato la cláusula que libere al asegurador en caso de culpa grave del asegurado. En estos términos, la ley condena en general todo afán de lucro que el asegurado pueda tener con la finalidad de acelerar un contrato de seguro contra daños.

CARACTERÍSTICAS DEL CONTRATO DE SEGURO

El contrato de seguro es *bilateral*, pues aun cuando la obligación principal de la empresa de resarcir un daño o pagar una suma de dinero depende para su existencia de verificar la eventualidad prevista, la empresa contrae la obligación, en virtud del contrato, de expedir la póliza y entregarla al asegurado.

Por otra parte, el asegurado está obligado a pagar la prima como contraprestación, sin que ello dependa de ninguna condición. Por tanto, el contrato genera obligaciones para ambas partes. Como el contrato de seguro establece provechos y gravámenes, será siempre oneroso. Esto se explica porque el resarcimiento del daño o el pago de una suma de dinero y el pago de la prima son gravámenes que constituyen provechos para la otra parte.

Dicho contrato es también *aleatorio* pues, en cuanto a la empresa aseguradora, "la prestación debida depende de un acontecimiento incierto, lo que constituye la nota distintiva de este tipo de contratos"! Dado que la obligación del asegurado es condicional y, según las leyes de seguros, no puede sujetarse a la condición del pago de la prima, el contrato es *consensual* en oposición al real y también consensual en oposición al formal, puesto que su validez no depende de ninguna formalidad o solemnidad.

La naturaleza de la obligación de la empresa aseguradora impone la noción de que se trata de un contrato *sucesivo*, porque es característica de toda condición que su realización o cumplimiento sea, además de posible, probable. En consecuencia, la realización de la eventualidad prevista para un solo instante determinado restringiría toda probabilidad de ver actualizada la obligación de la empresa, por lo cual el contrato de seguro siempre comprende o ampara un periodo más o menos largo que es determinado o determinable.

El contrato de seguro es *principal*, en virtud de que existe por sí solo. En general, los contratos accesorios tienen como finalidad establecer derechos igualmente accesorios de garantías de obligaciones. Es frecuente asegurar una cosa o contratar un seguro sobre la vida de un tercero a fin de dar seguridad a un crédito; no obstante, incluso en esos casos el contrato aún es principal porque no sigue la suerte del contrato que dio origen al crédito.

Seguridad informática

Prever un riesgo es controlar el perjuicio financiero que viene aparejado a su realización, de aquí que toda empresa deba controlar sus riesgos de acuerdo con su capacidad financiera, al hacer frente a las variaciones de dichos riesgos y cuidar que no exceda su presupuesto o activo si el siniestro llegara a suceder. Si se estudian los riesgos que pueden convertirse en siniestros o desastres informáticos en una compañía, se puede cuantificar su rentabilidad para solventarlos o añadir a una cobertura de seguro que proteja esa incertidumbre.

Es posible, en gran medida, que una empresa informática aplique tratamientos preventivos para suprimir o disminuir los riesgos, por ejemplo: la protección del centro de cómputo contra factores externos, control de cargas caloríficas en ellas o cualquier agente transmisor de circuitos o sobrecalentamientos, emplazamiento de extintores y muros contra fuego, supresión de aparatos o vías que canalicen agua hacia el interior del local, estrechamiento de seguridad contra sabotaje, empleo de técnicos expertos para el buen funcionamiento de los equipos, aseguramiento de los soportes que contienen o reproducir la información y el control en archivos separados, instalación de protecciones técnicas para los programas, supervisión adecuada de equipos y programas, etcétera.

Como se observa, la necesidad de que las empresas de computación o las compañías que emplean bienes o servicios informáticos recurran a los contratos de seguro para que éstos cubran o respalden la gama de riesgos informáticos existentes se convierte en imperioso menester.

En materia informático-contractual se denomina *agente de transformación* a la compañía aseguradora. Entre los agentes de transformación más conocidos están los aseguradores, los especuladores sobre los mercados a término, los agentes de seguros, los banqueros, etc. Las consecuencias financieras de un siniestro informático se aprecian según se trate de un daño al equipo, pérdida de control de confiabilidad en los tratamientos, o perjuicios causados a terceros. En este sentido, el perjuicio financiero se analiza según se trate de un perjuicio directo (costo del material destruido), un perjuicio consecutivo (el monto del margen beneficiario no realizado) o un perjuicio indirecto (la pérdida de mercado o del cliente).

En general se aseguran los perjuicios directos y consecutivos; no obstante, los riesgos informáticos ocasionan en su mayoría perjuicios indirectos, por lo que el ramo del seguro especializado en riesgos informáticos necesita una verídica apreciación del riesgo para que el asegurado lo cubra correctamente. Si el uso de los procesos de la informática no presenta factores de riesgo considerables, no serán por tanto motivo de tan exhaustiva precaución y bastará con cubrir los posibles riesgos mínimos; por otro lado, si los riesgos informáticos son mayores y significativos, en este caso sí justifican una prevención elaborada y eficaz, así como la necesidad de contratos de seguros de máxima cobertura adecuadamente adaptados a los requerimientos.

Algunos de los riesgos generales usualmente asegurables son el incendio y /o explosión, el humo sin incendio, la rotura de máquina por funcionamiento propio o por intervención externa, los daños eléctricos por corte de la alimentación o destrucción parcial de la planta; huelgas, motines, pillaje y sabotaje; tempestad, huracán y terremoto, al igual que los "riesgos magnéticos", en especial los provocados por tormenta magnética.

Un contrato de seguro de la forma "todo riesgo, salvo..." sólo limita esta lista en la medida en que todo siniestro que no entre en una exclusión esté cubierto. Un tratamiento de transformación es aquel en el que los riesgos permiten transferir la viabilidad en costo, por la intervención de una tercera parte, llamada *agente de transformación*.

El número y el tipo de exclusiones varían con las sociedades de seguros y los contratos que ellas proponen. Ciertos riesgos están excluidos de manera legal, como los siguientes:

1. Los no asegurables por ser contrarios al orden público (hecho intencional o doloso del asegurado o siniestro voluntario por la beneficiaria del contrato).

2. Los no previsibles y sin factor accidental (uso normal de los bienes asegurados, sequedad o humedad, exceso de temperatura, corrosión, oxidación, acumulación de polvo, a menos que estos hechos no resulten de daños materiales no excluidos y/o sean causados por la instalación del aire acondicionado).
3. Los que no presentan en un caso normal interés de cobertura (guerra civil o extranjera, secuestro, captura o destrucción en virtud de los reglamentos aduanales; destrucción, confiscación o requisa por órdenes de las autoridades civiles o militares, así como efectos directos o indirectos de la radiactividad).
4. Los que presentan interés de cobertura sólo por su aspecto específico (daños debidos a radiaciones provocadas por la aceleración de partículas o el disparo intempestivo de las instalaciones automáticas de protección).

Cabe mencionar que los dos últimos grupos de riesgos podrán cubrirse si se plantean estipulaciones particulares y sobreprimas. La vulnerabilidad de los bienes y las personas depende del valor que se dé a estas nociones y de los riesgos de exposición a los peligros contra los cuales se desea protegerlos. El costo de la vida humana es invaluable, por lo cual es ocioso analizar dicho aspecto en este libro.

Por el contrario, el valor de los bienes es más fácil de medir y representa lo que la empresa consentiría en pagar para reconstruir el (o los) bien(es) donado(s). El valor de los locales o de los equipos se puede estimar con relativa facilidad; empero, la destrucción de los archivos y las pérdidas de explotación revisten dificultades. Por ello, es difícil determinar con exactitud las sumas a invertir para obtener un costo de seguridad aceptable en determinadas condiciones de restitución. Dicho costo es resultante del gasto real efectuado para medir la seguridad y del riesgo de gastos en caso de daños.

Por otra parte, el presupuesto de la seguridad, cualquiera que sea su monto, incluye dos elementos: el primero cubre los equipos y el mantenimiento, en tanto que el segundo prevé el costo de recuperación después de un siniestro.

Como resultado de un siniestro, las consecuencias financieras asumidas por las aseguradoras son las siguientes:

- Reparación o reemplazo de los edificios, equipos, materias primas, productos terminados, modelos, diseños y documentos técnicos.
- Recursos de las víctimas o sus parientes en lo que se refiere a sus personas.
- Erogaciones de demolición.
- Reconstitución de los archivos informáticos.

- Erogaciones suplementarias ocasionadas por la reparación.
- Pérdidas de explotación.
- Intereses sobre cuentas pendientes.

Ahora bien, ciertas pérdidas no siempre están cubiertas, como es el caso de clientes insatisfechos o descontentos, dificultades de reconstrucción (fin del alquiler, depreciación por antigüedad, etc.) o pérdida de empleo total o parcial del personal. El reemplazo de los equipos depende del modo de adquisición. Si se trata de equipos rentados al proveedor, éste acompañará a su propuesta un contrato de aseguramiento. En todos los casos, el nombre del usuario debe aparecer como coasegurado en el contrato a fin de evitar que el seguro no se torne contra él en caso de siniestro. En razón de la rápida obsolescencia de ciertos equipos, siempre deberá considerarse que son nuevos.

El reemplazo de las materias primas, productos terminados, modelos, dibujos y documentos técnicos está vinculado con la reconstitución de los archivos informáticos. Ciertas aseguradoras no aceptan el pago del costo de reemplazo de los expedientes de análisis y programación; en consecuencia, éstos deben almacenarse por duplicado en locales diferentes. Las erogaciones suplementarias originadas por la reparación son siempre muy importantes. La evaluación del monto de dichos gastos estará a cargo de los informáticos de la empresa. Las pérdidas de explotación deben cubrir la eventual caída de la cifra de negocios durante el periodo de reconstitución. Los intereses sobre cuentas pendientes se deben a la imposibilidad de la empresa de facturar a sus clientes con motivo del siniestro. El problema financiero resultante puede compensarse por un apoyo bancario del que algunas aseguradoras aceptan pagar los intereses.

Pólizas aplicables

Pólizas convencionales

En México no existe propiamente un contrato de seguro específico que proteja en estos casos, de ahí que se adopten pólizas que estén en el mercado para cubrir los riesgos informáticos. La informática es una materia de reciente aparición en el país. Las industrias de cómputo se han desarrollado con rapidez y han hecho necesaria una adecuada cobertura especializada en materia de seguros referida a este particular, basada en un principio de análisis y estadísticas que demuestran el alto grado de incidencia de siniestros en materia informática.

Los seguros que podrían tener aplicación frente a este problema son los siguientes:

- La póliza de seguro múltiple para empresas, que abarca las siguientes coberturas:

  a) Seguro contra incendio.
  b) Seguro de responsabilidad civil general.
  c) Seguro contra robos.
  d) Protección contra gas neón.
  e) Seguro de cristales.

- La póliza de seguro de equipo electrónico.
- La póliza de transportes.

A continuación se analizan con detalle cada una de estas figuras:

1. Póliza de seguro múltiple para empresas

Esta póliza incluye varias coberturas para empresas según su giro; es una de las innovaciones más recientes en materia de seguros que se han vendido mucho en el mercado a tarifas accesibles. Cubre varios de los riesgos de tipo informático, como el riesgo de incendio, que según estadísticas tiene una incidencia media alta en las industrias; cubre también la responsabilidad civil de la empresa frente a terceros, que en su mayoría son clientes de las empresas informáticas. En esta cobertura se adecuan múltiples riesgos que serían altamente costosos para la empresa en caso de carecer de un contrato de seguro. Otro riesgo por cubrir es el robo, tema muy controvertido que se tratará a fondo para buscar una cobertura de seguro que convenga a la protección de anuncios luminosos y de cristales, los cuales están expuestos continuamente a riesgos, pues muchos locales informáticos se hallan instalados entre muros de cristal.

a) Seguro contra incendio

Esta cobertura es una de las más importantes con las que debe contar la empresa, pues un centro de cómputo está expuesto de manera constante a cortocircuitos, cambios bruscos de voltaje, explosiones y casos fortuitos, como un rayo que dañe o destruya el sistema, además de otras eventualidades.

b) Seguro de responsabilidad general

El riesgo que cubre este seguro es la responsabilidad de resarcir el daño patrimonial causado a un sujeto jurídico, al cual indemniza. Es un seguro de terceros. La responsabilidad civil general de una empresa informática se halla entre la clasificación de riesgos profesionales distintos del trabajo; este seguro tiene como finalidad reparar los daños ocasionados por el asegurado.

Dicho seguro es una cobertura imprescindible para cualquier empresa, incluidas las informáticas, pues los riesgos que pueden afectar a terceros, sobre todo a los clientes, son muchos, variados y costosos. Por citar algunos riesgos protegidos por este seguro en cuanto a una empresa informática están el daño o perjuicio que pueda ocasionar un programa elaborado por la empresa, la pérdida de datos confidenciales que el cliente haya transmitido a la empresa para que se le hiciera un programa, el mal uso de los datos confidenciales del cliente en los locales de la empresa o su extracción o pillaje, la destrucción de los soportes o bandas que contengan la información y los programas, la alteración o malversación de datos por operadores de la empresa, etcétera.

c) Seguro contra robos

El seguro contra robo se vende con dos coberturas: contra el robo de mercancías con violencia y/o asalto y contra el robo de dinero y valores.

El primero cubre las mercancías, productos terminados o en proceso, mobiliario, útiles, accesorios y demás equipo propio y necesario al negocio del asegurado mientras se encuentren dentro del edificio (dicha ubicación debe mencionarse en la carátula de la póliza). Asimismo, contra pérdidas o daños causados a los bienes como consecuencia de robo perpetrado por personas que, al usar la violencia del exterior al interior del local donde se encuentran los bienes asegurados, dejen señales visibles de violencia en el lugar por donde penetraron, así como a los bienes inmuebles; cubre también el intento de tal robo siempre que se dejen señales visibles de violencia en el lugar por donde se penetró, así como el robo por asalto dentro del inmueble mediante el uso de la fuerza o de violencia.

Es aconsejable que una compañía informática contrate ambas coberturas. La compañía no será responsable de pérdidas o daño alguno por robo en el que intervengan personas por las cuales el asegurado es civilmente responsable. Tampoco cuando el asegurado no mantenga una contabilidad en su negocio para determinar con exactitud el monto de la pérdida o daño y robo de cheques, letras, pagarés y demás documentos, contenidos de cajas fuertes, bóvedas o cajas registradoras; tampoco cubre las pérdidas causadas por robo que cometan los huelguistas o motines de obreros, alborotos populares, vandalismos, etcétera.

La compañía de seguros pagará de manera íntegra el importe de los daños sufridos hasta el monto de la suma asegurada siempre que el asegurado mantenga la cantidad mínima asegurada, la cual,

en caso de siniestro, el asegurado se obliga a reintegrar cuando haya sido indemnizado y pagará la prima adicional que corresponda. Si al ocurrir el siniestro los bienes tienen en conjunto un valor total superior a la cantidad asegurada, el seguro responderá sólo en forma proporcional al daño causado.

Respecto a la póliza de seguro contra robo de dinero y /o valores; es importante mencionar que se cubre dinero en efectivo en metálico o billetes de banco, valores u otros documentos negociables, como letras de cambio, pagarés, cheques, acciones, bonos hipotecarios, etc., y quedan cubiertos hasta por la cantidad de la suma asegurada dentro del local en cajas fuertes o de seguridad, cajas registradoras o colectoras o en poder de cajeros, pagadores, cobradores o de cualquier otro empleado dentro del local o en tránsito contra los siguientes riesgos: robo o intento de robo perpetrado con violencia, robo por asalto o intento de asalto en el local asegurado o sobre las personas encargadas de manejar los bienes asegurados mediante el uso de la fuerza o violencia moral o física, pérdidas de los bienes en las cajas fuertes causadas por explosión; pérdidas o robo de los bienes por enfermedad repentina o causada por un accidente que produzca pérdida del conocimiento, lesiones corporales o la muerte a las personas encargadas de manejar el dinero o los valores; también cubre la pérdida o robo de los bienes cuando el automóvil en el que viajaba el encargado de los bienes sufre un accidente, como colisión, volcadura, explosión, etcétera.

Dicho seguro no cubre las pérdidas o los daños causados a los bienes asegurados por robo sin violencia, extravío y desaparición misteriosa, huelguistas, bienes que no se encuentren físicamente en poder de la persona o personas encargadas de su custodia; tampoco cubrirá cuando el asegurado no tenga una contabilidad para determinar con exactitud el monto de las pérdidas o por acto fraudulento o abuso de confianza cometido por el asegurado, cajeros, pagadores, cobradores o cualquier otro de sus empleados. La compañía de seguros no se hace responsable en lo que respecta a valores por una suma superior al valor real en efectivo que estos valores tengan al concluir las operaciones de negocios el día anterior en que la pérdida se haya descubierto; cuando sean títulos nominativos, la pérdida a cargo de la aseguradora se limitará al costo de los gastos judiciales y de reimpresión para lograr la anulación de los títulos extraviados y su reposición por otros nuevos.

La aseguradora indemnizará la totalidad de las pérdidas o los daños a los bienes asegurados hasta por los límites de responsabilidad establecidos en la póliza sin exceder del interés económico que tenga el asegurado en los bienes al suceder el siniestro ni del valor real del mercado.

Debe quedar claro que, en caso de litigio, el asegurado debe proporcionar todos los datos y pruebas necesarias para la defensa de todo procedimiento civil y penal.

d) Protección contra gas neón

Esta cobertura ampara los anuncios luminosos contra todo riesgo por cualquier pérdida o daño causados mientras se encuentren instalados y fijos en el domicilio que se señala en la póliza. Tal seguro no cubre el uso, desgaste o depreciación normal o causado por vicio propio, cortocircuitos o desarreglos eléctricos mientras no causen un incendio, así como los trabajos de los operarios ocupados en la construcción, demolición, cambio o reparación del edificio en el que esté colocado el rótulo.

Dicha cobertura podría ser útil para los anuncios luminosos de una empresa informática prestadora de bienes o servicios.

e) Seguro de cristales

Este seguro cubre la rotura accidental de cristales del edificio, pero no, salvo convenio expreso, los daños y pérdidas materiales causados por remoción de los cristales mientras no queden debidamente colocados, el decorado del cristal por reparaciones, así como las alteraciones o mejoras al edificio o a los cristales asegurados. En caso de siniestro, la indemnización abarcará el costo de los cristales y gastos de instalación.

Esta póliza ha sido útil para las empresas y reviste importancia para un centro de cómputo cuando se encuentre rodeado de una coraza de cristal que pueda sufrir este tipo de riesgos.

2. Póliza para equipos electrónicos

Otra cobertura considerada importante respecto a los seguros existentes en México es la póliza para equipos electrónicos que se vende a industrias de este ramo y que cubre riesgos análogos a los de una industria informática. Los riesgos que se pueden cubrir con esta póliza en un centro de cómputo serían el mal funcionamiento o no funcionamiento del sistema, las fallas electromagnéticas y los cambios de voltaje y daños a los sistemas directrices, los cuales implican un alto costo de reparación.

La citada póliza señala que, cuando la instalación y la puesta en marcha de los bienes asegurados haya finalizado de manera satisfactoria, este seguro se aplicará ya sea que los bienes estén operando o se encuentren en reposo, hayan sido desmontados con el propósito de limpiarlos o repararlos o mientras sean trasladados dentro de los

predios o locales. No se indemnizará al asegurado en casos de guerra, invasión, guerra civil, actividades del enemigo extranjero, huelga, paro, conmoción civil, poder militar, grupos de personas maliciosas que provoquen daños, reacción nuclear, actos intencionales o negligencia manifestada por el asegurado o sus representantes. La responsabilidad de la aseguradora procederá sólo si se cumplen los términos de la póliza en lo relativo a cualquier cosa que deba hacer o cumplir el asegurado y en la veracidad de sus declaraciones. El asegurado debe tomar todas las precauciones razonables y cumplir con las recomendaciones que le haga la aseguradora.

Los aseguradores o sus representantes podrán inspeccionar y examinar el riesgo. Por otra parte, el asegurado deberá facilitarles todos los detalles o informaciones que requieran. Asimismo, el asegurado debe notificar de inmediato cualquier agravación del riesgo y, si es necesario, se ajustarán el alcance de la cobertura y la prima. Al ocurrir cualquier siniestro que pudiera dar lugar a una reclamación, el asegurado deberá notificar a la aseguradora inmediatamente por teléfono y luego confirmar por escrito, indicando la naturaleza y la extensión de las pérdidas o daños, así como tomar todas las medidas, dentro de sus posibilidades, para minimizar la extensión de la pérdida o daño, conservar las partes dañadas y ponerlas a disposición de un representante o experto de los aseguradores para su inspección; además, deberá suministrar la información y pruebas documentales que se le requieran. La aseguradora no será responsable por pérdida o daño de los cuales no haya recibido notificación dentro de los 14 días posteriores a su realización. Asimismo, los ajustadores deben inspeccionar la pérdida o el daño antes de que se efectúen las reparaciones o alteraciones; la responsabilidad de la aseguradora cesará si los bienes dañados continúan operando sin haber sido reparados.

En caso de existir diferencias entre el asegurado y el asegurador se pedirá la intervención de un árbitro. Los beneficios de esta cobertura se perderán si el cuestionario llenado por el asegurado no corresponde a las realidades existentes o si la reclamación fuere fraudulenta o se hicieren declaraciones falsas para apoyar la reclamación. La indemnización será pagadera a un mes después de que los aseguradores hayan determinado la cantidad total por pagar.

Esta póliza cubre específicamente los siguientes daños materiales: los bienes asegurados o cualquier parte de ellos por cortocircuito, azogamiento, arco voltaico, perturbaciones por campos magnéticos, aislamiento insuficiente, sobretensiones causadas por rayos, tostación de aislamientos, humo, hollín, gases, líquidos o polvos corrosivos, inundación, acción del agua y humedad, errores de construcción, fallas de montaje, defectos de los materiales, errores de manejo, descuido, impericia, así como daños malintencionados y dolo de terceros.

Existe un deducible o franquicia a cargo del asegurado fijado por él y se señala en la póliza. La compañía aseguradora no cubrirá las pérdidas o daños que sean consecuencia directa del funcionamiento continuo, desgaste, cavitación, erosión, corrosión o deterioro gradual debido a condiciones atmosféricas, ni los gastos erogados respecto al mantenimiento de los bienes asegurados, ni las pérdidas o daños cuya responsabilidad recaiga en el fabricante o el proveedor de los bienes asegurados (ya sea legal o contractualmente), ni los defectos estéticos.

Es requisito indispensable de este seguro que la suma asegurada sea igual al valor de reposición del bien asegurado por otro bien nuevo de la misma clase y capacidad. Cuando se puedan reparar los daños ocurridos a los bienes asegurados, los aseguradores indemnizarán aquellos gastos que sea necesario erogar para dejar la unidad dañada en las condiciones existentes antes de ocurrir el daño, en cuyo caso se tomará en cuenta el valor de cualquier salvamento que se produzca.

Una cláusula establece que los aseguradores acuerdan con el asegurado que si un daño material indemnizable diera lugar a una interrupción parcial o total de la operación del sistema electrónico, los aseguradores indemnizarán al asegurado por cualquier gasto adicional que el asegurado compruebe haber desembolsado al usar un sistema electrónico de procesamiento de datos ajeno y suplente. Es importante mencionar que gran parte de los riesgos que cubre esta póliza son de tipo informático, por lo cual aquí se ha hecho su estudio.

3. Póliza de seguro de transportes

Existe una póliza de seguro de transportes con condiciones generales, la cual se vende a empresas que transportan continuamente sus mercancías de un estado a otro o en actividades de importación y exportación al extranjero. Respecto a una empresa informática, contratar una póliza de seguro de transportes que cubra riesgos especiales cada que se realice un flete o embarque será suficiente. Este seguro se aplicará para el transporte del equipo al adquirirse de un estado a otro o en la misma ciudad con el fin de que vaya asegurado.

Se contrata una póliza específica por cada embarque o transporte de equipo, en cuyo caso debe señalarse la suma asegurada y fijar el asegurador la prima a pagar con base en dicho monto; por otra parte, ha de describirse el bien que se va a transportar, de tal modo que se especifiquen el medio de comunicación, así como el lugar de origen y el de destino.

Dicha póliza cubre los siguientes riesgos encontrados en las condiciones generales: daños materiales a los bienes causados por incendio, rayo y explosión, por caída de aviones, volcadura, colisión o descarri-

lamiento del vehículo u otro medio de transporte empleado, incluido el hundimiento o rotura de puentes. Se cubren también al sobrevenir desviación, cambio de ruta, transbordo u otra variación del viaje en razón del ejercicio de facultades concedidas al armador o porteador conforme al contrato de transporte, así como la omisión voluntaria o error al describir los bienes, el buque o el vehículo del viaje.

Cabe mencionar al respecto que si durante el transporte sobrevienen circunstancias anormales que hicieren necesario que entre los puntos de origen y destino los bienes quedasen almacenados o estacionados en bodegas, muelles o plataformas, el seguro continuará en vigor y el asegurado pagará la prima adicional que corresponda. El asegurado debe definir contra qué riesgos de los señalados en la póliza se ha de cubrir, ya sean robo de bulto por entero, robo parcial, mojadura de agua dulce, de mar o de ambas, contacto con otras cargas, manchas, oxidación, rotura, mermas y/o derrames, todo riesgo, ganado, huelgas y alborotos populares, embarques marítimos, terrestres o aéreos, bodega a bodega para embarques terrestres y aéreos, etc. Aquí se fija tradicionalmente de 1 a 31% como deducible sobre el valor total de la mercancía transportada o, en su caso, del monto de lo reclamado.

Pólizas específicas o particulares

El objetivo del presente estudio es sugerir la creación de una póliza de seguro especial que cubra los riesgos informáticos en su totalidad. En incisos anteriores se realizó un estudio comparativo de las pólizas de seguro que existen en el mercado, las cuales contienen coberturas factibles de aplicar para asegurar ciertos riesgos informáticos, algunos asimilables a los proveedores de bienes y servicios y otros a los usuarios.

La idea es que, con base en las pólizas existentes, se unifiquen y nazca una nueva, la cual deberá completarse con varias cláusulas a nivel general de dichos riesgos.

La sociedad mexicana ha empleado la informática a un ritmo muy acelerado en los últimos años, a la vez que grandes y pequeñas empresas poseen ya sus equipos de cómputo en los cuales invierten sumas considerables; por ello, es fundamental contratar adecuadas coberturas de seguro para proteger tanto los equipos como la información que manejan. Al ser estos riesgos aspectos nuevos en el campo del seguro, es indispensable que técnicos especializados realicen un minucioso análisis para estudiar de qué forma se pueden cubrir tanto en sus límites como en sus excepciones.

Es muy importante que los proveedores informáticos sean honestos, sobre todo al declarar los riesgos a los que están expuestos los bienes o servicios que ofrecen, es decir, que comuniquen circunstancias y situacio-

nes en forma verídica, para que permitan a la aseguradora observar esos riesgos y fijar una suma asegurada real respecto a archivos, programas, datos, etcétera.

Las compañías aseguradoras deberán contratar a técnicos ajustadores especializados que no sólo analicen los riesgos informáticos por cubrir, sino también exijan que se cumpla con las estructuras y medidas de seguridad para prevenir los daños y que ellos lleven a cabo los ajustes cuando sobrevenga un siniestro. Por otra parte, es conveniente realizar visitas para controlar la seguridad y el buen funcionamiento de los centros de cómputo.

Ahora bien, es importante que el usuario o cliente adquiera una cobertura de seguro al negociar con el proveedor la adquisición o renta del equipo informático, ya que, como se ha visto, los contratos informáticos y su carácter de adhesión presentan desventajas para el usuario. Por ello, es aconsejable contratar un seguro para cubrir el incumplimiento del proveedor en cuanto a las cláusulas pactadas, así como las garantías no establecidas en el contrato.

En resumen, se propone que, después de un detallado análisis al respecto, salga al mercado de seguros una póliza específica que cubra todos los riesgos informáticos existentes, la cual deberá contener un clausulado general con coberturas específicas y algunos endosos (todo ello extraído de las pólizas existentes más cláusulas especiales), a fin de que los proveedores y usuarios en su caso puedan cubrir ampliamente sus riesgos.

Dicha póliza deberá cubrir una gran variación de riesgos; en primer término: aplicar las cláusulas o condiciones generales de la póliza de seguro múltiple para empresas; asimismo, una cobertura para riesgos de incendio y rayos como actualmente existe, e incluir en las condiciones generales de la póliza las coberturas de riesgos informáticos en cuanto a granizo, ciclón, huracán, humo, filtraciones de agua, terremotos y erupción volcánica. Sin duda, la elaboración de pólizas específicas o particulares en torno a los riesgos informáticos es una labor difícil, y a pesar de que en algunos países occidentales como Francia se trabajan arduamente al respecto e incluso existen pólizas de seguros aplicables, aún queda mucho por hacer (sobre todo en México) a fin de atenuar, si no es que eliminar, las problemáticas emanadas de este tipo de riesgos.

SITUACIÓN NACIONAL

El problema suscitado por los contratos informáticos es actualmente objeto de un tratamiento en México en el ámbito de la administración pública, sobre todo en su campo federal, mediante el sistema de licitaciones Compranet, dependiente de la Secretaría de la Función Pública, en el cual se

dispone de infraestructuras normativas, técnicas y legales en apariencia mínimas para establecer los términos de una adecuada contratación de bienes y servicios informáticos.

Por otra parte, los particulares y las empresas pequeñas, quienes en general no cuentan con un soporte y apoyo técnico adecuado hacia la elección de un bien o servicio informático, se encuentran frente a una verdadera adversidad frente a los proveedores, acentuada por el hecho de que la administración pública no les ofrece un respaldo adecuado, a no ser la presentación de quejas frente a la Procuraduría Federal de Protección al Consumidor (Profeco).

Es importante hacer una reestructuración relacionada con la política gubernamental sobre este punto, así como una depuración equitativa de esta materia, como ocurre en aquellos países que, si bien con un nivel de informatización más pronunciado, ofrecen una serie de elementos, los cuales, debidamente capitalizados, permitirán disponer de un panorama prospectivo más prometedor.

CONSIDERACIONES FINALES

Es menester concientizarse del enorme auge que han adquirido en la actualidad los contratos informáticos, pues el descuido (por indiferencia o ignorancia) en que han incurrido los juristas para su negociación es inexcusable; así, se han agregado otras problemáticas accesorias en torno a la principal, como los riesgos informáticos y su necesario aseguramiento, los cuales dificultan aún más la búsqueda de soluciones jurídicas. No es posible seguir recurriendo a paliativos técnicos que por su carácter efímero no dan adecuado coto a las enormes pérdidas económicas suscitadas por dichas problemáticas. Por ello, la ciencia jurídica se obliga cada vez más a proveer figuras efectivamente aplicables acordes con las circunstancias del caso y no sujetas, como hasta ahora, a moldes tradicionalistas que remiten irremisiblemente a aforismos metajurídicos como el de "dejar hacer, dejar pasar".

VIII. Delitos informáticos

INTRODUCCIÓN

En la actualidad, las redes de comunicación electrónica y los sistemas de información forman parte de la vida diaria de los ciudadanos en el mundo y desempeñan un papel fundamental en el éxito de la economía universal. Cada vez están más interconectadas y es mayor la convergencia de los sistemas de información y las redes. Esta tendencia implica, sin duda, numerosas y evidentes ventajas, pero va acompañada también de un riesgo inquietante de ataques malintencionados contra los sistemas de información. Dichos ataques pueden adoptar formas muy distintas, incluido el acceso ilegal, la difusión de programas perjudiciales y ataques por denegación de servicio. Es posible lanzar estos ataques desde cualquier lugar hacia el resto del mundo y en cualquier momento. En el futuro podrían producirse nuevas formas de ataques inesperados.

Los ataques contra los sistemas de información constituyen una amenaza para la creación de una sociedad de la información más segura y de un espacio de libertad, seguridad y justicia, por lo que es importante abordar la temática con la mayor seriedad posible.[1]

CONCEPTO TÍPICO Y ATÍPICO

Dar un concepto acerca de delitos informáticos no es labor fácil, ya que su denominación alude a una situación muy especial porque para hablar de "delitos" en el sentido de acciones típicas (o tipificadas), es decir, contempladas en textos jurídico-penales, se requiere que la expresión *delitos informáticos* esté consignada en los códigos penales, lo cual en algunos países no ha sido objeto de tipificación. Empero, debido a la urgente necesidad de esto emplearemos dicha alusión, aunque, para efectos de una conceptuación, se debe establecer la diferencia entre lo típico y lo atípico.

[1] Comisión de las Comunidades Europeas, Bruselas, 19/04/2000, COM (2002) 173 final. 2002/0086 (CNS).

En ese orden de ideas, según el caso, los delitos informáticos son "actitudes ilícitas que tienen a las computadoras como instrumento o fin" (concepto atípico) o las "conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin" (concepto típico).

PRINCIPALES CARACTERÍSTICAS

1. Son conductas criminales de cuello blanco, *white collar crimes*, en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden cometerlas.
2. Son acciones ocupacionales en cuanto que muchas veces se realizan cuando el sujeto está trabajando.
3. Son acciones de oportunidad porque se aprovecha una ocasión creada o altamente intensificada en el campo de las funciones y organizaciones del sistema tecnológico y económico.
4. Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que los realizan.
5. Ofrecen facilidades de tiempo y espacio, ya que pueden cometerse en milésimas de segundo y sin una necesaria presencia física.
6. Son muchos los casos y pocas las denuncias, debido a la falta de regulación jurídica a nivel internacional.
7. Son muy sofisticados y relativamente frecuentes en el ámbito militar.
8. Presentan grandes dificultades para su comprobación, por su carácter técnico.
9. En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales.
10. Ofrecen a los menores de edad facilidades para su comisión.
11. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica en el ámbito internacional.

Las personas que cometen dichos delitos poseen ciertas características que no presentan el denominador común de los delincuentes. Esto es, los sujetos activos tienen habilidad para manejar los sistemas informáticos y en general por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible; o son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha comprobado que los autores de los delitos informáticos son muy diversos y que diferencia entre ellos es la naturaleza de los delitos cometidos. De esta forma, la persona que "ingresa" en un sistema informático sin intenciones delictivas es muy diferente del em-

pleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

Al respecto, según un estudio publicado en el *Manual de las Naciones Unidas para la prevención y control de delitos informáticos* (núms. 43 y 44), 90% de los delitos realizados mediante la computadora los cometían empleados de la empresa afectada. Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que 73% de las intrusiones efectuadas eran atribuibles a fuentes interiores y sólo 23% a la actividad delictiva externa.

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos no revela delincuencia informática, mientras otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudiera tener un empleado del sector de procesamiento de datos.

A pesar de lo anterior, teniendo en cuenta las características mencionadas de las personas que cometen los "delitos informáticos", los estudiosos en la materia los han catalogado como "delitos de cuello blanco", término introducido por primera vez por el criminólogo estadounidense Edwin Sutherland en 1943.

Efectivamente, el conocido criminólogo señala un sinnúmero de conductas que considera "delitos de cuello blanco", aun cuando muchas de ellas no están tipificadas en los ordenamientos jurídicos como delitos, entre las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas y la corrupción de altos funcionarios, entre otras".

Asimismo, este criminólogo dice que tanto la definición de los "delitos informáticos" como la de los "delitos de cuello blanco" no está de acuerdo con el interés protegido (como sucede en los delitos convencionales), sino según el sujeto activo que los comete. Algunas de las características comunes de ambos delitos son las siguientes: el sujeto activo del delito es una persona de cierto estatus socioeconómico y su comisión no puede explicarse por pobreza, ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima se hallen sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

CLASIFICACIÓN

Como instrumento o medio

En esta categoría se encuentran aquellas conductas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera).
b) Variación de los activos y pasivos en la situación contable de las empresas.
c) Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera).
d) "Robo" de tiempo de computadora.
e) Lectura, sustracción o copiado de información confidencial.
f) Modificación de datos tanto en la entrada como en la salida.
g) Aprovechamiento indebido o violación de un código para penetrar a un sistema con instrucciones inapropiadas (esto se conoce en el medio como *método del caballo de Troya*).
h) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como *técnica de salami*.
i) Uso no autorizado de programas de cómputo.
j) Inclusión de instrucciones que provocan "interrupciones" en la lógica interna de los programas, a fin de obtener beneficios.
k) Alteración en el funcionamiento de los sistemas.
l) Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.
m) Acceso a áreas informatizadas en forma no autorizada.
n) Intervención en las líneas de comunicación de datos o teleproceso.

Como fin u objetivo

En esta categoría se encuadran las conductas dirigidas en contra de la computadora, accesorios o programas como entidad física. Algunos ejemplos son los siguientes:

a) Programación de instrucciones que producen un bloqueo total al sistema.
b) Destrucción de programas por cualquier método.
c) Daño a la memoria.
d) Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etcétera).

e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
f) Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje, pago de rescate, etcétera).

TIPOS DE ATAQUES CONTRA LOS SISTEMAS DE INFORMACIÓN

La expresión *sistema de información* se utiliza deliberadamente aquí en su sentido más amplio, debido a la convergencia entre las redes de comunicación electrónica y los distintos sistemas que conectan. A efectos de la presente propuesta, los sistemas de información abarcan las computadoras personales autónomas, las agendas electrónicas personales, los teléfonos celulares, los intranets, los extranets y, naturalmente, las redes, servidores y otras infraestructuras de internet.

En su comunicación *Seguridad de las redes y de la información: propuesta para un enfoque político europeo*,[2] la Comisión de las Comunidades Europeas propuso la siguiente descripción de las amenazas contra los sistemas informáticos:

a) Acceso no autorizado a sistemas de información

Esto incluye el concepto de "piratería informática", la cual consiste en tener acceso de manera no autorizada a una computadora o a una red de computadoras. Puede tomar distintas formas, que van desde el mero uso de informaciones internas hasta ataques directos y la interceptación de contraseñas. Se realiza generalmente pero no siempre con una intención dolosa de copiar, modificar o destruir datos. La corrupción deliberada de sitios internet o el acceso sin previo pago a servicios restringidos puede constituir uno de los objetivos del acceso no autorizado.

b) Perturbación de los sistemas de información

Existen distintas maneras de perturbar los sistemas de información mediante ataques malintencionados. Uno de los medios más conocidos de denegar o deteriorar los servicios ofrecidos por internet es el ataque de tipo *denegación de servicio* (DdS), el cual es en cierta medida análogo a inundar las máquinas de fax con mensajes largos y repetidos. Los ataques del tipo denegación de servicio tienen por objeto sobrecargar los servidores o los proveedores de servicios internet

[2] Comunicación de la Comunicación al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de Regiones, *Seguridad de las redes y de la información: Propuesta para un enfoque político europeo*, 6 de junio de 2001, COM (2000) 298 final.

(PSI) con mensajes generados de manera automática. Otros tipos de ataques pueden consistir en perturbar los servidores que hacen funcionar el sistema de nombres de dominio (DNS) y los ataques contra los "encaminadores". Los ataques destinados a perturbar los sistemas han sido perjudiciales para algunos sitios *web* prestigiosos como los portales. Según estudios, estos ataques causan daños estimados en varios centenares de millones de dólares, sin contar el perjuicio no cuantificable en términos de reputación. Las empresas cuentan cada vez más con un sitio web propio y las que dependen de él para el suministro "justo a tiempo" son especialmente vulnerables.

c) Ejecución de programas informáticos perjudiciales que modifican o destruyen datos

El tipo más conocido de programa informático malintencionado es el virus. Los virus "I Love You", "Melissa" y "Kournikova" son ejemplos recientemente conocidos. Existen otros tipos de programas informáticos perjudiciales. Algunos dañan la computadora, mientras que otros utilizan la PC para atacar otros elementos de la red. Varios programas (llamados "bombas lógicas") pueden permanecer inactivos hasta que se desencadenan por algún motivo (por ejemplo, una fecha determinada) y causan graves daños al modificar o destruir datos. Otros programas parecen benignos, pero cuando se lanzan desencadenan un ataque perjudicial (por eso se denominan "caballos de Troya"). Otros programas (llamados "gusanos") no infectan otros más (como los virus), pero crean réplicas de ellos y éstas generan a su vez nuevas réplicas. De este modo termina por inundarse el sistema.

d) Intercepción de las comunicaciones

La intercepción malintencionada de comunicaciones afecta los requisitos de confidencialidad e integridad de los usuarios y se denomina a menudo *sniffing* (intromisión).

e) Declaraciones falsas

Los sistemas de información ofrecen nuevas posibilidades de declaraciones falsas y de fraude. Usurpar la identidad de otra persona en internet y utilizarla con fines malintencionados se llama *spoofing* (modificación de los datos).

Clasificación de acuerdo con las Naciones Unidas

Por su parte, el *Manual de las Naciones Unidas para la prevención y control de delitos informáticos* señala que cuando el problema aparece en el

ámbito internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de delito transnacional y su combate requiere una eficaz cooperación internacional concertada. Asimismo, la ONU resume de la siguiente manera los problemas relacionados con la cooperación internacional en el área de los delitos informáticos:

a) Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
b) Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
c) Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
d) No armonización entre las diferentes leyes procesales nacionales referentes a la investigación de los delitos informáticos.
e) Carácter transnacional de múltiples delitos cometidos mediante el uso de computadoras.
f) Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

Tipos de delitos informáticos reconocidos por Naciones Unidas

Delitos	Características
Fraudes cometidos mediante manipulación de computadoras	
Manipulación de los datos de entrada	Este tipo de fraude informático, conocido también como *sustracción de datos*, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. No requiere conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de éstos
Manipulación de programas	Es muy difícil descubrirla y a menudo pasa inadvertida debido a que el delincuente ha de tener conocimientos técnicos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado *caballo de Troya*, el cual consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal

Delitos	Características
Manipulación de los datos de salida	Para efectuarla se fija un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a partir de tarjetas bancarias robadas, pero en la actualidad se usan ampliamente equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y las de crédito
Fraude efectuado por manipulación informática	Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina *técnica del salami* en la cual "rodajas muy finas", apenas perceptibles, de transacciones financieras se sacan repetidamente de una cuenta y se transfieren a otra
Falsificaciones informáticas	
Como objeto	Cuando se alteran datos de los documentos almacenados en forma computarizada
Como instrumentos	Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, modificar documentos e incluso crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los auténticos
Daños o modificaciones de programas o datos computarizados	
Sabotaje informático	Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son: virus, gusanos, y bomba lógica o cronológica, los cuales se detallan a continuación
Virus	Es una serie de claves programáticas que pueden adherirse a los programas informáticos legítimos y propagarse a otros. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como mediante el método del caballo de Troya

Delitos	Características
Gusanos	Se fabrican de forma análoga al virus con miras a infiltrarlos en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos, podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita
Bomba lógica o cronológica	Exige conocimientos especializados ya que requiere programar la destrucción o modificación de datos en un futuro. Ahora bien, a diferencia de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar donde se halla
Falsificaciones informáticas	
Acceso no autorizado a sistemas o servicios	Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (*hacker*) hasta el sabotaje o espionaje informático
Piratas informáticos o hackers	El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para tener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder en aquellos sistemas en los que los usuarios pueden emplear contraseñas comunes o de mantenimiento que están en el sistema

Delitos	Características
Reproducción no autorizada de programas informáticos de protección legal	Ésta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico por tutelar es la propiedad intelectual

PORNOGRAFÍA INFANTIL EN INTERNET

La palabra *pornografía* se deriva de pornógrafo (del griego πορνογ, prostituta, y ράφος, escritura), y se define como el carácter obsceno de obras literarias o artísticas. A su vez, el concepto de obscenidad está referido a lo impúdico u ofensivo al pudor.

Debido a que el carácter de lo que es obsceno se vincula con las variantes culturales que existen en el mundo, el concepto de pornografía infantil difiere también conforme a las prácticas de comportamiento sexual, las creencias religiosas y los valores morales que tiene cada sociedad.

Dicha situación motiva que tanto la definición como las medidas que establecen los distintos países en sus legislaciones para evitar la pornografía infantil tengan alcances diferentes.

En el ámbito internacional, la Convención sobre los Derechos del Niño adoptada por Naciones Unidas en 1989 establece una referencia a la pornografía infantil, al mencionarla como forma de explotación y abuso sexual, contra la que deberá protegerse a los niños como compromiso de los Estados miembros.

Posteriormente, en 2000, el Protocolo Facultativo de la Convención sobre los Derechos del Niño, relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía, define a la pornografía infantil como "toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales".

En el Convenio sobre Cibercriminalidad del Consejo de Europa de 2001[3] se da una definición más amplia que incluye el material en siste-

[3] Véase Convenio sobre cibercriminalidad, Budapest, 23.XI. 2001, disponible [en línea] formato pdf, pp. 6-9 (pornografía infantil) http://www.interpol.int/Public/TechnologyCrime/Conferences/6thIntConf/ConventionEs.pdf

mas informáticos: "La pornografía infantil comprende todo material pornográfico que represente de manera visual: *a*) a un menor dedicado a un comportamiento sexualmente explícito; *b*) a alguien que parezca un menor dedicado a un comportamiento sexualmente explícito, y *c*) imágenes realistas que representen a un menor dedicado a un comportamiento sexualmente explícito."

En la legislación mexicana, el Código Penal Federal se refiere la pornografía infantil como a "los actos de exhibicionismo corporal, lascivos o sexuales con el objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro".

El uso masivo de internet ha propiciado un crecimiento exponencial de la pornografía infantil debido a la facilidad para dar visibilidad, publicidad y acceso a todo tipo de materiales.

Internet hace factible la consulta de páginas web con material pornográfico, pero mantiene al usuario en el anonimato. Los programas "peer to peer" hacen posible compartir el material ubicado en el disco duro de las computadoras, sin dejar rastro. El correo electrónico permite enviar fotografías o videos de una punta del mundo a la otra en cuestión de segundos, sin correr el riesgo de pasar por aduanas o controles policiales. Los chats, foros y páginas de comunidades facilitan la comunicación entre pedófilos e incluso el contacto directo con menores.

El uso más actual y novedoso es lo que se ha dado en llamar *pornografía virtual*, que consiste en la creación de contenidos sexuales con imágenes no reales, como dibujos y animaciones de menores. Esto suscita un hondo debate y provoca problemas al perseguir la pornografía infantil legal y judicialmente porque no existen las personas ni las situaciones reproducidas; a pesar de ello, fomenta el consumo de otros materiales que sí lo hacen.

Con base en el Informe sobre Pornografía Infantil en Internet de ANESVAD,[4] se estima que en el mundo existen más de 4 millones de sitios de internet que contienen material de sexo con menores y que cada día se crean 500 nuevos. Estas páginas reciben más de 2 000 millones de visitas anuales.

Respecto a la cantidad de material que incluyen, el mismo informe señala que la mayor base de datos de pornografía infantil, elaborada por la policía británica, cuenta con 3 millones de fotografías diferentes. A esto se suman los videos, relatos y otros modos de pornografía infantil. Aproximadamente 60% de estos sitios son de pago y cobran cuotas promedio de 40 dólares al mes.

[4] ANESVAD, *Informe sobre la pornografía infantil*, disponible [en línea], formato pdf, 35 páginas, http://www.anesvad.org/informe.pdf, consultada en mayo de 2008.

La mayoría de los sitios con pornografía infantil se encuentran en servidores de países de la antigua Unión Soviética y en algunos de América Latina, donde la legislación es mucho más permisiva con los menores.

Otros datos de la organización ECPAT, *End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes*[5] que ayudan a dimensionar el problema son los siguientes:

- En el Reino Unido, a fines de 2003, la tasa anual de arrestos se incrementó 6 500% desde 1988.
- En Estados Unidos, el programa del FBI *Innocent Images* registró un incremento de 2 050% en nuevos casos relacionados con la pornografía infantil entre 1988 y 2001.
- En 2005, la Policía Federal Argentina reportó que los casos de pornografía infantil se quintuplicaron en comparación con años anteriores.
- *Protégeles*, una ONG europea creada para rastrear y remover pornografía infantil de internet, recibió 28 900 denuncias e identificó 1 800 comunidades en el mundo de abusadores de niños entre 2001 y 2004.
- Un estudio del Servicio Aduanero de Estados Unidos realizado en 2001 encontró 100 000 sitios en internet relacionados con la pornografía infantil.

Esa organización efectuó en 2002 una investigación denominada *Nymphasex* en la que se ofrecieron "servicios con menores" y la posibilidad de comunicarse con ellos vía correo electrónico o videochat. Entre los datos que destacan, los países que efectuaron mayor número de accesos fueron Estados Unidos con 41.96%, España con 37.34% y México con 5.34 por ciento.

Convenciones internacionales

En el ámbito internacional existen diversas convenciones internacionales que se refieren a los derechos de los niños y buscan prevenir la explotación y abuso:

- *Declaración de Ginebra sobre los Derechos del Niño* (1924).
- *Declaración Universal de los Derechos Humanos* (1948).
- *Declaración de los Derechos del Niño* (1959).
- Convención sobre los Derechos del Niño (1989).

[5] ECPAT International, *Combatiendo el turismo sexual infantil. Preguntas y respuestas 2008.disponible, formato pdf, (inglés), 44 páginas, [en línea]*, http://www.ecpat.net/EI/PDF/CST/CST_FAQ_ENG.pdf consultada en junio de 2008.

- *Declaración Mundial sobre la Supervivencia, la Protección y el Desarrollo del Niño* (1990).
- *Declaración de la Organización Mundial del Turismo sobre la Prevención del Turismo Sexual Organizado* (1995).
- *Declaración de Estocolmo contra la Explotación Sexual Infantil con Fines Comerciales* (1996).
- *Declaración y Plan de Acción de los Niños y Jóvenes Víctimas de la Explotación Sexual* (1998).
- Convenio núm. 182 de la OIT, junto con su Recomendación núm. 190, sobre la prohibición de las peores formas de trabajo infantil y la acción inmediata para su eliminación (1999).
- Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que complementa la Convención de las Naciones Unidas contra la delincuencia organizada transnacional (2000).
- Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía (2000).
- Convenio sobre el Delito Cibernético del Consejo de Europa (2001).
- Compromiso mundial de Yokohama (2001).
- Decisión marco 2004/68/JAI del Consejo de Europa, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil (2003).

Entre esos instrumentos destaca la Convención sobre los Derechos del Niño, que define como niño a todo ser humano menor de dieciocho años de edad, excepto cuando, en virtud de la ley que le sea aplicable, haya alcanzado antes la mayoría de edad y, que como comentamos al analizar el concepto de pornografía infantil, establece como forma de abuso sexual la explotación del niño en espectáculos o materiales pornográficos.

Otro de los instrumentos que se refiere con mayor detalle a la pornografía infantil es el Protocolo Facultativo de la Convención de los Derechos del Niño de Naciones Unidas, que entró en vigor en enero de 2002 y que en junio de 2005 había sido ratificado por 111 países, entre ellos México.

En dicho protocolo se establece que los Estados partes prohibirán la pornografía infantil y deberán adoptar medidas en la legislación penal contra los actos de producción, distribución, divulgación, importación, exportación, oferta, venta o posesión, con fines de pornografía infantil, tanto si se han cometido dentro como fuera de sus fronteras, o si se han perpetrado individual o colectivamente. Estas disposiciones se aplicarán también en los casos de tentativa de cometer cualquiera de estos actos y de complicidad o participación en cualquiera de ellos.

Entre otros aspectos importantes, el protocolo establece para los Estados partes lo siguiente:

- Adopción de medidas para incautar y confiscar bienes, como materiales, activos y otros medios utilizados para cometer o facilitar la comisión de los delitos, y sus utilidades.
- Adopción de medidas para cerrar, temporal o definitivamente, los locales utilizados con el fin de cometer esos delitos.
- Reconocimiento de la vulnerabilidad de los niños víctimas y adaptar los procedimientos y medidas para protegerlos.
- Protección de la intimidad e identidad de los niños víctimas.
- Adopción de medidas a fin de asegurar asistencia a las víctimas, así como su plena reintegración social y recuperación física y psicológica.
- Adopción de medidas para fortalecer la cooperación internacional para la prevención, la detección, la investigación, el enjuiciamiento y el castigo de los responsables.

Por otra parte, se consideran importantes, porque buscan acciones preventivas, el Convenio 182 de la OIT sobre la Prohibición de las Peores Formas de Trabajo Infantil y la Acción Inmediata para su Eliminación, que señala que los Estados miembros deben establecer medidas inmediatas y eficaces para conseguir la prohibición y la eliminación de las peores formas de trabajo infantil, entre las que se señala el uso, el reclutamiento o la oferta de niños para la prostitución, la producción de pornografía o actuaciones pornográficas.

Por último, el instrumento internacional que detalla de manera más exhaustiva las infracciones y sanciones contra la pornografía infantil es la Decisión marco 2004/68/JAI del Consejo de Europa, del 22 de diciembre de 2003. Entre los aspectos interesantes se incluye como pornografía infantil, además del material de niños reales, el referente a una persona real que parezca ser niño y las imágenes realistas de un niño inexistente.

En esta decisión se establecen como infracciones relacionadas con la pornografía infantil, se realicen o no mediante sistemas informáticos: producción de pornografía infantil; distribución, difusión o transmisión de pornografía infantil; ofrecimiento o suministro de pornografía infantil, y adquisición o posesión de pornografía infantil.

Regulación jurídica a nivel internacional

A finales de la década de 1970 y comienzos de la de 1980 comenzó el impulso de medidas legislativas, centradas en la prohibición de la producción, venta y distribución de la pornografía infantil.

Algunas referencias acerca de los primeros antecedentes legislativos contra la pornografía infantil son los siguientes:

En Estados Unidos los intentos por regular y proscribir la pornografía eran frecuentemente criticados como censura y violación de la Primera Enmienda. No obstante, la Suprema Corte afirmó, en un caso de 1957, que la obscenidad no estaba protegida, por lo cual podrá prohibirse el material pornográfico si cumple con la definición legal de obscenidad. Posteriormente, en 1982 la Corte dictaminó que la pornografía infantil no estaba protegida por la Primera Enmienda, aun cuando no fuese definida de manera legal como obscena, dado que los niños no pueden consentir legalmente las relaciones sexuales.

El Congreso aprobó en 1984 el Acta de Protección Infantil, que brindaba restricciones más severas contra la pornografía infantil.

En 1968 Dinamarca emitió una ley con disposiciones referentes a acciones contra la obscenidad en la palabra escrita.

En 1988 la pornografía infantil se volvió ilegal en Gran Bretaña. Otros países empezaron a legislar más recientemente: Noruega en 1992, Alemania, Francia y Canadá en 1993, Austria en 1994 y Dinamarca, España y Bélgica en 1995.

Por lo que se refiere a pornografía infantil en internet, las legislaciones difieren considerablemente de un país a otro. Algunos países no tienen referencias específicas al uso de internet, aunque se puede enjuiciar a los autores en virtud de la legislación general sobre pornografía infantil o explotación o abusos sexuales de niños, como es el caso en Haití, Portugal y Togo.

En cuanto a la definición de pornografía infantil existen leyes que no la incluyen, como en Nueva Zelanda. Otras incluyen solamente imágenes reales (como las de México) y algunas otras (como las de Bélgica) incorporan medios y objetos visuales de cualquier tipo.

Por lo que respecta a los actos considerados ilícitos en relación con la pornografía infantil, algunos países incluyen la posesión de material (como Gran Bretaña) y otros sólo la producción, distribución y comercialización. En Suecia, por ejemplo, está prohibido poseer pornografía infantil, pero no verla, es decir, la posesión sólo será ilegal si las imágenes o películas se descargan y guardan. La Decisión del Consejo Europeo también excluye la información pornográfica para uso privado en ciertas situaciones.

En Australia se considera el delito de "captación", que se refiere a utilizar un servicio de comunicaciones para atraer a un menor a fin de que participe en una actividad sexual.

Respecto a la edad para ser sujeto de pornografía infantil, se establece en general de menos de 18 años, pero hay países que consideran una edad menor, por ejemplo: Australia, Portugal, Polonia y Suecia. A este respecto también existen contradicciones con la edad de consentimiento para la actividad sexual, como es el caso de Suiza. En México, la Comisión del Derecho del Niño ha observado contradicción con la edad para contraer matrimonio entre niños y niñas, por posibles implicaciones.

También existen diferencias en las legislaciones en relación con las sanciones impuestas. Algunos países establecen penas máximas de 5 años y otros llegan a 10 o 12.

En cuanto a los proveedores de servicios de internet, en general se regulan por códigos propios; empero, algunos países (como Dinamarca y Suecia) consideran en su legislación responsabilidades para ellos si conservan material ilegal, después de enterarse de su existencia.

Regulación jurídica a nivel nacional

En México existen varios instrumentos jurídicos que establecen disposiciones para la protección de los niños, en general, y contra el delito de la pornografía infantil, en particular.[6]

La reforma al artículo 4 de la *Constitución Política de los Estados Unidos Mexicanos* de 2000 elevó a rango constitucional el derecho de niñas y niños a satisfacer sus necesidades de alimentación, salud, educación y sano esparcimiento. Además, el deber de preservar estos derechos se amplía a los ascendientes, tutores y custodios y se especificó la obligación del Estado de proveer lo necesario para propiciar el respeto a la dignidad de la niñez y el ejercicio pleno de sus derechos.

La *Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes*, emitida el 29 de mayo de 2000, contiene un capítulo específico para el tema de la protección en la integridad y la libertad, así como contra el maltrato y el abuso sexual.

> ***Artículo 21.*** Niñas, niños y adolescentes tienen el derecho a ser protegidos contra actos u omisiones que puedan afectar su salud física o mental, su normal desarrollo o su derecho a la educación en los términos establecidos en el artículo 3o. constitucional. Las normas establecerán las formas de prever y evitar estas conductas. Enunciativamente, se les protegerá cuando se vean afectados por:
>
> A. El descuido, la negligencia, el abandono, el abuso emocional, físico y sexual.
> B. La explotación, el uso de drogas y enervantes, el secuestro y la trata de personas.
> C. Conflictos armados, desastres naturales, situaciones de refugio o desplazamiento, y acciones de reclutamiento para que participen en conflictos armados.

En el Código Penal Federal se realizaron reformas en 2000 para tipificar los delitos de pornografía infantil y las sanciones, conforme a lo siguiente:

[6] Véase el anexo X.

Artículo 201 bis. Al que procure o facilite por cualquier medio el que uno o más menores de dieciocho años, con o sin su consentimiento, lo o los obligue o induzca a realizar actos de exhibicionismo corporal, lascivos o sexuales, con el objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro, se le impondrán de cinco a diez años de prisión y de mil a dos mil días multa.

Al que fije, grabe o imprima actos de exhibicionismo corporal, lascivos o sexuales en que participen uno o más menores de dieciocho años se le impondrá la pena de diez a catorce años de prisión y de quinientos a tres mil días multa. La misma pena se impondrá a quien, con fines de lucro o sin él, elabore, reproduzca, venda, arriende, exponga, publicite o transmita el material a que se refieren las acciones anteriores.

Se impondrá prisión de ocho a dieciséis años y de tres mil a diez mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito a quien por sí o a través de terceros dirija, administre o supervise cualquier tipo de asociación delictuosa con el propósito de que se realicen las conductas previstas en los dos párrafos anteriores con menores de dieciocho años.

Para los efectos de este artículo, se entiende por pornografía infantil la representación sexualmente explícita de imágenes de menores de dieciocho años.

Artículo 201 bis 1. Si el delito de corrupción de menores o de quien no tenga capacidad para comprender el resultado del hecho o el de pornografía infantil es cometido por quien se valiese de una función pública que tuviese, se le impondrá hasta una tercera parte más de las penas a que se refieren los artículos 201 y 201 bis y destitución del empleo, cargo o comisión públicos e inhabilitación para desempeñarlo, hasta por un tiempo igual al de la pena impuesta para ejercer otro.

Artículo 201 bis 2. Si el delito es cometido con un menor de dieciséis años de edad, las penas aumentarán hasta una tercera parte más de las sanciones a que se refieren los artículos 201 y 201 bis. Si el delito se comete con menor de doce años de edad, las penas aumentarán hasta una mitad de las sanciones a que se refieren los artículos 201 y 201 bis de esta ley.

Artículo 201 bis 3. Al que promueva, publicite, invite, facilite o gestione por cualquier medio a persona o personas a que viaje al interior o exterior del territorio nacional y que tenga como propósito tener relaciones sexuales con menores de dieciocho años de edad se le impondrá una pena de cinco a catorce años de prisión y de cien a dos mil días multa.

Las mismas penas se impondrán a quien realice las acciones a que se refiere el párrafo anterior, con el fin de que persona o personas obtengan relaciones sexuales con menores de dieciocho años.

En abril de 2005 fueron aprobadas por la Cámara de Diputados y turnadas a la Cámara de Senadores las reformas de estos artículos, para separar en un solo capítulo los delitos de pornografía infantil. Entre los aspectos más relevantes se tipifica también el delito para quien almacene,

distribuya, compre e importe o exporte material, y se endurecen las penas y multas, además de hacer más específico el uso de computadoras y redes.

OTRAS CLASIFICACIONES

Por otra parte, existen diversos tipos de delito que pueden cometerse y que se encuentran ligados directamente con acciones efectuadas contra los sistemas, como los siguientes:

a) *Acceso no autorizado*: uso ilegítimo de *passwords* y la entrada de un sistema informático sin autorización del propietario.
b) *Destrucción de datos*: los daños causados en la red mediante la introducción de virus, bombas lógicas, etcétera.
c) *Infracción a los derechos de autor de bases de datos*: uso no autorizado de información almacenada en una base de datos.
d) *Intercepción de e-mail*: lectura de un mensaje electrónico ajeno.
e) *Fraudes electrónicos*: mediante compras realizadas al usar la red.
f) *Transferencias de fondos*: engaños en la realización de este tipo de transacciones.

Por otro lado, internet permite dar soporte para la comisión de otro tipo de delitos, a saber:

1. *Espionaje*: acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
2. *Terrorismo*: mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
3. *Narcotráfico*: transmisión de fórmulas para la fabricación de estupefacientes, para el lavado de dinero y para la coordinación de entregas y recogidas.
4. *Otros delitos*: las mismas ventajas que encuentran en la internet los narcotraficantes pueden ser aprovechadas para planificar otros delitos, como tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

NATURALEZA DEL RIESGO

Existe una necesidad clara de recoger informaciones confiables sobre la amplitud y la naturaleza de los ataques contra los sistemas de información. Los ataques más graves contra los sistemas de información se dirigen a

los operadores de redes de comunicaciones electrónicas y a los servidores de servicios o a las sociedades de comercio electrónico. Los ámbitos más tradicionales pueden también verse afectados seriamente debido al nivel de interconexión cada vez mayor en las comunicaciones modernas: las industrias manufactureras, los servicios, los hospitales, los organismos del sector público y los gobiernos. No obstante, no sólo las víctimas de los ataques son organizaciones, sino también los ataques pueden causar graves daños directos y perjudiciales a los particulares. La carga económica que suponen algunos de estos ataques a los organismos públicos, a las empresas y a las personas privadas es considerable y amenaza con hacer los sistemas de información más costosos y menos asequibles a los usuarios.

Los ataques descritos los efectúan a menudo individuos que actúan por cuenta propia, a veces menores que no están del todo conscientes de la gravedad de sus actos. A pesar de ello, el nivel de sofisticación y las ambiciones de los ataques podrían agravarse.

Existe una preocupación creciente de que bandas de delincuentes organizadas utilicen las redes de comunicación para lanzar ataques contra los sistemas de información. Los grupos de piratas informáticos especializados en la piratería y la degradación de sitios internet son cada vez más activos a escala mundial, e incluso algunos intentan extorsionar a sus víctimas al proponerles una asistencia especializada tras el pirateo de sus sistemas de información. La detención de importantes grupos de "piratas informáticos o hackers" hace pensar que la piratería podría constituir cada vez más un fenómeno organizado de delincuencia. Recientemente se han producido ataques sofisticados y organizados contra los derechos de propiedad intelectual y tentativas de robo de sumas importantes a servicios bancarios.

Las violaciones en la seguridad de las bases de datos mercantiles del comercio electrónico en las que se tiene acceso a información sobre los clientes, incluidos números de tarjeta de crédito, son también una causa de preocupación. Estos ataques suponen cada vez más medios para el fraude en el pago y obligan a la banca a cancelar y expedir de nuevo miles de tarjetas. Otra consecuencia es el daño no cuantificable a la reputación mercantil y a la confianza del consumidor en el comercio electrónico. Medidas preventivas, como requisitos mínimos de seguridad para negociantes en línea que aceptan tarjetas de pago, se analizan conforme al plan de acción para prevenir el fraude y la falsificación de los medios de pago no monetarios.

En realidad, en los últimos tiempos, las tensiones a escala internacional han supuesto un recrudecimiento de los ataques contra los sistemas de información y, de manera concreta, contra sitios internet. Unos ataques más graves podrían no solamente tener serias consecuencias financieras, sino además, en algunos casos, implicar la pérdida de vidas humanas (sis-

temas hospitalarios y sistemas de control del tráfico aéreo, por ejemplo). La importancia que le atribuyen los Estados miembros se refleja en la prioridad concedida a las distintas iniciativas de protección de infraestructuras vitales. Por ejemplo, el programa comunitario sobre tecnología de la sociedad de la información (TSI) estableció, en conexión con el Ministerio Estadounidense de Asuntos Exteriores, un grupo de trabajo conjunto Unión Europea/ Estados Unidos de América relacionado con la protección de las infraestructuras vitales.

NECESIDAD DE ARMONIZAR EL DERECHO PENAL A NIVEL INTERNACIONAL

En este ámbito, el derecho penal de los Estados involucrados contiene vacíos jurídicos y diferencias importantes susceptibles de obstaculizar la lucha contra la delincuencia organizada y el terrorismo, así como los graves ataques contra los sistemas de información perpetrados por particulares. La aproximación del derecho positivo en materia de delincuencia informática contribuirá a que las legislaciones nacionales sean lo suficientemente completas para que las graves formas de ataques contra los sistemas de información puedan ser objeto de investigaciones mediante las técnicas y los métodos disponibles en derecho penal.

Los autores de esos delitos deben ser identificados y llevados a juicio y los tribunales han de disponer de sanciones adecuadas y proporcionadas. Se enviará así un claro mensaje disuasivo a los autores potenciales de ataques contra los sistemas de información; además, los vacíos jurídicos y las diferencias pueden impedir una cooperación policial y judicial eficaz en caso de ataques contra sistemas de información. Estos ataques son a menudo transnacionales por su naturaleza y requieren una cooperación internacional policial y judicial. La aproximación de las legislaciones mejorará, pues esta cooperación garantiza que se cumpla la exigencia de doble incriminación (según la cual una actividad debe constituir un delito en los dos países involucrados para que éstos colaboren a nivel judicial en el marco de una investigación penal).

FORMAS DE CONTROL

Preventivo

Como se infiere de lo anterior, este tipo de ilícitos requieren un necesario control, que, al no encontrar en la actualidad un adecuado entorno jurídico,

ha tenido que manifestarse, en su función preventiva, mediante diversas formas de carácter administrativo, normativo y técnico, entre las que se cuentan las siguientes:

a) Elaboración de un examen psicométrico previo al ingreso al área de sistemas en las empresas.
b) Inclusión de cláusulas especiales en los contratos de trabajo con el personal informático que así lo requiera por el tipo de labores a realizar.
c) Establecimiento de un código ético de carácter interno en las empresas.
d) Adopción de estrictas medidas en el acceso y control de las áreas informáticas de trabajo.
e) Capacitación adecuada del personal informático, a efecto de evitar actitudes negligentes.
f) Identificación y, en su caso, segregación del personal informático descontento.
g) Rotación en el uso de claves de acceso al sistema (*passwords*).

Correctivo

Éste podrá aplicarse en la medida en que se incluya un conjunto de disposiciones jurídicas en los códigos penales sustantivos, ya que en caso de considerar este tipo de ilícitos como figuras análogas existentes se corre el riesgo de alterar de manera flagrante el principio de legalidad de las penas.

Cabe mencionar que una adecuada legislación al respecto traería consigo efectos no sólo correctivos sino eventualmente preventivos, de tal forma que se reducirían en gran número este tipo de acciones que tanto daño causan a los intereses individuales y sociales.

El objetivo de crear un espacio de libertad, seguridad y justicia debe ser alcanzado mediante la prevención y la lucha contra la delincuencia, organizada o no, incluido el terrorismo, mediante una cooperación más estrecha entre los servicios represivos y las autoridades judiciales de los distintos Estados interesados, armonizando las legislaciones y las normativas en materia de cooperación policial y judicial penal.

SITUACIÓN INTERNACIONAL

Estados Unidos

Este país adoptó en 1994 el *Acta Federal de Abuso Computacional* (18 U.S.C. Sec.1030) que modificó al *Acta de Fraude y Abuso Computacional* de 1986.

Con la finalidad de eliminar los argumentos exageradamente técnicos acerca de qué es y qué no es un virus, un gusano, un "caballo de Troya" y en qué difieren de los virus, la nueva acta prohíbe la transmisión de un programa, información, códigos o comandos que causen daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas (18 U.S.C. Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

La ley de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de quienes lo realizan con la intención de hacer estragos. Además, define dos niveles para el tratamiento de quienes crean virus:

a) Para los que intencionalmente causen un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa.
b) Para los que lo transmitan sólo de manera imprudencial, la sanción fluctúa entre una multa y un año de prisión.

La nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente al no definir los virus, sino al describir el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos de cualquier forma que se realicen. La nueva ley diferencia los niveles de delitos y da lugar a que se considere qué debe entenderse por acto delictivo.

Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa a la persona que defraude a otra mediante la utilización de una computadora o red informática.

Alemania

Este país sancionó en 1986 la *Ley contra la Criminalidad Económica*, que se refiere a los siguientes delitos:

a) Espionaje de datos.
b) Fraude informático.
c) Alteración de datos.
d) Sabotaje informático.

Austria

La ley de reforma del código penal, sancionada el 22 de diciembre de 1987, en el artículo 148 sanciona a aquellos que con dolo causen un per-

juicio patrimonial a un tercero de tal manera que influyan en la elaboración de datos automática, mediante el diseño del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además, establece sanciones para quienes comenten este hecho al utilizar su profesión de especialistas en sistemas.

Gran Bretaña

Debido a un caso de *hacking* en 1991, comenzó a regir en este país la Computer Misuse Act (*Ley de Abusos Informáticos*). Con esta ley, el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas.

Dicha ley tiene un apartado que especifica la modificación de datos sin autorización. Los virus están incluidos en esa categoría.

A su vez, liberar un virus tiene penas desde un mes hasta cinco años, lo cual depende del daño que causen.

Holanda

El 1 de marzo de 1993 entró en vigor la *Ley de Delitos Informáticos*, en la cual se penaliza el *hacking*, el *preacking* (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría) y la distribución de virus.

La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño.

Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero si se comprueba que fueron liberados con la intención de causar daño, la pena podrá ser hasta de cuatro años de prisión.

Francia

En enero de 1988, este país dictó la ley relativa al fraude informático, la cual prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique datos.

Asimismo, esta ley establece en su artículo 462-3 una conducta intencional y a sabiendas de vulnerar los derechos de terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos. Por su parte, el artículo 462-4 también incluye en su tipo penal una conducta intencional y a sabiendas de que viola los derechos de

terceros, en forma directa o indirecta, haya introducido datos en un sistema de procesamiento automatizado o haya suprimido o modificado los datos que éste contiene, o sus modos de procesamiento o de transmisión.

También la legislación francesa establece un tipo doloso y pena el mero acceso, además de agravar la pena cuando resultare la supresión o modificación de datos contenidos en el sistema, o la alteración del funcionamiento del sistema (sabotaje).

Por último, dicha ley sanciona en su artículo 462-2 tanto el acceso al sistema como al que se mantenga en él, y aumenta la pena correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

España

En el *Nuevo Código Penal de España*, el artículo 264-2 dispone que se aplicará la pena de prisión de uno a tres años y multa... a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

El código mencionado sanciona en forma detallada esta categoría delictual (violación de secretos/espionaje/divulgación), al aplicar pena de prisión y multa, agravadas cuando existe una intensión dolosa, y cuando el hecho es cometido por funcionarios públicos se penaliza con inhabilitación.

En materia de estafas electrónicas, el *nuevo Código Penal de España*, en su artículo 248, sólo tipifica las estafas con ánimo de lucro cuando el infractor se vale de alguna manipulación informática, pero no detalla las penas a aplicar en el caso de la comisión del delito.

SITUACIÓN NACIONAL[7]

En México, los delitos informáticos, están regulados en el Código Penal Federal en el título noveno, referido a la revelación de secretos y acceso ilícito a sistemas y equipos de informática, que en su capítulo II prescribe lo siguiente:

> ***Artículo 211 bis 1.*** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática pro-

[7] Véase el anexo X.

tegidos por algún mecanismo de seguridad se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Artículo 211 bis 3. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

Artículo 211 bis 4. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6. Para los efectos de los artículos 211 bis 4 y 211 bis 5 anteriores, se entiende por instituciones que integran el sistema financiero las señaladas en el artículo 400 bis de este código.

Artículo 211 bis 7. Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

COMENTARIOS FINALES

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades de la circulación nacional e internacional de datos conlleva también la posibilidad creciente de estos delitos; por eso, cabe afirmar que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

IX. Comercio electrónico

INTRODUCCIÓN

En sólo unos años, la revolución digital ha conquistado gran parte del mundo. En lo que a comunicaciones se refiere, internet es el fenómeno de más rápida expansión que se haya dado nunca. Los adelantos que lo han hecho posible no sólo han contribuido a que se produzcan cambios en el ámbito de las comunicaciones, sino también han propiciado un desarrollo espectacular de la nueva economía digital, reflejado en los mercados financieros y el flujo comercial, así como en las innovadoras formas de comercio y las nuevas posibilidades para los consumidores.[1]

Por el impresionante alcance de esas innovaciones, el comercio electrónico ha llegado a ser una actividad de gran trascendencia económica, política y social. El comercio realizado por medios electrónicos no es una novedad; sin embargo, la aparición de internet, una "red de redes" sin normas registradas, ha dado lugar a una expansión internacional extraordinaria respecto al número de usuarios y la gama de aplicaciones útiles en nuestra vida cotidiana. En muchas regiones del globo ha empezado a cambiar significativamente la manera como los particulares, las empresas y los gobiernos estructuran su labor, sus relaciones y la forma de llevar a cabo sus actividades comerciales.

El comercio electrónico se encuentra en sus primeras fases de evolución, la cual tiene lugar en un entorno tecnológico y comercial en constante transformación.

GENERALIDADES

Concepto

En los últimos años se ha generalizado el uso del término *comercio electrónico* y ha pasado a formar parte integrante de la terminología contem-

[1] Al respecto seguiremos el *Estudio sobre comercio electrónico y propiedad intelectual*, capítulo I, pp. 1 a 120, Organización Mundial de la Propiedad Intelectual, Ginebra, Suiza OMPI/OLO/EC/PRIMER, mayo de 2000, http://www.ecommerce.wipo.int.

poránea de las tecnologías de la información, fuente de profundos cambios en los últimos años del pasado milenio.[2] La expresión "comercio electrónico" se utiliza con frecuencia en los medios informativos, en los negocios y en el lenguaje común para referirse a una amplia gama de actividades que normalmente se asocian al uso de computadoras[3] y de internet para el comercio de bienes y servicios de una manera nueva, directa y electrónica.

Muchos estudios y publicaciones han abordado distintos aspectos del comercio electrónico y algunos de ellos han tratado de definir este nuevo modo de actividad comercial. En general, esas definiciones se centran en los medios electrónicos utilizados y en la naturaleza de las propias actividades comerciales. En lo que respecta a la evaluación de ese fenómeno y si se considera la rápida evolución de las actividades, quizá no sea posible todavía dar una definición precisa del comercio electrónico.[4] A efectos de este documento, lo más útil es analizar las palabras *comercio* y *electrónico* por separado.

Comercio

En este contexto, la palabra *comercio* hace referencia a una serie cada vez mayor de actividades que tienen lugar en redes abiertas —compra, venta, comercio, publicidad y transacciones de toda índole— que conducen a un intercambio de valor entre dos partes. Cabe citar como ejemplos las subastas, los servicios bancarios y demás servicios financieros, la venta de programas, y un número creciente de sitios internet que ofrecen una amplia gama de bienes o servicios de consumo, todos ellos en línea. En lo que atañe a los consumidores, un sitio web comercial que hace algún tiempo tuvo gran éxito es el sitio de venta de libros, mediante el cual el consumidor puede encargar un libro (y pagar por medios electrónicos como la tarjeta

[2] Con la evolución del uso del lenguaje, han surgido sinónimos de la expresión *comercio electrónico*, como *e-commerce*, *e-business* o incluso *m-business* (en referencia a los aparatos inalámbricos, como los teléfonos móviles o celulares).

[3] Además de las computadoras, es evidente que existen otros aparatos portátiles, inalámbricos y de acceso a internet que desarrollan un importante papel para facilitar el comercio electrónico.

[4] La OCDE, por ejemplo, ha señalado las dificultades que existen para cuantificar el comercio electrónico; ya que se trata de una actividad que se realiza en redes abiertas y ha pedido que se establezca una definición y una metodología básica para dar coherencia al acopio de datos. OCDE, *The Economic and Social Impacts of Electronic Commerce: Preliminary Findings and Research Agenda*, Organización de Cooperación y Desarrollo Económico, pp. 1 a 3 y 16 (1999), disponible [en línea] http://www.ocde.org/subject/e_commerce/summary.htm. La Oficina del Censo de Gobierno de Estados Unidos de América ha publicado recientemente un documento que pretender incluir un indicador de precisión en la definición. Véase *Measures Electronic Business Definitions, Underlying Concepts, and Measurement Plans*, Oficina del Censo de Gobierno de Estados Unidos de América (13 de octubre de 1999), disponible [en línea], en http://www.ecommerce.gov/ecomnewle-def.hmtl.

de crédito) que se le enviará por correo a su domicilio.[5] En la actualidad es posible adquirir otros productos mediáticos, como la música, y descargarlos directamente en forma digital en la computadora del consumidor (o en otros dispositivos digitales).

Aunque estos ejemplos muestran la manera como los particulares pueden realizar transacciones en internet, el auge del comercio electrónico se explica, ante todo, por la expansión de un sector menos visible: el de las transacciones de empresa a empresa. En ese caso, internet actúa como un poderoso medio para mejorar la calidad de la gestión y los servicios, al crear nuevas relaciones entre consumidores y proveedores, o al afianzar las existentes, y al aportar al mismo tiempo más eficacia y transparencia a las operaciones. Es un potente mecanismo para reducir los costos de carácter general, en particular los asociados a la producción, los inventarios, la gestión de ventas, la distribución y la compra.

Cabe mencionar al menos dos características de este comercio que tiene lugar en redes digitales. En primer lugar, su naturaleza internacional. Los medios electrónicos descritos anteriormente han creado un medio mundial sin límites, de manera que ninguna empresa que ofrezca bienes o servicios en internet tenga que dirigirse a un mercado geográfico concreto. La creación de un sitio web comercial puede dar, incluso a una empresa pequeña, acceso a mercados y a usuarios de internet de todo el mundo. En segundo lugar, la naturaleza interdisciplinaria del comercio electrónico, y el consiguiente efecto en las fuerzas de convergencia. Tanto las empresas grandes como las pequeñas han comprobado que lo que diferenciaba hasta ahora a los sectores comerciales, en razón de las características físicas de los bienes o servicios y de los diversos medios empleados para su distribución (por ejemplo, libros, películas, discos compactos, televisión, radio y retransmisiones por la web), está perdiendo su razón de ser. Esto origina presiones competitivas para reestructurar las actividades dentro de las industrias y entre ellas, lo cual supone nuevas oportunidades a la vez que problemas para las empresas.[6]

Electrónico

Por *electrónico* cabe entender la infraestructura mundial de tecnologías y redes de la informática y las telecomunicaciones que permiten el procesamiento y la transmisión de datos digitalizados. Numerosos estudios han

[5] Véase http://www.amazon.com, que ha ampliado la variedad de la oferta de su sitio web para competir con los grandes almacenes y ha incluido libros, juguetes, juegos, computadoras, aparatos electrónicos, artículos deportivos, música, video, ropa femenina y muchas otras cosas.

[6] Para un debate general sobre los cambios que se presentan en el mercado como consecuencia del comercio electrónico, véase OCDE, *The Economic and Social...*, cap. 5 (1999), disponible [en línea] en: http://www.ocde.org/subject/e_commerce/summary.htm

abordado la evolución desde las primeras redes privadas, en las que las transacciones electrónicas han sido moneda corriente durante varias décadas, hasta las redes abiertas con protocolos de uso público, como internet.[7] Un rasgo común de esas redes es que operan con base en propósitos definidos de manera específica y están destinadas exclusivamente para los participantes autorizados.

En cambio, internet permite que un número potencialmente ilimitado de participantes que quizá no hayan tenido contacto previo se comuniquen y realicen transacciones en una "red abierta",[8] que no exige dispositivos de seguridad. Internet ha evolucionado rápidamente de ser una red científica y académica, a una red cuyo principal elemento distintivo, la World Wide Web, ha sido adoptado a gran escala.[9] El carácter abierto de esta red, junto con su naturaleza multifuncional y un acceso cada vez más barato, han impulsado el potencial del comercio electrónico.[10] Al mismo tiempo, la red abierta proporciona acceso a un medio digital en el que pueden hacerse y transmitirse con facilidad múltiples copias perfectas de textos, imágenes y

[7] Véase, por ejemplo OCDE, *Business-to-Consumer Electronic Commerce Survey of Status and Issues*, OCDE/GD (97) 219 (1997), y David N. Townsend, *La regulación de las telecomunicaciones y el correo electrónico: informe orientativo*, del Informe de la Unión Internacional de Telecomunicaciones, Coloquio Normativo núm. 8 (1998). Ambos informes ofrecen una visón de conjunto del desarrollo de redes privadas, como las que se emplean para hacer las transferencias de un banco a otro, por ejemplo: la transferencia electrónica de fondos (TEF) y las redes creadas para ciertas transacciones comerciales, como el intercambio electrónico de datos (EDI).

[8] El término *red abierta* hace referencia a una red como internet, que usa protocolos no privados creados mediante un proceso para establecer normas sin restricciones. Internet se basa en un protocolo no privado, denominado Protocolo de Control de Transmisión/Protocolo Internet, (TCP/IP), y utiliza un sistema de codificación normalizado, el lenguaje de marcación hipertexto (HTML), para representar datos de manera gráfica en la World Wide Web. Véase OCDE, *The Economic and Social...*, capítulo 2, p. 1 (1999), disponible [en línea] http://www.oecd.org/subject/e-commerce/summary.htm. La World Wide Web, desde una perspectiva técnica, hace referencia a los servidores de hipertexto (servidores HTTP), que son servidores que permiten combinar texto, gráficos y ficheros audio. Véase UIT Challenges to the Network: Internet for Development, UIT, Glosario (1999).

[9] Al inicio, internet fue un medio no estrictamente comercial. Para consultar referencias de diversos documentos sobre los comienzos de internet, véase *History of the Internet*, sitio *web* de *Internet Society*, disponible [en línea] http://www.isoc.org/history-internet/. Véase también Townsend, *op. cit.*, nota 7, que explica que internet se puso en marcha en la década de 1960 como un proyecto de investigación denominado Arpanet, llevado a cabo por el departamento de Defensa de Estados Unidos de América, lanzada en 1990, la World Wide Web fue diseñada por científicos del Laboratorio Europeo de Física de Partículas, de Ginebra (CERN). A finales de 1993, el Centro Nacional para las Aplicaciones de Supercomputadoras de Estados Unidos de América (NCSA) dio a conocer el primer navegador internet integrado, Mosaic, cuya interfaz gráfica de usuario hacía más sencilla la navegación por esta red. Sin embargo, fue hasta 1994 cuando Netscape Communications Corporation, fundada por el doctor James Clark y Marc Andreessen, sacó a la luz y popularizó el primer navegador comercial de internet a gran escala. Véase el sitio web de Netscape en: http://home.netscape.com/company/about/backgrounder.html.#market.

[10] Un estudio divide el desarrollo de internet en *tres fases* relativas a las innovaciones de las tecnologías en la red. Véase *Defending the Internet Revolutions in the Broadband Era: When Doing Nothing is Doing Harm*, seis coautores, *E-conomy Working Paper* 12 (agosto de 1999), en [línea] http://e-conomy.berkeley.edu:80/pubs/wp/ewp12.html. En la primera fase, desde finales de la década de 1960

sonidos, propiciando el uso indebido de marcas, lo que origina problemas para los titulares de derechos de propiedad intelectual.

CARACTERÍSTICAS

En la actualidad, la mayoría de las transacciones de comercio electrónico entre empresas y consumidores están relacionadas con productos intangibles que pueden enviarse directamente a la computadora del consumidor a través de la red.[11] Aunque por su naturaleza esos productos son difíciles de cuantificar, el contenido que se ofrece está cada vez más sujeto a derechos de propiedad intelectual.

El crecimiento de internet y el comercio electrónico ha sido al menos meteórico y este ritmo vertiginoso no parece decaer. Nuevos elementos y estimaciones en los medios de información y otras publicaciones, sobre todo en los últimos tres años, explican las razones de ese auge. Como observación de carácter general, las múltiples previsiones que se han hecho de ese fenómeno en crecimiento se han puesto una y otra vez en tela de juicio, en respuesta a una tendencia (que ahora está por desaparecer) a subestimar la expansión de ese fenómeno. Hoy día, todo el mundo coincide en que internet es el fenómeno de más rápido crecimiento de todos los tiempos en el ámbito de las comunicaciones.

Se calcula que la población mundial en línea alcanzó los 500 millones de personas antes de 2005. Hay más de 100 millones de usuarios en Estados Unidos, Europa tiene ya 35 millones y se prevé que la tasa de crecimiento más rápida de los próximos años se produzca en Asia y América Latina.

Un examen de las principales estimaciones indica que, a partir de 0 prácticamente en 1995, el comercio electrónico mundial se cifró en 26 000 millones de dólares en 1997 y en 43 000 millones en 1998; se esperaba que alcanzara los 330 000 millones entre 2001 y 2002, y se previó que llegara a la extraordinaria cifra de 2 000 millones a 3 000 millones de dólares en 2003-2005.

---

hasta principios de la de 1990, internet se utilizaba fundamentalmente como prototipo de ingeniería y de red de interés para los sectores militar y de investigación, en los que la norma era que las pantallas fuesen monocromáticas y sólo presentaran texto. Las aplicaciones principales en esta primera fase fueron el correo-e y la transferencia de ficheros. La segunda fase de comienzo de los noventa hasta hoy se ha caracterizado por la adopción y la generalización de internet. Aprovechando la cobertura y el acceso a elementos clave de red telefónica mundial, dicha red puede ofrecer un acceso de banda ancha a sus usuarios fundamentalmente a través de módem de marcado que proporciona conexiones intermitentes con un ancho de banda mínimo. El auge de la *World Wide Web* puede considerarse el acontecimiento más destacado de la segunda fase. Según los autores, empieza la tercera fase, en la que habrá una propagación y un uso a gran escala de las tecnologías de banda ancha e incluso móvil. Los usuarios accederán a la red mediante una conexión permanente, y el abanico de servicios y aplicaciones ofrecidos irá más allá de lo que hoy día se conoce.

[11] *Ibid.* cap. 3, p. 8, La OCDE ha establecido cinco categorías que agrupan los diferentes productos intangibles del sector del comercio electrónico de empresa a empresa: ocio, viajes, periódicos, publicaciones, servicios financieros y correo electrónico.

La gran mayoría de este crecimiento proviene de las transacciones de empresa a empresa, en tanto que el aumento de las transacciones de los consumidores aún es perjudicado por impresiones muy extendidas respecto a la seguridad de los pagos, los posibles fraudes y los problemas de confidencialidad asociados al acopio de datos personales.

El comercio electrónico se puede definir, en un sentido amplio, como *cualquier forma de transacción o intercambio de información comercial basada en la transmisión de datos sobre redes de comunicación como internet*. En este sentido, el concepto de comercio electrónico no sólo incluye la compra y venta electrónica de bienes, información o servicios, sino también el uso de la red para actividades anteriores o posteriores a la venta, como los siguientes:

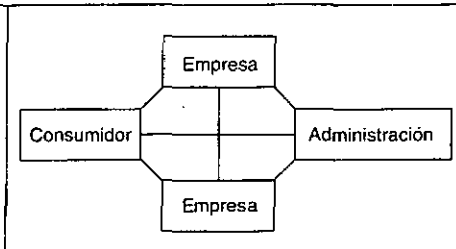
- La publicidad.
- La búsqueda de información acerca de productos, proveedores, etcétera.
- La negociación entre comprador y vendedor sobre precio, condiciones de entrega, etcétera.
- La atención al cliente antes y después de la venta.
- El cumplimiento de trámites administrativos relacionados con la actividad comercial.
- La colaboración entre empresas con negocios comunes (a largo plazo o sólo de forma coyuntural).

Estas actividades no tienen necesariamente que estar presentes en todos los escenarios de comercio electrónico.

Tipos de comercio electrónico

En el comercio electrónico participan como actores principales las empresas, los consumidores y las administraciones públicas. Así, se distinguen normalmente tres tipos básicos de comercio electrónico:

- Entre empresas (o B2B) (*Business to Business*)
- Entre empresa y consumidor o B2C (*Business to Consumers*)
- Entre empresa y la administración o B2A (*Business to Administration*)



Además de éstas, tenemos la de particular a particular como es el caso de www.ebay.com, etcétera.

Ventajas y desventajas

El comercio electrónico ofrece múltiples ventajas, a saber:

- Permite hacer más eficaces las actividades de cada empresa, así como establecer nuevas formas, más dinámicas, de cooperación entre empresas.
- Reduce las barreras de acceso a los mercados actuales, en especial para pequeñas empresas, y abre oportunidades de explotar mercados nuevos.
- Para el consumidor, amplía su capacidad para acceder a prácticamente cualquier producto y para comparar ofertas, a la vez que le facilita convertirse en proveedor de información.
- Reduce o incluso elimina por completo los intermediarios, por ejemplo: en la venta de productos en soporte electrónico (textos, imágenes, videos, música, software, etc.) que se pagan y entregan directamente a través de la red.

No obstante, en general, el comercio electrónico obliga a redefinir el papel que desempeñan los intermediarios entre productor y consumidor, al eliminarlos en algunos casos, pero también al crear la necesidad de contar con funciones de intermediación nuevas en otros. Igualmente, el comercio electrónico afecta el papel tradicional de otros actores, como las entidades financieras y los fedatarios públicos.

Empero, el comercio electrónico plantea también problemas nuevos o agudiza algunos existentes en el comercio tradicional, entre ellos:

- La validez legal de las transacciones y contratos "sin papel".
- La necesidad de llegar a acuerdos internacionales que armonicen las legislaciones sobre comercio.
- El control de las transacciones internacionales, incluido el cobro de impuestos.
- La protección de los derechos de propiedad intelectual.
- La protección de los consumidores en cuanto a publicidad engañosa o no deseada, fraude, contenidos ilegales y uso abusivo de datos personales.
- La dificultad de encontrar información en internet, comparar ofertas y evaluar la fiabilidad del vendedor (y del comprador) en una relación electrónica.
- La seguridad de las transacciones y medios de pago electrónicos.
- La falta de estándares consolidados y la proliferación de aplicaciones y protocolos de comercio electrónico incompatibles.

- La congestión de internet y la falta de accesos de usuario de suficiente capacidad.

Los problemas citados tienen, en mayor o menor medida, un componente legal y un componente tecnológico, por lo que su solución requiere actuaciones en ambos sentidos. Un buen ejemplo de esta doble componente de los problemas que plantea el comercio electrónico es la seguridad de las transacciones y pagos electrónicos, en particular por medio de internet.

SEGURIDAD DE INTERNET Y SEGURIDAD DEL COMERCIO ELECTRÓNICO

La seguridad, tanto desde el punto de vista técnico (algoritmos de cifrado, longitud de claves, etc.) como desde el de percepción de los usuarios, es un aspecto clave para generar en las empresas y en los consumidores la confianza necesaria con el fin que el comercio electrónico se desarrolle. La necesidad de generar confianza, en la que coinciden tanto las asociaciones de la industria como las administraciones públicas, es especialmente importante debido a que internet es una red abierta y a la sensación de inseguridad (a veces tal vez excesiva) que esto produce en los usuarios. Tal sensación negativa podrá cambiar si los usuarios conocen bien los sistemas de cifrado y de firma digital, el uso de tarjetas inteligentes como soporte de almacenamiento de claves privadas y la aparición de autoridades de certificación de claves públicas, en especial si se trata de entidades con una imagen tradicional de confiabilidad, como bancos o notarios.

Problemas jurídicos

El comercio electrónico ha empezado a tener repercusiones extraordinarias en la estructura de nuestros mercados y normativas; sin embargo, esos cambios también plantean problemas. En este capítulo se estudian tres campos en los que dichos problemas ya han producido efectos y plantean cuestiones que abarcan distintos sectores de interés jurídico. En esas áreas, las dimensiones internacionales del comercio electrónico dificultan la formulación de soluciones y exigen especial prudencia, sobre todo en cuanto a las iniciativas a nivel nacional que podrían pasar por alto las repercusiones potenciales más allá de las fronteras. Aunque estos temas son de vital importancia para el campo de la propiedad intelectual, también tienen efectos "horizontales" en otros ámbitos del derecho y la política, como los siguientes:

1. Entorno sin papel: contratos electrónicos.
2. Internet: jurisdicción y derecho aplicable.
3. Tecnología digital: problemas de observancia y confidencialidad.

1. Entorno sin papel: contratos electrónicos

Como se ha señalado, el comercio electrónico origina interactividad y transacciones entre partes que quizá no hayan tenido contacto previo. Hoy día, incluso las pequeñas empresas pueden considerarse multinacionales, en un entorno digital de "gravedad cero" en el que pueden negociar con otras partes de todo el mundo. Esas negociaciones pueden tener lugar en tiempo real entre empresas, o entre empresas y consumidores. Muchas de esas transacciones pueden ser simplemente acuerdos únicos, en los que ninguna de las partes considere la posibilidad inmediata de entablar una relación continua derivada de la transacción.

Esas transacciones precisan reglas que rijan la relación entre las partes. El elemento principal de esas reglas es el propio acuerdo: el contrato. Existe un reconocimiento cada vez mayor del papel esencial que pueden desempeñar los contratos en el mercado internacional del comercio electrónico. Como medio para aplicar el principio de autonomía de las partes y permitir una toma de decisiones descentralizada en relación con los derechos y obligaciones comerciales, el contrato es un mecanismo flexible, pero vinculante desde el punto de vista jurídico. En este sentido, el contrato quizá pueda considerarse la medida autorregulatoria más importante de que disponen las partes implicadas en el comercio electrónico.

En muchos contratos de comercio electrónico entran en juego los derechos de propiedad intelectual de una de las partes. Un contrato de explotación de derechos de propiedad intelectual puede revestir diversas formas: las licencias, la prestación de servicios, los acuerdos de distribución y franquicia, así como los acuerdos de operaciones conjuntas son algunas de las más comunes. Por ejemplo, una licencia es un contrato que autoriza al licenciatario a hacer algo que, de no existir esa licencia, constituiría, en circunstancias normales, una infracción al derecho de propiedad intelectual del licenciante. Cuando los consumidores de internet acceden a una composición musical, pueden hacerlo en virtud de un acuerdo de licencia. A cambio, la empresa que distribuye la música habrá obtenido una licencia del titular del derecho de autor y del productor de la grabación sonora. Debido a que en muchos países pueden residir las empresas y los consumidores y son muy numerosas las leyes nacionales y locales relativas tanto al derecho de obligaciones y contratos como a la propiedad intelectual, los contratos pueden ser operaciones mucho más complejas en el medio digital que en el ámbito fuera de línea.

En una primera iniciativa para dar seguridad respecto al entorno jurídico de los contratos electrónicos, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) creó una ley modelo sobre comercio electrónico en 1996.[12] Tal como se establece en el preámbulo de la ley modelo, la CNUDMI reconoce que "un número creciente de transacciones comerciales nacionales e internacionales se realizan por medio del intercambio electrónico de datos y *por otros medios de comunicación*,[13] habitualmente conocidos como *comercio electrónico*, en los que se usan métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel". Por otro lado, la CNUDMI explica que la decisión de formular una legislación modelo concerniente al comercio electrónico se tomó en respuesta al hecho de que, en muchos países, la legislación vigente en materia de comunicación y almacenamiento de información es inadecuada u obsoleta porque no contempla el uso del comercio electrónico. La ley modelo pretendía establecer un trato igual en el derecho para los contratos en línea y fuera de línea (es decir, un "entorno independiente del formato de los contratos"), proporcionando normas y reglas para dar validez a contratos concertados por medios electrónicos, definir las características de un escrito y una firma electrónicos válidos, y prestar asesoramiento acerca del reconocimiento jurídico de los mensajes de datos (por ejemplo, la admisibilidad y la fuerza probatoria que debe darse a los mensajes de datos).

En la *Guía para la Incorporación al Derecho Interno de la Ley Modelo* se señala que ésta no pretende interferir en la legislación sobre la formación de contratos, sino promover el comercio internacional al proporcionar mayor seguridad jurídica a la firma de contratos por medios electrónicos. Los contratos de comercio electrónico deberían seguir cumpliendo los principios tradicionales y neutrales, desde el punto de vista tecnológico, necesarios para su validez. Normalmente, determinar esos principios ha sido competencia del derecho interno o local.

En general, la oferta realizada por una parte y la aceptación de esa oferta por la otra es necesaria para la formación de un contrato. En este sentido, la ley modelo establece en el artículo 11:

---

[12] CNUDMI, *Ley Modelo sobre Comercio Electrónico con Guía para la incorporación al Derecho Interno* (1996), con el Artículo Suplementario 5 bis., como se aprobó en 1998, en [línea] http://www.uncitral.org.english/texts/elect/ml.ec.htm

[13] La Ley Modelo de la CNUDMI hace referencia al intercambio electrónico de datos (EDI), que no hace mucho se consideraba una de las formas más comunes de contrato en línea. Los acuerdos EDI se utilizaban con frecuencia en relaciones contractuales en curso que vinculaban a los minoristas o a los fabricantes con sus proveedores habituales, en un esfuerzo por controlar y evitar el inventario. Las condiciones de estos acuerdos renegociaban normalmente entre las partes a fin de establecer derechos y obligaciones pormenorizados en relación con su funcionamiento continuado. Véase M. Chissick y A. Kelman, *Electronic Commerce: Law and Practice*, p. 53 (Sweet y Maxwell, 1999).

"En la concertación de un contrato, de no convenir las partes otra cosa, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación un mensaje de datos."

También se requiere una contrapartida de peso (es decir, un valor) para que el acuerdo, el cual era una serie de promesas, se transforme en un contrato vinculante y ejecutorio. Sin embargo, esa contrapartida de peso se expone a muchas interpretaciones en el contexto del comercio electrónico.

El comercio electrónico plantea problemas en relación con algunas de las nuevas modalidades utilizadas para lograr una oferta y su aceptación en el entorno en línea.[14] Se concede mucha importancia a la claridad y la transparencia de las condiciones contractuales, sobre todo porque en los contratos electrónicos pueden intervenir partes de diferentes lugares del mundo que quizá tengan muy poco contacto entre sí, cuando no ninguno, aparte de sus comunicaciones en línea. Debido a estas limitaciones, las partes que redactan los contratos y las que los aceptan deben tener presentes algunas condiciones, como los descargos de responsabilidad, la elección del derecho y la competencia y el derecho aplicable, la protección del consumidor, la limitación en materia de responsabilidad y los problemas del derecho local imperativo. No conceder la debida importancia a estas cuestiones puede truncar las expectativas de las partes.[15]

En cuanto a las formalidades contractuales y probatorias, existe el creciente consenso de que, hasta que las comunicaciones electrónicas cuenten con un grado suficiente de seguridad, durabilidad e integridad respecto a su contenido, no se exigirá una forma o un procedimiento formal en particular destinado a garantizar su efectividad a los fines para los que se creó. La ley modelo establece que "cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos si la información que éste contiene es accesible para su ulterior consulta". En lo que referente al requisito jurídico de que la información esté en su "forma original", esa condición quedará satisfecha "con un mensaje

[14] Por ejemplo, un contrato puede constituirse mediante un mensaje de correo electrónico, pero este tipo de contrato puede despertar dudas sobre la autenticidad de las partes. También se puede celebrar un contrato a través de un sitio web. En ese caso, para indicar la aceptación se hace clic en un botón específico, es decir, en un cuadro de diálogo que obliga al cliente a examinar las condiciones antes de hacer clic en el botón "aceptar".

[15] Al igual que en algunos acuerdos adoptados fuera de línea, *off line*, en los que las partes apenas negocian las condiciones o no lo hacen en absoluto, los contratos en línea a menudo elaboran condiciones estándar. En lo que atañe al consumidor, cuando esas condiciones aparecen en un modelo uniforme de contrato preparado por la empresa e imponen condiciones restrictivas al consumidor, el acuerdo es un contrato de adhesión, lo que no puede plantear problemas de ejecución. Algunos instrumentos internacionales que se desarrollan para abordar cuestiones jurídicas como la jurisdicción establecen disposiciones especiales encaminadas a proteger a los consumidores.

de datos si existe alguna garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma". Además, en cuanto al requisito de la firma, basta con que el método empleado en una comunicación electrónica para identificar a una persona e indicar que ha aprobado la información contenida en el mensaje resulte "tan confiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente".

2. Internet-jurisdicción y derecho aplicable

Internet debe ser de jurisdicción internacional. Los usuarios pueden acceder a esta red prácticamente desde cualquier lugar del mundo. Debido a la tecnología de conmutación de paquetes y al complejo entramado de las redes digitales y la infraestructura de las telecomunicaciones, la información digitalizada puede viajar a través de diversos países y jurisdicciones, cada uno con su propio sistema jurídico, para alcanzar su destino.

Como este medio internacional repercute en un mundo conformado por países separados, los problemas jurídicos cobran mucha importancia, sobre todo en el contexto de la propiedad intelectual. Sin embargo, esos problemas sobrepasan el campo de la propiedad intelectual e inciden en otros ámbitos: en los contratos (mencionados anteriormente), el fraude y los comportamientos delictivos de toda índole, la protección del consumidor, la fiscalidad y la regulación del contenido en línea relativo a la obscenidad y el derecho penal. En el contexto del derecho internacional privado se plantean las siguientes cuestiones interrelacionadas:

- La potestad para atribuir una controversia a una jurisdicción (el fuero o *situs*).
- El derecho aplicable a la controversia (elección del derecho aplicable o conflicto de leyes).
- El reconocimiento y el cumplimiento de decisiones judiciales tomadas en jurisdicciones extranjeras.

En el comercio electrónico, estas cuestiones se complican porque una o más de las partes que intervienen (o de los procedimientos que se utilizan) en las actividades comerciales —en particular, los usuarios de internet, los proveedores de servicios y de contenido, los compradores, los vendedores, las empresas (y sus activos), los sistemas tecnológicos y los servidores informáticos— pueden encontrarse en países diferentes. La incertidumbre puede surgir no sólo respecto del *lugar* donde se realizan las actividades en cuestión, sino también las propias actividades pueden

tener consecuencias *previstas* o *imprevistas* en todo el mundo, lo cual genera incertidumbre cuando hay que localizar la controversia, determinar el derecho aplicable y los aspectos prácticos de seguir adelante con el cumplimiento o buscar alternativas adecuadas de solución de controversias. Los titulares de derechos de propiedad intelectual que desean gestionar sus derechos mediante acuerdos de licencia o hacerlos valer frente a posibles infracciones se enfrentan a problemas de difícil solución. En el caso de una licencia para proteger derechos en internet, se debe considerar cuáles leyes de qué países pueden afectar el acuerdo, en particular aquellas sobre contratos electrónicos, protección del consumidor, propiedad intelectual, descargo de responsabilidad y confidencialidad. En caso de que los titulares quieran hacer valer sus derechos, deberán decidir no sólo contra quién (o contra qué) ejercitan la acción, sino también en qué jurisdicción y de conformidad con qué legislación.

a) Evolución del derecho internacional privado

En el ámbito internacional, las cuestiones relativas a la jurisdicción, el derecho aplicable y el reconocimiento y el cumplimiento de decisiones judiciales extranjeras se han resuelto con base en el derecho internacional privado. En principio, cada país determina sus normas de derecho internacional privado. Aunque en ciertas regiones del mundo algunas de esas reglas se han armonizado mediante tratados, el panorama general sigue siendo un mosaico de complejas disposiciones. En el contexto del comercio electrónico, un entorno así no facilita el objetivo de resolver las controversias de propiedad intelectual, pues permite que se cometan infracciones sin que exista una jurisdicción clara y adecuada en la cual el titular pueda interponer una demanda, y fomenta la búsqueda del fuero más conveniente al generar incertidumbre y decisiones potencialmente conflictivas.

En junio de 1997, la Conferencia de La Haya de Derecho Internacional Privado convocó una comisión especial para estudiar la jurisdicción internacional y los efectos de las decisiones de los tribunales extranjeros sobre cuestiones civiles y comerciales. En el marco de una serie de reuniones, la comisión especial ha elaborado un "Anteproyecto de convenio sobre competencia judicial y resoluciones judiciales extranjeras en materia civil y mercantil". El proyecto tenía dos objetivos: en primer lugar, armonizar las normas jurídicas y limitar los lugares donde puede entablarse acciones judiciales ante un pequeño número de tribunales adecuados, evitando así una multiplicidad innecesaria de procedimientos y posibles decisiones judiciales contradictorias; y, en segundo, simplificar y agilizar el reconocimiento y el cumplimiento de las decisiones judiciales, siempre que satisfagan las disposiciones del anteproyecto de convenio.

b) Competencia y derecho aplicable

Cuando interviene un elemento extranjero, el primer paso del tribunal será decidir si es competente o no para conocer del caso. Tanto el Convenio de La Haya como la propuesta de Reglamento de la Unión Europea contienen disposiciones encaminadas a armonizar las reglas sobre este punto. Es importante tener en cuenta las consideraciones relativas a la propiedad intelectual, así como las repercusiones del comercio electrónico mundial, ya que esos instrumentos favorecen su posible aplicación y entrada en vigor. En este sentido, los seis puntos que se citan a continuación pretenden destacar aspectos de las disposiciones que regulan la competencia y el derecho aplicable.

c) Jurisdicción general y especial

El proyecto de Convenio de La Haya divide los criterios que fundamentan la competencia jurisdiccional en tres categorías:

- Causas obligatorias de competencia jurisdiccional, que pasarían a incorporarse al derecho interno como resultado de su ratificación.
- Causas que prohíben la competencia jurisdiccional.
- Causas autorizadas de competencia jurisdiccional en virtud del derecho interno, pero sometidas a la condición de que las decisiones judiciales basadas en esos motivos sean ejecutorias únicamente en virtud del derecho interno y no del convenio.

Dentro de la primera categoría, el artículo 3 contiene, como asunto de jurisdicción general, la disposición de que el acusado puede ser demandado judicialmente en el Estado donde resida habitualmente. La jurisdicción es general en el sentido de que el tribunal está autorizado a ocuparse de todas las demandas que haya contra el demandado, sin importar su naturaleza. Este concepto se acerca mucho al enfoque adoptado por el Convenio de Bruselas, pero se diferencia en que el vínculo pertinente no es el *domicilio* sino la *residencia habitual* del demandado.

El artículo 18.2 *e*), que pertenece a la segunda categoría de las mencionadas, excluye de forma expresa la posibilidad de asumir la jurisdicción general del derecho interno de un Estado contratante por la mera razón de "realizar actividades comerciales o de otra índole", pero permite una jurisdicción especial o especifica de conformidad con el derecho interno (véase la tercera categoría en el párrafo 46) si la controversia está "directamente relacionada" con esas actividades. En ese caso, la jurisdicción general sólo sería admisible cuando a las actividades comerciales o de otra naturaleza venga a sumarse el hecho de que el demandado reside habitualmente en el Estado del fuero.

Algunos expertos han señalado que esa regla podría alterar significativamente una base tradicional de jurisdicción en Estados Unidos, según la cual se acepta la jurisdicción general, cuando el demandado "ejerce actividades" de manera "sistemática y continua" en territorio de la jurisdicción.

La propuesta de Reglamento de la Comisión Europea se divide en jurisdicción general y normas jurídicas que se aplican en relación con áreas específicas cuando se demanda una persona de un Estado miembro ante los tribunales de otro Estado miembro (por ejemplo, contratos entre consumidores, contratos de trabajo y jurisdicción exclusiva). El artículo 2 establece la norma de jurisdicción general de que las personas "domiciliadas" en un Estado contratante "estarán sometidas (...) a los órganos jurisdiccionales de dicho Estado", a reserva de las demás disposiciones de la propuesta de reglamento (por ejemplo, la jurisdicción exclusiva, como se verá más adelante).

d) Controversias en relación con contratos en los que no ha habido elección del derecho aplicable

Algunos de estos problemas se reflejan en el proyecto de Convenio de La Haya y la propuesta de Reglamento de la Comisión Europea, concernientes a controversias derivadas de *relaciones contractuales* en las que las partes no hayan establecido el derecho aplicable para resolver sus diferencias. El proyecto de Convenio de La Haya estipula que puede presentarse una demanda ante los tribunales del Estado donde se hubiesen entregado o prestado, parcial o totalmente, los bienes o servicios o en asuntos relativos tanto a bienes como a servicios, en el lugar donde se hubiese cumplido la obligación principal, parcial o totalmente. La propuesta de reglamento prevé, de manera similar, que, en lo referente a contratos, una persona de un Estado miembro puede ser demandada en otro Estado miembro en los tribunales "del lugar de cumplimiento de la obligación particular". El "lugar de cumplimiento", respecto de los bienes o los servicios, se define, respectivamente, como el lugar donde, en virtud del contrato, éstos se entregan o prestan (o deberían haberse entregado o prestado).

En relación con las transacciones en las que se hace un pedido en línea, pero los bienes o servicios se envían al cliente fuera de línea, se aplican las normas vigentes de derecho internacional privado. Sin embargo, en las transacciones que se realizan exclusivamente en línea, el lugar del cumplimiento puede ser difícil de precisar. ¿Coincidiría con la ubicación de la computadora del comprador (por ejemplo, un programa que se descarga en la computadora del cliente) o con el sistema del vendedor (por ejemplo, la compra de valores en línea mediante procesos informáticos en el servidor del vendedor)? Para evitar esos

posibles problemas, siempre que sea posible en los acuerdos en línea se debería designar el lugar donde, de acuerdo con el contrato, se considera que el cumplimiento ha tenido lugar o, mejor aún, especificar el tribunal o tribunales que, previo acuerdo de las partes, tendrán autoridad jurídica en caso de controversia.

e) Derecho aplicable

Una vez que el tribunal haya determinado si es competente para conocer del caso, debe decidir qué derecho sustantivo ha de aplicarse para pronunciarse sobre el fondo de la controversia. Esto puede resultar difícil cuando interviene en el caso un elemento extranjero. La determinación del derecho aplicable guarda relación con muchas de las mismas cuestiones debatidas anteriormente en cuanto a determinar la jurisdicción adecuada; de hecho, los problemas en materia de conflictos de leyes se ven agravados por la incertidumbre al fijar el fuero competente en el ámbito de internet y el comercio electrónico. Por ejemplo, en el contexto del derecho de autor, cuando se pone material protegido a disposición de los consumidores de varios países o se les transmite, puede haber incertidumbre no sólo respecto de la jurisdicción adecuada para entablar una acción, sino también en lo atingente al país cuyo derecho regirá la determinación de la titularidad, el alcance de los derechos y la validez de los acuerdos contractuales. Estas cuestiones siempre son complicadas, pero revisten mayor complejidad en el entorno en línea.

En ese orden de ideas, en el derecho internacional privado la cuestión del derecho aplicable es casi tan complicada como otra cuestión estrechamente relacionada —la determinación del fuero jurisdiccional— y, como se verá más adelante, también repercute en la protección de los derechos de propiedad intelectual. Incluso sin los efectos del comercio electrónico, los contratos referentes a la explotación internacional de los derechos de propiedad intelectual siempre han dado lugar a complicados problemas de elección del derecho aplicable.

El principio normativo general, tal como se codifica en los instrumentos nacionales e internacionales pertinentes, es respetar la elección del derecho aplicable hecha por las partes. En Europa, el Convenio de Roma sobre la ley aplicable a las obligaciones contractuales regula este aspecto al establecer con carácter general que "los contratos se regirán por la ley elegida por las partes". En 1997, el gobierno de Estados Unidos formuló un "Marco para el comercio electrónico mundial", en el cual se establece que Estados Unidos debe colaborar de manera estrecha con otras naciones para aclarar las normas jurídicas aplicables y para *favorecer y reforzar con carácter general las dispo-*

siciones contractuales que permiten a las partes seleccionar normas sustantivas en materia de responsabilidad. Sin embargo, en la Unión Americana la disposición pertinente en muchos estados ha incluido una limitación considerada problemática, si se tiene en cuenta la nueva economía digital. El *Uniform Commercial Code*, un código que sirve como modelo para la legislación estatal, hace hincapié en que cuando una transacción da origen a una *relación razonable* para un Estado y para otro Estado o nación, las partes pueden acordar que el derecho del primero o del segundo Estado regule sus derechos y deberes. Por tanto, la elección del derecho aplicable de las partes sólo se considerará válida si la transacción da lugar a una "relación razonable" a juicio de la jurisdicción del derecho elegido. Se considera que existe una relación razonable cuando la celebración del contrato, o una parte significativa de su cumplimiento, se realiza en la jurisdicción designada. No obstante, en las transacciones que tienen lugar completamente en línea, determinar el lugar del contrato o el lugar del cumplimiento puede ser problemático.

A ese respecto no han dejado de tomarse iniciativas para crear nuevas normas aplicables en el entorno en línea. La *Uniform Computer Information Transactions Act* (UCITA), adoptada en julio de 1999 por la *National Conference of Commissioners on Uniform State Laws*, pasa por alto la prueba de la existencia de una relación razonable y establece simplemente que, salvo en el caso de los contratos que no hayan sido celebrados por los consumidores, las partes del acuerdo podrán elegir el derecho aplicable. Debido a la dificultad mencionada para determinar puntos de vinculación pertinentes, esta disposición, así como la del Convenio de Roma, resultan positivas para el comercio electrónico; además, reflejan el creciente consenso en cuanto a la necesidad de respetar el principio de libertad de contrato en la ley como manera de facilitar el comercio electrónico y las expectativas de las partes en un entorno jurídico internacional complejo. Lo mismo cabe decir de la explotación internacional de la propiedad intelectual, sujeta a cualquier limitación que establezca la política pública de un Estado.

f) Procedimientos alternativos de solución de controversias

Poner fin a actividades perjudiciales en un medio mundial en constante evolución como internet mediante mecanismos judiciales vinculados con un territorio puede convertirse en una tarea cada vez más compleja. Para complementar los procedimientos ante los tribunales puede recurrirse a procedimientos alternativos de solución de conflictos que quizá resulten útiles en la medida en que ofrezcan a los titulares de

derechos mecanismos para obtener medidas correctivas rápidas y eficaces, que tengan en cuenta la facilidad con la que pueden tener lugar las infracciones de derechos de propiedad intelectual en internet.

Esos procedimientos ofrecen una solución internacional a los problemas jurídicos mencionados. El *arbitraje* es un procedimiento privado y vinculante, a la vez que funciona en un marco jurídico internacional sólidamente establecido y aplicable en el ámbito público.[16] El arbitraje puede ofrecer una solución única a las controversias multijurisdiccionales derivadas del comercio en las redes mundiales. Al mismo tiempo, la naturaleza y la rapidez de las actividades comerciales electrónicas han presionado para que se agilice y reduzcan tanto el tiempo como los costos de los procedimientos arbitrales tradicionales.

Los procedimientos de solución de controversias en línea pueden mejorar el acceso a los mecanismos de solución, al tiempo que aumentan la velocidad y la eficacia con que se realizan esos procedimientos y se reducen los correspondientes costos. Muchas partes involucradas en controversias derivadas del comercio en internet quizá no conocen bien los procedimientos jurídicos requeridos. Permitir entablar una acción judicial o defenderse contra una denuncia accediendo a un sitio web y cumplimentando los formularios electrónicos, guiados en las diversas fases del proceso, reduciría, sin duda, las barreras de acceso a cualquier procedimiento existente. Además, la posibilidad de presentar documentos mediante internet permite que las partes remitan de manera inmediata un gran número de documentos a cualquier distancia, y sin costo alguno. Los documentos pueden procesarse, almacenarse y archivarse mediante sistemas automatizados de gestión, y las partes autorizadas pueden examinarlos desde cualquier lugar, las 24 horas del día, por medio de una interfaz de internet. Con el desarrollo de sistemas multimedia, las partes también podrán llevar a cabo reuniones en línea, con lo cual reducirán en gran medida los gastos de viaje y los costos de organización.

Junto con la creación de un sistema técnico que permita que los procesos se realicen en línea, es preciso establecer el marco jurídico necesario. Las reglas de arbitraje vigentes pueden proporcionar una base para cualquier adaptación al entorno en línea que se requiera. Entre las cuestiones que deben abordarse cabe destacar los derechos de acceso de las partes a los documentos, los procedimientos aplicables en caso de problemas de autenticidad, los datos de contacto a efectos de notificación, el cálculo de los periodos (habida cuenta de

[16] Véase el Convenio de Nueva York sobre el reconocimiento y el cumplimiento de las sentencias arbitrales extranjeras (1959), disponible [en línea] en: http://www.uncitral.org/en-index.htm

las posibles diferencias de huso horario entre los lugares desde los que las partes realizan las operaciones), y los requisitos para la escritura y firma de las cláusulas de controversias, las notificaciones a las partes y las sentencias. Además, los plazos para realizar los diversos trámites en el marco del procedimiento pueden acortarse, lo que se traducirá en un desarrollo más rápido y económico de los procedimientos.

3. Tecnología digital: problemas de observancia y confidencialidad[17]

a) Sistemas de clave pública y certificados digitales

La tecnología y la comprensión de las matemáticas inherentes a los sistemas *de clave pública* aparentemente confirman que estos sistemas serán muy convenientes para los servicios de comercio electrónico, si se adoptan y aplican decisiones políticas adecuadas en las relaciones entre un par de claves (la pública y la privada) y una entidad. Publicar una clave pública y asociarla a un nombre es un ejercicio sencillo, pero ¿cómo puede hacerse para demostrar dicha relación? La práctica actual invita a introducir la clave pública de un individuo en un *certificado digital* junto con información relativa a la clave (por ejemplo, la fecha de vencimiento) y al propietario de dicha clave (nombre, etc.). Luego, una tercera parte de confianza "firma" este certificado, lo cual significa que aprueba la reivindicación de identidad implícita en el certificado. Esta tercera parte de confianza, conocida como *autoridad de certificación*, da a conocer al público sus normas de comprobación de la identidad. Al comprobar esta firma, se puede determinar si la información que el certificado contiene ha sido o no manipulada (por ejemplo, si se ha asociado un nombre falso a la clave). Controlar la firma de la autoridad de certificación permite tener confianza en la identidad del remitente.

b) Confiabilidad de la autoridad de certificación

Naturalmente, algunas cuestiones clave corresponden al grado de confianza que las organizaciones de propiedad intelectual deberían conceder a las autoridades de certificación desconocidas. Por lo general, un usuario no sabrá nada de antemano acerca de las prácticas utilizadas por la autoridad de certificación para garantizar la identidad de un

[17] Enrique, Vázquez, *Comercio electrónico: visión general*, Julio Berrocal, Departamento de Ingeniería de Sistemas Telemáticos (http://www.dit.upm.es/), Universidad de Madrid.

individuo certificado por ella. Las autoridades de certificación suelen publicar sus prácticas de comprobación de la identidad en una *Declaración de prácticas de certificación* y en cada certificado incluyen información acerca de la práctica utilizada para la entidad correspondiente. Si la publicación es de una autoridad de certificación de confianza, en ella se encontrará toda la información necesaria para que el individuo decida si ha de confiar en la relación entre una entidad y un par de claves.

Desafortunadamente, aún queda pendiente la cuestión del profesionalismo general y de la confiabilidad de la autoridad de certificación. Podría ocurrir que una autoridad de certificación poco seria publique una declaración de prácticas de certificación con un procedimiento detallado de certificación de la identidad, pero que no siga ese procedimiento en ningún caso. Ello quebrantaría la confianza entre la autoridad de certificación y el público. Debido a que la mayoría de las autoridades de certificación son organizaciones no sujetas a un control por la comunidad de la propiedad intelectual, algunos comentaristas consideran razonable depositar su confianza en una tercera parte internacional de confianza que haga las veces de autoridad máxima de certificación o de autoridad de certificación puente para las transacciones relacionadas con la propiedad intelectual.

c) Infraestructura de clave pública (PKI)

Las cuestiones de gestión relativas al uso de las claves pública y privada se abordan merced al desarrollo de una *infraestructura de clave pública* (PKI) destinada a apoyar a los participantes que cooperan. A efecto de tratar correctamente estas cuestiones, una parte de confianza debe mantener la infraestructura para proporcionar estos y otros servicios. Habida cuenta del valor y del carácter delicado de la información referente a la propiedad intelectual, se plantea la cuestión de si dicha responsabilidad debería, en todos los casos, confiarse a las empresas comerciales. Otra opción sería que una organización internacional, como la OMPI, hiciera las veces de autoridad de certificación propiamente dicha o de autoridad de certificación puente, con lo cual no emitiría certificados propios (salvo quizá de forma interna y limitada), sino que serviría de puente en el ámbito de la confianza necesaria entre distintas autoridades de certificación a escala internacional. La autoridad de certificación puente emplearía medios bien definidos y públicos para validar los certificados emitidos de forma privada que se utilizarían en transacciones de propiedad intelectual. A continuación figura una lista con una serie de cuestiones "de gestión clave" para las autoridades de certificación.

d) Revocación de la clave

Las claves perdidas o comprometidas de cualquier otra forma plantean un problema de gestión. Si la clave privada de un individuo se encuentra comprometida, no será evidente que un usuario sepa que no se debe utilizar la clave pública asociada para garantizar la confidencialidad de un mensaje destinado a ese usuario. Además, de ninguna forma podrá el individuo sospechar que existen problemas con un mensaje autenticado con esa clave, ya que aún se dispondría de un certificado válido.

La solución de dicho problema consiste en poseer una *lista de revocación de certificados* a la que se pueda acceder con facilidad y en la que se incluyan todos los certificados revocados por un motivo u otro. Esta lista debería controlarse cada vez que se emplea una clave pública de cualquier usuario. Si bien no se puede obligar a los usuarios a utilizar dicha lista, su existencia puede hacer que las organizaciones interesadas elaboren políticas de acceso a ella. Cada una de las autoridades de certificación consideradas adecuadas por la comunidad de la propiedad intelectual deberá mantener listas de revocación de certificados.

e) Almacenamiento de claves

Este almacenamiento plantea una cuestión sutil aunque importante. Todas las claves privadas deben estar cuidadosamente protegidas y mantenerse aseguradas para garantizar la integridad del entorno del sistema de claves públicas. Las claves privadas generadas por aplicación (por ejemplo aquellas creadas por los exploradores de la web) se suelen almacenar en la máquina local del usuario, lo que tiende a restringir el uso de una clave en una máquina determinada. Si se almacena la clave en un medio portátil (por ejemplo, un disquete), podrá ser útil, pero aumentará el riesgo de tener problemas de seguridad ya que el disquete puede copiarse de manera fácil e inadvertida.

Un método relativamente seguro y conveniente de mejorar la integridad de almacenamiento de las claves consiste en usar las llamadas *tarjetas con microcircuito*. Una tarjeta con microcircuito es un pequeño instrumento electrónico personal que contiene la clave privada en cuestión. Esta tarjeta puede introducirse en un lector de tarjetas con microcircuito en el que el usuario debe incorporar un breve identificador personal para proteger la clave en caso de robo de la tarjeta. Si el identificador (por ejemplo, un número pequeño) es el correcto, el sistema pertinente leerá y utilizará la clave privada. Si bien se trata de una tecnología eficaz, sólo es segura en la medida en que el usuario elige el identificador. Existen muchos casos en los que deberían utili-

zarse (y compartirse) las tarjetas con microcircuito y las tecnologías de lectura de dichas tarjetas.

f) Recuperación de claves

Al cifrar los datos de forma muy segura, se vislumbra el espectro del desastre provocado por el error humano: la pérdida o el daño de una clave privada y la consiguiente pérdida de los datos codificados. Si se llega a perder o dañar una clave privada, no habrá forma de recuperar los datos cifrados, salvo mediante un ataque criptográfico. Las técnicas de recuperación de claves permiten a los usuarios autorizados recuperar una copia de una clave privada o secreta cuando el original está dañado o no se halla disponible por cualquier otra razón. En uno de los modelos, una clave de sesión, como la secreta DES o RC4 introducida en un sobre digital, figura por partida doble en el sobre. La primera copia está cifrada con la clave pública del destinatario y la segunda con la clave pública (muy sólida) de la autoridad de recuperación de claves. Por consiguiente, si no se dispone de la clave privada necesaria para recuperar la primera copia, será posible descifrar la segunda clave con ayuda de la autoridad de recuperación de claves. Es evidente que los sistemas de recuperación de claves pueden percibirse como una amenaza para la seguridad; no obstante, muchas prácticas comerciales exigen el acceso de la autoridad máxima a datos que, de otro modo, serían irrecuperables a causa de accidentes o actos de perversidad (por ejemplo, reacciones de empleados descontentos). La recuperación de claves es una opción que debería aprovecharse cuando no es posible aceptar la pérdida inevitable de información como consecuencia de errores humanos.

g) Firma electrónica y firma digital

El punto de partida en toda legislación en materia de firmas electrónicas reside en determinar cómo un mensaje de datos se puede "firmar" y luego ser enviado, recibido, archivado o comunicado en forma electrónica. Por lo común, esta "firma" se ha denominado *firma electrónica* o *firma digital*. Desgraciadamente, tales conceptos no se encuentran libres de confusión, por lo que, para efectos de esta ponencia, enseguida se definen según la tendencia internacional generalmente aceptada:

Firma electrónica. Es el término genérico y neutral para referirse al universo de tecnologías mediante las cuales una persona puede "firmar" un mensaje de datos. Si bien todas las firmas electrónicas son archivos digitales (compuestos de unos y ceros), pueden manifestarse

de diversas formas. Ejemplos de firmas electrónicas incluyen escribir el nombre del emisor al final de un correo electrónico, la digitalización de nuestra firma como un archivo gráfico, un número de identificación personal (NIP), ciertas biometrías utilizadas para efectos de identificación (como la huella digital o la retina) y las firmas digitales (creadas mediante el uso de criptografía).

Firma digital. Es simplemente el nombre que se da a cierto tipo de firma electrónica basada en el uso de criptografía, entre las cuales la más comúnmente usada es la llamada *criptografía asimétrica o de llave pública*. Éste es el tipo de firma alrededor del cual se han realizado las principales inversiones, esfuerzos tecnológicos y respuestas legislativas alrededor del mundo.

h) Encriptamiento

La criptografía (del griego *kryptos*, ocultar, y *grafos*, escribir, literalmente "escritura oculta") es el arte o ciencia de cifrar y descifrar información mediante el empleo de técnicas matemáticas que hagan posible el intercambio de mensajes de tal manera que sólo puedan leerlos las personas a quienes van dirigidos.

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y, en segundo, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea en realidad quien dice ser y que el contenido del mensaje enviado, por lo común denominado criptograma, no haya sido modificado en su tránsito.

En la actualidad, la criptografía se utiliza no sólo para comunicar información de forma segura ocultando su contenido a posibles fisgones. Una de las ramas de la criptografía que más ha revolucionado el panorama actual de las tecnologías de la información es el de la firma digital: tecnología que busca asociar al emisor de un mensaje con su contenido de forma tal que aquél no pueda repudiarlo después.

Criptografía simétrica o convencional. Esta criptografía es el método criptográfico que usa una misma clave para cifrar y para descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano en cuál clave usar. Una vez que ambas tienen acceso a esta clave, el remitente cifra un mensaje al utilizarla, lo envía al destinatario y éste lo descifra con ella.

Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se emplea. Sólo si el atacante obtuviera la clave, le serviría conocer el algoritmo. Los algoritmos de ci-

frado que se usan por ejemplo en el sistema GNU, GnuPG tienen estas propiedades.

Como toda la seguridad está en la clave, es importante que sea muy difícil adivinar el tipo de clave. Hoy las computadoras pueden adivinar claves con extrema rapidez, y por esta razón es importante el tamaño de la clave en los criptosistemas modernos. El algoritmo de cifrado DES utiliza una clave de 56 bits, lo cual significa que hay 2 elevado a 56 claves posibles. Esto representa un número muy alto de claves, pero una máquina computadora de uso general puede comprobar todo el espacio posible de claves en cuestión de días, aunque una máquina especializada puede hacerlo en horas. Por otra parte, algoritmos de cifrado de diseño más reciente como 3DES, Blowfish e IDEA usan todos claves de 128 bits, lo que significa que existen 2 elevado a 128 claves posibles.

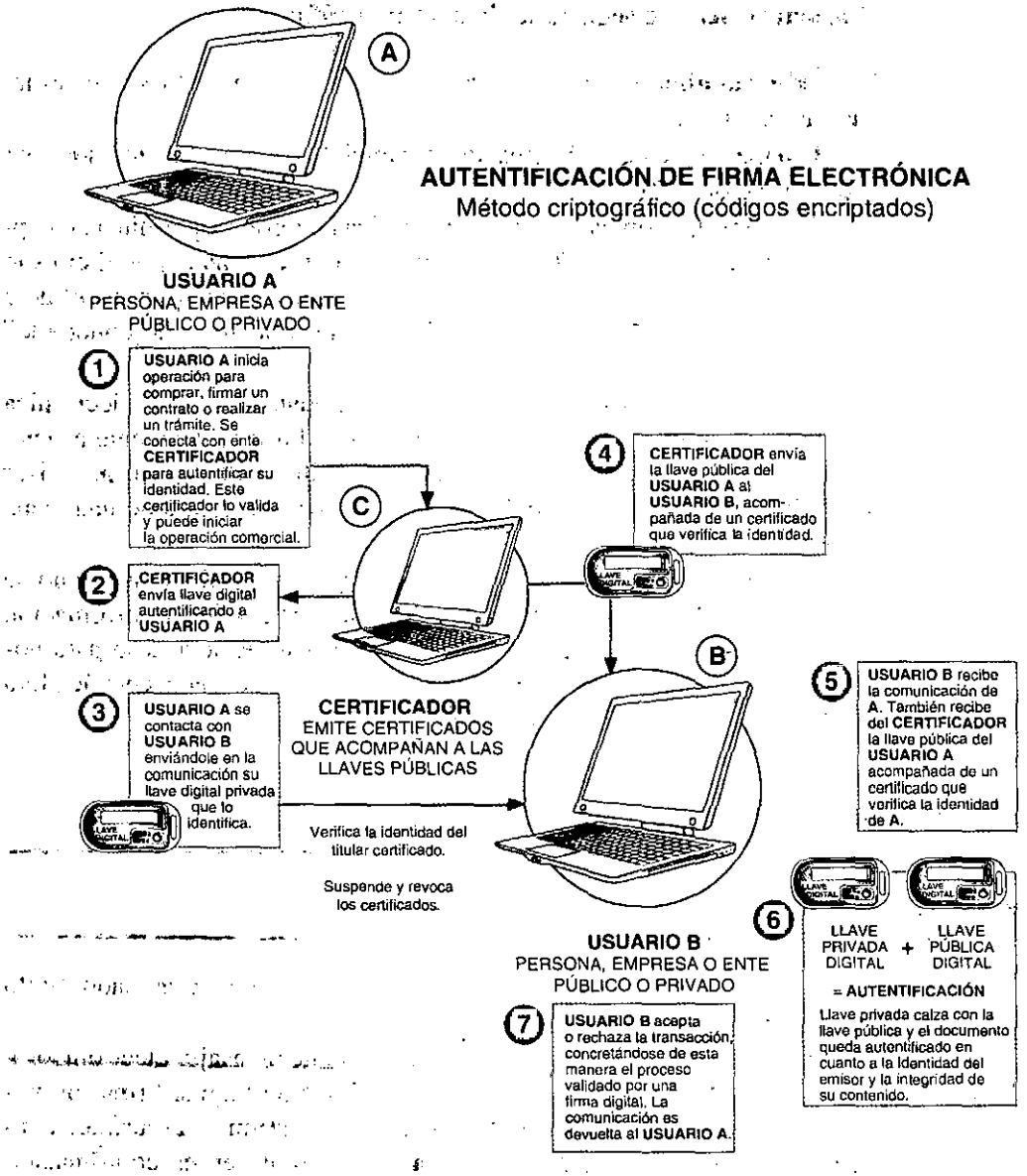
El principal problema con los sistemas de cifrado simétrico no está relacionado con su seguridad, sino con el intercambio de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero ¿qué canal de comunicación que sea seguro han empleado para transmitirse la clave entre sí? Sería mucho más fácil para un atacante interceptar una clave que probar las posibles combinaciones del espacio de claves. Otro problema es el número de claves que se necesitan. Si hay un número n de personas que deben comunicarse entre ellas, se requerirán $n(n\text{-}1)/2$ claves para cada pareja de personas que tengan que comunicarse de modo privado. Esto puede funcionar con un grupo reducido de personas, pero sería imposible llevarlo a cabo con grupos más grandes.

Criptografía asimétrica o de clave pública. Esta criptografía es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, mientras que la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella.

El remitente usa la clave pública del destinatario para cifrar el mensaje y, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje.

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos.

Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa clave pública podrá usarla cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.



Clave pública. Es uno de los documentos electrónicos que genera el uso de algoritmo asimétrico y que se publica junto con el certificado digital para cifrar información que desea enviar el propietario de la llave privada. La llave pública se presenta dentro del archivo de requerimiento para presentarlo ante el SAT y obtener un certificado digital.

Clave privada. Es uno de los documentos electrónicos que genera el uso de algoritmo asimétrico y que sólo debe conocer y resguardar el propietario del par de llaves (pública/privada). Con esta llave privada se realiza el firmado digital, el cual codifica el contenido de un mensaje.

Características de seguridad de la criptografía

Confidencialidad: se refiere al acceso a la información sólo por los usuarios autorizados.

Integridad: alude a la creación o cambio de la información sólo por usuarios autorizados.

La firma electrónica sustituye a la rúbrica autógrafa y permite al receptor del documento digital verificar la identidad proclamada por el emisor, mantener la integridad del contenido del documento digital transmitido e impedir al firmante desconocer la autoría del documento o "desconocerlo" después.

La firma electrónica avanzada son aquellos datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados a él por cualquier tecnología, cuyo propósito es identificar al emisor del mensaje como autor legítimo de éste, como si se tratara de una firma autógrafa.

Los certificados digitales tienen como objetivo identificar al dueño de una firma electrónica avanzada. Estos certificados contienen información diversa acerca del firmante, servicios a los que éste tiene acceso para utilizar su firma, la fecha de vigencia del certificado, la agencia certificadora que lo emitió, entre otras características.

SITUACIÓN INTERNACIONAL[18]

Estados Unidos

Ley del Estado de Utah sobre la Firma Digital. Código comentado, título 46, capítulo 3 (1996)

Objetivo: facilitar las transacciones mediante mensajes electrónicos y firmas digitales; reducir al mínimo la posibilidad de fraguar firmas digitales y el fraude en las transacciones electrónicas; instrumentar jurídicamente la incorporación de normas pertinentes, y establecer, en coordinación con diversos estados, normas uniformes acerca de la autenticación y confiabilidad de los mensajes de datos.

Ámbito de aplicación o cobertura: transacciones mediante mensajes electrónicos y firmas digitales, autenticación y confiabilidad de los mensajes de datos.

[18] Véase "Estudio comparativo de algunas leyes internacionales relativas a la firma digital", *Boletín de Política Informática del INEGI*, núm. 4, México, 2001.

Definiciones

a) *Firma digital*: transformación de un mensaje mediante un criptosistema asimétrico tal, que una persona posea el mensaje inicial y la clave pública del firmante pueda determinar con certeza si la transformación se creó con la clave privada que corresponde a la clave pública del firmante, y si el mensaje ha sido modificado desde que se efectuó la transformación.
b) *Criptosistema asimétrico*: algoritmo o serie de algoritmos que brindan un par de claves confiable.
c) *Certificado*: registro basado en la computadora que identifica a la autoridad certificante que lo emite; nombra o identifica a quien lo suscribe; contiene la clave pública de quien lo suscribe, y está firmado digitalmente por la autoridad certificante que lo emite.
d) *Repositorio*: sistema para almacenar y recuperar certificados y demás información pertinente a las firmas digitales.

Colombia

Ley de Comercio Electrónico en Colombia (Ley 527 de 1999)

Objetivo: definir y reglamentar el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, así como establecer las entidades de certificación.

Ámbito de aplicación o cobertura: empleo de firmas digitales en todo tipo de información en forma de mensaje de datos.

Definiciones

a) *Firma digital*: valor numérico que se adhiere a un mensaje de datos y que, por medio de un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.
b) *Mensaje de datos*: la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como el intercambio electrónico de datos (EDI), internet, el correo electrónico, el telegrama, el télex o el telefax.
c) *Entidad de certificación*: persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de

mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

d) *Sistema de información*: sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Perú

Ley Número 27269. Ley de Firmas y Certificados Digitales (2000)

Objetivo: utilizar la firma electrónica con la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.

Ámbito de aplicación o cobertura: firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a ellos, puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos.

Definiciones

a) *Firma digital*: firma electrónica que emplea una técnica de criptografía asimétrica, basada en el uso de un par de claves único, asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.

b) *Certificado digital*: documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada, confirmando su identidad.

c) *Entidad de certificación*: cumple con la función de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al certificado o aquellos que den seguridad al sistema de certificados en particular o del comercio electrónico en general; igualmente, podrán asumir las funciones de entidades de registro o verificación.

d) *Entidad de registro o verificación*: cumple con las funciones de acopiar datos y comprobar la información de un solicitante de certificado digital; identificar y autenticar al suscriptor de firma digital, y aceptar y autorizar solicitudes de emisión y cancelación de certificados digitales.

Venezuela

Ley sobre Mensajes de Datos y Firmas Electrónicas (2001)

Objetivo: otorgar y reconocer eficacia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato

electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los proveedores de servicios de certificación y los certificados electrónicos.

Ámbito de aplicación o cobertura: mensajes de datos y firmas electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro.

Definiciones

a) *Firma electrónica*: información creada o utilizada por el signatario, asociada al mensaje de datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.
b) *Mensajes de datos*: toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.
c) *Certificado electrónico*: mensaje de datos proporcionado por un proveedor de servicios de certificación que le atribuye certeza y validez a la firma electrónica.
d) *Proveedor de servicios de certificación*: persona dedicada a proporcionar certificados electrónicos y demás actividades previstas en este decreto-ley.
e) *Sistema de información*: aquel utilizado para generar, procesar o archivar de cualquier forma mensajes de datos.

Argentina

Decreto núm. 427/98, que permite usar firma digital para los actos internos del sector público nacional (1998)

Objetivo: optimizar la actividad de la administración pública nacional, mediante la adecuación de sus sistemas de registración de datos, la tendencia a eliminar el uso del papel y automatizar sus circuitos administrativos.

Ámbito de aplicación o cobertura: uso de la firma y el documento digital dentro del sector público nacional.

Definiciones

a) *Firma digital*: resultado de una transformación de un documento digital mediante el empleo de un criptosistema asimétrico y un digesto seguro, de tal forma que una persona que posea el documento digital inicial y la clave pública del firmante pueda determinar con certeza:

- Si la transformación se llevó a cabo con la clave privada que corresponde a la clave pública del firmante, lo que impide su repudio.
- Si el documento digital ha sido modificado desde que se efectuó la transformación, lo que garantiza su integridad. La conjunción de los dos requisitos anteriores garantiza su no repudio y su integridad.

b) *Documento digital*: representación digital de actos, hechos o datos jurídicamente relevantes.
c) *Documento digital firmado*: documento digital al que se le ha aplicado una firma digital.

Chile

Normatividad que regula el uso de la firma digital y los documentos electrónicos en la administración del Estado (1999)

Objetivo: regular el uso de la firma digital y los documentos electrónicos como soporte alternativo a la instrumentalización en papel de las actuaciones de los órganos de la administración del Estado.

Ámbito de aplicación o cobertura: firma digital y documentos electrónicos utilizados en la administración del Estado, salvo la Contraloría General de la República, el Banco Central y las municipalidades.

Definiciones

a) *Firma electrónica*: código informático que permite determinar la autenticidad de un documento electrónico y su integridad, pero que impide a su transmisor desconocer la autoría del mensaje en forma posterior.
b) *Firma digital*: especie de firma electrónica que resulta de un proceso informático validado, puesto en práctica por medio de un sistema criptográfico de claves públicas y privadas.
c) *Documento electrónico*: toda representación informática que da testimonio de un hecho.
d) *Certificado de firma digital*: documento electrónico por el ministro de fe del servicio respectivo que acredita la correspondencia entre una clave pública y la persona que es titular de ella.

Comunidad Europea

Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para la firma electrónica (1998).

Objetivo: garantizar el buen funcionamiento del mercado interior en el área de la firma electrónica, al instituir un marco jurídico homogéneo y adecuado para la Comunidad Europea y al definir criterios que fundamenten su reconocimiento legal.

Ámbito de aplicación o cobertura: la directiva regula el reconocimiento legal de la firma electrónica, pero no otros aspectos relacionados con la celebración y validez de los contratos u otras formalidades no contractuales que precisen firma. Asimismo, la directiva establece un marco jurídico para determinados servicios de certificación accesibles al público.

Definiciones

a) *Firma electrónica*: firma en forma digital integrada en unos datos, ajena o asociada con ellos, que utiliza un signatario para expresar conformidad con su contenido y que cumple los siguientes requisitos:

- Estar vinculada con el signatario de manera única.
- Permitir la identificación del signatario.
- Haber sido creada por medios que el signatario pueda mantener bajo su exclusivo control.
- Estar asociada con los datos relacionados de tal modo que se detecte cualquier modificación ulterior de éstos.

b) *Dispositivo de creación de firma*: los datos únicos, como códigos o claves criptográficas privadas, o un dispositivo físico de configuración única, que el signatario utiliza para crear la firma electrónica.

c) *Dispositivo de verificación de firma*: los datos únicos, como códigos o claves criptográficas públicas, o un dispositivo físico de configuración única, utilizado para verificar la firma electrónica.

d) *Certificado reconocido*: certificado digital que vincula un dispositivo de verificación de firma a una persona y confirma su identidad, y que cumple los requisitos establecidos en el anexo Y.

e) *Proveedor de servicios de certificación*: persona o entidad que expide certificados o presta otros servicios al público en relación con la firma electrónica.

Alemania

Ley de firma digital alemana (1997).

Objetivo: crear las condiciones generales para las firmas digitales con las que se puedan considerar seguras y que las falsificaciones de firmas digitales y las falsificaciones de información firmada puedan verificarse sin lugar a duda.

Ámbito de aplicación o cobertura: uso de firmas digitales, verificación y falsificación.

Definiciones

a) *Firma digital*: sello creado con una clave privada de firma sobre información digital; tal sello permite, mediante el uso de la clave pública asociada rotulada por un certificado de clave de un certificador o de una autoridad, verificar quién es el propietario de la clave de firma y la no falsificación de la información.
b) *Certificador*: persona física o jurídica que da fe a la atribución de claves públicas de firma de personas físicas y que mantiene una licencia para ese motivo.
c) *Certificado*: certificación digital rotulada con una firma digital respecto a la atribución de una clave de firma pública a una persona física (certificado de clave de firma), o una certificación digital especial que se refiere inequívocamente a un certificado de clave de firma y contiene información adicional (certificado de atributos).

España

Real decreto-ley 14/1999, del 17 de septiembre, sobre firma electrónica (1999)

Objetivo: establecer una regulación clara del uso de firma electrónica, a la que le atribuye eficacia jurídica y que prevé el régimen aplicable a los prestadores de servicios de certificación.

Ámbito de aplicación o cobertura: el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación. Las normas sobre esta actividad aplican a los prestadores de servicios establecidos en España.

Definiciones

a) *Firma electrónica*: conjunto de datos, en forma electrónica, ajenos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar de manera formal al autor o a los autores del documento que la recoge.
b) *Firma electrónica avanzada*: firma electrónica que permite identificar al signatario y creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente a él

y a los datos a los que se refiere, lo cual facilita detectar cualquier modificación ulterior de éstos.

c) *Certificado*: certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad.

d) *Prestador de servicios de certificación*: persona física o jurídica que expide certificados y que puede prestar otros servicios en relación con la firma electrónica.

Análisis de la legislación internacional sobre la firma digital

De acuerdo con el contenido de los rubros señalados, los puntos relevantes son los siguientes:

Objetivo

El objetivo general es regular el uso de la firma digital, al otorgarle validez y eficacia jurídica. En el caso de Argentina y Chile, se busca optimizar la actividad de la administración pública al sustituir el papel por el uso de medios electrónicos.

El estado de Utah considera reducir el fraude en las transacciones electrónicas, así como la falsificación de las firmas digitales.

Colombia dedica una parte al comercio electrónico de mercancías, es decir, integra en una misma ley el comercio electrónico, la firma digital y el acceso y empleo de mensajes de datos.

Ámbito de aplicación o cobertura

Las legislaciones se aplican al uso de firmas digitales que cumplan con lo establecido legalmente y que está previsto en cada una de sus respectivas leyes.

El ámbito de aplicación en Argentina y Chile es el sector público, es decir, los órganos de la administración del Estado que cada país reconoce.

Colombia señala que la ley no será aplicable a aquella información relacionada con las obligaciones contraídas por el Estado en los convenios y tratados internacionales, así como en las advertencias que deban ir impresas por disposición legal en ciertos productos, en razón del riesgo que implica su comercialización, uso o consumo.

La Comunidad Europea no regula aspectos relacionados con la celebración y validez de los contratos u otras formalidades no contractuales que precisen firma.

Definiciones

Las legislaciones contemplan los términos de firma electrónica y firma digital:

Firma electrónica: Chile, Venezuela y España coinciden en que es la información creada o utilizada que permite determinar su autenticidad y atribuirse a su autor.

Firma digital: el estado de Utah, Colombia, Perú, Argentina, Chile, la Comunidad Europea, Alemania y España coinciden en utilizar un criptosistema asimétrico basado en el uso de un par de claves (una pública y una privada relacionadas entre sí), de tal forma que, si una persona posee el mensaje inicial y la clave pública del firmante pueda determinar con certeza si la transformación se creó con la clave privada que corresponde a la clave pública del firmante y si el mensaje se modificó desde que se efectuó la transformación. España utiliza el término *firma electrónica avanzada* en lugar del de *firma digital* y Chile define ambos términos.

LA SITUACIÓN EN MÉXICO

En la década de 1990, México enmendó y adaptó sus leyes para promover el comercio electrónico. La apertura del país en la materia en el año 2000 ha sido un importante factor que ha influido en la decisión de adoptar nuevas tecnologías. Actualmente, más de 15 000 empresas mexicanas utilizan los medios de transacción electrónicos, por lo general el IED (intercambio electrónico de datos) e internet. México inició su principal actividad en 1998 con la creación de un grupo encargado de elaborar la primera ley sobre el comercio electrónico, basada en la ley modelo CNUDMI y en el estudio de las leyes de Estados Unidos, Canadá y algunos países de la Comunidad Europea. A la postre, esto trajo consigo que el 29 de mayo de 2000 se publicaran en el *Diario Oficial de la Federación* reformas, adiciones y modificaciones legislativas en materia de comercio electrónico al *Código Civil Federal* (reformas a los artículos 1o., 1803, 1805 y 1811 y adiciones al artículo 1834 bis), al *Código Federal de Procedimientos Civiles* (adiciones el artículo 210-A), al *Código de Comercio* (reformas a los artículos 18, 20, 21 párrafo primero, 22, 23, 24, 25, 26, 27, 30, 31, 32, 49, 80 y 1205 y adiciones a los artículos 20 bis, 21 bis, 21 bis 1, 30 bis, 30 bis 1 y 32 bis 1298-A; al Título II, que se denomina "Del Comercio Electrónico", y que comprende los artículos 89 a 94, así como modificaciones a la denominación del Libro Segundo), además de a la *Ley Federal de Protección al Consumidor* (reformas al párrafo primero del artículo 128, y adiciones a la fracción VIII al artículo 1o., la fracción IX bis al artículo 24 y el Capítulo VIII bis *a*), que contendrá el artículo 76 bis). A mayor abundamiento, véase el anexo respectivo que contiene dichas disposiciones.

Importancia de la firma en el comercio electrónico en México

No hay que perder de vista que una firma, sea en papel o electrónica, esencialmente es un símbolo que acredita nuestra voluntad. En consecuencia, las reformas de mayo de 2000 al *Código Civil Federal* señalan que el consentimiento expreso de la voluntad puede manifestarse verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.[19]

Además de servir para demostrar nuestra voluntad de contratar, una firma tiene otras dos funciones significativas: primero, la firma de una persona puede usarse para identificar al firmante y segundo, puede emplearse para acreditar la integridad de un documento (de ahí la costumbre de rubricar todas las hojas de un contrato).

En el ciberespacio, estas dos últimas características de una firma desempeñan un papel fundamental, sobre todo en la medida en que se automatizan los procesos y los contratos se realizan entre ausentes que muchas veces ni siquiera se conocen. En estos casos, la necesidad de identificar al firmante y garantizar la integridad del mensaje se tornan esenciales.

De este modo, mientras que la firma autógrafa sirve la mayoría de las veces principalmente para acreditar el deseo de contratar, en el entorno electrónico tiene tres funciones de igual trascendencia:

- Evidenciar la voluntad de contratar.
- Identificar al emisor.
- Garantizar la integridad del mensaje.

Nuestro actual *Código de Comercio*, promulgado en 1889, obviamente no consideraba las transacciones en línea. Lo más cercano a éstas era la contratación por correspondencia telegráfica. Este tipo de contratos eran válidos, pero sólo producían efectos cuando los contratantes, previamente y por escrito, habían admitido este tipo de operaciones. Si bien existían algunas excepciones para la industria financiera y bancaria, en términos generales, ésa era la regla. Como era de esperarse, este hecho ponía en una delicada situación a quienes llevaban a cabo este tipo de operaciones.

El *Código de Comercio* fue reformado y en él se estipula ahora que "Los convenios y contratos mercantiles que se celebren por correspondencia, telégrafo o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología quedarán perfeccionados desde que se reciba la aceptación de la propuesta...", lo cual elimina la necesidad de celebrar previamente contratos normativos.

[19] Véase ponencia presentada el 21 de noviembre de 2000 en el VII Congreso Iberoamericano del Derecho e Informática, elaborado por Sergio Rodríguez Castillo, Thomas J. Smedinghoff y Ruth Hill Bro. Baker & McKenzie Abogados, S.C. http://www.bakerinfo.com/ecommerce.

Con base en ello, cabe responder de manera enfática que en la actualidad es perfectamente válido celebrar un contrato por medios electrónicos.

Las reformas del 29 de mayo, en busca de la neutralidad tecnológica, dejan algunas interrogantes sin respuesta y se limitan a señalar, en relación con el *Código Civil Federal*, que cuando la ley exija la forma escrita en los contratos y su firma por las partes, estos requisitos se tendrán por cumplidos si se utilizan medios electrónicos, siempre que la información generada o comunicada se mantenga:

- íntegra
- atribuible a su emisor y
- accesible para su ulterior consulta (nótese cómo las reformas hacen especial énfasis en las tres funciones mencionadas como características de la firma digital).

Asimismo, la reforma del *Código de Comercio* señala: "Cuando la ley exija la forma escrita para los contratos y la firma de los documentos relativos, esos supuestos se tendrán por cumplidos tratándose de mensajes de datos, siempre que éste sea atribuible a las personas obligadas y accesible para su ulterior consulta", en cuanto a la legalidad de los contratos mercantiles celebrados en línea. De esta manera, las reformas dan solución al hecho de que aun para muchos contratos, la legislación comercial exige como formalidad que el contrato se celebre por escrito y que las partes lo firmen, con lo cual se evita tener que modificar todos los artículos del *Código de Comercio* y leyes relacionadas.

Como se aprecia, la falta de una definición clara respecto de lo que se considera una firma puede llevar a confusiones, toda vez que cualquier tipo de firma electrónica que cumpla con los requisitos marcados por la norma (incluido un NIP o un "click") podrían ser considerados una firma válida. Es previsible que esta indefinición, de no aclararse, puede ser motivo de controversia y litigios.

Si bien las reformas no indican qué puede calificar como firma, hay indicios de ello en la ley modelo de la UNCITRAL, la cual estipula que, cuando la ley exija la firma de un documento, este requisito quedará satisfecho mediante un mensaje de datos cuando:

- Se utilice un método para identificar a su emisor.
- Se incluya una forma para que el emisor manifieste su aprobación con la información contenida en el mensaje.
- El método utilizado sea confiable, en relación con el propósito para el que se generó o comunicó el mensaje de datos.

De los tipos de firmas electrónicas descritas, la firma digital brinda los más altos niveles de certeza y seguridad para cumplir con estos requisitos; no obstante, conviene reiterar que por la manera como se redactaron las re-

formas, no sólo las firmas digitales pueden calificar como manifestaciones válidas de la voluntad de una persona y, por ende, como fuentes válidas de contratos exigibles.

Respecto a qué tipo de transacciones se pueden realizar por estos medios, Sergio Rodríguez menciona, que al no existir limitación alguna, prácticamente todo contrato que se rija en forma supletoria por el *Código Civil Federal* y/o el *Código de Comercio* (prácticamente todos) puede ser celebrado por medios electrónicos. Sin embargo, es menester tomar con cuidado esta afirmación, pues el hecho de que un contrato se pueda llevar a cabo por medios electrónicos no exime de la obligación de cumplir con las demás formalidades que exija la legislación específica.

La confianza es uno de los factores determinantes en toda transacción, sea ésta en línea o en papel. Por ello, éste es uno de los retos más complejos para el desarrollo del comercio electrónico, pues la confianza es algo que no se puede otorgar por decreto, y finalmente, sin confianza entre las partes, no habrá contrato alguno.

La Unión Europea menciona en su iniciativa de comercio electrónico: "El primer objetivo es construir confianza. A fin de que el Comercio Electrónico se desarrolle, es necesario que tanto consumidores como comerciantes tengan la confianza de que sus transacciones no serán interceptadas o modificadas, que el vendedor y el comprador efectivamente son quienes dicen ser y que los mecanismos de la transacción son legales y seguros."

Desde la perspectiva legal, a fin de confiar en un mensaje de datos como se menciona en las aludidas reformas, los factores que deben tenerse en cuenta son tres: la autenticidad del mensaje, su integridad y la no repudiación de éste por su emisor, en caso de disputas.

Elementos por considerar en el mensaje de datos

a) **Autenticidad**

La autenticidad se refiere al origen de la comunicación, el cual es uno de los puntos en los que hace mayor hincapié la reforma, al señalar que un mensaje se considerará firmado cuando sea atribuible a la persona que se supone lo envía.

b) **Integridad**

La integridad se relaciona con el hecho de que el mensaje no sea alterado o modificado desde su envío y hasta su recepción. Sólo si el receptor confía en que el mensaje recibido efectivamente indica la voluntad exacta de su emisor, aceptará el contrato y cumplirá con su contenido. De igual manera, las reformas hacen énfasis en la importancia de que el mensaje de datos se genere, comunique, reciba y archive en forma íntegra.

c) **Confidencialidad**

Consiste en mantener un mensaje de datos como inaccesible para terceros ajenos a él.

d) **No repudiación o rechazo**

Se refiere a la posibilidad de exigir al emisor que cumpla con su ofrecimiento, plasmado en el mensaje de datos. Con base en la teoría de las obligaciones, se refiere a que el deudor no pueda desconocer una obligación válidamente adquirida con un acreedor. Su importancia radica en que el receptor sólo cumplirá con su parte en una transacción cuando tenga la certeza de que su contraparte (el emisor) no podrá desconocer la emisión, transmisión, envío o contenido del mensaje de datos.

Es necesario recordar que en el "mundo real" un contratante cuenta con numerosos indicadores que le permiten suponer que su contraparte no desconocerá sus obligaciones. Tales indicadores incluyen el contrato firmado (en ocasiones incluso en papel membretado y con testigos que también firman), comunicaciones previas escritas a mano, acuses de recibo de documentos, contactos personales, etc.; sin embargo, en las transacciones electrónicas no existe ninguno de estos indicadores y sólo se cuenta con un mensaje digital que, para complicar las cosas, es fácilmente modificable y reproducible.

El tema de la no repudiación no es mencionado de manera directa en la reforma, pero si un mensaje es considerado íntegro y auténtico, difícilmente podrá repudiarlo su emisor.

A fin de fomentar la confianza en el uso de firmas digitales (que, como se dijo, representan en la actualidad una de las formas más seguras y disponibles de firma electrónica) se celebraron recientemente los acuerdos con la Asociación del Notariado y el Colegio de Corredores Públicos. La intención es que, al involucrar a terceros confiables (fedatarios públicos), los particulares confíen poco a poco en estos esquemas que son seguros en lo tecnológico.

Asimismo, con ese afán de fomento, las reformas del 29 de mayo reconocieron expresamente como prueba en todo procedimiento civil o mercantil, la información generada o comunicada que conste en medios tecnológicos, siempre que cumpla con los requisitos señalados.

Con excepción de estos casos, el legislador mexicano fue extremadamente conservador en cuanto a la validez de los mensajes de datos, al omitir darles un valor probatorio específico, a diferencia de lo que han hecho algunos otros ordenamientos, que otorgan una presunción *juris tantum* en favor de los mensajes de datos que usan firmas digitales. Quedará al arbitrio de los jueces determinar, en cada caso, el valor probatorio específico de tales mensajes de datos.

LOS CONSUMIDORES Y EL COMERCIO ELECTRÓNICO

Electrónicos o tradicionales, los actos de comercio generan responsabilidades y derechos a ambas partes (consumidores y vendedores), por lo cual es crítico asegurar la aplicación de los marcos legales de comercio existentes, o en su defecto crear nuevos, que protejan adecuadamente a ambas partes. En este documento es de especial interés el análisis de las leyes existentes y en desarrollo para proteger a los ciberconsumidores, así como visualizar los riesgos a los que se enfrentan en el ámbito electrónico y medidas recomendadas al realizar transacciones electrónicas. A pesar de la amplia gama de aplicaciones y ventajas que ofrecen las transacciones de comercio electrónico (también conocidas como *transacciones en línea*), la explotación de éstas no ha experimentado el crecimiento que se esperaba. Estudios al respecto demuestran que las causas principales de este fenómeno de lento crecimiento del comercio electrónico en México se deben principalmente a la incertidumbre y el desconocimiento de los consumidores acerca del funcionamiento de estas transacciones en línea.

Con el propósito de adecuar la base legal que garantiza los derechos de los consumidores en el ámbito electrónico, se reformó en México (en marzo de 2000) la *Ley Federal de Protección al Consumidor* en su capítulo VIII bis "De los derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología". La Profeco (Procuraduría Federal del Consumidor), como organismo de regulación en esta materia, da a conocer los detalles de esta reforma en su página web. En el mismo sitio, la Profeco difunde artículos con información detallada acerca de los riesgos a los que se enfrentan los consumidores en internet, así como medidas recomendadas para protegerse de ellos. Otro organismo que cuenta con información valiosa es la Condusef (Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros), la cual ha elaborado una *Guía para compras seguras por internet*, en la que responde de manera sencilla y clara las dudas más comunes en torno a transacciones de compra por esta red, como subastas, manejo de seguridad, pagos con tarjeta de débito o crédito y otros más.

ELEMENTOS POR CONSIDERAR EN LOS PORTALES DE COMERCIO ELECTRÓNICO DE ACUERDO CON LA *LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR*

1. **Identidad del vendedor.** El vendedor debe especificar su domicilio físico, dirección de correo electrónico, número telefónico y fax.
2. **Información sobre la transacción.**

a) **Costos.** El vendedor debe indicar el precio total del producto o servicio en su denominación correcta (incluidos gastos de envío).
b) **Condiciones de entrega.** El vendedor debe dar detalle del envío (tiempo aproximado de entrega y medio de traslado).
c) **Restricciones, limitaciones o condiciones de compra.** Éstas deben señalarse durante la transacción.
d) **Condiciones de devolución, reembolso y cancelación.** El sitio deberá proporcionar la información relacionada con políticas de cancelación, devolución, reembolsos y cambios.

3. **Políticas de privacidad.** La privacidad y seguridad de los datos se encuentran reguladas por la LFPC, la cual prohíbe que se difundan los datos, a menos que lo autorice el propietario de la información.
4. **Sitios seguros.** Para evitar riesgos de intercepción de datos por medio de alguna herramienta que escuche a la red, utilizada por un tercero malintencionado, debe emplearse alguna herramienta que asegure los datos con algún método eficaz de encriptación de datos; en este caso, el sistema más utilizado es el SSL (Secure Socket Layer), con el cual no sólo se crea una conexión aislada a internet (o túnel virtual) entre el cliente y el servidor, sino también se codifican y decodifican los datos en cada extremo cliente y servidor o viceversa de manera respectiva.

Identidad del vendedor	Domicilio
	Correo electrónico
	Número telefónico
Información acerca de la transacción	Descripción detallada de bienes o servicios
	Costos totales
	Plazos de entrega
	Condiciones de devolución, reembolso y cancelación
	Ayuda en caso de dudas para consultar la página
	Corrección de errores en la orden de compra
Políticas de privacidad	Políticas explícitas de privacidad o de seguridad
	Especifica para qué utilizarán la información proporcionada por el usuario
	Especifica quiénes van a tener acceso a esa información
Seguridad del sitio	Para datos personales
	Para datos financieros

X. *Regulación jurídica del SPAM (correo electrónico no deseado o solicitado)*

INTRODUCCIÓN

Internet ha permitido rebasar fronteras y tener al alcance de la mano muchos tipos de información; sin embargo, uno de los medios más utilizados como el e-mail suele ser aprovechado por individuos o empresas mal intencionados que hacen envíos de correo masivo a personas que no lo han solicitado. El objetivo de este envío de correos es, sobre todo, difundir publicidad de sus productos y/o servicios, que por derivarse de medios de comunicación en línea y de forma masiva, tienen un bajo costo, lo que para estas organizaciones e individuos resulta ser el medio más atractivo para hacer y difundir negocios. El *SPAM* causa congestionamientos en los servidores de correo y, por consiguiente, una disminución en el espacio disponible para sus usuarios, además de una pérdida en el nivel de calidad del servicio.

Se incluyen una breve descripción de los orígenes de tal práctica, así como el análisis de diversas leyes y regulaciones creadas por distintos países en un intento por proteger a sus usuarios y los resultados que se obtienen.

ORÍGENES

La palabra *spam* surgió de la contracción del nombre de los productos de comida enlatada llamada ***Shoulder Pork and hAM/SPiced hAM*** (spam) que era enviada de forma masiva e indiscriminada a las tropas estadounidenses durante la Segunda Guerra Mundial. De ahí se deriva el concepto del spam para referirse a "la práctica de enviar correo de manera indis-

criminada a través de la red de internet, sin importar el receptor final del correo y como un modo masivo de publicitar productos o servicios".

Hace aproximadamente 11 años tuvo su origen lo que hoy se conoce como spam o envío de correo no solicitado: curiosamente, no fue ningún *hacker,* sino una pareja de abogados en Nueva York que buscaba promocionar su despacho a un mayor número de clientes con el menor costo posible. Ellos no tenían listas de usuarios de correos electrónicos, sino que usaron las direcciones de sus clientes de manera que ellos lo reenviaran a sus conocidos, lo cual dio origen al mercadeo directo y al spam.

CONCEPTOS

Spam[1]

Según definiciones de la NACPEC, el spam es "el correo comercial no solicitado, generalmente enviado a las direcciones electrónicas de los consumidores sin su autorización y consentimiento; suele ser enviado por empresas de mercadeo o telemercadeo, compañías legítimas o por individuos comisionados sólo para dicho fin".

Scam

Similar al spam es el término *Junk mail* o *scam* (correo chatarra), utilizado para referirse a correos relacionados con publicidad engañosa (enriquecimiento al instante, pornografía, premios, etc.) y cadenas (correos que incluyen textos en los que solicitan ser reenviados a otras personas con la promesa de cumplir deseos, traer buena suerte o ganar dinero).

Spim

Además del *spam*, ha surgido una nueva vertiente de este tipo de ataque cibernético, denominado *spim*, un tipo de *spam* que, en vez de atacar a través de los correos electrónicos, lo hace por medio de la mensajería instantánea.

Phishing

El *phishing* es una nueva modalidad de fraude en internet contenida en sitios que se asemejan a los de los bancos, sistemas de pago o proveedores

[1] Véase Symantec, el Informe sobre spam, versión 2007 y mensual de mayo de 2008, disponible [en línea] en: http://www.symantec.com/es/mx/business/theme.jsp?themeid=state_of_spam, http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_05-2008.en-us.pdf

conocidos en los que en general se señala una falla en el sistema o que la información no se ha actualizado debidamente y, por lo tanto, solicitan al consumidor acceder a una página web por medio de un *link* o enlace. Al ser abierto éste, los defraudadores solicitan información de carácter personal: datos personales, números de cuenta de tarjeta de crédito o débito del cliente, passwords o NIP (número de identificación personal), dirección, teléfono o cualquier otro tipo de información confidencial.

En esencia, el spam es una forma de violencia, pues constituye una agresión a nuestro ser, a nuestras creencias, pensamientos o ideologías. "La conducta agresiva es una acción intencional ejecutada con propósitos definidos y dirigida hacia objetivos establecidos anticipadamente." El correo electrónico es la herramienta de internet que más se usa en la actualidad, sobre todo debido a su fácil manejo y a que no requiere equipos sofisticados. El envío indiscriminado y persistente de correo spam (*spamming*) causa molestia en muchos usuarios, ya que con la recepción de *spam* y *junk mail* se satura el espacio disponible en los servidores de correo electrónico, al igual que se incrementa el riesgo de infección por virus a través de algún archivo o código malicioso anexado al e-mail. A raíz de esto, en la actualidad se han adoptado medidas legales en distintos países con el propósito de limitar y regular esta práctica para así proteger a sus usuarios.

Por desgracia, como pertenece a internet, el spam resulta más fácil de lograr para los ciberdelincuentes, pues como este medio es anónimo, se presta a crear organismos inexistentes que saturen nuestras cuentas de correo o, peor aún, tomar direcciones existentes y robar su identidad para enviar correos basura a todas las listas de direcciones que ellos quieran. Tal es el caso revelado por un usuario llamado "Fernando", quien por no proteger su servidor fue víctima de un spammer que tomó su identidad para enviar spam y ahora se encuentra en la "lista negra", por lo cual su dirección se ve afectada y ya no puede utilizarla más. Tendrá que esperar tiempo para ver si al depurar estas listas lo quitan de ellas o deberá solicitar a cada entidad administradora de estas listas para que lo borren de ella, lo cual es difícil de lograr.

REGULACIONES EXISTENTES

Unión Europea

En la Directiva 2002/58/EC acerca del procesamiento de datos personales y la protección de la privacidad en el sector de comunicaciones electrónicas (Directiva de la Privacidad y Comunicaciones Electrónicas) se establecen los lineamientos de esta directiva, los cuales concuerdan con los de la

Directiva 95/46/CE del 24 de octubre de 1995 referente a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos; además, sustituye a la Directiva 97/66/CE del 15 de diciembre de 1997, concerniente al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. En sus artículos estipula que para realizar una comunicación o transmisión de ésta, el proveedor debe informar de los detalles al usuario, obtener su consentimiento expreso e inequívoco antes de que le sea enviada, indicar la duración del periodo de dicha comunicación, y sólo debe ser realizada por él, evitando compartir la información personal para otros socios comerciales. En cualquier momento, el usuario ha de tener la capacidad para solicitar dejar de recibir la comunicación o en su caso ser eliminado de las listas de distribución de ella. Los mensajes enviados deben contener los datos correctos y completos de la empresa que lo envía, incluido el asunto del mensaje. La directiva prohíbe que los mensajes intenten disimular u ocultar la identidad del remitente, así como proporcionar los datos incorrectos para que el usuario pueda rechazar la comunicación en casos ulteriores.[2]

En la Directiva 2000/31/CE, referente a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva acerca del comercio electrónico), se establece no sólo que pueden existir listados de personas que no desean recibir comunicaciones electrónicas no solicitadas, sino también que las empresas que deseen enviar correos no solicitados deben respetar dichas listas. Aunado a eso, deberán cumplir con lo previsto en la directiva mencionada, que indica que antes de enviar alguna comunicación han de obtener autorización de quien la recibirá. Asimismo, para los envíos de correos no solicitados, deberá identificarse el mensaje como tal para facilitar el uso de herramientas de filtrado.

Argentina

La *Ley 25 326 de Protección de los Datos Personales* establece que las empresas que deseen enviar correo no solicitado pueden obtener los datos de la persona siempre y cuando lo hagan por publicación en algún listado público o con el consentimiento de la persona que recibirá el correo. El usuario no recibirá cargo alguno por recibir esta promoción y en cualquier momento podrá solicitar que se le retire de la lista de distribución.

[2] Véase detalle de los artículos 30 y 31 de la Directiva 2000/31/CE, disponible [en línea], formato pdf, 16 pp., en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:ES:PDF consultada en mayo de 2008.

Estados Unidos

En la Unión Americana, el 1 de enero de 2004 entró en vigor la *Ley CAN-SPAM 2003*, la cual fue titulada *Ley para el Control de la Mercadotecnia y Publicidad Pornográfica No Solicitada*, ordenamiento legal que cuenta con 15 secciones. La sección dos se refiere a lo importante que se ha vuelto el correo electrónico tanto en la vida privada de las personas como en las actividades comerciales y profesionales de éstas. Reconoce la problemática del correo no solicitado y da una estadística en la cual se indica que en 2001 el spam era de 7% de correos y hoy día totaliza casi 50% de correos enviados dentro de Estados Unidos. Esta sección alude además al costo en moneda y en tiempo en que el receptor incurre por culpa del correo no solicitado; los principales son el costo de almacenaje en los servidores y el tiempo invertido en la lectura y borrado de estos mensajes. Dicha sección define también que algunas personas que envían los correos no solicitados disfrazan los mensajes a fin de obligar al receptor a abrir los correos, así como reconoce que la ley por sí misma no será suficiente para eliminar el correo chatarra, sino que solicita tanto la ayuda de la tecnología en forma de desarrollos tecnológicos que permitan luchar contra este mal, como la cooperación mundial. Esta ley tiene sustento en las consideraciones siguientes:

1. El creciente interés del gobierno para regular lo concerniente al correo electrónico comercial.
2. Prohíbe el envío de mensajes con títulos disfrazados a fin de ocultar el verdadero contenido del correo.
3. El receptor podrá en todo momento declinar la recepción de estos mensajes por parte de la misma fuente de origen.

En la sección 4 de esta ley se definen los lineamientos que separan al correo basura del normal; esta barrera se ha establecido en 2 500 correos enviados en 24 horas, 25 000 en 30 días y 250 000 durante un año. Si se rebasa esta barrera, se impondrán multas punitivas y/o de cárcel.

La sección 6 indica claramente que el envío de correo con material con contenido sexual deberá identificarse en el título del correo.

La sección 9 sienta las bases para que, a no más de seis meses de la puesta en operación de esta ley, se cree un procedimiento para que los usuarios que no deseen recibir correo basura puedan suscribirse a una lista y evitar recibir esos correos. Además, se indica que se deben crear los métodos adecuados con el fin de que tales listas estén disponibles para los niños con correos electrónicos.

En general, el gobierno de Estados Unidos está consciente del problema que significa el correo no solicitado y el alto costo que representa para

las compañías y personas. Sin embargo, la misma ley permite un límite de correos, a efecto de no afectar el legítimo envío de correos como forma de mercadotecnia masiva; asimismo, da a las empresas una solución mediante la cual, si el usuario acepta el envío de dichos correos, éstas quedarán liberadas de cualquier límite establecido hasta que el usuario solicite su remoción.

Canadá

En 2004, Canadá reconoció el alto costo que tiene el spam dentro de la economía del país, así como el alto grado de preocupación en la población, y señaló con claridad que era el momento de iniciar una serie de actividades encaminadas al control del spam. El 11 de mayo de 2004, el ministro de la Industria anunció el establecimiento de un grupo de ataque cuya misión principal sería poner en marcha un plan para reducir el volumen de spam; esta fuerza de ataque estaría formada por expertos en tecnología, representantes de los proveedores de acceso a internet, representantes de la industria privada, miembros del público en general y representantes del gobierno.

Este grupo llegó a un consenso sobre cuatro puntos principales:

1. Como la mayor parte de los correos no solicitados se consideran una agresión, en gran medida no contienen la venta de productos o servicios ilegales.
2. Los miembros del equipo reconocen que la elaboración de nuevas leyes funcionará siempre que sean acompañadas por una serie de medidas técnicas o tecnológicas y, sobre todo, por un cambio en el comportamiento de los usuarios. Las leyes por sí solas no harán que el spam desaparezca.
3. Existe un consenso entre los miembros del equipo respecto a que el gobierno no debe imponer soluciones detalladas en cuanto a aspectos tecnológicos, dado que la tecnología avanza con rapidez y dichas soluciones quedarían obsoletas en un tiempo corto; por el contrario, se debe acudir a las mejores prácticas o la mejor tecnología disponible en el momento.

Una solución de fondo implica la colaboración mundial de todos los gobiernos y Canadá se ofrece para encabezar el esfuerzo internacional contra la lucha al spam.

En lugar de hacer una nueva ley que luche contra el spam, Canadá optó por adecuar las leyes existentes; por esta razón, la *Ley de Protección de Datos Personales y Documentos Electrónicos* fue modificada en enero de 2004 a fin de considerar los correos electrónicos como información

personal. En esta modificación se indica que quienes envíen correos en grandes cantidades deberán haber obtenido primeramente la autorización clara del receptor.

Tanto para el código penal como para la ley de competencia, el envío de correos masivos y/o de mercadotecnia masiva por correo normal no se consideran delitos; pero se pena el envío de correos masivos disfrazados o que den una idea errónea al receptor, mediante los cuales se obligue a abrir el contenido del mensaje. Para estos casos, el código penal establece penas punitivas y de cárcel similares a las del fraude.

Aunque es mucho lo que la industria y los proveedores de internet pueden hacer para limitar el spam, el verdadero punto final debe provenir de los usuarios, quienes habrán de ser educados respecto a las medidas y opciones que tienen disponibles para evitar el spam. Los canales de comunicación y educación deben ser replanteados a fin de hacer llegar el mensaje a los usuarios.

México

El spam en México se encuentra regulado por los artículos 17, 18, 76 bis y 128 de la *Ley Federal de Protección al Consumidor* (LFPC).

El artículo 17 dispone que la publicidad que se envíe a los consumidores deberá indicar el nombre, domicilio, teléfono o dirección electrónica del proveedor o la empresa que envíe la publicidad a nombre del proveedor. Además, aclara que los consumidores tienen el derecho a solicitar que no se les envíe información con fines publicitarios, y especifica exigir a los proveedores y empresas que utilicen la información no transmitirla a terceros para su uso.

El artículo 18 establece que la procuraduría llevará el caso cuando un consumidor no haya aprobado el uso de su información personal y ésta haya sido utilizada por proveedores y/o empresas para el envío de publicidad.

Por último, la fracción VI del artículo 76 bis señala claramente que el proveedor respetará la decisión del consumidor de recibir o no avisos comerciales. Y la fracción VII de este artículo indica que el proveedor deberá abstenerse de utilizar estrategias publicitarias o de venta que no proporcionen información clara y suficiente sobre los servicios ofrecidos al consumidor.

La Profeco puede imponer multas que van desde $150 hasta $2 520 000, lo cual depende de cuatro factores:

1. El perjuicio causado al consumidor.
2. El carácter intencional de la infracción.

3. La condición económica del infractor.
4. La reincidencia en que se incurra con este acto.

Dichas multas son impuestas de acuerdo con el criterio de las autoridades de la Profeco y pueden variar según las circunstancias de cada caso.

La Profeco forma parte del Comité de Políticas del Consumidor (CCP) de la OCDE (Organización para la Cooperación y el Desarrollo Económicos), cuyo fin es lograr la protección del consumidor en el contexto del comercio electrónico, así como evitar las prácticas transfronterizas fraudulentas y engañosas. Este comité busca analizar las tendencias de las prácticas comerciales internacionales referente al comercio electrónico y adopta medidas generales que apelan a la cooperación internacional para evitar el daño a los consumidores.

ACCIONES CONTRA EL SPAM

- Activar el modo de filtrado de correo no deseado en las diferentes compañías que ofrecen servicios de correo electrónico: *Hotmail* (Microsoft), *Yahoo*!; solicitar a los proveedores de internet herramientas de filtrado de correo electrónico, en caso de no contar con ello; conseguir software que permita este filtrado, como Junk Email AntiSpam, Spam Inspector, Mozilla, entre otros, o adquirirlos desde: http://www.spamfilterreview.com/
- Hacer caso omiso a las peticiones de enviar un correo a todas las direcciones.
- No abrir correos con título sospechoso, ya que algunos tienen programación maliciosa que se reenvía a toda su libreta de direcciones.
- Tener cuidado al contratar algún servicio en línea; algunos proveedores solicitan al usuario llenar sus preferencias, con el fin de enviarle promociones y noticias al respecto, lo cual permite a dicha empresa dar a conocer su dirección a socios comerciales que pueden saturar su correo con diversas promociones.
- Evitar que su dirección de e-mail sea incluida en listas de distribución o directorio público (de correo).
- Solicitar que su dirección de e-mail sea retirada de listas de distribución que no resulten de su interés.
- Denunciar a los *spammers*.
  - — Mediante una queja o reclamación ante la Profeco siempre y cuando los mensajes provengan de una empresa, compañía publicitaria o individuo ubicado en territorio nacional a los cuales no les haya otorgado su consentimiento por escrito o en forma electrónica para recibir su publicidad.

— Contactar a la policía cibernética policia_cibernetica@ssp.gob.mx y presentar la denuncia.
- Navegar en sitios seguros.
- Instalar en la computadora antivirus y filtros antispam.
- Verificar constantemente estados de cuenta bancarios y de tarjetas de crédito.

Cuando el spam que recibo proviene de un país extranjero y en un idioma distinto del español

- No contestar este tipo de mensajes.
- Visitar la página http://www.econsumer.gov o www.spamhaus.org y reenviar todo el spam recibido, o en su caso los datos del remitente.

Métodos para identificar el spam

- Analizadores de contenido
- Filtro de palabras
- Sistemas de puntuación basados en reglas
- Filtros bayesianos
- Listas negras
- Listas de hoyos negros en tiempo real
- Revisión de registros MX
- Revisiones de DNS a la inversa
- Diversos nuevos sistemas de revisión a la inversa
- Lista negra de direcciones
- Frascos de miel (honeypot)
- Sistemas de reto/respuesta
- Sistemas computacionales de reto
- Controles de frecuencia

COMENTARIOS FINALES

El spam es uno más de los problemas que se presentan en el mundo virtual, pero no es algo nuevo, sino una técnica de ventas tradicional transformada y adaptada al mundo virtual. Muchas veces hemos recibido en nuestro buzón panfletos y volantes con mercadotecnia y propaganda no solicitada; en múltiples ocasiones los tomamos y así como están los tiramos al bote de la basura. Cuántas veces hemos ido a las tiendas departamentales y en la entrada del establecimiento se encuentra un batallón de vendedoras de perfumes y lociones dispuestas a rociarnos de producto sin haber obteni-

do nuestro consentimiento. Éstos son ejemplos de spam en la vida real. Sabemos que la mercadotecnia y las ventas no pueden existir una sin la otra, que los creativos idean nuevas formas de hacernos llegar los mensajes de compra por cualquier medio posible y con la llegada de internet llegó también una forma económica y masiva de hacer publicidad, lo cual es el sueño dorado de cualquier publicista.

El problema radica en la economía de escala y el anonimato que presenta internet para la publicidad, pues, como puede ser una maravillosa herramienta para promocionar productos y enriquecer el comercio electrónico, la aprovechan cada día con más frecuencia personas sin escrúpulos que, al ver el costo tan bajo de este tipo de publicidad, no dudan en enviar millones de correos sin importarles las consecuencias y, peor aún, los disfrazan para que caigamos en una trampa. Esto es alevosía, premeditación y ventaja y no resulta justo para el receptor de los mensajes.

Pero la tecnología sólo puede ayudar parcialmente, porque es imposible establecer el filtro perfecto, pues de un día a otro estaríamos invadidos de nuevo por mensajes no deseados para los cuales nuestros filtros han quedado obsoletos. Como toda agresión, hay que saber defenderse y la mejor defensa es el conocimiento que se pueda obtener acerca de las diferentes áreas que ayudan a combatir el spam: la tecnología, las leyes y el sentido común.

Es erróneo considerar que el spam es el único medio para realizar publicidad de productos o servicios ofrecidos por la red; sin embargo, resulta difícil hacernos a otra idea, pues esto "normalmente" se utiliza como medio publicitario tanto en organismos grandes como pequeños, y lo torna cada vez más un medio "tolerable" por el que se hace publicidad sin darnos cuenta de los daños que puede ocasionar. Sin embargo, dichos negocios podrán sacarle el mayor provecho posible a este medio de publicidad, mientras no se tomen las medidas preventivas y correctivas necesarias para aplicarlas a tales organismos.

En nuestro país, la Profeco ha desempeñado un papel primordial y significativo en contra del spam y se ha interesado por prevenir y proteger tanto a individuos como a organizaciones completas de este tipo de ataque. Su deseo por ayudar a la población mexicana y prevenir tales ataques ha tenido tanta relevancia que la inquietud por este organismo de poner en marcha una campaña en febrero como el mes de la prevención ha sido un gran ejemplo del mencionado avance por combatir cada día estos ataques.

Sin embargo, se debe tener presente que el spam avanza con la tecnología, por lo que requiere la acción coordinada de todos los sectores: tanto social como gubernamental y empresarial, además de la cooperación internacional para realizar los contraataques de una manera más certera y eficaz.

XI. Aspectos laborales de la informática: ergonomía y teletrabajo

NOCIONES FUNDAMENTALES

La acepción *ergonomía informática*, si bien nueva, alude, de acuerdo con su etimología, al conjunto de enunciados referidos a la aplicación de la informática en el ámbito laboral. Proviene de *ergon* (energía, trabajo) y *nomos* (tratado) y del vocablo informática ya mencionado.

Ahora bien, si se quiere dar un concepto breve y claro acerca de dicha disciplina, cabe decir que es el "conjunto de implicaciones de orden normativo-laboral provocadas por el uso de la informática". Toca en turno, entonces, analizar cuáles son esas implicaciones.

PRINCIPALES IMPLICACIONES

Pocos fenómenos han provocado tantos cambios dentro del contexto laboral como la informática y, más específicamente, el uso de las computadoras. Modificaciones que si bien se acentúan día con día, no han sido objeto de un tratamiento jurídico adecuado.

Movilización de puestos (desplazamiento laboral)

Respecto a la generación de nuevos empleos que ha traído consigo el desarrollo informático, basta con ver en los periódicos, revistas especializadas y otros medios la gran cantidad de solicitudes de personal informático, situación no privativa de las empresas del sector público.

Sin embargo, no se debe soslayar que así como la informática es generadora de empleo, también lo es de movilidad de puestos (algo que también se puede encuadrar en las consideraciones de desplazamiento laboral), o sea, en el seno de una empresa en la que se presente un proceso de informatización, determinadas labores son objeto de restructuración de tal forma que se modifique o aun se suprima la actividad de uno o más empleados, lo cual trae aparejada (suponiendo la anuencia del trabajador) una movilización de puestos, en teoría hacia niveles más trascendentes.

Desempleo

Por otra parte, un fenómeno más significativo y con repercusiones aún más considerables es el del desempleo, ya que las computadoras han incursionado seriamente en todo tipo de ámbitos: fábricas, oficinas, escuelas, etc., de tal modo que muchos (en gran desproporción respecto a los empleos generales) pierden y seguirán perdiendo su trabajo debido a la automatización de actividades (en gran parte provocada por la ausencia de una adecuada política informática), lo cual en última instancia se perfila como un problema tan serio como para que el derecho se avoque a él.

Condiciones de trabajo

Sin lugar a dudas, entre las implicaciones laborales suscitadas por la informática están aquellas que se refieren a las condiciones de trabajo, por lo que a continuación se estudiarán algunos de dichos aspectos.[1]

Jornada de trabajo

La jornada de trabajo, entendida como el tiempo durante el cual el trabajador está a disposición del patrón para prestar su labor, deberá estar concertada a razón de siete a ocho horas diarias máximo según el tipo de jornada de que se trate, aunque puede ajustarse de acuerdo con la naturaleza de la labor que se desarrolle. A este respecto es innegable que la computadora ofrece, en numerosas labores (sobre todo administrativas), el soporte más que idóneo para trabajar una jornada relativamente corta. Por ello, es conveniente vislumbrar de manera adecuada esta situación, además de las consideraciones propias en función de los necesarios descansos intermedios en el desempeño de dichas labores, pues si bien sus repercusiones

[1] Análisis realizado a la luz de la *Ley Federal del Trabajo* (LFT) de México.

cuantitativas en cuanto al tiempo y volumen de trabajo se circunscriben en determinadas situaciones, esto no es lo mismo en cuanto a los caracteres cualitativos, ya que estas actividades en general requieren una disposición física o mental muy específica, lo cual, como se verá, puede provocar algunos trastornos.

Vacaciones y días de descanso

Por lo que hace a este punto, es conveniente considerar que tanto las vacaciones como los días de descanso de los trabajadores informáticos deben ser satisfactorios para producir una recuperación física y sobre todo mental. En cuanto al tipo de actividad desempeñada y con base en algunos "consejos empresariales", es recomendable que en el caso de empleados informáticos descontentos por el tipo de labor que desempeñan, que pudieran provocar problemas a la empresa, éstos sean segregados de manera temporal del centro de trabajo, mediante la concesión de días de descanso o vacaciones adicionales.

Salario

El salario, entendido como la retribución que debe pagar el patrón al empleado por su trabajo, fijada de acuerdo con las circunstancias, presenta una particular relevancia en el caso de las labores informáticas, en función de sus características objetivas y subjetivas. De aquí que las actividades de esta índole estén muy cotizadas en la actualidad (tal vez sobrevaluadas por momentos) y que pudiera ofrecer algunos puntos de discusión, pues se menciona que a trabajo igual, desempeñado en puesto, jornada y condiciones de eficiencia iguales, debe corresponder salario igual, en cuyo caso se ha de precisar quiénes son los iguales y quiénes los desiguales.

DERECHOS Y OBLIGACIONES DE LOS PATRONES Y TRABAJADORES

Otro de los aspectos sustancialmente aparejados a la informatización laboral es el referente a los derechos y obligaciones de los patrones y trabajadores.[2]

[2] *Ídem.*

a) Obligaciones de los patrones:

- Proporcionar a los trabajadores los útiles, instrumentos y materiales (en este caso informáticos) necesarios para la ejecución del trabajo, en buen estado y con buena calidad.
- Dar capacitación y adiestramiento a los trabajadores informáticos, de manera tal que limite al mínimo las eventuales acciones negligentes o imprudenciales y con ello las graves repercusiones de suscitarse en estas actividades.
- Montar las instalaciones de tal forma que se limiten eventuales riesgos en cuanto a la labor que se desempeña.

b) Obligaciones de los trabajadores:

- Cumplir con las disposiciones de las normas laborales que le sean conducentes, lo cual es muy importante en los trabajos informáticos en función de sus características propias.
- Observar las medidas preventivas en materia de seguridad y protección, por ejemplo: tomar reposos periódicos acordes con el grado de intensidad de su trabajo informático.
- Guardar escrupulosamente los secretos técnicos comerciales y de fabricación de los productos a cuya elaboración concurran directa o indirectamente o de los cuales tengan conocimiento por razón del trabajo que desempeñen y cuya divulgación pueda causar perjuicios a la empresa. Sin duda, ésta es una de las principales obligaciones de gran parte de los trabajadores informáticos en lo concerniente al tipo de información que manejan, lo cual incluso constituye una causal de rescisión del contrato respectivo.

Invenciones de los trabajadores

Acerca de este punto,[3] tan susceptible de suscitarse en dichas actividades, la atribución de los derechos será como sigue:

- En cuanto al nombre, al autor de la invención.
- Respecto a la propiedad y explotación de la patente al patrón, siempre que el desarrollo haya tenido lugar en el seno de la empresa, el trabajador-inventor tendrá derecho a una compensación salarial fijada de mutuo acuerdo o por la autoridad respectiva.
- En cualquier otro caso, la propiedad de la invención corresponderá a quien la realizó, y el patrón tendrá, en igualdad de circunstancias, un derecho preferente sobre el uso exclusivo o la adquisición de la invención, así como de las patentes que correspondan.

[3] *Idem.*

Categoría contractual

Por lo que hace a este punto, si el tipo de actividad vinculada con la informática (de acuerdo con sus condiciones, naturaleza e importancia) no amerita que el empleado sea considerado según las especificaciones de un trabajador de confianza, recibirá el tratamiento de un trabajador de base. Esto tiene que apreciarse debidamente, ya que de ello dependerá en gran medida el tipo de relación laboral que se establezca.

Sobre el particular, cabe mencionar que si bien la *Ley Federal del Trabajo* en México contempla un título exclusivo (el sexto) para los llamados "Trabajos especiales", en él no se consagra regulación alguna acerca de los trabajadores informáticos. Por ello, es recomendable incluir un capítulo específico dentro de ese rubro alusivo a estos trabajadores, ya que la labor que desarrollan amerita, sin duda, un tratamiento especial.

En cuanto al tipo de relación de trabajo (individual o colectivo), éste estribará, en gran medida, de acuerdo con la clase de actividad particular que desarrolle el trabajador informático, lo cual lo posibilitaría a ejercer (si así fuere el caso) determinados derechos, como la huelga.

Riesgos de trabajo

Los riesgos de trabajo, como los accidentes y las enfermedades a que están expuestos los trabajadores (en este caso informáticos) en ejercicio o con motivos del trabajo,[4] ameritan una especial consideración respecto al tema que se analiza.

Dichos accidentes o enfermedades de trabajo, considerados desde una perspectiva fisiológica y psicológica, constituyen la parte medular de una eventual regulación jurídica de la informática laboral porque aquí está de por medio uno de los valores más significativos de todo ser humano: la salud.

Los incipientes estudios ergonómicos en torno a este punto[5] demuestran que la computadora, en caso de no ser debidamente controlada su fabricación (componentes, conformación, tipo de teclado, pantalla, contorno de caracteres, movilidad, etc.), su funcionamiento y sobre todo su uso, puede provocar serias repercusiones psicosomáticas en ocasiones

[4] *Ídem.*

[5] A este respecto, los estudios realizados en Suecia, Francia, Alemania y Suiza, entre otros países, revelan la existencia de trastornos físicos, como la irritación de ojos, miopía, dolores frontales, musculares, de columna y de hombros, mareos, náuseas, etc. Por otro lado, a nivel de efectos psicológicos hay atrofiamientos, fatiga, ansiedad, sensación de inutilidad, mecanización, despersonalización, etc., todo ello derivado de un uso o un entorno inadecuado referido a las computadoras.

irreversibles. Por ello, es de suma importancia la participación activa de autoridades, patrones y trabajadores a fin de que dicha situación no alcance niveles más trascendentes, ya que estos riesgos (por más que pudieran identificarse[6] como incapacidades —totales o parciales— o incluso hasta el fallecimiento aun con su respectiva "indemnización", no puede tener cabida, al igual que muchas otras situaciones de adversidad social, con el pretexto de que son el precio que debe pagar el hombre por su desarrollo.

Situación nacional

Como se infiere en atención a lo anteriormente expresado, en México es urgente estudiar y tratar este tema, pues si bien no existe un grado de informatización tan pronunciado como en otros países, es suficiente que una sola persona, entiéndase trabajador, se cause un daño inconsciente (ya sea físico o moral) por la simple obligación (o más bien necesidad) de tener que trabajar para vivir. Más reprochable aún es que proveedores informáticos, empresarios y gobierno, sobre quienes en última instancia recae más responsabilidad (y no tanto los efectos negativos directos en sí), no se preocupen por tener en cuenta y resolver el problema, aun cuando se dispone de los elementos necesarios para hacerlo. Ahora bien, cabe mencionar que también en otros países, incluso con mayor nivel de automatización que México, tampoco se le ha atribuido la importancia suficiente, pero esto de todas maneras deja latente el problema.

EL TELETRABAJO

Generalidades

El término *teletrabajo* suele usarse sin definición previa, ya que existe una comprensión intuitiva de a qué se refiere; por ello, no hace falta establecer criterios a cumplir para saber si se trata de teletrabajo o no. Esto ha llevado a la aparición de un gran número de definiciones del teletrabajo, sin que haya una general y precisa.

Una de las definiciones que se da al teletrabajo es la de "forma flexible de organización del trabajo, que consiste en el desempeño de la actividad

[6] Dicha identificación requeriría peritos muy capacitados para determinar las causas en función del daño causado.

profesional sin la presencia física del trabajador de la empresa durante una parte importante de su horario laboral".[7]

El teletrabajo es una forma flexible de organización del trabajo que se realiza con ayuda de las tecnologías de la información y las comunicaciones, en un lugar distinto y alejado del que ocupa la organización o la persona para quien se realiza el trabajo. Por tanto, se trata de una de las formas de trabajo más características de la sociedad de la información, cuya base es el uso de las tecnologías de la información y las comunicaciones para llevar el trabajo hasta el trabajador y no a la inversa.

Las primeras referencias al término *teletrabajo* se remontan a la década de 1970, cuando el físico Jack Nilles buscaba formas de ahorro energético y abogaba por el trabajo a distancia, para lo cual utilizaba las incipientes tecnologías de la comunicación.[8]

Según Talia Besga,[9] en cualquier definición acerca de qué es el teletrabajo se deben tener en cuenta los siguientes puntos:

a) *Lugar de trabajo*: parte del tiempo de trabajo debe llevarse a cabo fuera del entorno tradicional de la oficina. Esto provoca una nueva división del tiempo de trabajo entre la residencia familiar del teletrabajador, las oficinas tradicionales situadas en el centro de las ciudades y posibles centros de trabajo cercanos a las residencias de los teletrabajadores, que se suelen denominar *satellite office*.

Algunas de las razones de estos centros son las siguientes:

1. La necesidad de compartir el costo de los equipos que se requieren para trabajar.
2. Evitar la soledad del teletrabajador.
3. Crear cultura de empresa con estos encuentros.

b) *Distribución del tiempo de trabajo*: para considerar que una persona es teletrabajador debe pasar una parte importante de su jornada laboral fuera de su entorno habitual de trabajo.

c) Uso intensivo de las tecnologías de la información y comunicación. Es necesario que el teletrabajador emplee estas tecnologías de forma habitual.

---

[7] Véase http://www.um.es/undis/jornadas/p1 1español.html

[8] Bernard E. Gbezo, "Otro modo de trabajar: la revolución del teletrabajo", en *Revista de la OIT*, núm. 14, Ginebra, Suiza, 1995

[9] Talia Besga, abogada y especialista en derecho laboral y nuevas tecnologías, noviembre de 2000, *El teletrabajo: ventajas e inconvenientes* [en línea] en: http://www.delitosinformáticos.com/trabajos/teletrabajo.htm

Aspectos particulares

El teletrabajo responde a una serie de tendencias:

a) *Tendencias sociales*: mejoras tecnológicas, importantes avances en las telecomunicaciones, mayor sensibilización ante el empleo, globalización de la economía, y problemas medioambientales.
b) *Tendencias en el individuo*: necesidad de flexibilidad, y autoempleo.
c) *Tendencias de la empresa*: mayor complejidad, dinamismo, competencia en el entorno, *outsourcing*, y necesidad de cambio.

El teletrabajo no se puede aplicar a todos los puestos de trabajo ni a todos los empleados de las organizaciones. Para ser parte de esta nueva forma de trabajo se requieren características específicas; en cuanto a los empleados es necesario que realicen tareas relacionadas con la información en menor o mayor grado.

Existen cuatro tipos de personas que podrían ser teletrabajadores:

- Los que trasladan la información de un soporte a otro: mecanógrafos, grabadores de datos, transcriptores de datos, etcétera.
- Los que gestionan la información: agentes de seguros, documentalistas, contadores, etcétera.
- Los que producen información: periodistas, informadores, analistas, programadores, etcétera.
- Los que deben mantener relaciones con una clientela local: oficinas de información, ventas por correspondencia y por teléfono, etcétera.

Ahora bien, con la denominación teletrabajo, trabajo periférico, trabajo a distancia o trabajo remoto pueden englobarse diversas situaciones:[10]

a) *Teletrabajadores en el domicilio*. Son aquellos que desarrollan la mayor parte de su actividad profesional en su casa. Acuden a la oficina de vez en cuando por alguna reunión o para recoger material de trabajo. En esta categoría se incluye, por ejemplo, a los programadores y analistas informáticos, empleos que han tenido un papel destacado en la bibliografía del teletrabajo.

[10] En éste y otros puntos ulteriores, seguiremos al doctor Álvaro Castro Estrada, director general de Asuntos Jurídicos de la Secretaría del Trabajo y Previsión Social, *El teletrabajo y la legislación laboral mexicana*, documento presentado en el seminario "Retos y Áreas de Oportunidad del Teletrabajo en Europa y México", México, noviembre de 2000.

b) *Teletrabajadores móviles.* Son aquellos que pasan la mayor parte del tiempo fuera de la oficina o en las oficinas de los clientes. Por lo general se trata de agentes de ventas, técnicos, consultores, ajustadores de seguros, etc. La oficina base de un teletrabajador móvil puede ser su casa, una oficina convencional o incluso un vehículo.
c) *Telecentros o centros de teletrabajo.* Se trata de una situación intermedia entre la oficina tradicional y el trabajo a domicilio. En estos casos, el teletrabajador evita el aislamiento de trabajar en casa y ahorra los costos, tiempos e inconvenientes del mantenimiento.

OUTSOURCING

Según Emilio del Peso Navarro, el *outsourcing*, también llamado *tercerización* o *externalización*, es el proceso económico en el cual una empresa determinada mueve o destina los recursos orientados a cumplir ciertas tareas a una empresa externa, por medio de un contrato.

Otra definición sería: "empresa o conjunto de empresas que suministran recursos humanos a otras (*clientes*) con la finalidad de sustituir la relación laboral y fiscal de esas empresas".

Incluso, puede decirse que es contratar y delegar a largo plazo uno o más procesos no esenciales para nuestro negocio, a un proveedor más especializado que nosotros para conseguir mayor efectividad que nos permita orientar nuestros mejores esfuerzos a las necesidades neurálgicas para el cumplimiento de una misión.

En España, el outsourcing se conoce como *deslocalización* e implica "la transferencia de empleos a otro país, bien contratando empresas locales o bien estableciendo una base en sitios donde la mano de obra es barata, es decir, por subcontratación se define la gestión o ejecución diaria de una función empresarial por un proveedor externo de servicios. La empresa subcontratante deberá transferir parte del control administrativo y operacional a la empresa subcontratada, de modo que ésta pueda realizar su trabajo apartada de la relación normal de la empresa subcontratante y sus clientes. La subcontratación también implica un considerable grado de intercambio bidireccional de información, coordinación y confianza".

El derecho mexicano no reconoce ni define en forma alguna la palabra *outsourcing*; empero, del contexto de su vocablo a nivel mundial, se refiere a la subcontratación.

Ventajas y desventajas del teletrabajo

El teletrabajo es un fenómeno reciente. En efecto, en los últimos 20 años se ha presentado, sobre todo en las sociedades industrializadas y con ma-

yor avance tecnológico, una serie de transformaciones que ha propiciado la necesidad de rediseñar los límites geográficos y organizativos de las empresas tradicionales. Algunas de sus principales ventajas y desventajas, son las siguientes:

Ventajas del teletrabajo

Las ventajas de este sistema se pueden dividir en tres grupos: para el teletrabajador, para las empresas y para la sociedad.

a) Ventajas para el trabajador

El teletrabajo significa un incremento en la flexibilidad tanto de horarios como del orden de las tareas por afrontar. Esta característica permite distribuir el tiempo de la forma que crea más conveniente, facilita mayor autocontrol y suele dar lugar a un incremento de la productividad del trabajador.

Una de las características más valoradas del teletrabajo es la posibilidad de combinar de forma aceptable y satisfactoria la vida laboral y la familiar. Trabajar desde el propio domicilio permite dedicar más tiempo a la familia e incluso participar en tareas como el cuidado de los hijos, de ancianos o de familiares con incapacidades.

La reducción de los desplazamientos y de la supervisión directa por los jefes o directivos, aunada a la reducción de roces y rencillas que surgen de la convivencia diaria en las oficinas, contribuye a la reducción del estrés, uno de los males de nuestro tiempo y factor causante de enfermedades y descensos de productividad.

b) Ventajas para las empresas

La ventaja más evidente y que motiva a un mayor número de empresarios a implantar sistemas de teletrabajo la constituye la reducción de los costos, sobre todo los de alquiler de inmuebles, mobiliario, transporte, etc. Según algunas experiencias, a veces la implantación del teletrabajo ha significado ahorros de 50 a 70% en estos campos.

El teletrabajo otorga mayor flexibilidad a las organizaciones empresariales. Las nuevas estructuras de dirección apuntan a una organización no piramidal, sino horizontal. La implantación del teletrabajo conlleva la migración hacia un sistema de control por objetivos-resultados. En este sistema no se juzgan las horas que el trabajador está en su puesto, sino sólo la calidad del trabajo realizado y el cumplimiento de los plazos previstos para ello.

Así, la empresa que pretenda instalar el teletrabajo podrá obtener las siguientes ventajas:

- Acceso remoto a los sistemas y a las bases de datos de la empresa.
- Multilocalización geográfica de capacidades externas.
- Incremento de la productividad.
- Presencia internacional de la empresa.
- Fortalecimiento de su presencia en el mercado.
- Ahorro en personal, costos fijos y en espacio de oficina.
- Mejora en la calidad del trabajo.
- Reducciones en los costos de gestión de clientes.
- Mejoras en las condiciones de trabajo y en la calidad de vida.
- Mayor conocimiento en los hábitos de los clientes.
- Permanencia del servicio.
- Velocidad de acción.

c) Ventajas para la sociedad

Reducción del tráfico y de la consiguiente contaminación. Tanto en Estados Unidos como en la Unión Europea existen políticas que tienden a favorecer el teletrabajo por sus beneficios para el medio ambiente. Por ejemplo, cabe señalar que una cuarta parte de los trabajadores europeos emplean más de una hora diaria en sus desplazamientos, con importantes consecuencias negativas en lo que respecta a la salud y la seguridad, el consumo de energía, la contaminación y la pérdida de tiempo. Estas características no resultan ajenas a lo que ocurre en la Ciudad de México.

El teletrabajo puede favorecer el desarrollo de zonas aisladas o marginadas. En España cada vez son más frecuentes las denominadas televillages (telepueblos), que propician la conformación de pequeñas y medianas empresas rurales (pymes). De esta manera, el trabajo se realiza en ambientes más favorables, con la consecuente reducción de desequilibrios demográficos interregionales.

El teletrabajo propicia la integración e incorporación a la vida laboral a segmentos de la población que tradicionalmente no han recibido una adecuada atención. En este rubro destacan los discapacitados, las mujeres embarazadas o las amas de casa, así como las personas que no pueden acceder a un puesto de trabajo debido a la dificultad que representa su desplazamiento.

Desventajas del teletrabajo

La implantación del teletrabajo implica en ocasiones el surgimiento de elementos negativos o desventajas. En este caso, cabe establecer la di-

ferencia en tres grandes grupos: desventajas para las personas, para las empresas y para la sociedad.

a) Desventajas para las personas

Una de las principales desventajas puede ser la sensación de soledad. La falta de interacción diaria entre compañeros, de vida social o de la posibilidad de contacto cara a cara puede provocar crisis y sensaciones de aislamiento o soledad.

Otra de las consecuencias negativas a superar es la sensación del teletrabajador de que su carrera no avanza. Piensa que si no ven su trabajo no podrán valorarlo en su justa medida; por tal motivo, atribuirá a su ausencia en la empresa el que se promueva a otros compañeros en lugar de a él.

También es importante considerar que no todos los trabajadores son capaces de compaginar trabajo y familia, ya que no separar ambos mundos puede llevar a la excesiva injerencia de las responsabilidades familiares en el trabajo de la persona o viceversa.

De manera secundaria, con frecuencia se presenta en las empresas cierta incapacidad de los directivos o jefes para aceptar el nuevo tipo de relación laboral, ya que la falta de contacto con sus empleados conlleva a la sensación de pérdida de las señales visibles de estatus. Es decir, en cierta medida se desvanecen las características de respeto cotidiano o deferencia hacia el jefe, indicativo del poder alcanzado en la organización.

b) Desventajas para las empresas

La más evidente de las desventajas de este tipo de trabajo consiste en el costo de los equipos y la infraestructura que es necesario invertir para que haya un correcto funcionamiento. Desde luego, no todas las empresas son susceptibles de instrumentar modalidades de teletrabajo (aunque, de acuerdo con los especialistas, prácticamente 50% de los trabajos de oficina y 100% de los trabajos relacionados con la informática pueden realizarse a distancia y, por tanto, son susceptibles de articularse mediante el teletrabajo).

Una de las desventajas del teletrabajo es que no puede aplicarse a todas las empresas. Para que en una compañía se pueda implantar el teletrabajo deben cumplirse tres requisitos:

- Uso intensivo de las tecnologías de la información.
- Sistema de control de gestión altamente formalizado.
- Sistemas de trabajo basados en la dirección por objetivos o en el trabajo por proyectos.

En una empresa con teletrabajadores también existen diversos problemas, a saber:

1. *Respecto a los sistemas de control*: cuanto más capacitado en lo profesional está un trabajador, más independiente y resistente se muestra a los controles. Por tanto, con menores medios de control en lugares de trabajo geográficamente dispersos serán necesarios más controles en los resultados.
2. *En cuanto a las recompensas*: el dinero, empleado tradicionalmente como recompensa a los trabajadores en las oficinas, no sirve para este nuevo tipo de trabajadores, aunque los trabajadores muy calificados suelen responder mejor a recompensas no pecuniarias.
3. *En relación con la carrera profesional*: los trabajadores externos no son visibles en la oficina para que se piense en ellos al hacer promociones. Esto puede privar al teletrabajador de opciones para promocionarse y causar un estancamiento en su carrera.
4. *El aislamiento*: al ser un trabajo más independiente, se puede llegar al aislamiento del individuo. Para evitar esto se intentan realizar contactos formales de manera periódica.
5. Las distracciones a las cuales está sometido el trabajador son mayores que las que tendría en una oficina tradicional. El trabajador deberá trabajar en casa y atender al mismo tiempo las peticiones del entorno familiar, por lo que muchos trabajadores acaban por abandonar la experiencia.
6. El teletrabajo a tiempo parcial lleva finalmente a un fracaso ya que los trabajadores no se comprometen del todo con la empresa. Los trabajadores que empiecen con un trabajo a tiempo parcial acaban buscando el entorno de la oficina tradicional, con relaciones con otros compañeros. Por tanto, la empresa no sólo debe ponderar los beneficios para ella, sino también deberá tener en cuenta los costos y beneficios para el trabajador.

c) Desventajas para la sociedad

Por lo que respecta a la principal desventaja del teletrabajo desde la óptica de la sociedad, cabe destacar el desfase legislativo o lagunas legales que existen en la mayoría de los países.

A reserva de hacer una profundización ulterior, es procedente adelantar que en un gran número de legislaciones laborales, a falta de disposiciones expresas y específicas aplicables al teletrabajo, con frecuencia se recurre a las disposiciones del denominado trabajo a domicilio, para normarlo y regularlo.

Puntos fuertes	Puntos débiles
— Flexibilidad en la organización de la empresa. — Se da mayor confianza a los empleados, lo que les reporta mayor satisfacción. — Mejora la productividad de los empleados. — Reduce los costos de funcionamiento interno de la empresa. — Es una innovación en la empresa.	— Necesidad de contar con una formación adecuada. — Escasa implementación de tecnologías de la información necesarias, como el correo electrónico. — Falta de conocimiento acerca de cómo dirigir el teletrabajo. — Pérdida de control de los empleados. — Puede dificultar la comunicación entre los empleados.
Amenazas	**Oportunidades**
— Posible pérdida de la cultura de la empresa, por la fragmentación del personal. — Inseguridad acerca de la información sensible de la empresa. — Mala imagen que del teletrabajo existe en la sociedad. — Posibilidad de que los empleados pierdan la vinculación con la empresa y se vayan a otra.	— Obtención de ventaja competitiva por la reducción de costos. — Mayor atención al mercado. — Mejores costos de funcionamiento. — Grandes posibilidades de expansión comercial a costos muy reducidos. — Concentración en lo que mejor sabe hacer la empresa, mediante el trabajo vía *outsourcing*.
Factor clave: integrar el teletrabajo de tal modo que se adapten sus sistemas de información en la estrategia global de la empresa, como soporte de aquél.	

Características que deben reunir las tareas susceptibles de ser incluidas en un proyecto de teletrabajo

Dichas características son las siguientes:

- Que sean claramente definibles en cuanto a la función a desempeñar y los objetivos a conseguir.
- Que los resultados sean controlables y cuantificables en función de los objetivos propuestos. El control de asistencia pierde sentido.
- Que impliquen principalmente trabajos de tipo intelectual.
- Que sean de tipo repetitivo o, por el contrario, actividades totalmente creativas que puedan ser desarrolladas igual o incluso mejor en el domicilio que en las oficinas centrales.

Principales repercusiones

Algunos de los principales efectos que propicia el teletrabajo son los siguientes:

1. El primero, que influye directamente en la economía, se refiere a la reducción de costos de los servicios. Dado que los servicios se pueden realizar a distancia, se permite a los empleados tener contratos sólo por horas, por tarea realizada, etcétera.
2. Todo ello, en segundo lugar, tiende a modificar las ideas tradicionales sobre la fuerza laboral y la membresía de los sindicatos.

   La posibilidad de presión, las negociaciones colectivas, el concepto de estabilidad laboral y principios como los de jornada, tiempos de descanso y prestaciones de seguridad social se alteran con esta todavía *sui géneris* pero cada vez más frecuente modalidad de empleo.
3. Un tercer efecto es la revaloración del trabajo individual, cuya evaluación ya no depende de criterios que puedan aplicarse únicamente en los centros laborales.
4. En cuarto término, el teletrabajo afecta la organización habitual en las oficinas. Habrá empleados que sólo acudan de vez en vez para recibir instrucciones directas. Otros incluso no tengan necesidad de asistir a las oficinas porque toda su carga laboral la cumplen desde su domicilio. La idea espacial y funcional de las oficinas puede modificarse a partir de tales tendencias.
5. En quinto lugar, el hecho de que el hogar sea al mismo tiempo sitio de trabajo plantea concepciones inéditas en términos urbanos y sociológicos en este nuevo contexto doméstico.

REGULACIÓN JURÍDICA DEL TELETRABAJO

En ocasiones pareciera que el teletrabajo, por su propia naturaleza, rompe los esquemas tradicionales de las relaciones laborales. Esta disyuntiva ha propiciado dos grandes posturas:

a) La primera señala que, al tratarse de un fenómeno reciente, la figura del teletrabajo no encuentra sustento o regulación expresa en las normas laborales. Por tal motivo, el teletrabajo debe entenderse contenido en las reglas del trabajo a domicilio.

b) Otras opiniones sostienen que los preceptos que regulan el trabajo a domicilio suelen limitarse a tareas manuales y no se aplican, en consecuencia, a cuestiones especializadas como el teletrabajo.

Una vez que la empresa implanta el teletrabajo, debe determinar el marco regulador según el cual se regirá. Se deben contemplar aspectos generales que han de ocurrir en una relación de teletrabajo. Las diferentes legislaciones de los países suelen no considerar de modo expreso el teletrabajo, pero tampoco lo prohíben.

En muchas empresas en las que se ha instalado el teletrabajo (por ejemplo, IBM), más que un contrato de trabajo se ha redactado un documento guía en el cual se recogen las normas de funcionamiento para organizar su empleo y evitar problemas durante el desarrollo de la experiencia.

Estas guías o contratos no pueden abarcar todos los temas, pero sí los problemas para el momento en que puedan surgir. Se deben incluir algunos temas, como los siguientes:

- Comunicación con los trabajadores por parte de la empresa.
- Procedimientos y normas a seguir.
- Horarios en los que el trabajador ha de estar localizable por la empresa.
- Frecuencias y lugares de las reuniones, así como el horario.
- Días laborables y de vacaciones, jornadas de seguimiento y de puesta en común.

Ahora bien, en caso de que se pretenda redactar un contrato específico en materia de trabajo, éstos son algunos rubros importantes, que deberán tenerse en cuenta en el clausulado de dicho contrato:

a) Lugar de trabajo

Una parte de la vivienda o una habitación debe estar reservada para la actividad profesional. El teletrabajador se compromete a tenerla limpia y en condiciones como si se tratara de la oficina.

b) Equipos y útiles de trabajo

Los equipos y materiales necesarios para el ejercicio de la actividad profesional serán suministrados por la empresa y mantenidos por ella. Tales equipos y útiles aún son propiedad de la empresa y deberán restituirse en caso de que cesen las relaciones contractuales con ésta.

La entrega, la instalación y la eventual puesta en servicio de los equipos, útiles y materiales en el lugar de trabajo será por cargo de la empresa.

c) Desplazamientos

El trabajador participará regularmente en las reuniones de información y de trabajo exigidas por el cumplimiento de su tarea. Los despla-

zamientos profesionales se reembolsarán con base en los viáticos en vigor de la empresa. Cabe la posibilidad de que el trabajador sea obligado a desplazarse de manera ocasional a otras sedes de la empresa.

d) Duración de la relación de teletrabajo

En las situaciones de teletrabajo hay algunos puntos intocables en lo que se refiere a la relación laboral y otros sujetos a revisión, por ejemplo: la duración del teletrabajo.

También se considera el "arrepentimiento" del teletrabajador, es decir, el deseo de regresar presencialmente a la empresa, porque descubre que no le conviene la experiencia o porque llega a la conclusión de que el trabajo no es idóneo para realizarlo en casa, o pueden cambiar sus circunstancias personales y las de su entorno, por ejemplo: la existencia de problemas familiares.

e) Los gastos de transporte

La casuística en este caso es muy amplia. En principio no se deben pagar gastos por el transporte en los días en que se estipule que el teletrabajador tiene que ir a la sede de la empresa. Muy pocas empresas tienen en cuenta el pago de este tipo de desplazamientos.

f) Gastos de vivienda

El teletrabajo origina gastos adicionales de luz, teléfono, conexión a internet, etc. Se ha de considerar que además se debe tener una habitación para el teletrabajo, lo cual es uno de los aspectos que más dificultades plantea, ya que muchos teletrabajadores son reacios a dedicar una habitación para trabajar y suelen hacerlo en la sala de estar o en la misma habitación.

De todas formas, debe especificarse en el contrato que los teletrabajadores guarden todos los recibos relacionados con el teletrabajo y los presenten en la empresa.

g) Accidentes de trabajo

Todas las legislaciones tienen muy definido el accidente de trabajo, concepto, circunstancias en que se produce, responsabilidad y derechos de cada afectado.

Con el teletrabajo, las circunstancias del teletrabajador cambian, a veces de manera muy amplia. Los lugares de trabajo son otros, no sólo para él, sino también para otras personas que interaccionan con él (como los técnicos de mantenimiento). Los accidentes que se pro-

duzcan en el domicilio varían en el sentido de que pueden ocurrir por motivos de trabajo o no. En la práctica, la jornada del teletrabajador puede ser de 24 horas cada día.

Lógicamente surgen preguntas tales como: ¿serán accidentes los que se produzcan a cualquier hora?, ¿se considerarán sólo los que surjan en las horas consideradas de presencia obligada, de acuerdo con las condiciones estipuladas en el contrato de trabajo? o ¿han de tenerse en cuenta todos los desplazamientos que haga el teletrabajador durante su teórica jornada laboral?

Los que en principio no conllevan dudas son los accidentes que ocurran en el camino para asistir a las reuniones en la empresa, programadas o no. Un caso típico, que ha habido muchas veces y en el que los tribunales han fallado a favor del teletrabajador, es aquel en el que éste se cae por la escalera al ir a buscar a otro piso de la vivienda algo que necesita para su trabajo (un documento, un disquete, un libro, etc.), aunque el problema reside en demostrar que efectivamente es imprescindible para seguir trabajando.

h) Salario

En condiciones normales, este apartado no suele sufrir ninguna alteración. Sin embargo, a veces los empleadores prefieren ahorrarse vacaciones, pagos por maternidad, enfermedades, etc., y se niegan a mantener las mismas condiciones a todos sus trabajadores. Según cuáles sean las empresas e incluso los sectores y los países, pueden originarse situaciones muy distintas.

Normalmente hay empresas que dan al empleado un pago extra cuando trabaja en el propio domicilio para compensar los gastos que tiene en exceso, como luz, calefacción, refrigeración, etc. No obstante, en otros casos, a los teletrabajadores se les ha pagado incluso menos salario que a quienes se quedan en la empresa, para lo cual se aduce, primero, que el teletrabajo es algo voluntario y que se puede considerar con un premio y, segundo, que el teletrabajador tiene menos gastos en transporte, ropa, comidas, etcétera.

i) Aspectos fiscales

Algunas legislaciones conceden ventajas fiscales a las empresas que emplean a teletrabajadores. Pero el problema consiste en demostrar que esa persona es un empleado de la empresa y no pagar por otros conceptos, como la seguridad social y las vacaciones.

Siempre tiene que quedar muy claro si el trabajador es autónomo o no, para lo cual la empresa ha de poner cuidado en exigir o no el cumplimiento de un horario, por ejemplo. Es decir, quizá sea inte-

resante para la empresa beneficiarse de concesiones fiscales, con el argumento de que las personas que teletrabajan son empleados suyos, pero entonces ha de poner los medios para que no se la obligue a considerar a esos trabajadores en nómina. En muchas legislaciones no está clara la definición de lo que convierte a una persona en un empleado, de lo que constituye un trabajador autónomo o de lo que es un autoempleo individual.

Su asimilación como trabajo a domicilio

En el trabajo a domicilio se combinan los siguientes criterios:

a) El trabajo a domicilio implica una relación de empleo entre el trabajador a domicilio y el empleador o patrón. El acuerdo puede ser implícito o explícito, verbal o escrito, tal como se especifique en la legislación nacional.
b) El lugar de trabajo está fuera de los establecimientos del empleador. Sin embargo, no todas las formas de trabajo a domicilio están necesariamente basadas en casa, sino que pueden realizarse en instalaciones cercanas, talleres o establecimientos que no pertenezcan al empleador. Esto significa que hay poca supervisión directa o regulación de los métodos de trabajo por el empleador.
c) La forma de pago suele ser por piezas o unidad de producción, pero no todos los trabajadores a tarifa por pieza son trabajadores a domicilio.
d) En relación con el suministro de materiales y herramientas, en algunos casos los trabajadores tienen sus propias herramientas, mientras que en otros el empleador las proporciona a préstamo o con base en una venta a plazos. De forma similar, los trabajadores a domicilio pueden comprar sus materias primas en el mercado o al empleador, o subcontratista y venderle los productos terminados o semiacabados.

Como se observa, en principio parecería que el concepto de trabajo a domicilio constituye la norma reguladora del teletrabajo. Ciertamente, existe una gran similitud entre ambas formas de organización laboral que hacen pensar en una primera instancia que el trabajo a domicilio engloba al teletrabajo.

Sin embargo, cabe mencionar que la legislación especial que ampara a los trabajadores a domicilio se limita a actividades o tareas fundamentalmente artesanales o manuales, por lo que no se puede aplicar al moderno teletrabajo. Es decir, el argumento fundamental de esas opiniones descansa en el hecho de que las actividades que no incorporan las telecomunicaciones o la informática para el desempeño de las actividades a realizar no pueden considerarse teletrabajo.

Luego, las características modernas del teletrabajo no pueden estar sujetas a esquemas normativos de cierta antigüedad que, en el mejor de los casos, ni siquiera tomaron en cuenta el desarrollo tecnológico y sus consiguientes efectos en las organizaciones laborales.

El teletrabajo y los sindicatos

Para los sindicalistas, en términos teóricos, el teletrabajo es una forma de prestación laboral; está caracterizado fundamentalmente no sólo por la base tecnológica, común a muchos trabajos presenciales en los que todas las tecnologías de la información y las telecomunicaciones se generalizan, sino también es un trabajo a distancia, lo cual hace romper el carácter clásico de la relación laboral presente en los centros de trabajo. A los sindicatos no les sorprende el teletrabajo ni la dimensión que pueda cobrar la cantidad de teletrabajadores que pueda existir en un futuro, porque piensan que el trabajo a distancia es una manera de flexibilizar la relación laboral; empero, también lo ven como una forma más flexible de organizar el trabajo y de prestar servicios, como una parte más de la tendencia flexibilizadora en los modelos organizativos de las empresas.

Lo que ven los sindicatos es, en definitiva, un proceso continuo de transformación en el mundo laboral, cómo trabajar y cómo buscar nuevas formas organizativas para responder a nuevas necesidades y paradigmas empresariales.

En cuanto a quién debe pagar las herramientas, los sindicatos plantean que cuando se produzca una oportunidad laboral por iniciativa de la empresa de pasar de un trabajo presencial a trabajar a distancia, todos los costos originados en este cambio organizativo de la prestación laboral debe erogarlos la empresa por los ahorros en costos que supone para ella. Otra cuestión es el trabajo autónomo o teletrabajo por cuenta propia, en el cual hay algunas reticencias, pues en algunos casos se trata de situaciones de trabajo encubiertas, por lo que la empresa debería hacerse cargo de parte de los costos.

Situación internacional

Algunos países han adoptado legislación específica para regular los términos y condiciones según los cuales puede proporcionarse trabajo a domicilio (Argentina, Austria, Alemania, Italia, Marruecos, Perú y Uruguay).

En otros, la legislación sobre trabajo a domicilio sólo se aplica a ciertas industrias o actividades económicas en las que principalmente tiene lugar esta forma de organización (India, Holanda, Noruega, Polonia, Portugal y Suiza).

Algunos otros países dedican una sección de sus códigos laborales al trabajo a domicilio (Bolivia, Colombia, Costa Rica, República Dominicana, Ecuador, El Salvador, Guinea Ecuatorial, Francia, Guatemala, Haití, Honduras, Nicaragua, Panamá, Paraguay, España y Venezuela).

En los países donde no hay legislación acerca del trabajo a domicilio o donde se limita su ámbito de aplicación, la legislación general de trabajo puede aplicarse en forma supletoria a la legislación sobre trabajo a domicilio.

Situación en México

La *Ley Federal del Trabajo*, en el Título Sexto denominado Trabajos Especiales, prevé un capítulo específico que abarca de los artículos 311 a 330 para hacer referencia al trabajo a domicilio.

Así, se indica que el trabajo a domicilio es el que se ejecuta habitualmente para un patrón, en el domicilio del trabajador o en un local elegido de manera libre por él, sin vigilancia ni dirección inmediata de quien proporciona el trabajo. Si el trabajo se ejecuta en condiciones distintas de las señaladas en el párrafo anterior, se regirá por las disposiciones generales de esta ley (artículo 311 de la LFT).

Como nota relevante, la legislación mexicana señala que los patrones que den trabajo a domicilio deberán inscribirse previamente en el Registro de patrones del trabajo a domicilio, que funcionará en la Inspección del Trabajo. En el registro constarán el nombre y el domicilio del patrón para el que se ejecutará el trabajo y los demás datos que señalen los reglamentos respectivos (artículo 317 de la LFT).

Además, los patrones están obligados a llevar un libro de registro de trabajadores a domicilio, autorizado por la Inspección del Trabajo, en el que constarán diferentes datos vinculados con las características del trabajo, como los siguientes:

a) Datos generales del trabajador.
b) Domicilio o local donde se ejecutará el trabajo.
c) Días y horarios para la entrega y recepción del trabajo y para el pago de los salarios.
d) Naturaleza, calidad y cantidad del trabajo, entre otros.

La posible solución

A decir del catedrático italiano Marco Biagi, "es preferible la negociación colectiva a la promulgación de legislación. Después de todo, la legislación de muchos países es algo obsoleta y no puede tomar fácilmente en cuenta

las situaciones nuevas, tales como las actuales modalidades de trabajo. La legislación no puede revisarse con la misma rapidez con que evolucionan las nuevas tecnologías, razón por la cual las prácticas de empleo deberían reglamentarse sólo una vez que estuvieran razonablemente consolidadas". Esas reglas se pueden ajustar de forma periódica para tener en cuenta las ventajas y los inconvenientes de cada situación. Por medio de la negociación colectiva, resulta posible llegar a un auténtico consenso, no a una postura impuesta por el gobierno, sino a un consenso alcanzado conjuntamente para aprovechar todas las ventajas de la tecnología moderna.

De acuerdo con lo anterior, cabe señalar que no existe una posición definitiva acerca de la regulación del teletrabajo. El hecho cobra relevancia, pues, según estudios de la Unión Europea, el ritmo de introducción de nuevas tecnologías es tal que en los próximos 10 años se considera que 80% de las tecnologías en uso serán distintas de las actualmente conocidas. Ochenta por ciento de los usuarios habrán cumplido su formación antes de que nazcan estas tecnologías y sólo 20% de los ciudadanos se habrá formado en el mismo periodo.

De cualquier manera, aquellas personas cuyas actividades estén relacionadas con el teletrabajo no deben quedar desprotegidas bajo ningún concepto. Al menos, la posición de las autoridades laborales deberá orientarse para evitar menoscabos o afectaciones a los derechos laborales.

Recuérdese que el régimen jurídico mexicano señala que, a falta de disposición expresa en la Constitución, en la *Ley Federal del Trabajo*, en sus reglamentos o en los tratados internacionales celebrados por México, se tomarán en cuenta las disposiciones que regulen casos semejantes, los principios generales del derecho, la jurisprudencia, la costumbre y la equidad, y, más aún, en la interpretación de las normas de trabajo debe prevalecer la interpretación que resulte más favorable para el trabajador (artículos 17 y 18 de la LFT).

XII. Valor probatorio de los documentos electrónicos

EVOLUCIÓN DEL DERECHO DE PRUEBA

La evolución del llamado derecho probatorio va de acuerdo con el devenir de las doctrinas filosófico-políticas y con la estructura particular de cada sociedad. Los diversos sistemas filosóficos predicados en las distintas etapas de la historia de la humanidad le han impreso su sello característico correspondiente al sistema probatorio. Se sabe bien que desde este punto de vista existen el individualismo grecorromano, el feudal y el derivado del capitalismo, así como el del socialismo. A cada uno de ellos corresponde determinada fisonomía probatoria procesal. Por ejemplo, la filosofía feudalista llevó su idea de clases sociales hasta la valoración de los testimonios, la filosofía católica trasladó sus principios a la confesión judicial y al juramento; con la Revolución francesa, el rito procesal probatorio se democratizó y se impuso el íntimo convencimiento como sistema elevador de una prueba; y el capitalismo de los Estados industrializados impuso más tarde la noción de la verdad formal y del sistema dispositivo que hace del juez un pasivo espectador del proceso. En cierta ocasión alguien dijo con fortuna que, al leer las normas legales reguladoras de la prueba judicial, se deduce cuál es la filosofía que impera en un país determinado.

A dicha evolución habrá que agregar que el desarrollo de las ciencias y de las técnicas ha contribuido, de manera particular en el último siglo, a dar una nueva orientación a los sistemas probatorios. De esta manera, los avances de la psicología, de la lógica formal y de la lógica dialéctica, por ejemplo, han orientado en este periodo la valoración de la prueba judicial, ¿Acaso la informática no constituye un factor de cambio respecto al fenómeno probatorio? Esta evolución ha sido distinta en los países de derecho consuetudinario (*Common Law*) y en aquellos de derecho escrito; nos ceñiremos sólo al caso de estos últimos.

ALGUNAS CONSIDERACIONES ACERCA DE LA PRUEBA Y LA TEORÍA GENERAL DEL PROCESO

La teoría de la prueba se subordina a la teoría general del proceso, entendido éste como el conjunto complejo de actos, provenientes del Estado, de las partes y de terceros ajenos a la relación sustancial. De esta manera, es menester mencionar el debate en materia probatoria referente a la unidad o diversidad de procesos, para plantear igualmente la existencia de distintas pruebas (civiles, laborales, contenciosas, administrativas). Al respecto, es válido pensar que la prueba judicial es única, sin importar el área jurisdiccional donde se utilice, porque los principios universales que rigen el proceso son también los que orientan la prueba.

Por otra parte, la teoría de la prueba judicial no se limita de manera exclusiva a la temática de la prueba procesal, sino que está referida a consideraciones extrapotenciales, técnicas y procedimientos. En cuanto a la mayor o menor utilización de ciertos medios de prueba en determinada rama de enjuiciamiento se suscitan divergencias, por el criterio valorativo aplicable o por el orden a seguir en el procedimiento; sin embargo, los problemas de la prueba son los mismos en todos los procesos.

En cuanto a la noción de prueba se tiene hoy en día un concepto uniforme y generalizado. Las pruebas son hechos, surgen de la realidad extrajurídica y el orden natural de las cosas, constituyen una creación del derecho, su existencia y valor se toman de la realidad extrajurídica como fuentes (documento, testigo, cosa litigiosa, etc.) y se integran como medios (actuaciones judiciales, como la declaración de un testigo).

DIFERENTES MEDIOS DE PRUEBA

Entre los principales medios de prueba cabe destacar los siguientes:

a) *Confesional.* Es una declaración que contiene el reconocimiento de un hecho de consecuencias jurídicas desfavorables para el confesante.
b) *Documental.* También llamada literal, es la que se hace por medio de documentos en la forma establecida en las leyes procesales.
c) *Pericial.* Se deriva de la apreciación de un hecho por un observador con preparación especial obtenida mediante el estudio de la materia a que se refiere o simplemente por la experiencia personal.
d) *Testimonial.* Dada por los testigos como aquellas personas que comunican al juez el conocimiento que posee acerca de determinado hecho (o hechos) cuyo esclarecimiento interesa para la decisión de un proceso.
e) *Inspección judicial.* Consiste en un examen directo por el juez de la cosa mueble o inmueble sobre la que recae para formar su convicción

concerniente al estado o situación en que se encuentra al realizarla (ésta se puede llevar a cabo fuera o dentro del juzgado).

f) *Fama pública.* Estado de opinión acerca de un hecho que se prueba mediante el testimonio de personas que la ley considera hábiles para este efecto.

g) *Presuncionales.* Operaciones lógicas mediante las cuales, a partir de un hecho conocido, se llega a la aceptación como existente de otro desconocido o incierto.

SISTEMAS DE APRECIACIÓN PROBATORIA

Sistema de libre apreciación o convicción

La libre apreciación es la facultad del juez de resolver la acreditación de la prueba; sin embargo, no hay un valor previamente establecido. Por ejemplo, en la legislación mexicana se prevé en los artículos 16 constitucional y 841 de la *Ley Federal del Trabajo*.

Sistema de la prueba legal o tasada

La forma de otorgar valor a las pruebas se establece en las normas. El *Código Fiscal de la Federación* aún conserva cierta tendencia en este tipo de valoración.

Sistema mixto

Según dicho sistema, algunos aspectos están previstos y regulados por el legislador y otros dejan libertad al juzgador. Este sistema regula la existencia del sistema de prueba legal de la libre apreciación, aunque predomina la primera.

Un ejemplo del sistema mixto se encuentra en el *Código Federal de Procedimientos Civiles* (artículos 197 a 218), en el *Código de Comercio* (artículos 1287 a 1306) y en el *Código Federal del Procedimientos Penales* (artículos 279 a 290).

Sistema de la sana crítica

La decisión del juzgador debe sustentarse en una actitud prudente y razonable, expresada con argumentos lógicos, sin diferir de lo establecido en la jurisprudencia o la doctrina.

El predominio de la consensualidad como regla en el consentimiento y perfeccionamiento de los contratos electrónicos explica por sí sola la importancia de este tipo de prueba. En armonía con la validez y eficacia de la modalidad electrónica en su doble dimensión de consentimiento expreso y forma del contrato, se generaliza en el marco comparado la admisibilidad de la prueba electrónica.

PRUEBA DOCUMENTAL

Si bien la mayoría de los medios de prueba enunciados pueden interrelacionarse con las computadoras, la prueba documental, en última instancia, guarda un vínculo más estrecho en cuanto a que el fundamento legal pueda constar como documento.

Concepto de documento

El vocablo *documento* deriva de la palabra griega *dekos*, que significaba en materia religiosa las manos extendidas para ofrecer y recibir. De esta raíz nace el verbo latino *doceo*, que significa enseñar, y el vocablo *documentum*, que tiene la acepción de "aquello con el que alguien enseña o instruye"; se trata de algo que nos enseña del pasado.

El concepto de enseñar implica también el demostrar, indicar; y éstos a su vez el de presentar, es decir, poner algo en presencia de uno. Cuando ese mostrar se produce a través de otra cosa, estamos ante la representación. De este modo la figura, imagen o idea sustituye la realidad.

Según el *Diccionario de la Real Academia Española*, documento es... "el diploma, carta o escrito que nos ilustra acerca de algún hecho, especialmente de los históricos, o también como escrito en el que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo....".

En matera jurídica, documento es "todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier tipo de relevancia jurídica".

Con ese concepto, son documentos, además de los escritos en papel, los planos gráficos, los dibujos, las fotografías, los videos, el cine, las cintas magnetofónicas, los discos informáticos, etcétera.

El documento, en sentido amplio, es toda representación material destinada e idónea para reproducir cierta manifestación del pensamiento.[1] De

[1] Chiovenda, *Principios de derecho procesal civil*, t. II, p. 334.

esta manera, los documentos escritos no son, por tanto, la única manifestación de la prueba documental, de modo que fotografías, copias fotostáticas, registros, etc., pueden constituir, en última instancia, variedades de dicha prueba documental.

En este sentido, el documento, como el testimonio o la confesión, es el resultado de la actividad humana; es decir, poner algo en presencia de uno, produciéndose lo que podría llamarse una "representación", que al decir de Carnelutti, es la imagen de la realidad la que se presenta al intelecto a través de los sentidos. En consecuencia, documento es una cosa que sirve para representar a otra, de lo que se concluye que mientras que el acto, testimonio o confesión es por sí mismo representativo del hecho testimoniado o confesado, el acto que crea el documento no es representativo del hecho narrado en éste, sino que se limita a crear el vehículo de representación que es ese documento.

En términos amplios puede afirmarse que documento es cualquier objeto que contiene una información que narra, hace conocer o representa un hecho, cualquiera que sea su naturaleza, su soporte o su continente, su proceso de elaboración o su tipo de firma.

La idoneidad de tales documentos para perpetuar hechos pasados (que en algunos casos pueden constituir una prueba extraordinariamente pertinente) es indiscutible.

Los documentos públicos y privados

Los documentos escritos se suelen dividir en públicos y privados. Los primeros son otorgados por autoridades o funcionarios públicos dentro de los límites de sus atribuciones o por personas investidas de fe pública en el ámbito de su competencia en forma legal, y pueden ser notariales, administrativos, judiciales y mercantiles según su origen.

Por otra parte, los documentos privados son aquellos en los que se consigna alguna disposición o convenio por personas particulares, sin la intervención del escribano ni de otro funcionario que ejerza cargo por autoridad pública, o con la intervención de estos últimos, pero respecto a actos que no se refieren al ejercicio de sus funciones.

En cuanto al valor y eficacia de estas pruebas, las actuaciones judiciales hacen prueba plena y los privados sólo lo harán contra su autor cuando fueren reconocidos de manera legal.

Diferencias con el instrumento

De la palabra documento, también se distingue la palabra "instrumento" (como algo destinado a instruirnos e informarnos del pasado). En la base

de la noción de documento está la idea de docencia, y en el de instrumento la de prueba.[2]

Existe una tendencia a identificar los conceptos de documento e instrumento o escrito, siendo esto consecuencia de que el Código Civil de Napoleón hace referencia sólo a los instrumentos o escritos, clasificándolos en públicos o privados. Pero dicha identificación es errónea, pues hay documentos no instrumentales que no son escritos, tales como dibujos, cuadros, fotografías, películas., etc., que son aceptados como medios de prueba.

El concepto de documento es muy amplio, y comprende todos los objetos que pueden ser llevados ante un juez y que sirven de medio probatorio porque representan un pensamiento. En cambio, el instrumento es una variedad del documento; son aquellos escritos destinados a consignar una relación jurídica.

Los hechos jurídicamente relevantes (materiales, en el sentido de transformación de la realidad, o inmateriales, como expresión de la memoria, la voluntad la inteligencia) suelen quedar reflejados en objetos o aparatos, que sirven de soporte a tales rastros. El soporte puede tener la maciza obviedad de la piedra o la magnética sofisticación de un disco de PC. Son los llamados "instrumentos".[3]

Clasificación

El documento puede clasificarse desde el punto de vista de su contenido en *declarativo o representativo*, cuando contenga una declaración de quien lo crea, lo otorga o simplemente lo suscribe, como es el caso de los escritos públicos o privados; pero puede ser *únicamente representativo* (no declarativo) cuando no contenga ninguna declaración, como ocurre con los planos, cuadros o fotografías. Por tanto, el documento no es siempre un escrito, pudiendo reunirse ambos caracteres en un mismo documento. [4] Su carácter representativo aparece en su etimología, porque la voz "documento", como se ha expresado, deriva de *docere* (enseñar, hacer, conocer), y lo distingue siempre de las cosas u objetos que, sin ser documentos, pueden servir de prueba indiciaria, como una huella, un arma, una herida, etc.[5] En tanto *representación*, el documento refiere, en principio, a los hechos ya

[2] Pelosi, *El documento notarial*, 1980, pp. 12 y ss.

[3] *Conf.* Palacio, Lino Enrique y Alvarado Velloso, Adolfo, *Código Procesal Civil y Comercial de la Nación*, Rubinzal-Culzoni, Santa Fe, t. 8o., p. 147; Devis Echandía, Hernando, *Compendio de la prueba judicial*, Rubinzal-Culzoni, Santa Fe, 1984, t. II p. 197.

[4] "De acuerdo con su función los documentos pueden clasificarse en constitutivos y meramente probatorios" (Palacio y Alvarado Velloso, ob. cit., t. 8o., p. 148).

[5] Devis Echandía, Hernando, Teoría general de la prueba judicial, Zabalía, 1988, t. II p. 486.

pasados. Y en tanto *declaración*, expresa la intención del otorgante respecto de las circunstancias presentes, pasadas o futuras, pero formuladas en el pasado.[6] En cualquiera de los dos casos se trata de una referencia no actual, sino histórica, de lo registrado en el documento.

José V. Acosta señala que la tecnología permite incorporar un tercer contenido en el documento: el de la *transmisión*. Imaginemos un juicio (no necesariamente penal): si en el transcurso del procedimiento probatorio se invocara un hecho nuevo relativo a la causa que *estuviese ocurriendo* fuera de la sala (no importa si a pocos o a muchos kilómetros) y es televisado, el documento (imágenes y sonidos captados por la cámara y receptados en la sala de audiencias) no contendrá ya la expresión *histórica* del hecho, sino la *actual*. Tenemos, entonces, documentos *representativos*, documentos *declarativos* y documentos *transmisivos*.[7]

Según Devis Echandía,[8] son requisitos para la existencia jurídica del documento:

- Que se trate de una cosa u objeto con aptitud representativa;
- Derivado de un acto humano;
- Que represente un hecho cualquiera;
- Que tenga una significación probatoria.

De acuerdo con lo anterior, la doctrina dominante limita la noción de documento a los objetos representativos y considera a los demás como "piezas de convicción", que pueden servir de indicios mediante la operación mental, lógica y crítica del juez.[9]

El documento electrónico

La evolución tecnológica de los últimos tiempos ha provocado una verdadera conmoción que afecta todos los ámbitos de la actividad jurídica y comercial, surgiendo nuevas modalidades de contratación y de actos jurídicos. Se está revelando una necesidad en la ciencia del derecho de hallar las formas y maneras de optimizar las oportunidades que presenta la tecnología, de cara a los medios tradicionales, como la del documento en soporte de papel o la firma, que pierden utilidad práctica y vigencia.

---

[6] Los documentos declarativos, a su vez, atendiendo a la declaración que contienen, pueden clasificarse en dispositivos e informativos. *Confr.* Palacio y Alvarado Velloso, *op. cit.*

[7] Acosta, José V. *Visión jurisprudencial de la prueba civil*, Rubinzal-Culzoni, 1996, t. II p. 9.

[8] Devis Echandía, Hernando, "Concepto, naturaleza y funciones jurídicas del documento en el ámbito procesal", en *Revista Argentina de Derecho procesal*, núm. 3, julio-septiembre de 1969, pp. 317 y ss.

[9] De Santo, Víctor; *La Prueba Judicial. Teoría y Práctica*, Universidad, 1992, pp. 143 y 144.

Hoy existe la tecnología suficiente para realizar todo tipo de transacciones por medios electrónicos, por lo que correspondería preguntarse si nuestro sistema jurídico se encuentra capacitado para responder a las nuevas exigencias generadas por la tecnología de la información.

El análisis de la temática del documento digital debe abarcar, por un lado, la necesidad de otorgar la más eficaz y vasta utilización de los medios de información que se intercambien electrónicamente, y por el otro, la necesidad de tutelar la confianza de los usuarios en la seguridad de los nuevos documentos.

Desde la recepción del Derecho Romano, el documento con soporte en papel ha gozado de pleno reconocimiento y absoluta validez en función de dos elementos: *a*) en función de su autoría (*in manu publica confecta*); y *b*) en función de su forma (*in publica forma confecta*).

En los documentos informáticos ninguno de estos dos elementos se dan de manera tradicional, de allí el reto del enfoque.

Concepto de documento electrónico

El avance de la tecnología con los distintos medios informáticos que brinda se está implementando velozmente, constituyendo un fenómeno que parece presentar un carácter irreversible, a tal punto que no es aventurado pensar que en un futuro no muy lejano casi toda la actividad documental se llevará a cabo en forma automatizada. De esta manera, el documento redactado en las formas tradicionales (documento manual, mecánicas o fotográficas) será prácticamente sustituido por el documento electrónico.[10]

Al referirnos al documento electrónico se alude a que el lenguaje magnético constituye la acreditación, materialización o documentación de una voluntad ya expresada en las formas tradicionales, y en que la actividad de una computadora o de una red sólo comprueban o consignan electrónica, digital o magnéticamente un hecho, una relación jurídica o una regulación de intereses preexistentes. Se caracterizan porque sólo pueden ser leídos o conocidos por el hombre gracias a la intervención de sistemas o dispositivos traductores que hacen comprensibles las señales digitales. El ejemplo más común lo constituyen los documentos especialmente construidos para el uso de las terminales de un sistema, como es el caso de las tarjetas magnéticas para acceder a las cuentas bancarias, vía cajeros automáticos.

Técnicamente el *documento electrónico* es un conjunto de impulsos eléctricos que recaen en un soporte de computadora, y que, sometidos a un

[10] Valcarce, Arodin, "Valor probatorio del documento electrónico", en *Revista de Jurisprudencia Provincial*, Buenos Aires, septiembre de 1995, año 5, núm. 9, pp. 741/747.

adecuado proceso, permiten su traducción a lenguaje natural mediante una pantalla o una impresora.

Cabe aclarar que lo que se lee en la pantalla o lo impreso no son el documento electrónico original sino copias, ya que el original no se podrá utilizar directamente, debido a que su contenido no puede ser aprehendido directamente por nuestros sentidos.

Sobre este concepto hay gran discusión en la denominación. Unos lo llaman documento electrónico, otros documento digital, y finalmente hay quienes, como quien esto escribe, preferimos llamarles documento informático.

El documento informático, en su sentido más general, es el documento que se crea con la intervención no ya de una computadora, sino de todo un sistema informático (la computadora en combinación de sus periféricos de entrada y salida).

En el Derecho Italiano, resuelven el tema de manera simplista e identifican el concepto, y se define como documento electrónico o informático a toda representación en forma informática o electrónica de actos, hechos y datos jurídicamente relevantes.

Otro concepto de documento electrónico es el de la fijación de un soporte electrónico de información, que queda registrada en la memoria auxiliar de la computadora, incluyendo en este concepto los medios de recuperación de la información. En realidad, documento electrónico en sentido estricto es el que aparece instrumentado sobre la base de impulsos electrónicos y no sobre un papel; es el conservado en forma digital en la memoria central de la computadora o en las memorias de masa, y que no puede ser leído o conocido por el hombre sino como consecuencia de un proceso de traducción que hace perceptible y comprensible el código de señales digitales.

Sin embargo, coincidimos en que puede hablarse de *documento electrónico* en sentido amplio, que es el formado por la computadora (o dispositivo electrónico) a través de sus propios órganos de salida, y que es perceptible por el hombre sin la necesidad de máquinas traductoras. En esta materia se ha distinguido entre los documentos introducidos en la memoria de base a través de la intervención humana y los introducidos por medio de una máquina o dispositivo (lector óptico). También se distingue con el documento electrónico en sentido amplio entre la documentación (simple operación representativa) y la reproducción o repetición de la declaración del negocio. Se señala que la declaración sucesiva que naturalmente tiende a facilitar la prueba no la produce el mismo sujeto autor de la primera, sino la computadora, pero la misma voluntad que dio vida a la declaración precedente (que queda comprendida en la computadora) al mismo tiempo admitió que fuera plasmada en un documento elaborado por ésta.

Características

Las características esenciales del documento electrónico, sin las cuales no sería posible darle la importancia y utilidad en el ámbito jurídico, son las siguientes:

a) Inalterabilidad

El principal obstáculo para la admisibilidad y eficacia probatoria de los nuevos soportes de información se plantea en relación con el carácter de *permanente*, que se menciona como esencial en la definición de "documento". El temor sobre la posibilidad de reinscripción o reutilización de los soportes informáticos disminuye su seguridad y confiabilidad.

b) Autenticidad

Un documento es *auténtico* cuando no ha sufrido alteraciones que varíen su contenido, lo que implica decir que la autenticidad está íntimamente vinculada con la inalterabilidad. Un documento será más seguro cuanto más difícil sea alterarlo y sea más fácil de verificarse la alteración que podría haberse producido o reconstruir el texto originario.

c) Durabilidad

Se denomina así a toda reproducción indeleble del original que importe una modificación irreversible del soporte. Se entiende por *modificación irreversible del soporte* la imposibilidad de reinscripción del mismo; por *indeleble* la inscripción o imagen estable en el tiempo y que no puede ser alterada por una intervención externa sin dejar huella. Se dice que el papel es un razonable soporte físico porque no es fácil de alterar, lo que es relativo, ya que no es inalterable y es posible la falsificación de instrumentos. El papel se deteriora e incluso su conservación es problemática por la capacidad de absorción de partículas de polvo.

d) Seguridad

Se cuestionan los documentos no escritos con relación a la autenticidad de la representación. Con el desarrollo de claves de cifrado y otras medidas criptográficas, el documento electrónico es al menos equivalente al instrumento escrito y firmado sobre soporte de papel en cuanto a la seguridad.

El requisito de la firma de las partes es requerido como condición esencial para la existencia de todo acto bajo forma privada. La *firma* es un signo personal autógrafo, trazado por la mano del autor, que sirve para informar sobre la identidad del autor de la declaración de voluntad, así como del acuerdo de éste con el contenido del acto y que luego sirve para probar la autoría.

La impresión digitopulgar, aunque asimilada a la firma, no la suple legalmente. Creemos que en materia de prueba de los actos jurídicos esta noción de autoría por medio de la firma debe ampliarse, incorporando otro medio técnico que asegure la verificación de la autoría atribuida y de la autenticidad de la declaración de voluntad contenida en el documento. Las técnicas de seguridad de los datos basados en la biometría o las técnicas criptográficas (sistema de registro y sistema de cifrado literal) brindan seguridad similar, cuando no superiores. La premisa de que la firma de una persona física colocada a continuación de un texto implica el conocimiento del mismo y su conformidad, es decir, *representa el consentimiento*, estaba basada en el simple hecho de no existir otras maneras de registro permanente de la voluntad expresada por las personas. La imprenta, telégrafo, teléfono, gramófono y la radiofonía ampliaron las posibilidades de comunicación, pero en el plano jurídico no tuvieron el mismo efecto por la desconfianza sobre la autenticidad del mensaje. Se enfrenta de nuevo esta situación con las redes, en especial con *internet*. El documento privado puede prescindir de la firma en la medida que por otros medios pueda cumplir con las finalidades perseguidas con su utilización, es decir, la determinación de la autoría y autenticidad de la declaración. La autenticidad e inalterabilidad depende de la seguridad que rodee el proceso de elaboración y emisión de documento.

Clasificación

Lo expuesto corresponde para los documentos electrónicos en sentido estricto, los cuales se encuentran contenidos o escritos en soportes de naturaleza magnética o interna o transmitidos vía redes telemáticas. Pero existe una segunda especie de documento electrónico que surge cuando son impresos computacionalmente o provienen de un sistema informatizado, es decir que ha sido plasmado al papel o llevado a la pantalla de la computadora con información proveniente de un documento electrónico en sentido estricto.

Bajo documento electrónico se consideran datos o informaciones que tienen relevancia jurídica, los cuales son transmitidos o registrados por vía electrónica, especialmente a través del procesamiento electrónico de datos, pero también por medio de simples soportes de sonido.

El documento electrónico es el que está en la memoria de la máquina y cuyo contenido o texto está en el lenguaje de la máquina, el que puede ser pasado a lenguaje natural y eventualmente ser impreso para facilitar su utilización y lectura por parte de los usuarios.

De acuerdo con Giannantonio,[11] los documentos electrónicos pueden ser clasificados así:

a) *Documento formado por la computadora.* En este caso la computadora no se limita a materializar una voluntad, una decisión o una regulación de intereses ya formada, sino que, conforme a una serie de parámetros y datos y a un adecuado programa, decide en el caso concreto el contenido de una regulación de intereses. La computadora no se limitará a documentar una voluntad externa, sino que determinará el contenido de tal voluntad; el lenguaje electrónico no constituye simple documentación de una voluntad en las formas tradicionales, sino que constituye la forma entendida como elemento expresivo necesario de tal voluntad, la manifestación exterior necesaria de la regulación de intereses.

b) *Documento formado por medio de la computadora.* Éste es un caso distinto, pues la computadora documenta una regulación de intereses ya expresados en otras instancias o en otras formas. Aquí su actividad se dirige sólo a comprobar y no a constituir.

Son estos últimos los llamados *documentos electrónicos en sentido estricto*, ya que se encuentra contenido en la memoria central de la computadora o en la memoria de masa (es decir, en soportes distintos a él, y generalmente externos: cintas, floppy disk, hard disck, CD-ROM, etc.) y cuya característica común es que no pueden ser leídos por el hombre sino mediante una máquina que haga perceptible y comprensible la señal digital de que están constituidos.

También los documentos electrónicos pueden ser clasificados con relación al grado de *conservación*:

a) De carácter *volátil*. Por ejemplo, los datos contenidos en las memorias circuitales RAM (Random Access Memory), los cuales se pierden inmediatamente al cortar la energía a la computadora.

b) *Permanentes*. Son aquellos contenidos en algunas memorias de masa, como cintas y floppy disk. A diferencia de la anterior categoría, los datos allí almacenados desaparecen sólo al ser borrados; en caso contrario, se mantienen en el tiempo.

[11] Giannantonio, Etore, "El valor jurídico del documento electrónico" en *Informática y Derecho (Aportes de doctrina internacional)*, p. 100, Depalma, 1987.

c) *Inalterables*. Son aquellos que una vez grabados no pueden ser alterados, sino sólo leídos. Dentro de éstos se encuentran las memorias RAM (Read Only Memory), que consisten en un circuito o chip integrado a la computadora, o que se le puede incorporar a voluntad, y los CD-ROM, que son una memoria de masa contenida en un disco láser.

Así, y coincidiendo con De Prada, puede afirmarse que los documentos informáticos son de dos tipos:

1. *Documentos informáticos sobre soporte papel*. Se trata de los documentos producidos por medio de la computadora. Son los documentos creados mediante el uso de un periférico de salida, que generalmente es la impresora láser, y se le dota de soporte papel para ser leído, corregido, autorizado y si contienen un hecho o acto jurídico para ser otorgado mediante la impresión en él de las firmas ológrafas de las partes.
2. *Documentos informáticos sobre soporte electrónico*. Son los documentos producidos no por medio de la computadora, sino en la computadora, y que sólo pueden ser leídos con la aplicación de la técnica informática. En este tipo de documentos, el informático sólo tiene un soporte electrónico. La combinación de la computadora y la telemática dio origen a la comunicación de dos o más computadoras a través de una línea telefónica y permitió la creación, lectura y almacenamiento de documentos informáticos.

Tipos de soportes informáticos

Los principales soportes informáticos son:

1. Los soportes magnéticos, que almacenan la información digitalmente, que son:
   a) El disco duro (hard disk), que viene en el hardware de la computadora; y
   b) El disco móvil (disquete), que es intercambiable y fácilmente transportable.
2. Los soportes ópticos de lectura láser, que son los CD similares a los discos compactos de música. Tienen ventaja sobre los disquetes porque son más durables y tienen mayor capacidad de almacenamiento.
3. Los códigos ópticos impresos, conocidos como códigos de barras, que se han utilizado básicamente en el comercio para leer el precio y la identificación del producto.
4. Nuevos dispositivos electrónicos portátiles.

Desventajas del documento únicamente con soporte electrónico

El autor italiano Tarizzo señala que las principales desventajas del documento electrónico son:

- Estar escrito en un lenguaje que sólo es comprensible por dispositivos electrónicos.
- Es descifrable y utilizable sólo con el auxilio de la computadora u otro dispositivo electrónico.
- Es fácilmente alterable.
- Está desprovisto de toda certeza en orden a su autoría y datación.
- Se archiva en formatos soportes concretos que no son siempre compatibles con otras computadoras.

Una categoría particular de documentos en sentido estricto está constituida por aquellos documentos expresamente creados para el uso de las terminales de una sistema (por ejemplo, las tarjetas magnéticas para acceder a un sistema de ventas o a una cuenta bancaria). En Estados Unidos tales documentos están comprendidos en la más amplia categoría de los *access devices*.

Más allá de los documentos electrónicos en sentido estricto, existen además una serie de documentos que pueden ser formados por la computadora mediante sus órganos de salida. En tales casos no están escritos en forma digital, sino en forma de un texto alfanumérico, un diseño o gráfico estampado en soporte papel, en una tarjeta o una cinta perforada, y en general por cualquier objeto material con las características de un documento formado por una máquina conectada a una computadora.

La característica esencial de esta categoría es que son perceptibles, y en el caso de los textos alfanuméricos, legibles directamente por el hombre sin necesidad de la intervención de máquinas traductoras. Podría decirse, en sentido estricto, que son copias del documento electrónico.

Asimismo, el documento electrónico puede ser clasificado, según su modo de formación:

a) *Por intervención humana:* el documento es introducido en la memoria de la computadora directamente por el hombre (por ejemplo, tecleándolo).
b) *Por intervención de una máquina:* cuando se utiliza un lector óptico o escáner que "fotocopie" un documento escrito en papel y lo guarde en una memoria de masa.

Esta distinción tiene su relevancia jurídica en que la memorización de un documento papel preexistente puede verificarse, bien mediante la transcripción del documento en un lenguaje electrónico, bien por la reproduc-

ción en facsímil de la forma y del contenido del documento original. En el primer caso se forma un nuevo documento, aun si su contenido es igual al del documento transcrito; en el segundo caso, el documento no constituye ya la transcripción, sino la reproducción automática de la forma y del contenido del documento original, o bien de un hecho o de un suceso. En este último caso el órgano de inmisión no se limita a registrar sobre un soporte los caracteres alfabéticos o numéricos contenidos en el documento, sino que desarrolla una función más compleja en cuanto procede:

- A reproducir la imagen del documento;
- A dividir la imagen obtenida en una serie de elementos uniformemente distribuidos, denominados PEL (Pictures Elements); y
- A transformar tales puntos en forma digital, es decir, en bits, de modo tal que pueden ser conservados en la memoria del elaborador, y eventualmente ser transmitidos a los terminales conectados.

El resultado es un documento electrónico que constituye no la simple transcripción, sino la reproducción completa y fiel de la forma y del contenido del documento original preexistente.[12]

Naturaleza del documento electrónico

El documento se diferencia del soporte o del contenido en que el soporte informático es un disco magnético, una cinta magnética, un disco óptico o una tarjeta perforada; es, como ya se vio en la composición del documento, el continente, la materialidad.

En cambio, el contenido es aquella información de que da cuenta el soporte, el continente. Cuando los datos ingresan a la máquina, quedan registrados y el documento ya ha sido creado. La computadora no forma, sino que documenta una regulación de intereses ya expresados de otras formas. La computadora no constituye; comprueba.

Para tener una idea clara de la naturaleza del documento electrónico es necesario determinar algunos conceptos técnicos que devienen del uso de la computadora; éstos son: programa o software, datos o información o dato elaborado.

El *programa* hace funcionar a la computadora, es el cerebro de la misma y se le puede definir como "un conjunto ordenado de instrucciones que actúan entre sí para llegar a un resultado final". Estas instrucciones son establecidas previamente por el ser humano en su calidad de programador con el fin de llegar a un resultado por él deseado. Este resultado puede ser

[12] Giannantonio, Ettore, ob. cit., pp. 94/99.

información, o bien una decisión. Aquí es donde debe tenerse muy presente que es el ser humano quien toma la decisión, ya que la máquina no hace sino cumplir órdenes explícitas y claras.

Los *datos* son aquellos elementos que llegan a la computadora por diversos medios y que son la base por medio de la cual trabajan los diversos programas, convirtiéndolos en información útil. Estos datos pueden tener su origen en la misma computadora o en otra, pero siempre debe tenerse en cuenta que lo que está detrás de todo ello es la mano del hombre.

La *información* es el dato elaborado, es el producto final de la interacción hombre-máquina, y dicha información puede llegar a plasmarse en una decisión, pero ésta siempre tendrá por origen el intelecto humano.

Contenido del documento electrónico

Respecto de los documentos electrónicos, puede decirse que poseen los mismos elementos que un documento escrito en soporte papel:

a) constan en un soporte material (cintas, disquetes, circuitos, chips de memorias, redes) sobre el cual se grava el documento electrónico;
b) contienen un mensaje escrito con el lenguaje convencional de los dígitos binarios o "bits", entidades magnéticas que los sentidos humanos no pueden percibir;
c) están escritos en un idioma o código determinado, y
d) pueden ser atribuidos a una persona determinada en calidad de autor mediante una firma digital, clave o llave electrónica.

En conclusión, puede afirmarse que el documento electrónico es "información", producto de una interacción hombre-máquina, cuyo origen es el hombre, y que tiene valor de escrito ya que es un mensaje (texto alfanumérico o gráfico) en lenguaje convencional (bits) sobre un soporte material mueble (cintas o discos magnéticos, discos ópticos o memorias de circuitos).[13]

IMPLICACIONES PROBATORIAS DE LOS DOCUMENTOS ELECTRÓNICOS

En la actualidad los sectores esenciales de actividad tanto en el ámbito público como privado están sujetos —en la práctica de sus asuntos y en ra-

[13] Ruiz, Fernando, "El documento electrónico frente al Derecho Civil y Financiero"; publicado en internet en la Sección Doctrinal del "Derecho.org."

zón de su clientela o naturaleza de sus actividades— a reglas judiciales de prueba (al margen de la jurisprudencia de que se trate), como la redacción y firma de escritos[14]

Por otra parte, el creciente aumento en el volumen y la complejidad de las actividades a realizar ha provocado que manifestaciones como la elaboración de documentos escritos sean modificadas total o parcialmente en función de razones de orden práctico por otro tipo de soportes derivados de la evolución de la tecnología, mejor adaptados a las estrategias de gestión moderna. Así, existen la informática, la microfilmación, los archivos magnéticos, etc. Sin embargo, en la mayoría de las ocasiones dichas prácticas no tienen en cuenta las disposiciones legales y estas últimas, a su vez, no consideran consignas específicas en torno a tales soportes.

Considérense, por ejemplo, los soportes informáticos que figuran actualmente en diversos documentos (como facturas, cheques, letras de cambio, pagarés, etc.), realizados por medios computarizados, los cuales, no obstante ser cada vez más comunes, enfrentan serias dificultades para ser valorados por los jueces, sino ni siquiera los acuerdan los órganos jurisdiccionales respectivos; además, se discuten su originalidad (en dónde radicar dicho elemento), la estabilidad del contenido de compromisos que supone un soporte inalterable y aun la misma identificación del autor por medio de la firma, ya que muchos documentos, al estar impresos con la firma, permiten dudar no tanto de la identidad del signante, sino de la voluntad de compromiso de éste.

Con estas consideraciones no se puede soslayar que el fenómeno de informatización ha provocado un giro en cuanto a los escritos bajo su forma tradicional, lo cual altera el funcionamiento normal de las reglas formales del derecho de la prueba.

La redacción de un escrito firmado es una regla de prudencia para todos los convenios importantes: una prueba literal está aquí "preparada" para toda impugnación eventual. Sin embargo, este tipo de prueba no tiene cabida en la lógica de informatización que tiende a simplificar los compromisos repetitivos que no dan lugar a redactar un escrito (por ejemplo, órdenes de giro transmitidas por computadora), así como a fijar la información acerca de tipos de soportes más o menos alejados de los escritos tradicionales y difícilmente "asimilables" por el derecho clásico de la prueba, como listados, bandas magnéticas, cintas magnéticas, microfichas, etcétera.

La manifestación de actos no existe o éstos no guardan conformidad con los ordenamientos jurídicos. El derecho de prueba se halla frente a un

[14] Instituto Nacional de Estadística y Geografía, INEGI, *Boletín de política informática*, 2002, núm. 6, "El notario ante los retos de la informática", Francisco Xavier Arredondo Galván, Notario núm. 173 de la ciudad de México, http://www.inegi.gob.mx/informatica/español/servicios/boletin/2002/bpi6-02/2notario.thml.

enorme desafío generado por el desarrollo informático, superior a cualquier otro presentado hasta estos momentos por la tecnología moderna.

VALORACIÓN DEL DOCUMENTO ELECTRÓNICO

Dicha valoración es el acto intelectual o fundamental del juzgador que tiene como finalidad conocer el mérito o valor de convicción que puede deducirse del medio probatorio.

Elementos

- Subjetivo: consiste en el acto intelectual que realiza el juzgador.
- Material: reside en determinar qué grado de validez y convicción tiene el medio probatorio.

El documento electrónico y la firma

El documento electrónico en sentido estricto, no tiene firma autógrafa del autor, es un documento que tiene una nueva forma jurídica, que no admite la firma manuscrita.

Siendo la firma el único requisito esencial para la generalidad de los casos, en principio el sistema del código civil permitiría una amplia libertad de registración, que incluiría los medios electrónicos, siempre que los mismos pudieran ser reproducidos.

El mismo principio aplicado al "idioma" que se utilice, conforme la total libertad de elección permitida por el artículo 1020, autoriza el empleo de los "idiomas" informáticos. Pero la amplia libertad que tienen las partes en los instrumentos privados respecto del soporte material, queda limitada por la necesidad de que sea firmado por ellas.

SITUACIÓN INTERNACIONAL

En los países donde el nivel de informatización ha llegado a niveles considerables, el problema del valor probatorio de los soportes informáticos ha adquirido matices importantes; sin embargo, cabe mencionar que en Estados Unidos, Gran Bretaña, Alemania y los países nórdicos (donde predomina el principio de la libertad de prueba, que consiste en otorgar libertad a los juzgadores para determinar los medios de prueba, su eficacia probatoria y la manera de producirlos), el problema no llega a ser tan profundo como en Francia, Bélgica e Italia, países fieles al principio de la exigencia legal de la prueba escrita. A pesar de ello, en Gran Bretaña, Aus-

tralia, República Federal de Alemania, Austria, Suiza, Suecia y Francia se han hecho modificaciones que atribuyen una buena acogida a otro tipo de medios de prueba derivados fundamentalmente de la aparición de nuevas técnicas.

Analícese, por ejemplo, el caso de Francia: en este país hubo una reforma legislativa que data del 12 de julio de 1980, referida a la aceptación y valoración de los medios de prueba. Estas innovaciones jurídicas en Francia, así como las surgidas en Gran Bretaña en su ley de evidencia civil de 1968 —cuyo artículo 5 está consagrado a la informática—, o la ley de enmienda sobre la evidencia sudaustraliana de 1972, que aun da detalles técnicos como la descripción de los *outputs* y que considera a la informática un derecho de prueba eficaz (sección 14), demuestran la preocupación de algunas naciones, siempre conscientes de la necesaria y continua actualización de dichos textos de adaptar los ordenamientos legales —en este caso en materia en prueba— respecto a los cambios provocados por el incontenible avance de la tecnología informática.

Entre otras cosas, nuevas reglas permiten a las compañías de seguros, bancos, sociedades de crédito y aquellas instituciones que requieren archivar numerosos documentos contractuales reemplazarlos por copias que tengan las calidades de "durabilidad" y de "fidelidad al original" (como el uso de microfichas), siempre que no sean susceptibles de modificaciones a nivel de borraduras o enmendaduras.

Asimismo, se resuelven de manera implícita los problemas suscitados por la generalización de la telecopia, en la que los originales quedan en manos de los titulares, mientras que las copias, como son más inalterables, pueden aportarse en niveles contenciosos o también aquellos provocados por la introducción de soportes irreversibles tratables por computadora. A este respecto, en caso de litigio corresponde a aquel que produce una copia satisfacer las exigencias legales del caso.

Otra de las reformas versa en cuanto a la no convalidación de soportes magnéticos como pruebas, esto es, al igual que las copias de calidad insuficiente, los soportes magnéticos no se veían reconocidos en cuanto a su valor probatorio; sin embargo, éstos pueden valer hasta ahora como si se tratara de elementos de una prueba escrita. Ello les atribuye un carácter complementario, aunque esté sujeto a las valoraciones realizadas por el juez, quien, sin un apoyo técnico, no permitiría pensar en una ponderación pertinente.

También se menciona la aceptación de nuevos modos de firma, así como la teletransmisión de documentos por digitalización y criptografía.

A nivel mundial hay coincidencia respecto de la importancia y necesidad de reconocimiento de validez jurídica al soporte electrónico para que la firma electrónica adquiera operatividad. La tendencia general es que dicha firma sea reconocida por la ley.

Estados Unidos

En un principio adoptó un sistema menos reglamentarista, regulándose con base en la jurisprudencia emanada de los tribunales, surgiendo así normas federales como la *Uniform Business Records as Evidence Act, Voluminous Writing Exception* y la *Uniform Rules of Evidence (Archivos de Negocio Uniformes como Acto de la Evidencia, la Escritura Voluminosa Excepción y las Reglas Uniformes de Evidencia)*, que constituían una excepción para la producción en juicio de la prueba con documento electrónico, que fue conocida como la *Business Records Exception.*

El primero en legislar sobre la materia fue el estado norteamericano de UTAH, que el 1 de mayo de 1995 sancionó la "UTAH Digital Signature Act", implementando un nuevo uso en la autopista informática. Ante la ausencia de una ley modelo, la Ley de la Firma Digital de UTAH se ha convertido en la referencia obligada para los demás estados, conformando un esquema regulatorio que brinda efectos legales a la firma digital, un sistema de doble clave que brinda protección, verificación y autenticación a transacciones en línea (on-line), y decide la intervención de una tercera parte, que es la autoridad certificante, encargada de emitir los certificados indispensables para poder utilizar el sistema.

Dicha iniciativa fue luego seguida por la mayoría de los estados de la Unión Americana, que tomaron como modelo tanto esa normativa como la Guía de Firma Digital (Digital Signature Guidelines) publicada en octubre de 1995 por The American Bar Association's Information Security Committee (Comité de Seguridad de la Información de la Asociación Americana de Abogados).

El 1 de octubre de 2000 entró en vigor en Estados Unidos la primera ley nacional sobre firmas digitales. Esta ley concede a la firma digital la misma validez que a la tradicional escrita sobre papel.

Naciones Unidas

Por las dificultades para llegar a un acuerdo internacional respecto a la negociación mediante medios electrónicos, las Naciones Unidas (por conducto de la UNCITRAL) se ha manifestado a favor de una rápida adecuación de las legislaciones de cada país como medida de carácter más pragmático. Por lo anterior, dicho organismo ha emitido un valioso documento, titulado *Legal Value of Computer Records*, en el que expresa que las normas o reglas concernientes a las pruebas relativas a documentos electrónicos (si bien dice *registros de computadora*) no deben suponer un obstáculo para el uso de las tecnologías emergentes tanto a nivel doméstico como internacional, y señala que las normas redactadas por algunos países deben

superar los problemas que genera el lenguaje empleado, pues incorpora referencias culturales que todavía suponen un freno al desarrollo.

Italia

La legislación Italiana en esta materia está conformada por el Reglamento de actos, documentos y contratos en forma electrónica aprobado el 5 de agosto de 1997. El capítulo 1 hace referencia a los principios generales, dando en su primer artículo un conjunto de definiciones de lo que debe entenderse por documento informático, que es la representación informática de actos, hechos o datos jurídicamente relevantes; por firma digital, el resultado del proceso informático basado en un sistema de claves o llaves asimétricas (una pública y otra privada) que permite al firmante mediante la llave privada, y al destinatario por la llave pública, respectivamente, hacer manifiesta y verificar la proveniencia y la integridad de uno o varios documentos informáticos.

Asimismo, define lo que debe entenderse por llave privada, por llave pública, por certificación, mediante el cual se garantiza la correspondencia biunívoca entre la llave pública y el sujeto titular a la que ésta pertenece, se identifica a este último, y se declara el periodo de validez de la citada llave; por certificador, el sujeto público privado, que efectúa la certificación.

El artículo 5 de este Reglamento trata acerca de la eficacia probatoria del documento informático, en el sentido de que el documento informático firmado con firmas digitales tiene la eficacia de documento privado y que el documento informático revestido de los requisitos previstos en el presente Reglamento tiene la eficacia prevista en el artículo 2712 del Código Civil.

El artículo 12 refiere la transmisión del documento por vía telemática; se entiende enviado y recibido al destinatario, si se transmite a la dirección electrónica por éste declarada, teniendo en cuenta que la fecha y hora de formación, de transmisión o de recepción de un documento informático redactado de conformidad con las disposiciones del Reglamento será oponible a terceros, y que la transmisión del documento informático por vía telemática con modalidad que asegura la futura recepción equivale a la notificación por medio de correo en los casos permitidos por la ley. También se hace una especial consideración a los documentos informáticos de las administraciones públicas, así como la firma de esos documentos informáticos.

Francia

Francia es uno de los países pioneros en este campo, pues el 12 de junio de 1980 se sancionó la ley 80/525, reformando el artículo 1348 del Código

Civil, estableciéndose así que el documento electrónico tendría el mismo valor probatorio que el documento en soporte de papel escrito y firmado cuando cumpliera determinados requisitos que son *inalterabilidad* y *durabilidad*. La doctrina jurisprudencial ha marcado ese mismo valor probatorio cuando cumplían con los requisitos expresados en la norma referida.

El Código Civil de la República de Francia fue reformado mediante la Ley número 2000-230 de 13 de marzo de 2000, introduciendo modificaciones al capítulo VI, De la prueba de las obligaciones y del pago, en sus artículos 1315 inciso 1 y artículo 1316 incisos 1 a 4, refiriéndose dicha reforma a la prueba de las nuevas tecnologías de la información y de la firma electrónica.

El nuevo texto expresa lo siguiente:

> ***Artículo 1315.*** El que reclama el cumplimiento de una obligación debe probarla. Recíprocamente, el que se pretende liberado, debe justificar el pago o el hecho que produce la extinción de su obligación.
>
> ***Artículo 1316.*** La prueba literal, o prueba por escrito, resulta de un seguido de letras, caracteres, cifras o todo otro signo o símbolo dotados de significado inteligible, cualquiera sea su soporte y sus modalidades de transmisión.
>
> ***Artículo 1316-1.*** El escrito en forma electrónica está admitido como prueba con igual fuerza que el escrito en soporte papel, bajo reserva de que pueda ser debidamente identificada la persona de la que emana, y que sea generado y conservado en condiciones que permitan garantizar su integridad.
>
> ***Artículo 1316-2.*** En el caso en que la ley no haya establecido otros principios, y en defecto de acuerdo válido entre las partes, el juez resuelve los conflictos de prueba literal determinando por cualquier medio el título más válido, cualquiera sea su soporte.
>
> ***Artículo 1316-3.*** El escrito en soporte electrónico tiene la misma fuerza probatoria que el escrito en soporte papel.

España

La legislación española ha previsto en distintas normas la validez del documento electrónico y de las comunicaciones telemáticas como prueba documental. Asimismo, la jurisprudencia ha reconocido que, a los efectos probatorios, ha de entenderse por documento el escrito, en sentido tradicional, o aquella otra cosa que sin serlo pueda asimilarse al mismo (por ejemplo, un disquete, un documento de ordenador, un video, una película, etc.), con un criterio moderno de interacción de las nuevas realidades tecnológicas, en el sentido en que la palabra documento figura en algunos diccionarios como "cualquier cosa que sirve para ilustrar o comprobar algo", siempre que el llamado "documento" tenga un soporte material,

que es lo que sin duda exige la norma penal. En la actualidad dicha fórmula jurisprudencial tiene adecuada correspondencia en la norma contenida en el artículo 26 del nuevo Código Penal, según el cual "A los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica".

En lo que respecta a la firma electrónica, el Real Decreto-Ley 14/1999, de 17 de septiembre, establece un régimen específico aplicable a las relaciones telemáticas. Este régimen persigue básicamente dotar de *seguridad* a estas relaciones. En 2003 se publicó la ley de firma electrónica, la ley 59/2003, cuyo contenido coincide en términos generales con el Real Decreto-Ley, y por tanto con la Directiva Comunitaria en la que ésta se inspira. El nuevo texto legal introduce algunas modificaciones, reformas, mejoras, e incluso supresiones, de diversas cuestiones reguladas en el Real Decreto-Ley 14/1999.

SITUACIÓN NACIONAL

Ley del Mercado de Valores

Por reformas del *Diario Oficial de la Federación* del 4 de enero de 1990 a la ley del Mercado de Valores del DOF de 2 de enero de 1975 se introdujo un capítulo VIII, referente a la contratación bursátil, llamado *contrato de intermediación bursátil*, por virtud del cual la casa de bolsa, en el desempeño de su encargo, actuará conforme a las instrucciones del cliente que reciba el apoderado para celebrar operaciones con el público designado por la propia casa de bolsa, o el que en su ausencia temporal la misma casa de bolsa designe.

Esto se incluyó en la fracción II del artículo 91, que señalaba que a menos que en el contrato se pacte el manejo discrecional de la cuenta, las instrucciones del cliente para la ejecución de operaciones concretas o movimiento en la cuenta del mismo podrá hacerse de manera escrita, verbal o telefónica, debiéndose precisar en todo caso el tipo de operación o movimiento, así como el género, especie, clase, emisor, cantidad, precio y cualquier otra característica necesaria para identificar los valores materia de cada operación o movimiento de la cuenta.

De igual forma, las partes podrán convenir libremente el uso de carta, telégrafo, télex, telefax o cualquier *otro medio electrónico, de cómputo o de telecomunicaciones* para el envío, intercambio o en su caso confirmación de las órdenes de la clientela inversionista y demás avisos que deban darse conforme a lo estipulado en el contrato, así como los casos en que cualquiera de ellas requiera otra confirmación por esas vías.

Lo más importante para el problema que nos ocupa está plasmado en la fracción V del mismo artículo, en el que establecimos y se consiguió lo siguiente:

> En el caso en que las partes convengan el uso de medios electrónicos, de cómputo o de telecomunicaciones para el envío, intercambio y en su caso confirmación de las órdenes y demás avisos que deban darse, habrá de precisar las claves de identificación recíproca y las responsabilidades que conlleve su utilización.

Las claves de identificación que se convenga utilizar conforme a este artículo sustituirán a la firma autógrafa, por lo que las constancias documentales o técnicas en donde aparezcan *producirán los mismos efectos que las leyes otorguen a los documentos escritos por las partes y, en consecuencia, tendrán el mismo valor probatorio.* Estos preceptos se mantienen en la nueva LMV vigente de DOF 30/XII/2005 en el artículo 200 fcs. II y V.

En los años noventa se nos invitó a participar en una nueva reforma de esta ley DOF 23 julio 1993 por virtud de la cual se introdujo el capítulo X, referido a la automatización, que establece, entre otros, que las casas de bolsa, especialistas bursátiles y bolsas de valores, instituciones para el depósito de valores, instituciones calificadoras de valores y contrapartes centrales, deberán llevar su contabilidad y el registro de sus operaciones en que intervengan mediante sistemas automatizados (artículo 112).

Dichos sistemas deberán reunir, de acuerdo con el artículo 113, una serie de características, entre las que destacan:

a) La compatibilidad técnica con los equipos y programas de la Comisión Nacional Bancaria y de Valores (CNByV).
b) Los asientos contables y registros de operaciones que emanen de dichos sistemas, expresados en lenguaje natural o informático, se emitirán de conformidad con las disposiciones legales en materia probatoria, a fin de garantizar la autenticidad e inalterabilidad de la información respecto a la seguridad del sistema empleado.
c) El uso de claves de identificación en los términos y con los efectos señalados en el artículo 91, fracción V, de dicha ley.

Por último, el artículo 116 establece que la información contenida en soportes materiales, o bien provenientes de procesos telemáticos, siempre que esté validada por la autoridad receptora y la entidad emisora, de acuerdo con las características y dentro de los plazos que determine la autoridad, así como la información que cumpliendo con dichos requerimientos se integre a las bases de datos, *producirán los mismos efectos que las leyes otorgan a los documentos originales y, en consecuencia, tendrá igual valor probatorio.*

Estos preceptos se retomaron en la ley actual en los arts. 202, 203, 208, 210, 245 *in fine*, dando pauta a otras actualizaciones al respecto.

Como podemos ver, desde hace casi veinte años (y mucho nos honramos en haber sido artífices de ello), los documentos electrónicos ya son aceptados como medio de prueba y con un valor pleno (al menos en materia bursátil), por lo que nos extrañan los triunfalismos sin fundamento de personas e instituciones que apenas de manera más reciente han comenzado a abordar este tema en específico.

Reformas legislativas en materia de comercio electrónico

Como se vio en capítulos anteriores, en virtud del decreto publicado en el *Diario Oficial de la Federación* (*DOF*) el 29 de mayo de 2000,[15] se hicieron reformas a diversos ordenamientos, con el propósito de regular el comercio electrónico en México.

Al efecto, cabe destacar que en las modificaciones al Código Federal de Procedimientos Civiles (CFPC), el artículo 289 del *Código Federal de Procedimientos Civiles* señalaba de manera expresa los medios de prueba, pero en la actualidad la redacción de este artículo ha cambiado, al incluir la expresión de que "son admisibles como medios de prueba aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos".

Entre las modificaciones al *Código Federal de Procedimientos Civiles*, su artículo 210-A reconoce como prueba "la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología". El numeral continúa: "Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la confiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta."

Por su parte, el *Código de Comercio*, en su artículo 1205, establece: "Son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos y, en consecuencia, serán tomadas como pruebas las declaraciones de las partes, terceros, peritos, documentos públicos o privados, inspección judicial, fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, mensajes de datos, reconstrucciones de hechos

[15] Véase anexo IV.

y en general cualquier otra similar u objeto que sirva para averiguar la verdad."

Por último, el artículo 1298-A, dispone: "Se reconocen como prueba los *mensajes de datos*. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la confiabilidad del método en que haya sido generada, archivada, comunicada o conservada."

Es importante señalar que con el decreto (publicado en el *DOF* el 29 de agosto de 2003) se complementa la regulación al respecto ya que se establecen los lineamientos que deberán seguirse para la utilización de la firma electrónica, los mensajes de datos, los certificados electrónicos y los requisitos y obligaciones de los prestadores de servicio de certificación (PSC), adoptando básicamente los principios de la Ley modelo sobre firma electrónica, de la CNUDMI.

Anexo I

Compromiso de Túnez (Adoptado en la Cumbre Mundial sobre la Sociedad de la Información, celebrada en Túnez, noviembre de 2005)

1. Nosotros, representantes de los pueblos del mundo, reunidos en Túnez del 16 al 18 de noviembre de 2005 con motivo de la segunda fase de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), reiteramos nuestro apoyo categórico a la *Declaración de Principios de Ginebra* y al *Plan de Acción* adoptados en la primera fase de la Cumbre Mundial sobre la Sociedad de la Información celebrada en Ginebra en diciembre de 2003.
2. Reafirmamos nuestra voluntad y nuestro compromiso de construir una Sociedad de la Información centrada en la persona, abierta a todos y orientada al desarrollo, con arreglo a los objetivos y principios de la *Carta de las Naciones Unidas*, el derecho internacional y el multilateralismo, y respetando plenamente y apoyando la *Declaración Universal de los Derechos Humanos*, a fin de que todos los pueblos del mundo puedan crear, consultar, utilizar y compartir la información y el conocimiento para alcanzar su pleno potencial y lograr las metas y los objetivos de desarrollo acordados internacionalmente, incluidos los Objetivos de Desarrollo del Milenio.
3. Reafirmamos la universalidad, indivisibilidad, interdependencia e interrelación de todos los derechos humanos y las libertades fundamentales, incluido el derecho al desarrollo, enunciados en la *Declaración de Viena*. También reafirmamos que la democracia, el desarrollo sustentable y el respeto por los derechos humanos y las libertades fundamentales, así como el buen gobierno en todos los niveles son interdependientes y se refuerzan entre sí. Resolvemos además fortalecer el respeto al estado de derecho en los asuntos internacionales y nacionales.
4. Reafirmamos los *párrafos 4, 5* y *55* de la *Declaración de Principios de Ginebra*. Reconocemos que la libertad de expresión y la libre circulación de la información, las ideas y los conocimientos son esenciales para la Sociedad de la Información y benéficos para el desarrollo.

5. La Cumbre de Túnez constituye para nosotros una oportunidad excepcional de crear mayor conciencia acerca de las ventajas que las tecnologías de la información y la comunicación (TIC) pueden aportar a la humanidad y de la manera como pueden transformar las actividades y la vida de las personas, además de su interacción, despertando así mayor confianza en el futuro.
6. Esta cumbre constituye una etapa importante en los esfuerzos desplegados en todo el mundo para erradicar la pobreza y alcanzar las metas y objetivos de desarrollo acordados internacionalmente, incluidos los Objetivos de Desarrollo del Milenio. Mediante las decisiones adoptadas en Ginebra, hemos establecido un vínculo coherente a largo plazo entre el proceso de la CMSI y otras importantes conferencias y cumbres relevantes de las Naciones Unidas. Invitamos a los gobiernos, al sector privado, a la sociedad civil y a las organizaciones internacionales a aunarse para implementar los compromisos enunciados en la *Declaración de Principios* y *Plan de Acción de Ginebra*. En este contexto, adquieren especial relevancia los resultados de la *Cumbre Mundial de 2005* celebrada recientemente sobre el examen de la puesta en marcha de la *Declaración del Milenio*..
7. Reafirmamos los compromisos contraídos en Ginebra, que reforzamos en Túnez al hacer hincapié en los mecanismos financieros destinados a colmar la brecha digital, en el gobierno de internet y cuestiones afines, así como en el seguimiento y la implementación de las decisiones de Ginebra y Túnez, indicadas en la *Agenda de Túnez para la Sociedad de la Información*.
8. Aunque reafirmamos las importantes funciones y responsabilidades de todas las partes interesadas, según se indica en el *párrafo 3* del *Plan de Acción de Ginebra*, reconocemos el papel y la responsabilidad fundamental de los gobiernos en el proceso de la CMSI.
9. Reafirmamos la decisión de proseguir nuestra búsqueda para garantizar que todos se beneficien de las oportunidades que puedan brindar las TIC, recordando que los gobiernos, el sector privado, la sociedad civil, las Naciones Unidas y otras organizaciones internacionales deben colaborar para acrecentar el acceso a la infraestructura y las tecnologías de la información y la comunicación, así como a la información y al conocimiento, crear capacidades, incrementar la confianza y la seguridad en cuanto a la utilización de las TIC, crear un entorno habilitador en todos los niveles, desarrollar y ampliar las aplicaciones TIC, promover y respetar la diversidad cultural, reconocer el cometido de los medios de comunicación, abordar las dimensiones éticas de la Sociedad de la Información y alentar la cooperación internacional y regional. Confirmamos que éstos son los principios clave de la construcción de una Sociedad de la Información integradora, cuya elaboración ha sido enunciada en la *Declaración de Principios de Ginebra*.
10. Reconocemos que el acceso a la información y el intercambio y la creación de conocimientos contribuyen de manera significativa a fortalecer el desarrollo económico, social y cultural, lo que ayuda a todos los países a alcanzar las metas y los objetivos de desarrollo acordados internacionalmente, en especial los de la *Declaración del Milenio*. Este proceso se podrá mejorar si se eliminan las barreras que impiden el acceso universal, ubicuo, equitativo y asequible a la información. Subrayamos la importancia de eliminar estas barreras

con el fin de colmar la brecha digital, especialmente las que impiden alcanzar el pleno desarrollo económico, social y cultural de los países y el bienestar de su gente, sobre todo en los países en desarrollo.

11. Por otra parte, las TIC hacen posible que una población sumamente más numerosa que en cualquier otro momento del pasado participe en la ampliación y el intercambio de las bases del conocimiento humano, y contribuyen a su crecimiento en todos los ámbitos de la actividad humana, así como a su aplicación a la educación, la salud y la ciencia. Las TIC tienen enormes posibilidades de acrecentar el acceso a una educación de calidad, favorecer la alfabetización y la educación primaria universal, además de facilitar el proceso de aprendizaje, que sentará de esa forma las bases para la creación de una Sociedad de la Información totalmente integradora y orientada al desarrollo y de una economía del conocimiento que respete la diversidad cultural y lingüística.
12. Insistimos en que la adopción de las TIC por las empresas desempeña un papel fundamental en el crecimiento económico. El mayor crecimiento y productividad que generan inversiones bien realizadas en las TIC puede conducir a un aumento del comercio y a empleos más numerosos y mejores. Por este motivo, las políticas de desarrollo empresarial y las relativas al mercado del trabajo desempeñan un papel fundamental en la adopción de las TIC. Invitamos a los gobiernos y al sector privado a mejorar la capacidad de las pequeñas, medianas y microempresas (PMYME), ya que ofrecen el mayor número de puestos de trabajo en la mayoría de las economías. En colaboración con las partes interesadas, crearemos un marco político, jurídico y reglamentario que propicie la actividad empresarial, en particular para las pequeñas, medianas y microempresas.
13. Reconocemos también que la revolución de las TIC puede tener enormes consecuencias positivas como instrumento del desarrollo sustentable. Además, un entorno habilitador apropiado, que exista a escala nacional e internacional, podría impedir el aumento de las divisiones sociales y económicas y de las disparidades entre los países, las regiones y los individuos ricos, y los países, regiones e individuos pobres, incluidas las existentes entre hombres y mujeres.
14. Reconocemos asimismo que, además de crear la infraestructura TIC, se ha de insistir de manera adecuada en desarrollar las capacidades humanas y crear aplicaciones TIC y contenidos digitales en idioma local, cuando proceda, a fin de garantizar un planteamiento amplio de la fundación de una Sociedad de la Información mundial.
15. Reconocemos los principios de acceso universal y sin discriminación a las TIC para todas las naciones, la necesidad de tener en cuenta el nivel de desarrollo social y económico de cada país, y respetamos la orientación hacia el desarrollo de la Sociedad de la Información, para subrayar que las TIC son un instrumento eficaz destinado a promover la paz, la seguridad y la estabilidad, así como para propiciar la democracia, la cohesión social, el buen gobierno y el estado de derecho en los planos regional, nacional e internacional. Se pueden utilizar las TIC para promover el crecimiento económico y el desarrollo de las empresas. El desarrollo de infraestructuras, la creación de capacidades

humanas, la seguridad de la información y la seguridad de la red son decisivos para alcanzar esos objetivos. Además, reconocemos la necesidad de afrontar eficazmente las dificultades y amenazas que representa la utilización de las TIC para fines que no corresponden a los objetivos de mantener la estabilidad y seguridad internacionales y podrían afectar negativamente la integridad de la infraestructura dentro de los Estados, en detrimento de su seguridad. Es necesario evitar que se abuse de las tecnologías y de los recursos de la información para fines delictivos y terroristas, respetando siempre los derechos humanos.

16. Asimismo, nos comprometemos a evaluar y a seguir de cerca los progresos hacia el cierre de la brecha digital, teniendo en cuenta los diferentes niveles de desarrollo, con miras a lograr las metas y objetivos de desarrollo internacionalmente acordados, incluidos los Objetivos de Desarrollo del Milenio, y a evaluar la eficacia de la inversión y los esfuerzos de cooperación internacional encaminados a constituir la Sociedad de la Información.
17. Instamos a los gobiernos a que utilicen el potencial de las TIC para generar sistemas públicos de información acerca de leyes y reglamentos, en los que se considere un desarrollo mayor de los puntos de acceso públicos y se apoye una amplia disponibilidad de esta información.
18. Por tanto, nos esforzaremos en promover sin tregua el acceso universal, ubicuo, equitativo y asequible a las TIC, incluidos el diseño universal y las tecnologías auxiliares para todos, con atención especial a los discapacitados, en todas partes, con objeto de garantizar una distribución más uniforme de sus beneficios entre las sociedades y dentro de cada una de ellas, y de reducir la brecha digital a fin de crear oportunidades digitales para todos y beneficiarse del potencial que brindan las TIC para el desarrollo.
19. La comunidad internacional debe tomar las medidas necesarias para garantizar que todos los países del mundo dispongan de un acceso equitativo y asequible a las TIC, a fin de que sus beneficios en los campos del desarrollo socioeconómico y del cierre de la brecha digital sean verdaderamente integradores.
20. Para ello, daremos especial atención a las necesidades particulares de los grupos marginados y vulnerables de la sociedad, entre ellos los emigrantes e inmigrantes, los desplazados internos, los refugiados, los desempleados, las personas desfavorecidas, las minorías, los pueblos nómadas, las personas mayores y los discapacitados.
21. Con esa finalidad, **tendremos especial atención** en las necesidades particulares de los habitantes de los países en desarrollo, de las naciones con economías en transición, de los países menos desarrollados, de los pequeños Estados insulares en desarrollo, de las naciones en desarrollo sin litoral, de los países pobres muy endeudados, de las naciones y territorios ocupados, y de los países que aún se recuperan de conflictos o de catástrofes naturales.
22. En la evolución de la Sociedad de la Información se debe dar una atención especial a la situación particular de los pueblos indígenas, así como a la preservación de su patrimonio y de su legado cultural.
23. Reconocemos la existencia en la sociedad de una brecha entre los géneros que forma parte del ámbito digital, y reafirmamos nuestro compromiso con

la promoción de la mujer y con una perspectiva de igualdad de género, a fin de que podamos superar esta brecha. Además, reconocemos que la plena participación de las mujeres en la Sociedad de la Información es necesaria para garantizar la integración y el respeto de los derechos humanos dentro de ella. Animamos a todas las partes interesadas a respaldar la participación de la mujer en los procesos de adopción de decisiones y a contribuir a la conformación de todos los ámbitos de la Sociedad de la Información en los niveles internacional, regional y nacional.

24. Reconocemos el papel que desempeñan las TIC en la protección y en la mejora del progreso de los niños. Reforzaremos las medidas de protección de los niños contra cualquier tipo de abuso y las de defensa de sus derechos en el contexto de las TIC. En ese contexto, insistimos en que el interés de los niños es el factor primordial.
25. Reafirmamos nuestro compromiso con la capacitación de los jóvenes como contribuyentes clave para constituir una sociedad de información integradora. Fomentaremos activamente la contratación de jóvenes para programas de desarrollo innovadores basados en las TIC y ampliaremos las oportunidades de participación de la juventud en procesos de ciberestrategia.
26. Reconocemos la importancia de las aplicaciones y contenidos creativos para colmar la brecha digital y para contribuir a alcanzar las metas y los objetivos de desarrollo acordados internacionalmente, incluidos los Objetivos de Desarrollo del Milenio.
27. Reconocemos que el acceso equitativo y sustentable a la información requiere poner en práctica estrategias para conservar a largo plazo la información digital que se crea.
28. Reafirmamos nuestro deseo de construir redes TIC y desarrollar aplicaciones, en asociación con el sector privado, basadas en normas abiertas o compatibles que sean asequibles y accesibles para todos, disponibles en cualquier lugar, en cualquier momento, para cualquier persona y sobre cualquier dispositivo, conducentes a una red ubicua.
29. Nuestra convicción es que los gobiernos, el sector privado, la sociedad civil, las comunidades científica y académica, así como los usuarios puedan utilizar diversas tecnologías y modelos de concesión de licencias, incluidos los sistemas protegidos y los de código abierto y libre, de acuerdo con sus intereses y con la necesidad de disponer de servicios fiables y aplicar programas eficaces para los ciudadanos. Considerando la importancia del software protegido en los mercados de los países, reiteramos la necesidad de fomentar y promover el desarrollo colaborativo, las plataformas interoperativas y el software de código abierto y libre de tal manera que refleje las posibilidades de los diversos modelos de software principalmente para programas educativos, científicos y de inclusión digital.
30. Reconociendo que la mitigación de los desastres puede contribuir significativamente a estimular el desarrollo sustentable y la reducción de la pobreza, reafirmamos nuestro compromiso para aprovechar las capacidades y el potencial de las TIC mediante la promoción y el fortalecimiento de la cooperación en los niveles nacional, regional e internacional.

31. Nos comprometemos a trabajar juntos con miras a poner en marcha la Agenda de Solidaridad Digital, según se estipula en el *párrafo 27* del *Plan de Acción de Ginebra*. La plena y rápida implementación de dicha Agenda, observando el buen gobierno en todos los niveles, requiere en particular una solución oportuna, eficaz, amplia y duradera a los problemas relacionados con las deudas de los países en desarrollo cuando así convenga, así como un sistema de comercio multilateral universal, reglado, abierto, no discriminatorio y equitativo, que también pueda estimular el desarrollo en todo el mundo, de tal forma que beneficie a los países en todas las etapas de desarrollo, además de buscar y aplicar eficazmente soluciones y mecanismos concretos de carácter internacional, con el fin de aumentar la cooperación internacional y la ayuda para colmar la brecha digital.
32. Nos comprometemos además a promover la inclusión de todos los pueblos en la Sociedad de la Información mediante el desarrollo y la utilización de los idiomas indígenas y locales en las TIC. Seguiremos esforzándonos en proteger y promover la diversidad cultural, así como las identidades culturales, dentro de la Sociedad de la Información.
33. Reconocemos que, aunque la cooperación técnica puede ser de utilidad, la creación de capacidades a todos los niveles es necesaria para velar por la disponibilidad de la experiencia de los conocimientos institucionales e individuales requeridos.
34. Reconocemos la necesidad de contar con recursos tanto humanos como financieros y nos esforzaremos por movilizarlos, de acuerdo con el *Capítulo Dos de la Agenda de Túnez para la Sociedad de la Información*, con el fin de incrementar la utilización de las TIC para el desarrollo y llevar a cabo los planes a corto, medio y largo plazos destinados a crear la Sociedad de la Información, en seguimiento e implementación de los resultados de la CMSI.
35. Reconocemos el papel protagonista de la política pública en el establecimiento del marco en el cual se pueden movilizar los recursos.
36. Valoramos las posibilidades que ofrecen las TIC para fomentar la paz y prevenir conflictos que, entre otras cosas, afectan negativamente el logro de los objetivos de desarrollo. Las TIC pueden usarse para identificar situaciones de conflicto mediante sistemas de alerta temprana con objeto de prevenirlos, fomentar su resolución pacífica, prestar apoyo a las actividades humanitarias (entre ellas la protección de los civiles en los conflictos armados), facilitar las tareas de mantenimiento de la paz y colaborar en la consolidación de la paz después de los conflictos y la reconstrucción.
37. Estamos persuadidos de que nuestros objetivos pueden lograrse mediante la participación, la cooperación y la asociación de los gobiernos y otras partes interesadas (es decir, el sector privado, la sociedad civil y las organizaciones internacionales), y de que la cooperación y la solidaridad internacional en todos los niveles son indispensables para que los frutos de la Sociedad de la Información beneficien a todos.
38. No debemos poner fin a nuestros esfuerzos una vez concluida la cumbre. El origen de la sociedad mundial de la información a la que todos contribuimos ofrece oportunidades cada vez mayores para todas las personas y para una

comunidad mundial integradora, inimaginables apenas unos años atrás. Debemos aprovecharlas hoy y apoyar su desarrollo y progreso futuros.

39. Reafirmamos nuestra decidida resolución de desarrollar y aplicar una respuesta eficaz y sustentable a los retos y oportunidades para construir una Sociedad de la Información verdaderamente mundial en beneficio de todos nuestros pueblos.
40. Estamos convencidos de que se aplicarán completa y oportunamente las decisiones adoptadas en Ginebra y en Túnez como se indica en la *Agenda de Túnez para la Sociedad de la Información*.

Anexo II

Reformas al artículo sexto de la Constitución Política de los Estados Unidos Mexicanos (DOF *del 20 de julio y 13 de noviembre de 2007), a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (extracto del* DOF *del 11 de junio de 2002) y a los Lineamientos de Protección de Datos Personales expedidos por el IFAI*

(DOF *del 30 de septiembre de 2005)*

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS

Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.

Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que

fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.

II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión.

V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.

VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.

VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.

Transitorios

Primero. El presente Decreto entrará en vigor al día siguiente al de su publicación en el *Diario Oficial de la Federación*.

Segundo. La Federación, los Estados y el Distrito Fedral, en sus respectivos ámbitos de competencia, deberán expedir las leyes en materia de acceso a la información pública y transparencia, o en su caso, realizar las modificaciones necesarias, a más tardar un año después de la entrada en vigor de este Derecho.

Tercero. La Federación, los Estados y el Distrito Federal deberán contar con sistemas electrónicos para que cualquier persona pueda hacer uso remoto de los mecanismos de acceso a la información y de los procedimientos de revisión a los que se refiere este Decreto, a más tardar en dos años a partir de la entrada en vigor del mismo. Las leyes locales establecerán lo necesario para que los municipios con población superior a setenta mil habitantes y las demarcaciones territoriales del Distrito Federal cuenten en el mismo plazo con los sistemas electrónicos respectivos.

México, D.F., a 13 de junio de 2007. Sen. **Manlio Fabio Beltrones Rivera**. Presidente. Sen. **Javier Orozco Gómez**, Secretario. Rúbricas."

En cumplimiento de lo dispuesto por la fracción I del Artículo 89 de la Constitución Política de los Estados Unidos Mexicanos, y para su debida publicación y observancia, expido el presente Decreto en la Residencia del Poder Ejecutivo Federal, en la Ciudad de México, Distrito Federal, a los dieciocho días del mes de

julio de dos mil siete- **Felipe de Jesús Calderón Hinojosa.** Rúbrica. El Secretario de Gobernación, **Francisco Javier Ramírez Acuña.** Rúbrica.

LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL

Título primero

Disposiciones comunes para los sujetos obligados

Capítulo IV

Protección de datos personales

Artículo 20. Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:

I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con los lineamientos que al respecto establezca el Instituto o las instancias equivalentes previstas en el artículo 61;
II. Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el artículo 61;
IV. Procurar que los datos personales sean exactos y actualizados;
V. Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación, y
VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

Artículo 21. Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.

Artículo 22. No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:

I. Los necesarios para la prevención o el diagnóstico médico, la prestación de asistencia médica o la gestión de servicios de salud y no pueda recabarse su autorización;
II. Los necesarios por razones estadísticas, científicas o de interés general previstas en la ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;
III. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;
IV. Cuando exista una orden judicial;
V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquellos para los cuales se les hubieren transmitido, y
VI. En los demás casos que establezcan las leyes.

Artículo 23. Los sujetos obligados que posean, por cualquier título, sistemas de datos personales, deberán hacerlo del conocimiento del Instituto o de las instancias equivalentes previstas en el artículo 61, quienes mantendrán un listado actualizado de los sistemas de datos personales.

Artículo 24. Sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales. Aquélla deberá entregarle, en un plazo de diez días hábiles contados desde la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente, o bien, le comunicará por escrito que ese sistema de datos personales no contiene los referidos al solicitante.

La entrega de los datos personales será gratuita, debiendo cubrir el individuo únicamente los gastos de envío de conformidad con las tarifas aplicables. No obstante, si la misma persona realiza una nueva solicitud respecto del mismo sistema de datos personales en un periodo menor a doce meses a partir de la última solicitud, los costos se determinarán de acuerdo con lo establecido en el artículo 27.

Artículo 25. Las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifiquen sus datos que obren en cualquier sistema de datos personales. Con tal propósito, el interesado deberá entregar una solicitud de modificaciones a la unidad de enlace o su equivalente, que señale el sistema de datos personales, indique las modificaciones por realizarse y aporte la documentación que motive su petición. Aquélla deberá entregar al solicitante, en un plazo de 30 días hábiles desde la presentación de la solicitud, una comunicación que haga constar las modificaciones o bien, le informe de manera fundada y motivada las razones por las cuales no procedieron las modificaciones.

Artículo 26. Contra la negativa de entregar o corregir datos personales, procederá la interposición del recurso a que se refiere el artículo 50. También procederá en el caso de falta de respuesta en los plazos a que se refieren los artículos 24 y 25.

LINEAMIENTOS DE PROTECCIÓN DE DATOS PERSONALES (IFAI)

Capítulo I

Disposiciones generales

Objeto y ámbito de aplicación

Primero. Los presentes Lineamientos tienen por objeto establecer las políticas generales y procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales, con el propósito de asegurar su adecuado tratamiento e impedir su transmisión ilícita y lesiva para la dignidad y derechos del afectado.

Para tal efecto, este ordenamiento establece las condiciones y requisitos mínimos para el debido manejo y custodia de los sistemas de datos que se encuentren en posesión de la Administración Pública Federal en el ejercicio de sus atribuciones.

Elementos de los datos personales

Segundo. A efecto de determinar si la información que posee una dependencia o entidad constituye un dato personal, deberán agotarse las siguientes condiciones:

1. Que la misma sea concerniente a una persona física, identificada o identificable, y
2. Que la información se encuentre contenida en sus archivos.

Definiciones

Tercero. Para efectos de la aplicación de los presentes Lineamientos, además de las definiciones establecidas en los artículos: 3o. de la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*, 2o. de su Reglamento, y las referidas en los Lineamientos expedidos por el Instituto, publicados en el *Diario Oficial de la Federación* el 25 de agosto de 2003 y 6 de abril de 2004, se entenderá por:

I. **Destinatario.** Cualquier persona física o moral pública o privada que recibe datos personales.
II. **Encargado.** El servidor público o cualquier otra persona física o moral facultado por un instrumento jurídico o expresamente autorizado por el Responsable para llevar a cabo el tratamiento físico o automatizado de los datos personales.
III. **Sistema "Persona".** Aplicación informática desarrollada por el Instituto para mantener actualizado el listado de los sistemas de datos personales que posean las dependencias y entidades para registrar e informar sobre las transmisiones, modificaciones y cancelaciones de los mismos.

IV. **Responsable.** El servidor público titular de la unidad administrativa designado por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales.

V. **Titular de los datos.** Persona física a quien se refieren los datos personales que sean objeto de tratamiento.

VI. **Transmisión.** Toda entrega total o parcial de sistemas de datos personales realizada por las dependencias y entidades a cualquier persona distinta al titular de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras, interconexión de bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.

VII. **Transmisor.** Dependencia o entidad que posee los datos personales objeto de la transmisión.

VIII. **Tratamiento.** Operaciones y procedimientos físicos o automatizados que permitan recabar, registrar, reproducir, conservar, organizar, modificar, transmitir y cancelar datos personales.

IX. **Usuario.** Servidor público facultado por un instrumento jurídico o expresamente autorizado por el Responsable que utiliza de manera cotidiana datos personales para el ejercicio de sus atribuciones, por lo que accede a los sistemas de datos personales, sin posibilidad de agregar o modificar su contenido.

Sistema de datos personales

Cuarto. Un sistema de datos personales constituye el conjunto ordenado de datos personales que estén en posesión de una dependencia o entidad, con independencia de su forma de acceso, creación, almacenamiento u organización.

Los sistemas de datos personales podrán distinguirse entre físicos y automatizados, definiéndose cada uno de ellos de la siguiente forma:

a) *Físicos*: Conjunto ordenado de datos que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos.

b) *Automatizados*: Conjunto ordenado de datos que para su tratamiento han sido o están sujetos a un tratamiento informático y que por ende requieren de una herramienta tecnológica específica para su acceso, recuperación o tratamiento.

Capítulo II

Principios rectores de la protección de los datos personales

Principios de la protección de datos personales

Quinto. En el tratamiento de datos personales, las dependencias y entidades deberán observar los principios de licitud, calidad, acceso y corrección, de información, seguridad, custodia y consentimiento para su transmisión.

Licitud

Sexto. La posesión de sistemas de datos personales deberá obedecer exclusivamente a las atribuciones legales o reglamentarias de cada dependencia o entidad y deberán obtenerse a través de los medios previstos en dichas disposiciones.

Los datos personales deberán tratarse únicamente para la finalidad para la cual fueron obtenidos. Dicha finalidad debe ser determinada y legítima.

Calidad de los datos

Séptimo. El tratamiento de datos personales deberá ser exacto, adecuado, pertinente y no excesivo, respecto de las atribuciones legales de la dependencia o entidad que los posea.

Acceso y corrección

Octavo. Los sistemas de datos personales deberán almacenarse de forma tal que permitan el ejercicio de los derechos de acceso y corrección previstos por la Ley, el Reglamento y los Lineamientos emitidos por el Instituto.

De información

Noveno. Se deberá hacer del conocimiento del Titular de los datos, al momento de recabarlos y de forma escrita, el fundamento y motivo de ello, así como los propósitos para los cuales se tratarán dichos datos.

Seguridad

Décimo. Se deberán adoptar las medidas necesarias para garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado.

Custodia y cuidado de la información

Undécimo. Los datos personales serán debidamente custodiados y los Responsables, Encargados y Usuarios deberán garantizar el manejo cuidadoso en su tratamiento.

Consentimiento para la transmisión

Duodécimo. Toda transmisión de datos personales deberá contar con el consentimiento del Titular de los datos, mismo que deberá otorgarse en forma libre, expresa e informada, salvo lo dispuesto en el Lineamiento vigesimosegundo.

Capítulo III

Del tratamiento

Tratamiento exacto, adecuado, pertinente y no excesivo

Decimotercero. A efecto de cumplir con el principio de calidad a que se refiere el Lineamiento Séptimo, se considera que el tratamiento de datos personales es:

a) *Exacto*: Cuando los datos personales se mantienen actualizados de manera tal que no alteren la veracidad de la información que traiga como consecuencia que el Titular de los datos se vea afectado por dicha situación;
b) *Adecuado*: Cuando se observan las medidas de seguridad aplicables;
c) *Pertinente*: Cuando es realizado por el personal autorizado para el cumplimiento de las atribuciones de las dependencias y entidades que los hayan recabado, y
d) *No excesivo*: Si la información solicitada al Titular de los datos es estrictamente la necesaria para cumplir con los fines para los cuales se hubieran recabado.

Corrección de oficio

Decimocuarto. En caso de que los Responsables, Encargados o Usuarios detecten que hay datos personales inexactos deberán, de oficio, actualizarlos en el momento en que tengan conocimiento de la inexactitud de los mismos, siempre que posean los documentos que justifiquen la actualización.

Conservación de los datos

Decimoquinto. Los datos personales que hayan sido objeto de tratamiento y no contengan valores históricos, científicos, estadísticos o contables deberán ser dados de baja por las dependencias y entidades, o bien, los que contengan dichos valores serán objeto de transferencias secundarias, de conformidad con lo establecido por los catálogos de disposición documental a que se refieren los Lineamientos Generales para la organización y conservación de archivos de las Dependencias y Entidades de la Administración Pública Federal, teniendo en cuenta los siguientes plazos:

a) El que se haya establecido en el formato físico o electrónico por el cual se recabaron;
b) El establecido por las disposiciones aplicables;
c) El establecido en los convenios formalizados entre una persona y la dependencia o entidad, y
d) El señalado en los casos de transmisión.

Condiciones técnicas

Decimosexto. Los datos personales sólo podrán ser tratados en sistemas de datos personales que reúnan las condiciones de seguridad establecidas en los presentes Lineamientos y las demás disposiciones aplicables.

Información al titular de los datos

Decimoséptimo. En el momento en que se recaben datos personales, la dependencia o entidad deberá hacer del conocimiento al Titular de los datos tanto en los formatos físicos como en los electrónicos utilizados para ese fin, lo siguiente:

a) La mención de que los datos recabados serán protegidos en términos de lo dispuesto por la Ley;
b) El fundamento legal para ello, y
c) La finalidad del Sistema de datos personales.

Modelo de leyenda para informar al titular de los datos

Decimoctavo. Sin perjuicio de que las dependencias y entidades elaboren sus propios formatos para informar al Titular de los datos lo establecido por el Lineamiento anterior, podrán utilizar el siguiente modelo:

Los datos personales recabados serán protegidos y serán incorporados y tratados en el Sistema de datos personales (indicar nombre[1]), con fundamento en (indicar[2]) y cuya finalidad es (describirla[3]), el cual fue registrado en el Listado de sistemas de datos personales ante el Instituto Federal de Acceso a la Información Pública (www.ifai.org.mx), y podrán ser transmitidos a (indicar[4]), con la finalidad de (indicar[5]), además de otras transmisiones previstas en la Ley. La Unidad Administrativa responsable del Sistema de datos personales es (indicarlo[6]), y la dirección donde el interesado podrá ejercer los derechos de acceso y corrección ante la misma es (indicarla[7]). Lo anterior se informa en cumplimiento del Decimoséptimo de los Lineamientos de Protección de Datos Personales, publicados en el Diario Oficial de la Federación (incluir fecha[8]).

Otros medios para recabar los datos

Decimonoveno. Las dependencias y entidades que recaben datos personales a través de un servicio de orientación telefónica, u otros medios o sistemas, deberán

---

[1] Indicar el nombre del sistema de datos personales.

[2] Señalar el fundamento legal que faculta a la dependencia o entidad para recabar los datos personales en el sistema de datos personales.

[3] Describir la finalidad del sistema de datos personales.

[4] Indicar las personas u organismos a los que podrán transmitirse los datos personales contenidos en el sistema de datos personales.

[5] Describir la finalidad de la transmisión.

[6] Señalar el nombre de la unidad administrativa responsable del sistema de datos personales.

[7] Indicar la dirección de la unidad de enlace de la dependencia o entidad que posee el sistema de datos personales.

[8] Anotar la fecha de publicación en el *Diario Oficial de la Federación* de los presentes Lineamientos.

establecer un mecanismo por el que se informe previamente a los particulares que sus datos personales serán recabados, la finalidad de dicho acto así como el tratamiento al cual serán sometidos, cumpliendo con lo establecido en el Decimoséptimo de los presentes Lineamientos.

Disociación de datos

Vigésimo. La disociación consiste en el procedimiento por el cual los datos personales no pueden asociarse al Titular de éstos, ni permitir, por su estructura, contenido o grado de desagregación, la identificación individual del mismo.

El tratamiento de datos personales para fines estadísticos deberá efectuarse mediante la disociación de los datos, de conformidad con la *Ley de Información Estadística y Geográfica*, así como las demás disposiciones aplicables.

Tratamiento de datos por terceros

Vigesimoprimero. Cuando se contrate a terceros para que realicen el tratamiento de datos personales, deberá estipularse en el contrato respectivo la implementación de medidas de seguridad y custodia previstas en los presentes Lineamientos, en la normatividad aplicable a las dependencias y entidades contratantes, así como la imposición de penas convencionales por su incumplimiento.

Capítulo IV

De la transmisión

Transmisión sin consentimiento del titular de los datos

Vigesimosegundo. Las dependencias y entidades podrán transmitir datos personales sin el consentimiento del Titular de los datos, en los casos previstos en el artículo 22 de la Ley. Asimismo, deberán otorgar acceso a aquellos datos que no se consideran como confidenciales por ubicarse en los supuestos establecidos por sus artículos 7, 12 y 18 último párrafo.

Transmisión con el consentimiento del titular de los datos

Vigesimotercero. Para los efectos del artículo 21 de la Ley y en los casos no previstos por el artículo 22 de la Ley, las dependencias y entidades sólo podrán transmitir datos personales cuando:

a) Así lo prevea de manera expresa una disposición legal, y
b) Medie el consentimiento expreso de los titulares.

Consentimiento

Vigesimocuarto. Para la transmisión de los datos, el consentimiento del Titular de los mismos deberá otorgarse por escrito incluyendo la firma autógrafa y la copia de identificación oficial, o bien a través de un medio de autenticación. En su caso,

las dependencias y entidades deberán cumplir con las disposiciones aplicables en materia de certificados digitales y/o firmas electrónicas.

El servidor público encargado de recabar el consentimiento del Titular de los datos para la transmisión de los mismos deberá entregar a éste, en forma previa a cada transmisión, la información suficiente acerca de las implicaciones de otorgar, de ser el caso, su consentimiento.

Informes sobre la transmisión

Vigesimoquinto. Las transmisiones totales o parciales de sistemas de datos personales que realicen las dependencias y entidades en el ejercicio de sus atribuciones deberán ser notificadas por el Responsable al Instituto en los términos establecidos por el Cuadragésimo de los presentes Lineamientos.

Requisitos del informe

Vigesimosexto. El informe a que hace referencia el Lineamiento anterior deberá contener, al menos, lo siguiente:

I. Identificación del Sistema de datos personales, del transmisor y del destinatario de los datos;
II. Finalidad de la transmisión, así como el tipo de datos que son objeto de la transmisión;
III. Las medidas de seguridad y custodia que adoptaron o fueron adoptadas por el transmisor y destinatario;
IV. Plazo por el que conservará el destinatario los datos que le hayan sido transmitidos, el cual podrá ser ampliado mediante aviso al Instituto, y
V. Señalar si una vez concluidos los propósitos de la transmisión, los datos personales deberán ser destruidos o devueltos al transmisor, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de la transmisión.

Capítulo V

De la seguridad de los sistemas de datos personales

Medidas de seguridad

Vigesimoséptimo. Para proveer seguridad a los sistemas de datos personales, los titulares de las dependencias y entidades deberán adoptar las medidas siguientes:

I. Designar a los Responsables;
II. Proponer al Comité de Información la emisión de criterios específicos sobre el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales, los cuales no podrán contravenir lo dispuesto por los presentes Lineamientos;

III. Proponer al Comité la difusión de la normatividad entre el personal involucrado en el manejo de los sistemas de datos personales, y
IV. Proponer al Comité la elaboración de un plan de capacitación en materia de seguridad de datos personales dirigida a los Responsables, Encargados y Usuarios.

Acciones sobre seguridad

Vigesimooctavo. En cada dependencia o entidad, el Comité coordinará y supervisará las acciones de promoción del manejo, mantenimiento, seguridad y protección de los sistemas de datos personales, así como de la integridad, confiabilidad, disponibilidad y exactitud de la información contenida en dichos sistemas de datos personales.

Reserva de la información

Vigesimonoveno. La documentación generada para la implementación, administración y seguimiento de las medidas de seguridad administrativa, física y técnica tendrá el carácter de información reservada y será de acceso restringido.

El personal que tenga acceso a dicha documentación deberá evitar que ésta sea divulgada, a efecto de no comprometer la integridad, confiabilidad, confidencialidad y disponibilidad de los sistemas de datos personales, así como del contenido de éstos.

Resguardo de sistemas de datos personales físicos

Trigésimo. El Responsable deberá:

a) Adoptar las medidas para el resguardo de los sistemas de datos personales en soporte físico, de manera que se evite su alteración, pérdida o acceso no autorizado;
b) Autorizar expresamente, en los casos en que no esté previsto por un instrumento jurídico, a Encargados y Usuarios, y llevar una relación actualizada de las personas que tengan acceso a los sistemas de datos personales que se encuentran en soporte físico, y
c) Informar al Comité los nombres de los Encargados y Usuarios.

Sitio seguro para sistemas de datos personales automatizados

Trigesimoprimero. Las dependencias y entidades deberán:

I. Asignar un espacio seguro y adecuado para la operación de los sistemas de datos personales;
II. Controlar el acceso físico a las instalaciones donde se encuentra el equipamiento que soporta la operación de los sistemas de datos personales, debiendo registrarse para ello en una bitácora;
III. Contar con al menos dos lugares distintos, que cumplan con las condiciones de seguridad especificadas en estos Lineamientos, destinados a almacenar medios de respaldo de sistemas de datos personales;

IV. Realizar procedimientos de control, registro de asignación y baja de los equipos de cómputo a los Usuarios que utilizan datos personales, considerando al menos las siguientes actividades:

a) Si es asignación, configurarlo con las medidas de seguridad necesarias, tanto a nivel operativo como de infraestructura, y
b) Verificar y llevar un registro del contenido del equipo para facilitar los reportes del Usuario que lo recibe o lo entrega para su baja.

V. Implantar procedimientos para el control de asignación y renovación de claves de acceso a equipos de cómputo y a los sistemas de datos personales;
VI. Implantar medidas de seguridad para el uso de los dispositivos electrónicos y físicos de salida, así como para evitar el retiro no autorizado de los mismos fuera de las instalaciones de la entidad o dependencia, y
VII. En el caso de requerirse disponibilidad crítica de datos, instalar y mantener el equipamiento de cómputo, eléctrico y de telecomunicaciones con la redundancia necesaria. Además, realizar respaldos que permitan garantizar la continuidad de la operación.

Seguridad en la red

Trigesimosegundo. En relación con los aspectos de seguridad al utilizar la red de comunicación donde se transmitan datos personales, es necesario establecer:

I. Procedimientos de control de acceso a la red que consideren perfiles de usuarios o grupos de usuarios para el acceso restringido a las funciones y programas de los Sistemas de datos personales;
II. Mecanismos de auditoría o rastreabilidad de operaciones que mantengan una bitácora para conservar un registro detallado de las acciones llevadas a cabo en cada acceso, ya sea autorizado o no, a los Sistemas de datos personales.

Documento de seguridad

Trigesimotercero. Las dependencias y entidades, a través del Comité y conjuntamente con el área de tecnología de la información, informática o su equivalente, expedirán un documento que contenga las medidas administrativas, físicas y técnicas de seguridad aplicables a los sistemas de datos personales, tomando en cuenta los presentes Lineamientos y las recomendaciones que en la materia emita el Instituto.

El documento de seguridad será de observancia obligatoria para todos los servidores públicos de las dependencias y entidades, así como para las personas externas que debido a la prestación de un servicio tengan acceso a los sistemas de datos personales y/o al sitio donde se ubican los mismos.

Requisitos del documento de seguridad

Trigesimocuarto. El documento mencionado en el Lineamiento anterior deberá contener, como mínimo, los siguientes aspectos:

I. El nombre, cargo y adscripción de los Responsables, Encargados y Usuarios;
II. Estructura y descripción de los sistemas de datos personales;
III. Especificación detallada del tipo de datos personales contenidos en el sistema;
IV. Funciones y obligaciones de los servidores públicos autorizados para acceder al sitio seguro y para el tratamiento de datos personales;
V. Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido en los presentes Lineamientos, los cuales deberán incluir lo siguiente:

a) Establecer procedimientos para generar, asignar, distribuir, modificar, almacenar y dar de baja usuarios y claves de acceso para la operación del Sistema de datos personales;
b) Actualización de información contenida en el Sistema de datos personales;
c) Procedimientos de creación de copias de respaldo y de recuperación de los datos;
d) Bitácoras de acciones llevadas a cabo en el Sistema de datos personales;
e) Procedimiento de notificación, gestión y respuesta ante incidentes, y
f) Procedimiento para la cancelación de un Sistema de datos personales.

El contenido del documento deberá actualizarse anualmente.

Registro de incidentes

Trigesimoquinto. El Encargado deberá llevar un registro de incidentes en el que se consignen los procedimientos realizados para la recuperación de los datos o para permitir una disponibilidad del proceso, indicando la persona que resolvió el incidente, la metodología aplicada, los datos recuperados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

Accesos controlados y bitácoras

Trigesimosexto. En cada acceso a un Sistema de datos personales deberán guardarse como mínimo:

I. Datos completos del Responsable, Encargado o Usuario;
II. Modo de autenticación del Responsable, Encargado o Usuario;
III. Fecha y hora en que se realizó el acceso o se intentó el mismo;
IV. Sistema de datos personales accedido;
V. Operaciones o acciones llevadas a cabo dentro del Sistema de datos personales, y
VI. Fecha y hora en que se realizó la salida del Sistema de datos personales.

Operaciones de acceso, actualización, respaldo y recuperación

Trigesimoséptimo. En las actividades relacionadas con la operación de los sistemas de datos personales tales como el acceso, actualización, respaldo y recupera-

ción de información, las dependencias y entidades deberán llevar a cabo en forma adicional las siguientes medidas:

I. Contar con manuales de procedimientos y funciones para el tratamiento de datos personales que deberán observar obligatoriamente los Responsables, Encargados o Usuarios de los sistemas de datos personales;
II. Llevar control y registros del Sistema de datos personales en bitácoras que contengan la operación cotidiana, respaldos, usuarios, incidentes y accesos, así como la transmisión de datos y sus destinatarios, de acuerdo con las políticas internas que establezca la dependencia o entidad;
III. Procedimientos de control de acceso a la red que incluyan perfiles de usuarios o grupos de usuarios para el acceso restringido a las funciones y programas de los sistemas de datos personales;
IV. Mecanismos de auditoría o rastreabilidad de operaciones;
V. Garantizar que el personal encargado del tratamiento de datos personales sólo tenga acceso a las funciones autorizadas del Sistema de datos personales según su perfil de usuario;
VI. Aplicar procedimientos de respaldos de bases de datos y realizar pruebas periódicas de restauración;
VII. Llevar control de inventarios y clasificación de los medios magnéticos u ópticos de respaldo de los datos personales;
VIII. Utilizar un espacio externo seguro para guardar de manera sistemática los respaldos de las bases de datos de los sistemas de datos personales;
IX. Garantizar que durante la transmisión de datos personales y el transporte de los soportes de almacenamiento, los datos no sean accesados, reproducidos, alterados o suprimidos sin autorización;
X. Aplicar procedimientos para la destrucción de medios de almacenamiento y de respaldo obsoletos que contengan datos personales;
XI. En los casos en que la operación sea externa, convenir con el proveedor del servicio que la dependencia o entidad tenga la facultad de verificar que se respete la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales; revisar que el tratamiento se está realizando conforme a los contratos formalizados, así como que se cumplan los estándares de seguridad planteados en estos Lineamientos;
XII. Diseñar planes de contingencia que garanticen la continuidad de la operación y realizar pruebas de eficiencia de los mismos;
XIII. Llevar a cabo verificaciones a través de las áreas de tecnología de la información, informática o su equivalente respecto de medidas técnicas establecidas en los presentes Lineamientos y, en su caso, remitirlos al Órgano Interno de Control, y
XIV. Cualquier otra medida tendente a garantizar el cumplimiento de los principios de protección de datos personales señalados en el Capítulo II de los presentes Lineamientos.

Estas medidas deberán ser integradas como anexos técnicos al documento de seguridad mencionado en el Lineamiento Trigesimotercero.

Recomendaciones sobre estándares mínimos de seguridad

Trigesimooctavo. El Instituto emitirá anualmente las recomendaciones sobre los estándares mínimos de seguridad, aplicables a los sistemas de datos personales que se encuentren en poder de las dependencias y entidades de la Administración Pública Federal y determinará, en su caso, el nivel de protección que amerite la naturaleza de los datos personales.

Capítulo VI

Del sistema "Persona"

Trigesimonoveno. Para dar cumplimiento a lo dispuesto por el artículo 23 de la Ley, el Instituto pondrá a disposición de las dependencias y entidades el Sistema "Persona".

Cuadragésimo. Los Responsables deberán registrar e informar al Instituto, dentro de los primeros diez días hábiles de enero y julio de cada año, lo siguiente:

a) Los sistemas de datos personales;
b) Cualquier modificación sustancial o cancelación de dichos sistemas, y
c) Cualquier transmisión de sistemas de datos personales de conformidad a lo dispuesto por los Lineamientos Vigesimoquinto y Vigesimosexto de los presentes Lineamientos.

Datos del registro

Cuadragesimoprimero. El registro de cada Sistema de datos personales deberá contener los siguientes datos:
a) Nombre del sistema;
b) Unidad administrativa en la que se encuentra el sistema;
c) Nombre del responsable del sistema;
d) Cargo del Responsable;
e) Teléfono y correo electrónico del Responsable;
f) Finalidad del sistema, y
g) Normatividad aplicable al sistema.

El Instituto otorgará al Responsable un folio de identificación por cada Sistema de datos personales registrado.

Vínculo al Sistema "Persona"

Cuadragesimosegundo. Las dependencias y entidades deberán establecer un vínculo en sus sitios de Internet al Sistema "Persona", a efecto de dar cumplimiento a lo establecido en los artículos 48 y Sexto transitorio del Reglamento de la Ley.

Capítulo VII

Del Instituto

Supervisión de la Protección

Cuadragesimotercero. Las dependencias y entidades deberán permitir a los servidores públicos del Instituto o a terceros previamente designados por éste el acceso a los lugares en los que se encuentran y operan los sistemas de datos personales, así como poner a su disposición la documentación técnica y administrativa de los mismos, a fin de supervisar que se cumpla con la Ley, su Reglamento y los presentes Lineamientos.

Irregularidades

Cuadragesimocuarto. En caso de que el Instituto determine que algún servidor público pudo haber incurrido en responsabilidades por el incumplimiento de los presentes Lineamientos, lo hará del conocimiento del Órgano Interno de Control correspondiente, a efecto de que determine lo conducente, con base en el capítulo de Responsabilidades y Sanciones establecido en el Título IV de la ley, así como en la *Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.*

Anexo III

Ley Federal del Derecho de Autor (extracto)

(Publicada en el DOF *el 24 de diciembre de 1996)*

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

I. ...
XI. Programas de cómputo;
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.

Capítulo IV

De los Programas de Computación y las Bases de Datos

Artículo 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.

Artículo 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.

Artículo 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.

Artículo 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 a 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.

Artículo 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.

Artículo 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 decompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.

Artículo 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.

Artículo 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 cinco años.

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, 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 exceptuadas 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.

Capítulo II

De las Infracciones en Materia de Comercio

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

I. ...
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;

Artículo 232. Las infracciones en materia de comercio previstas en la presente Ley serán sancionadas por el Instituto Mexicano de la Propiedad Industrial con multa:

I. De cinco mil hasta diez mil días de salario mínimo en los casos previstos en las fracciones I, III, IV, V, VII, VIII y IX del artículo anterior;
II. ...

Se aplicará multa adicional de hasta quinientos días de salario mínimo general vigente por día a quien persista en la infracción.

Artículo 233. Si el infractor fuese un editor, organismo de radiodifusión o cualquier persona física o moral que explote obras a escala comercial, la multa podrá incrementarse hasta en un cincuenta por ciento respecto de las cantidades previstas en el artículo anterior.

Artículo 234. El Instituto Mexicano de la Propiedad Industrial sancionará las infracciones materia de comercio con arreglo al procedimiento y las formalidades previstas en los Títulos Sexto y Séptimo de la *Ley de la Propiedad Industrial*.

El Instituto Mexicano de la Propiedad Industrial podrá adoptar las medidas precautorias previstas en la *Ley de la Propiedad Industrial*.

Para tal efecto, el Instituto Mexicano de la Propiedad Industrial tendrá las facultades de realizar investigaciones, ordenar y practicar visitas de inspección, y requerir información y datos.

Artículo 236. Para la aplicación de las sanciones a que se refiere este Título se entenderá como salario mínimo el salario mínimo general vigente en el Distrito Federal en la fecha de la comisión de la infracción.

Anexo IV

Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, *del* Código Federal de Procedimientos Civiles, *del* Código de Comercio *y de la* Ley Federal de Protección al Consumidor *(extracto)*

(Publicado en el* DOF *el 29 mayo de 2000)

Artículo primero. Se modifica la denominación del *Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal*, y con ello se reforman sus artículos 1o., 1803, 1805 y 1811, y se le adiciona el artículo 1834 bis, para quedar como sigue:

CÓDIGO CIVIL FEDERAL

Artículo 1o. Las disposiciones de este Código regirán en toda la República en asuntos del orden federal.

Artículo 1803. El consentimiento puede ser expreso o tácito; para ello, se estará a lo siguiente:

I. Será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y
II. El tácito resultará de hechos o de actos que lo presupongan o que autoricen a presumirlo, excepto en los casos en que por ley o por convenio la voluntad deba manifestarse expresamente.

Artículo 1805. Cuando la oferta se haga a una persona presente, sin fijación de plazo para aceptarla, el autor de la oferta quedará desligado si la aceptación no se hace inmediatamente. La misma regla se aplicará a la oferta hecha por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta en forma inmediata.

Artículo 1811. ... Tratándose de la propuesta y aceptación hechas a través de medios electrónicos, ópticos o de cualquier otra tecnología no se requerirá de estipulación previa entre los contratantes para que produzca efectos.

Artículo 1834 bis. Los supuestos previstos por el artículo anterior se tendrán por cumplidos mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, siempre que la información generada o comunicada en forma íntegra a través de dichos medios sea atribuible a las personas obligadas y accesible para su ulterior consulta.

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán generar, enviar, recibir, archivar o comunicar la información que contenga los términos exactos en que las partes han decidido obligarse, mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, en cuyo caso el fedatario público deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuye dicha información a las partes y conservar bajo su resguardo una versión íntegra de la misma para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

Artículo segundo. Se adiciona el artículo 210-A al *Código Federal de Procedimientos Civiles*, en los términos siguientes:

"***Artículo 210-A.*** Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.

Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente a la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible, atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.

Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta".

Artículo tercero. Se reforman los artículos 18, 20, 21 párrafo primero, 22, 23, 24, 25, 26, 27, 30, 31, 32, 49, 80 y 1205, y se adicionan los artículos 20 bis, 21 bis, 21 bis 1, 30 bis, 30 bis 1 y 32 bis 1298-A; el Título II que se denominará "Del Comercio Electrónico", que comprenderá los artículos 89 a 94, y se modifica la denominación del Libro Segundo del *Código de Comercio*, disposiciones todas del referido *Código de Comercio*, para quedar como sigue:

"***Artículo 18.*** En el Registro Público de Comercio se inscriben los actos mercantiles, así como aquellos que se relacionan con los comerciantes y que conforme a la legislación lo requieran.

La operación del Registro Público de Comercio está a cargo de la Secretaría de Comercio y Fomento Industrial, en adelante la Secretaría, y de las autoridades responsables del Registro Público de la Propiedad en los estados y en el Distrito Federal, en términos de este Código y de los convenios de coordinación que se suscriban conforme a lo dispuesto por el artículo 116 de la *Constitución Política de los Estados Unidos Mexicanos*. Para estos efectos existirán las oficinas del Registro Público de Comercio en cada entidad federativa que demande el tráfico mercantil.

La Secretaría emitirá los lineamientos necesarios para la adecuada operación del Registro Público de Comercio, que deberán publicarse en el *Diario Oficial de la Federación*.

Artículo 20. El Registro Público de Comercio operará con un programa informático y con una base de datos central interconectada con las bases de datos de sus oficinas ubicadas en las entidades federativas. Las bases de datos contarán con al menos un respaldo electrónico.

Mediante el programa informático se realizará la captura, almacenamiento, custodia, seguridad, consulta, reproducción, verificación, administración y transmisión de la información registral.

Las bases de datos del Registro Público de Comercio en las entidades federativas se integrarán con el conjunto de la información incorporada por medio del programa informático de cada inscripción o anotación de los actos mercantiles inscribibles, y la base de datos central con la información que los responsables del Registro incorporen en las bases de datos ubicadas en las entidades federativas.

El programa informático será establecido por la Secretaría. Dicho programa y las bases de datos del Registro Público de Comercio serán propiedad del Gobierno Federal.

En caso de existir discrepancia o presunción de alteración de la información del Registro Público de Comercio contenida en la base de datos de alguna entidad federativa, o sobre cualquier otro respaldo que hubiere, prevalecerá la información registrada en la base de datos central, salvo prueba en contrario.

La Secretaría establecerá los formatos, que serán de libre reproducción, así como los datos, requisitos y demás información necesaria para llevar a cabo las inscripciones, anotaciones y avisos a que se refiere el presente Capítulo. Lo anterior deberá publicarse en el *Diario Oficial de la Federación*.

Artículo 20 bis. Los responsables de las oficinas del Registro Público de Comercio tendrán las atribuciones siguientes:

I. Aplicar las disposiciones del presente Capítulo en el ámbito de la entidad federativa correspondiente;
II. Ser depositario de la fe pública registral mercantil, para cuyo ejercicio se auxiliará de los registradores de la oficina a su cargo;
III. Dirigir y coordinar las funciones y actividades de las unidades administrativas a su cargo para que cumplan con lo previsto en este Código, el reglamento respectivo y los lineamientos que emita la Secretaría;
IV. Permitir la consulta de los asientos registrales que obren en el Registro, así como expedir las certificaciones que le soliciten;

V. Operar el programa informático del sistema registral automatizado en la oficina a su cargo, conforme a lo previsto en este Capítulo, el reglamento respectivo y en los lineamientos que emita la Secretaría;
VI. Proporcionar facilidades a la Secretaría para vigilar la adecuada operación del Registro Público de Comercio, y
VII. Las demás que se señalen en el presente Capítulo y su reglamento.

Artículo 21. Existirá un folio electrónico por cada comerciante o sociedad, en el que se anotarán:

I a XIX. ...

Artículo 21 bis. El procedimiento para la inscripción de actos mercantiles en el Registro Público de Comercio se sujetará a las bases siguientes:

I. Será automatizado y estará sujeto a plazos máximos de respuesta;
II. Constará de las fases de:

a) Recepción, física o electrónica de una forma precodificada, acompañada del instrumento en el que conste el acto a inscribir, pago de los derechos, generación de una boleta de ingreso y del número de control progresivo e invariable para cada acto;
b) Análisis de la forma precodificada y la verificación de la existencia o inexistencia de antecedentes registrales y, en su caso, preinscripción de dicha información a la base de datos ubicada en la entidad federativa;
c) Calificación, en la que se autorizará en definitiva la inscripción en la base de datos mediante la firma electrónica del servidor público competente, con lo cual se generará o adicionará el folio mercantil electrónico correspondiente, y
d) Emisión de una boleta de inscripción que será entregada física o electrónicamente.

El reglamento del presente Capítulo desarrollará el procedimiento registral de acuerdo con las bases anteriores.

Artículo 21 bis 1. La prelación entre derechos sobre dos o más actos que se refieran a un mismo folio mercantil electrónico se determinará por el número de control que otorgue el registro, cualquiera que sea la fecha de su constitución o celebración.

Artículo 22. Cuando, conforme a la ley, algún acto o contrato deba inscribirse en el Registro Público de la Propiedad o en registros especiales, su inscripción en dichos registros será bastante para que surtan los efectos correspondientes del derecho mercantil, siempre y cuando en el Registro Público de Comercio se tome razón de dicha inscripción y de las modificaciones a la misma.

Artículo 23. Las inscripciones deberán hacerse en la oficina del Registro Público de Comercio del domicilio del comerciante, pero si se trata de bienes raíces o derechos reales constituidos sobre ellos, la inscripción se hará, además, en la oficina correspondiente a la ubicación de los bienes, salvo disposición legal que establezca otro procedimiento.

Artículo 24. Las sociedades extranjeras deberán acreditar, para su inscripción en el Registro Público de Comercio, estar constituidas conforme a las leyes de su

país de origen y autorizadas para ejercer el comercio por la Secretaría, sin perjuicio de lo establecido en los tratados o convenios internacionales.

Artículo 25. Los actos que conforme a este Código u otras leyes deban inscribirse en el Registro Público de Comercio deberán constar en:

I. Instrumentos públicos otorgados ante notario o corredor público;
II. Resoluciones y providencias judiciales o administrativas certificadas;
III. Documentos privados ratificados ante notario o corredor público, o autoridad judicial competente, según corresponda, o
IV. Los demás documentos que de conformidad con otras leyes así lo prevean.

Artículo 26. Los documentos de procedencia extranjera que se refieran a actos inscribibles podrán constar previamente en instrumento público otorgado ante notario o corredor público, para su inscripción en el Registro Público de Comercio.

Las sentencias dictadas en el extranjero sólo se registrarán cuando medie orden de autoridad judicial mexicana competente y de conformidad con las disposiciones internacionales aplicables.

Artículo 27. La falta de registro de los actos cuya inscripción sea obligatoria hará que éstos sólo produzcan efectos jurídicos entre los que lo celebren, y no podrán producir perjuicio a tercero, el cual sí podrá aprovecharse de ellos en lo que le fueren favorables.

Artículo 30. Los particulares podrán consultar las bases de datos y, en su caso, solicitar las certificaciones respectivas, previo pago de los derechos correspondientes.

Las certificaciones se expedirán previa solicitud por escrito que deberá contener los datos que sean necesarios para la localización de los asientos sobre los que deba versar la certificación y, en su caso, la mención del folio mercantil electrónico correspondiente.

Cuando la solicitud respectiva haga referencia a actos aún no inscritos, pero ingresados a la oficina del Registro Público de Comercio, las certificaciones se referirán a los asientos de presentación y trámite.

Artículo 30 bis. La Secretaría podrá autorizar el acceso a la base de datos del Registro Público de Comercio a personas que así lo soliciten y cumplan con los requisitos para ello, en los términos de este Capítulo, el reglamento respectivo y los lineamientos que emita la Secretaría, sin que dicha autorización implique en ningún caso inscribir o modificar los asientos registrales.

La Secretaría certificará los medios de identificación que utilicen las personas autorizadas para firmar electrónicamente la información relacionada con el Registro Público de Comercio, así como la de los demás usuarios del mismo, y ejercerá el control de estos medios a fin de salvaguardar la confidencialidad de la información que se remita por esta vía.

Artículo 30 bis 1. Cuando la autorización a que se refiere el artículo anterior se otorgue a notarios o corredores públicos, dicha autorización permitirá, además, el envío de información por medios electrónicos al Registro y la remisión que éste efectúe al fedatario público correspondiente del acuse que contenga el número de control a que se refiere el artículo 21 bis 1 de este Código.

Los notarios y corredores públicos que soliciten dicha autorización deberán otorgar una fianza a favor de la Tesorería de la Federación y registrarla ante la Secretaría, para garantizar los daños que pudieran ocasionar a los particulares en la operación del programa informático, por un monto mínimo equivalente a 10 000 veces el salario mínimo diario vigente en el Distrito Federal.

En caso de que los notarios o corredores públicos estén obligados por la ley de la materia a garantizar el ejercicio de sus funciones, sólo otorgarán la fianza a que se refiere el párrafo anterior por un monto equivalente a la diferencia entre ésta y la otorgada.

Dicha autorización y su cancelación deberán publicarse en el *Diario Oficial de la Federación*.

Artículo 31. Los registradores no podrán denegar la inscripción de los documentos mercantiles que se les presenten, salvo cuando:

I. El acto o contrato que en ellos se contenga no sea de los que deben inscribirse;
II. Esté en manifiesta contradicción con los contenidos de los asientos registrales preexistentes, o
III. El documento de que se trate no exprese, o exprese sin claridad suficiente, los datos que deba contener la inscripción.

Si la autoridad administrativa o judicial ordena que se registre un instrumento rechazado, la inscripción surtirá sus efectos desde que por primera vez se presentó.

El registrador suspenderá la inscripción de los actos a inscribir, siempre que existan defectos u omisiones que sean subsanables. En todo caso se requerirá al interesado para que en el plazo que determine el reglamento de este Capítulo las subsane, en el entendido de que, de no hacerlo, se le denegará la inscripción.

Artículo 32. La rectificación de los asientos en la base de datos por causa de error material o de concepto sólo procede cuando exista discrepancia entre el instrumento donde consten el acto y la inscripción.

Se entenderá que se comete error material cuando se escriban unas palabras por otras, se omita la expresión de alguna circunstancia o se equivoquen los nombres propios o las cantidades al copiarlas del instrumento donde conste el acto, sin cambiar por eso el sentido general de la inscripción ni el de alguno de sus conceptos.

Se entenderá que se comete error de concepto cuando al expresar en la inscripción alguno de los contenidos del instrumento, se altere o varíe su sentido porque el responsable de la inscripción se hubiere formado un juicio equivocado del mismo, por una errónea calificación del contrato o acto en él consignado o por cualquier otra circunstancia similar.

Artículo 32 bis. Cuando se trate de errores de concepto, los asientos practicados en los folios del Registro Público de Comercio sólo podrán rectificarse con el consentimiento de todos los interesados en el asiento.

A falta del consentimiento unánime de los interesados, la rectificación sólo podrá efectuarse por resolución judicial.

El concepto rectificado surtirá efectos desde la fecha de su rectificación.

El procedimiento para efectuar la rectificación en la base de datos lo determinará la Secretaría en los lineamientos que al efecto emita.

Artículo 49. Los comerciantes están obligados a conservar por un plazo mínimo de diez años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones.

Para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. La Secretaría de Comercio y Fomento Industrial emitirá la Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos.

LIBRO SEGUNDO

Del comercio en general

[...]

Artículo 80. Los convenios y contratos mercantiles que se celebren por correspondencia, telégrafo, o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedarán perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que ésta fuere modificada.

Título II

Del comercio electrónico

Artículo 89. En los actos de comercio podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, a la información generada, enviada, recibida, archivada o comunicada a través de dichos medios se le denominará mensaje de datos.

Artículo 90. Salvo pacto en contrario, se presumirá que el mensaje de datos proviene del emisor si ha sido enviado:

I. Usando medios de identificación, tales como claves o contraseñas de él, o
II. Por un sistema de información programado por el emisor o en su nombre para que opere automáticamente.

Artículo 91. El momento de recepción de la información a que se refiere el artículo anterior se determinará como sigue:

I. Si el destinatario ha designado un sistema de información para la recepción, ésta tendrá lugar en el momento en que ingrese en dicho sistema, o
II. De enviarse a un sistema del destinatario que no sea el designado o de no haber un sistema de información designado, en el momento en que el destinatario obtenga dicha información.

Para efecto de este Código, se entiende por sistema de información cualquier medio tecnológico utilizado para operar mensajes de datos.

Artículo 92. Tratándose de la comunicación de mensajes de datos que requieran de un acuse de recibo para surtir efectos, bien sea por disposición legal o por así requerirlo el emisor, se considerará que el mensaje de datos ha sido enviado cuando se haya recibido el acuse respectivo.

Salvo prueba en contrario, se presumirá que se ha recibido el mensaje de datos cuando el emisor reciba el acuse correspondiente.

Artículo 93. Cuando la ley exija la forma escrita para los contratos y la firma de los documentos relativos, esos supuestos se tendrán por cumplidos tratándose de mensaje de datos siempre que éste sea atribuible a las personas obligadas y accesible para su ulterior consulta.

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de mensajes de datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

Artículo 94. Salvo pacto en contrario, el mensaje de datos se tendrá por expedido en el lugar donde el emisor tenga su domicilio y por recibido en el lugar donde el destinatario tenga el suyo.

Artículo 1205. Son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos y, en consecuencia, serán tomadas como pruebas las declaraciones de las partes, terceros, peritos, documentos públicos o privados, inspección judicial, fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, mensajes de datos, reconstrucciones de hechos y en general cualquier otra similar u objeto que sirva para averiguar la verdad.

Artículo 1298-A. Se reconoce como prueba los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada.

Artículo cuarto. Se reforma el párrafo primero del artículo 128 y se adiciona la fracción VIII al artículo 1o., la fracción IX bis al artículo 24 y el Capítulo VIII bis a la *Ley Federal de Protección al Consumidor*, que contendrá el artículo 76 bis, para quedar como sigue:

"***Artículo 1o.***

...

...

I a VII. ...

VIII. La efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos aportados.

Artículo 24. ...

I a IX. ...

IX bis. Promover en coordinación con la Secretaría la formulación, difusión y uso de códigos de ética, por parte de proveedores, que incorporen los principios previstos por esta Ley respecto de las transacciones que celebren con consumidores a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología;

X a XXI. ....

Capítulo VIII bis

De los derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología

Artículo 76 bis. Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:

I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;
II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;
III. El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;
IV. El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás disposiciones que se deriven de ella;
V. El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor;
VI. El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y
VII. El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, y cuidará las prácticas de mercadotecnia dirigidas a población vulnerable, como niños, ancianos y enfermos, incorpo-

rando mecanismos que adviertan cuando la información no sea apta para esa población.

Artículo 128. Las infracciones a lo dispuesto por los artículos 8, 10, 12, 60, 63, 65, 74, 76 bis, 80 y 121 serán sancionadas con multa por el equivalente de una y hasta dos mil quinientas veces el salario mínimo general vigente para el Distrito Federal.

Anexo V

Política de solución de controversias en materia de nombres de dominio para .MX (LDRP)

1. Procedimiento de solución de controversias

   a) Controversias aplicables.

   Todas las personas que estimen afectados sus derechos (promovente) y que deseen solicitar la cancelación del registro o transmisión de la titularidad del registro de un nombre de dominio en .MX aceptan someterse a la política de solución de controversias en materia de nombres de dominio para .MX (LDRP) y al reglamento respectivo, ante un proveedor de servicios de solución de controversias, autorizado por NIC-México, conformado por un grupo independiente e imparcial de expertos, en los siguientes casos:

   i) El nombre de dominio es idéntico o semejante en grado de confusión con respecto a una marca de productos o de servicios registrada, aviso comercial registrado, denominación de origen o reserva de derechos sobre la que el promovente tiene derechos; y
   ii) El titular no tiene derechos o intereses legítimos respecto del nombre de dominio, y
   iii) El nombre de dominio ha sido registrado o se utiliza de mala fe.

   b) Pruebas del registro o utilización de mala fe. Las circunstancias siguientes, entre otras, constituirán la prueba del registro o utilización de mala fe de un nombre de dominio:

   i) Circunstancias que indiquen que se ha registrado o adquirido el nombre de dominio fundamentalmente con el fin de vender, alquilar o ceder de otra manera el registro del nombre de dominio al promovente que es el titular de la marca de productos o servicios registrada, aviso comercial registrado, denominación de origen o reserva de derechos a un competidor del promovente, por un valor

cierto que supera los costos diversos documentados que están relacionados directamente con el nombre de dominio, o

ii) Se ha registrado el nombre de dominio a fin de impedir que el titular de la marca de productos o servicios registrada, aviso comercial registrado, denominación de origen o reserva de derechos refleje su denominación en un nombre de dominio correspondiente, siempre y cuando el titular haya desarrollado una conducta de esa índole; o

iii) Se ha registrado el nombre de dominio fundamentalmente con el fin de perturbar la actividad comercial de un competidor, o

iv) Se ha utilizado el nombre de dominio de manera intencionada con el fin de atraer, con ánimo de lucro, usuarios de Internet a un sitio Web o a cualquier otro sitio en línea, creando la posibilidad de que exista confusión con la denominación del promovente en cuanto a la fuente, patrocinio, afiliación o promoción del sitio Web o del sitio en línea o de un producto o servicio o bien jurídicamente tutelado por alguna reserva de derechos que figure en el sitio Web o en el sitio en línea.

c) Se demostrarán derechos y legítimos intereses sobre el nombre de dominio cuando se presenten cualquiera de las circunstancias que de manera enunciativa mas no limitativa se presentan a continuación:

i) Antes de haber recibido cualquier aviso de la controversia, se ha utilizado el nombre de dominio, o se han efectuado preparativos demostrables para su utilización, o un nombre correspondiente al nombre de dominio en relación con una oferta de buena fe de productos o servicios o bien jurídicamente tutelado por alguna reserva de derechos;

ii) El titular (en calidad de particular, empresa u otra organización) ha sido conocido comúnmente por el nombre de dominio, aun cuando no haya adquirido derechos de marcas de productos o de servicios registrada, aviso comercial registrado, denominación de origen o reserva de derechos; o

iii) Se hace un uso legítimo y leal o no comercial del nombre de dominio, sin intención de desviar a los consumidores de manera equívoca o de empañar el buen nombre de la marca de productos o de servicios registrada, aviso comercial registrado, denominación de origen o reserva de derechos en cuestión con ánimo de lucro.

d) Inicio del procedimiento. Los requisitos para el inicio y el procedimiento de la política LDRP, así como para la selección de un grupo administrativo de expertos están establecidos en el Reglamento del procedimiento de solución de controversias relativo al registro abusivo de nombres de dominio en .MX (el "Reglamento") y en el Reglamento Adicional del proveedor, en su caso. El promovente seleccionará el proveedor de entre los autorizados por NIC-México, transmitiendo dicho promovente su solicitud de resolución de controversia relativa a nombres de dominio directamente a dicho proveedor.

e) Transferencia de titularidad durante una controversia. El titular no podrá transferir la titularidad del nombre de dominio durante un procedimiento de solución de controversias en materia de nombres de dominio para .MX (LDRP) pendiente, iniciado de conformidad con esta política; NIC México se reserva el derecho de cancelar cualquier transferencia de titularidad de un nombre de dominio que infrinja lo establecido en el presente apartado.

f) Tasas y honorarios. Todas las tasas y honorarios relacionados con cualquier controversia ante un grupo administrativo de expertos se pagarán según lo establecido por cada proveedor.

g) Efectos. Los efectos disponibles para el promovente de conformidad con cualquier procedimiento ante un grupo administrativo de expertos se limitarán a:

i) Solicitar la cancelación del registro del nombre de dominio, o
ii) Solicitar la transmisión al promovente de la titularidad del nombre de dominio.

h) Resoluciones. El titular de un nombre de dominio en .MX y el promovente aceptan acatar las resoluciones de cualquier grupo de expertos expresamente señalado por NIC-México como proveedor de servicios en resolución de controversias de nombre de dominio en .MX, así como la ejecución que de la resolución dictada por este grupo haga NIC-México.

i) Participación de NIC-México en la solución de controversias. El titular y el promovente aceptan y conocen que NIC-México no participa ni participará en la administración o realización de ningún procedimiento ante un grupo de expertos. Además, el titular y el promovente aceptan y conocen que NIC-México no será responsable de ninguna resolución dictada por un grupo administrativo de expertos si no actúa de conformidad con su autoridad, o consecuencias de la aplicación de las mismas.

j) Notificación y publicación. El proveedor notificará en idioma español a NIC-México cualquier resolución adoptada por un grupo de expertos respecto de un nombre de dominio. Todas las resoluciones adoptadas en virtud de la presente política aplicable a las controversias se publicarán en la página de NIC-México http://www.nic.mx Internet, excepto cuando un grupo de expertos determine, haciendo uso de sus facultades exclusivas, que no ha de publicarse la resolución.

k) Aviso. El promovente notificará inmediatamente por escrito (dirección postal de NIC-México y al correo electrónico: legal@nic.mx) a NIC-México cualquier procedimiento iniciado respecto de un nombre de dominio en .MX.

2. Modificaciones de la Política

a) Cualquier modificación o actualización a las Políticas de registro de un nombre de dominio serán publicadas con un aviso de 15 días naturales inmediatos anteriores a la fecha de su entrada en vigor, en la página del NIC-México: http://www.nic.mx, con objeto de que el titular manifieste

lo que a sus intereses convenga. Transcurrido este plazo sin que el titular haya manifestado lo conducente, los cambios y modificaciones tendrán plena validez y efectos legales y serán considerados obligatorios para las partes.

b) Salvo que se haya presentado una solicitud de resolución de controversia con anterioridad a la entrada en vigor de la(s) nueva(s) versión(es) de esta Política, en cuyo caso se aplicará la versión de la Política que estaba en vigor en el momento de presentación de la solicitud de resolución de controversia, la(s) nueva(s) versión(es) de la Política vinculará(n) al titular del dominio en cualquier controversia en materia de registros de nombres de dominio en .MX, independientemente de que los hechos generadores de la controversia hayan surgido con anterioridad a la fecha de entrada en vigor del cambio, en dicha fecha o con posterioridad a la misma.

ANEXO A

Proveedor de servicios de solución de controversias.

NIC-México señala que cuentan con su autorización como proveedores de servicios de solución de controversias:

- Centro de Mediación y Arbitraje de la Organización Mundial de la Propiedad Intelectual
- Sitio en Internet (http://arbiter.wipo.int/domains/index-es.html)
- Costos (http://arbiter.wipo.int/domains/fees/index-es.html)

Es la intención de NIC-México seleccionar a otros proveedores de servicios de solución de controversias en el futuro.

Anexo VI

Decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio *en materia de firma electrónica*

Título segundo: del comercio electrónico

Capítulo I: de los mensajes de datos

Artículo 89. Las disposiciones de este Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte.

Las actividades reguladas por este Título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del Mensaje de Datos en relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa.

En los actos de comercio y en la formación de los mismos podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efectos del presente Código se deberán tomar en cuenta las siguientes definiciones:

Certificado: todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica.

Datos de Creación de Firma Electrónica: son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante.

Destinatario: la persona designada por el Emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho Mensaje.

Emisor: toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario.

Firma Electrónica: los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

Firma Electrónica Avanzada o Fiable: aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97.

En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica.

Firmante: la persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa.

Intermediario: en relación con un determinado Mensaje de Datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho Mensaje o preste algún otro servicio con respecto a él.

Mensaje de Datos: la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.

Parte que Confía: la persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica.

Prestador de Servicios de Certificación: la persona o institución pública que preste servicios relacionados con firmas electrónicas y que expide los Certificados, en su caso.

Secretaría: se entenderá la Secretaría de Economía.

Sistema de Información: se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma Mensajes de Datos.

Titular del Certificado: se entenderá a la persona a cuyo favor fue expedido el Certificado.

Artículo 89 bis. No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un Mensaje de Datos.

Artículo 90. Se presumirá que un Mensaje de Datos proviene del Emisor si ha sido enviado:

I. Por el propio Emisor;
II. Usando medios de identificación, tales como claves o contraseñas del Emisor o por alguna persona facultada para actuar en nombre del Emisor respecto a ese Mensaje de Datos, o
III. Por un Sistema de Información programado por el Emisor o en su nombre para que opere automáticamente.

Artículo 90 bis. Se presume que un Mensaje de Datos ha sido enviado por el Emisor y, por tanto, el Destinatario o la Parte que Confía, en su caso, podrá actuar en consecuencia cuando:

I. Haya aplicado en forma adecuada el procedimiento acordado previamente con el Emisor, con el fin de establecer que el Mensaje de Datos provenía efectivamente de éste, o

II. El Mensaje de Datos que reciba el Destinatario o la Parte que Confía resulte de los actos de un Intermediario que le haya dado acceso a algún método utilizado por el Emisor para identificar un Mensaje de Datos como propio.

Lo dispuesto en el presente artículo no se aplicará:

I. A partir del momento en que el Destinatario o la Parte que Confía haya sido informado por el Emisor de que el Mensaje de Datos no provenía de éste y haya dispuesto de un plazo razonable para actuar en consecuencia, o
II. A partir del momento en que el Destinatario o la Parte que Confía tenga conocimiento, o debiere tenerlo, de haber actuado con la debida diligencia o aplicado algún método convenido, que el Mensaje de Datos no provenía del Emisor.

Salvo prueba en contrario y sin perjuicio del uso de cualquier otro método de verificación de la identidad del Emisor, se presumirá que se actuó con la debida diligencia si el método que usó el Destinatario o la Parte que Confía cumple los requisitos establecidos en este Código para la verificación de la fiabilidad de las Firmas Electrónicas.

Artículo 91. Salvo pacto en contrario entre el Emisor y el Destinatario, el momento de recepción de un Mensaje de Datos se determinará como sigue:

I. Si el Destinatario ha designado un Sistema de Información para la recepción de Mensajes de Datos, ésta tendrá lugar en el momento en que ingrese en dicho Sistema de Información;
II. De enviarse el Mensaje de Datos a un Sistema de Información del Destinatario que no sea el Sistema de Información designado, o de no haber un Sistema de Información designado, en el momento en que el Destinatario recupere el Mensaje de Datos, o
III. Si el Destinatario no ha designado un Sistema de Información, la recepción tendrá lugar cuando el Mensaje de Datos ingrese en un Sistema de Información del Destinatario.

Lo dispuesto en este artículo será aplicable aun cuando el Sistema de Información esté ubicado en un lugar distinto de donde se tenga por recibido el Mensaje de Datos conforme al artículo 94.

Artículo 91 bis. Salvo pacto en contrario entre el Emisor y el Destinatario, el Mensaje de Datos se tendrá por expedido cuando ingrese en un Sistema de Información que no esté bajo el control del emisor o del intermediario.

Artículo 92. En lo referente a acuse de recibo de Mensajes de Datos, se estará a lo siguiente:

I. Si al enviar o antes de enviar un Mensaje de Datos el Emisor solicita o acuerda con el Destinatario que se acuse recibo del Mensaje de Datos, pero no se ha acordado entre éstos una forma o método determinado para efectuarlo, se podrá acusar recibo mediante:

a) Toda comunicación del Destinatario, automatizada o no, o
b) Todo acto del Destinatario, que baste para indicar al Emisor que se ha recibido el Mensaje de Datos.

II. Cuando el Emisor haya indicado que los efectos del Mensaje de Datos estarán condicionados a la recepción de un acuse de recibo, se considerará que el Mensaje de Datos no ha sido enviado en tanto que no se haya recibido el acuse de recibo en el plazo fijado por el Emisor o dentro de un plazo razonable atendiendo a la naturaleza del negocio, a partir del momento del envío del Mensaje de Datos;

III. Cuando el Emisor haya solicitado o acordado con el Destinatario que se acuse recibo del Mensaje de Datos, independientemente de la forma o método determinado para efectuarlo, salvo que:

a) El Emisor no haya indicado expresamente que los efectos del Mensaje de Datos estén condicionados a la recepción del acuse de recibo, y
b) No se haya recibido el acuse de recibo en el plazo solicitado o acordado o, en su defecto, dentro de un plazo razonable atendiendo a la naturaleza del negocio.

El Emisor podrá dar aviso al Destinatario de que no ha recibido el acuse de recibo solicitado o acordado y fijar un nuevo plazo razonable para su recepción, contado a partir del momento de este aviso. Cuando el Emisor reciba acuse de recibo del Destinatario se presumirá que éste ha recibido el Mensaje de Datos correspondiente;

IV. Cuando en el acuse de recibo se indique que el Mensaje de Datos recibido cumple con los requisitos técnicos convenidos o establecidos en ley, se presumirá que ello es así.

Artículo 93. Cuando la ley exija la forma escrita para los actos, convenios o contratos, este supuesto se tendrá por cumplido tratándose de Mensaje de Datos, siempre que la información en él contenida se mantenga íntegra y sea accesible para su ulterior consulta, sin importar el formato en el que se encuentre o represente.

Cuando adicionalmente la ley exija la firma de las partes, dicho requisito se tendrá por cumplido tratándose de Mensaje de Datos, siempre que éste sea atribuible a dichas partes.

En los casos en que la Ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de Mensajes de Datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

Artículo 93 bis. Sin perjuicio de lo dispuesto en el artículo 49 de este Código, cuando la Ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho respecto a un Mensaje de Datos:

I. Si existe garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como Mensaje de Datos o en alguna otra forma, y
II. De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.

Para efectos de este artículo, se considerará que el contenido de un Mensaje de Datos es íntegro si éste ha permanecido completo e inalterado independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido será determinado conforme a los fines para los que se generó la información y de todas las circunstancias relevantes del caso.

Artículo 94. Salvo pacto en contrario entre el Emisor y el Destinatario, el Mensaje de Datos se tendrá por expedido en el lugar donde el Emisor tenga su establecimiento y por recibido en el lugar donde el Destinatario tenga el suyo. Para los fines del presente artículo:

I. Si el Emisor o el Destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal, y
II. Si el Emisor o el Destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

Artículo 95. Conforme al artículo 90, siempre que se entienda que el Mensaje de Datos proviene del Emisor o que el Destinatario tenga derecho a actuar con arreglo a este supuesto, dicho Destinatario tendrá derecho a considerar que el Mensaje de Datos recibido corresponde al que quería enviar el iniciador, y podrá proceder en consecuencia. El Destinatario no gozará de este derecho si sabía o hubiera sabido, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que la transmisión había dado lugar a un error en el Mensaje de Datos recibido.

Se presume que cada Mensaje de Datos recibido es un Mensaje de Datos diferente, salvo que el Destinatario sepa, o debiera saber, de haber actuado con la debida diligencia, o de haber aplicado algún método previamente acordado, que el nuevo Mensaje de Datos era un duplicado.

Capítulo II: de las firmas

Artículo 96. Las disposiciones del presente Código serán aplicadas de modo que no excluyan, restrinjan o priven de efecto jurídico cualquier método para crear una Firma Electrónica.

Artículo 97. Cuando la Ley requiera o las partes acuerden la existencia de una Firma en relación con un Mensaje de Datos, se entenderá satisfecho dicho requerimiento si se utiliza una Firma Electrónica que resulte apropiada para los fines para los cuales se generó o comunicó ese Mensaje de Datos.

La Firma Electrónica se considerará Avanzada o Fiable si cumple por lo menos los siguientes requisitos:

I. Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante;
II. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante;
III. Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y
IV. Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.

Lo dispuesto en el presente artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera la fiabilidad de una Firma Electrónica; o presente pruebas de que una Firma Electrónica no es fiable.

Artículo 98. Los Prestadores de Servicios de Certificación determinarán y harán del conocimiento de los usuarios si las Firmas Electrónicas Avanzadas o Fiables que les ofrecen cumplen o no los requerimientos dispuestos en las fracciones I a IV del artículo 97.

La determinación que se haga, con arreglo al párrafo anterior, deberá ser compatible con las normas y criterios internacionales reconocidos.

Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado.

Artículo 99. El Firmante deberá:

I. Cumplir las obligaciones derivadas del uso de la Firma Electrónica;
II. Actuar con diligencia y establecer los medios razonables para evitar la utilización no autorizada de los Datos de Creación de la Firma;
III. Cuando se emplee un Certificado en relación con una Firma Electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el Certificado, con su vigencia o que hayan sido consignadas en el mismo son exactas.
El Firmante será responsable de las consecuencias jurídicas que deriven por no cumplir oportunamente las obligaciones previstas en el presente artículo, y
IV. Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el Destinatario conociere de la inseguridad de la Firma Electrónica o no hubiere actuado con la debida diligencia.

Capítulo III: de los prestadores de servicios de certificación

Artículo 100. Podrán ser Prestadores de Servicios de Certificación, previa acreditación ante la Secretaría:

I. Los notarios públicos y corredores públicos;
II. Las personas morales de carácter privado, y
III. Las instituciones públicas, conforme a las leyes que les son aplicables.

La facultad de expedir Certificados no conlleva fe pública por sí misma; así, los Notarios y Corredores Públicos podrán llevar a cabo certificaciones que impliquen o no la fe pública, en documentos en papel, archivos electrónicos, o en cualquier otro medio o sustancia en el que pueda incluirse información.

Artículo 101. Los Prestadores de Servicios de Certificación a los que se refiere la fracción II del artículo anterior contendrán en su objeto social las actividades siguientes:

I. Verificar la identidad de los usuarios y su vinculación con los medios de identificación electrónica;
II. Comprobar la integridad y suficiencia del Mensaje de Datos del solicitante y verificar la Firma Electrónica de quien realiza la verificación;
III. Llevar a cabo registros de los elementos de identificación de los Firmantes y de aquella información con la que haya verificado el cumplimiento de fiabilidad de las firmas electrónicas avanzadas y emitir el Certificado, y
IV. Cualquier otra actividad no incompatible con las anteriores.

Artículo 102. Los prestadores de servicios de certificación que hayan obtenido la acreditación de la Secretaría deberán notificar a ésta la iniciación de la prestación de servicios de certificación dentro de los 45 días naturales siguientes al comienzo de dicha actividad.

A) Para que las personas indicadas en el artículo 100 puedan ser prestadores de servicios de certificación, se requiere acreditación de la Secretaría, la cual no podrá ser negada si el solicitante cumple los siguientes requisitos, en el entendido de que la Secretaría podrá requerir a los prestadores de servicios de certificación que comprueben la subsistencia del cumplimento de los mismos:

I. Solicitar a la Secretaría la acreditación como Prestador de Servicios de Certificación;
II. Contar con los elementos humanos, materiales, económicos y tecnológicos requeridos para prestar el servicio, a efecto de garantizar la seguridad de la información y su confidencialidad;
III. Contar con procedimientos definidos y específicos para la tramitación del Certificado, y con medidas que garanticen la seriedad de los Certificados emitidos, la conservación y consulta de los registros;
IV. Quienes operen o tengan acceso a los sistemas de certificación de los Prestadores de Servicios de Certificación no podrán haber sido condenados por delito contra el patrimonio de las personas o que haya merecido pena privativa de la libertad, ni que por cualquier motivo hayan sido inhabilitados para el ejercicio de su profesión, para desempeñar un puesto en el servicio público, en el sistema financiero o para ejercer el comercio;

V. Contar con fianza vigente por el monto y condiciones que se determinen en forma general en las reglas generales que al efecto se expidan por la Secretaría;
VI. Establecer por escrito su conformidad para ser sujeto a Auditoría por parte de la Secretaría, y
VII. Registrar su Certificado ante la Secretaría.

B) Si la Secretaría no ha resuelto respecto a la petición del solicitante, para ser acreditado conforme al artículo 100 anterior, dentro de los 45 días siguientes a la presentación de la solicitud, se tendrá por concedida la acreditación.

Artículo 103. Las responsabilidades de las Entidades Prestadoras de Servicios de Certificación deberán estipularse en el contrato con los firmantes.

Artículo 104. Los Prestadores de Servicios de Certificación deben cumplir las siguientes obligaciones:

I. Comprobar por sí o por medio de una persona física o moral que actúe en nombre y por cuenta suyos la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de los Certificados, utilizando cualquiera de los medios admitidos en derecho, siempre y cuando sean previamente notificados al solicitante;
II. Poner a disposición del Firmante los dispositivos de generación de los Datos de Creación y de verificación de la Firma Electrónica;
III. Informar, antes de la emisión de un Certificado, a la persona que solicite sus servicios de su precio, de las condiciones precisas para la utilización del Certificado, de sus limitaciones de uso y, en su caso, de la forma en que garantiza su posible responsabilidad;
IV. Mantener un registro de Certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión, pérdida o terminación de vigencia de sus efectos. A dicho registro podrá accederse por medios electrónicos, ópticos o de cualquier otra tecnología y su contenido público estará a disposición de las personas que lo soliciten. El contenido privado estará a disposición del Destinatario y de las personas que lo soliciten cuando así lo autorice el Firmante, así como en los casos a que se refieran las reglas generales que al efecto establezca la Secretaría;
V. Guardar confidencialidad respecto a la información que haya recibido para la prestación del servicio de certificación;
VI. En el caso de cesar en su actividad, los prestadores de servicios de certificación deberán comunicarlo a la Secretaría a fin de determinar, conforme a lo establecido en las reglas generales expedidas, el destino que se dará a sus registros y archivos;
VII. Asegurar las medidas para evitar la alteración de los Certificados y mantener la confidencialidad de los datos en el proceso de generación de los Datos de Creación de la Firma Electrónica;
VIII. Establecer declaraciones sobre sus normas y prácticas, las cuales harán del conocimiento del usuario y el Destinatario, y
IX. Proporcionar medios de acceso que permitan a la Parte que Confía en el Certificado determinar:

a) La identidad del Prestador de Servicios de Certificación;
b) Que el Firmante nombrado en el Certificado tenía bajo su control el dispositivo y los Datos de Creación de la Firma en el momento en que se expidió el Certificado;
c) Que los Datos de Creación de la Firma eran válidos en la fecha en que se expidió el Certificado;
d) El método utilizado para identificar al Firmante;
e) Cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los Datos de Creación de la Firma o el Certificado;
f) Cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el Prestador de Servicios de Certificación;
g) Si existe un medio para que el Firmante dé aviso al Prestador de Servicios de Certificación de que los Datos de Creación de la Firma han sido de alguna manera controvertidos, y
h) Si se ofrece un servicio de terminación de vigencia del Certificado.

Artículo 105. La Secretaría coordinará y actuará como autoridad Certificadora y registradora respecto de los Prestadores de Servicios de Certificación, previstos en este Capítulo.

Artículo 106. Para la prestación de servicios de certificación, las instituciones financieras y las empresas que les prestan servicios auxiliares o complementarios relacionados con transferencias de fondos o valores se sujetarán a las leyes que las regulan, así como a las disposiciones y autorizaciones que emitan las autoridades financieras.

Artículo 107. Serán responsabilidad del Destinatario y de la Parte que Confía, en su caso, las consecuencias jurídicas que entrañe el hecho de que no hayan tomado medidas razonables para:

I. Verificar la fiabilidad de la Firma Electrónica, o
II. Cuando la Firma Electrónica esté sustentada por un Certificado:

a) Verificar, incluso en forma inmediata, la validez, suspensión o revocación del Certificado, y
b) Tener en cuenta cualquier limitación de uso contenida en el Certificado.

Artículo 108. Los Certificados, para ser considerados válidos, deberán contener:

I. La indicación de que se expiden como tales;
II. El código de identificación único del Certificado;
III. La identificación del Prestador de Servicios de Certificación que expide el Certificado, razón social, su domicilio, dirección de correo electrónico, en su caso, y los datos de acreditación ante la Secretaría;
IV. Nombre del titular del Certificado;
V. Periodo de vigencia del Certificado;
VI. La fecha y hora de la emisión, suspensión y renovación del Certificado;
VII. El alcance de las responsabilidades que asume el Prestador de Servicios de Certificación, y

VIII. La referencia de la tecnología empleada para la creación de la Firma Electrónica.

Artículo 109. Un Certificado dejará de surtir efectos para el futuro en los siguientes casos:

I. Expiración del periodo de vigencia del Certificado, el cual no podrá ser superior a dos años, contados a partir de la fecha en que se hubieren expedido. Antes de que concluya el periodo de vigencia del Certificado, podrá el Firmante renovarlo ante el Prestador de Servicios de Certificación;
II. Revocación por el Prestador de Servicios de Certificación, a solicitud del Firmante, o por la persona física o moral representada por éste o por un tercero autorizado;
III. Pérdida o inutilización por daños del dispositivo en el que se contenga dicho Certificado;
IV. Por haberse comprobado que al momento de su expedición, el Certificado no cumplió con los requisitos establecidos en la Ley, situación que no afectará los derechos de terceros de buena fe, y
V. Resolución judicial o de autoridad competente que lo ordene.

Artículo 110. El Prestador de Servicios de Certificación que incumpla con las obligaciones que se le imponen en el presente Capítulo, previa garantía de audiencia y mediante resolución debidamente fundada y motivada, tomando en cuenta la gravedad de la situación y reincidencia, podrá ser sancionado por la Secretaría con suspensión temporal o definitiva de sus funciones. Este procedimiento tendrá lugar conforme a la Ley Federal de Procedimiento Administrativo.

Artículo 111. Las sanciones que se señalan en este Capítulo se aplicarán sin perjuicio de la responsabilidad civil o penal y de las penas que correspondan a los delitos en que, en su caso, incurran los infractores.

Artículo 112. Las autoridades competentes harán uso de las medidas legales necesarias, incluyendo el auxilio de la fuerza pública, para lograr la ejecución de las sanciones y medidas de seguridad que procedan conforme a esta Ley. Incluso, en los procedimientos instaurados se podrá solicitar a los órganos competentes la adopción de las medidas cautelares que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte.

Artículo 113. En el caso de que un Prestador de Servicios de Certificación sea suspendido, inhabilitado o cancelado en su ejercicio, el registro y los Certificados que haya expedido pasarán, para su administración, a otro Prestador de Servicios de Certificación que para tal efecto señale la Secretaría mediante reglas generales.

Capítulo IV: reconocimiento de certificados y firmas electrónicas extranjeros

Artículo 114. Para determinar si un Certificado o una Firma Electrónica extranjeros producen efectos jurídicos o en qué medida los producen, no se tomará en consideración cualquiera de los siguientes supuestos:

I. El lugar en que se haya expedido el Certificado o en que se haya creado o utilizado la Firma Electrónica, y
II. El lugar en que se encuentre el establecimiento del prestador de servicios de certificación o del Firmante.

Todo Certificado expedido fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma que un Certificado expedido en la República Mexicana si presenta un grado de fiabilidad equivalente a los contemplados por este Título.

Toda Firma Electrónica creada o utilizada fuera de la República Mexicana producirá los mismos efectos jurídicos en la misma que una Firma Electrónica creada o utilizada en la República Mexicana si presenta un grado de fiabilidad equivalente.

A efecto de determinar si un Certificado o una Firma Electrónica presentan un grado de fiabilidad equivalente para los fines de los dos párrafos anteriores, se tomarán en consideración las normas internacionales reconocidas por México y cualquier otro medio de convicción pertinente.

Cuando, sin perjuicio de lo dispuesto en los párrafos anteriores, las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y Certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

Anexo VII

Ley Orgánica de Protección de Datos de Carácter Personal (España)

(Publicada en el* BOE *el 13 de diciembre de 1999)

Título I

Disposiciones generales

Artículo 1. Objeto.

La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar.

Artículo 2. Ámbito de aplicación.

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

   Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

   a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
   b) Cuando al responsable del tratamiento no establecido en territorio español le sea de aplicación la legislación española en aplicación de normas de Derecho internacional público.
   c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

   a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
   b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
   c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

3. Se regirán por sus disposiciones específicas y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

   a) Los ficheros regulados por la legislación de régimen electoral.
   b) Los que sirvan a fines exclusivamente estadísticos y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.
   c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.
   d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes.
   e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

Artículo 3. Definiciones.

A los efectos de la presente Ley Orgánica se entenderá por:

a) *Datos de carácter personal*: cualquier información concerniente a personas físicas identificadas o identificables.
b) *Fichero*: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
c) *Tratamiento de datos*: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
d) *Responsable del fichero o tratamiento*: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
e) *Afectado o interesado*: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado *c*) del presente artículo.

f) *Procedimiento de disociación*: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) *Encargado del tratamiento*: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

h) *Consentimiento del interesado*: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) *Cesión o comunicación de datos*: toda revelación de datos realizada a una persona distinta del interesado.

j) *Fuentes accesibles al público*: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencias que, en su caso, el abono de una contraprestación. Tienen consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

Título II

Principios de la protección de datos

Artículo 4. Calidad de los datos.

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.
3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan como veracidad a la situación actual del afectado.
4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.
5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.
7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Artículo 5. Derecho a información en la recogida de datos.

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

   a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
   b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
   c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
   d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
   e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

   Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.
3. No será necesaria la información a que se refieren las letras *b*), *c*) y *d*) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras *a*), *d*) y *e*) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o de organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

   Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

Artículo 6. Consentimiento del afectado.

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.
2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.
3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.
4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

Artículo 7. Datos especialmente protegidos.

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.
2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades

religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.
4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.
5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.
6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

   También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 8. Datos relativos a la salud.

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Artículo 9. Seguridad de los datos.

1. El responsable del fichero y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana del medio físico o natural.
2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10. Deber de secreto.

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 11. Comunicación de datos.

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.
2. El consentimiento exigido en el apartado anterior no será preciso:

   a) Cuando la cesión está autorizada en una ley.
   b) Cuando se trate de datos recogidos de fuentes accesibles al público.
   c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente concesión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
   d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
   e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos y científicos.
   f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilita al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.
4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.
5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Artículo 12. Acceso a los datos por cuenta de terceros.

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.
2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con el fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

   En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.
3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser distribuidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.
4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

Título III

Derechos de las personas

Artículo 13. Impugnación de valoraciones.

1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.
2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.
3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.
4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 14. Derecho de consulta al Registro General de Protección de Datos.

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Artículo 15. Derecho de acceso.

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.
2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible o inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.
3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

Artículo 16. Derecho de rectificación y cancelación.

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.
2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.
3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.
4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.
5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Artículo 17. Procedimiento de oposición, acceso, rectificación o cancelación.

1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.
2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

Artículo 18. Tutela de los derechos.

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.
2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.
3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.
4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

Artículo 19. Derecho a indemnización.

1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.
2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.
3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

Título IV

Disposiciones sectoriales

Capítulo I

Ficheros de titularidad pública

Artículo 20. Creación, modificación o supresión.

1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el *Boletín Oficial del Estado* o *Diario Oficial* correspondiente.
2. Las disposiciones de creación o de modificación de ficheros deberán indicar:

   a) La finalidad del fichero y los usos previstos para el mismo.
   b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
   c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
f) Los órganos de las Administraciones responsables del fichero.
g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

3. En las disposiciones que se dicten para la supresión de los ficheros se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

Artículo 21. Comunicación de datos entre Administraciones públicas.

1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.
3. No obstante lo establecido en el artículo 11.2 *b*), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.
4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

Artículo 22. Ficheros de las Fuerzas y Cuerpos de Seguridad.

1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.
2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.
4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.
A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 23. Excepciones a los derechos de acceso, rectificación y cancelación.

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.
2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.
3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Artículo 24. Otras excepciones a los derechos de los afectados.

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.
2. Lo dispuesto en el artículo 15 y en el apartado 1 del artículo 16 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección.

Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.

Capítulo II

Ficheros de titularidad privada

Artículo 25. Creación.

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 26. Notificación e inscripción registral.

1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.
2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que deba contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.
3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.
4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.
   En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.
5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

Artículo 27. Comunicación de la cesión de datos.

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.
2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras *c*), *d*), *e*) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.

Artículo 28. Datos incluidos en las fuentes de acceso público.

1. Los datos personales que figuren en el censo promocional o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3 *j*) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.
2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial.

   Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes.

   La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado, cualquiera que sea el soporte en que se edite.
3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico perderán el carácter de fuente accesible con la nueva edición que se publique.

   En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.
4. Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica.

Artículo 29. Prestación de servicios de información sobre solvencia patrimonial y crédito.

1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.
2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.
3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos,

así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos.

Artículo 30. Tratamientos con fines de publicidad y de prospección comercial.

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.
2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.
3. En el ejercicio del derecho de acceso, los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.
4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél a su simple solicitud.

Artículo 31. Censo promocional.

1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de dirección, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.
2. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público.
3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilio de los que así lo hayan solicitado.
4. Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático.

Artículo 32. Códigos tipo.

1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupan podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.
2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.
   En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.
3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

Título V

Movimiento internacional de datos

Artículo 33. Norma general.

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.
2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes

de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. Excepciones.
Lo dispuesto en el artículo anterior no será de aplicación:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios.
d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.
e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.
h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.
k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

Título VI

Agencia de Protección de Datos

Artículo 35. Naturaleza y régimen jurídico.

1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus

funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.

2. En el ejercicio de sus funciones públicas y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la *Ley 30/1992*, de 26 de noviembre, *de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común*. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.
3. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.
4. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

   a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.
   b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.
   c) Cualesquiera otros que legalmente puedan serle atribuidos.

5. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Artículo 36. El Director.

1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un periodo de cuatro años.
2. Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas.
   En todo caso, el Director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.
3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del periodo a que se refiere el apartado 1, a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.
4. El Director de la Agencia de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para el cargo algún miembro de la carrera judicial o fiscal, pasará asimismo a la situación administrativa de servicios especiales.

Artículo 37. Funciones.

Son funciones de la Agencia de Protección de Datos:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.
c) Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.
d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.
e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.
f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.
g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.
h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.
i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.
j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.
k) Redactar una memoria anual y remitirla al Ministerio de Justicia.
l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.
m) Velar por el cumplimiento de las disposiciones que la *Ley de la Función Estadística Pública* establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.
n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

Artículo 38. Consejo Consultivo.

El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:

Un Diputado, propuesto por el Congreso de los Diputados.

Un Senador, propuesto por el Senado.

Un representante de la Administración Central, designado por el Gobierno.

Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.

Un miembro de la Real Academia de la Historia, propuesto por la misma.

Un experto en la materia, propuesto por el Consejo Superior de Universidades.

Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.

Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma.

Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.

El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 39. El Registro General de Protección de Datos.

1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.
2. Serán objeto de inscripción en el Registro General de Protección de Datos:

   a) Los ficheros de que sean titulares las Administraciones públicas.
   b) Los ficheros de titularidad privada.
   c) Las autorizaciones a que se refiere la presente Ley.
   d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley.
   e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Artículo 40. Potestad de inspección.

1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.

   A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.
2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

   Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 41. Órganos correspondientes de las Comunidades Autónomas.

1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados *j*), *k*) y *l*) y en los apartados *f*) y *g*) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49 en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido.
2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.
3. El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

Artículo 42. Ficheros de las Comunidades Autónomas en materia de su exclusiva competencia.

1. Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia, podrá requerir a la Administración correspondiente que se adopten las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento.
2. Si la Administración pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

Título VII

Infracciones y sanciones

Artículo 43. Responsables.

1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.
2. Cuando se trate de ficheros de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 46, apartado 2.

Artículo 44. Tipos de infracciones.

1. Las infracciones se calificarán como leves, graves o muy graves.
2. Son infracciones leves:

   a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.
   b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.
   c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.
   d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.
   e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

3. Son infracciones graves:

   a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el Boletín Oficial del Estado o Diario Oficial correspondiente.
   b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.
   c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.
   d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituye infracción muy grave.
   e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.
   f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.
   g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y

crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora.

k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

4. Son infracciones muy graves:

a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Artículo 45. Tipo de sanciones.

1. Las infracciones leves serán sancionadas con multa de 100 000 a 10 000 000 de pesetas.
2. Las infracciones graves serán sancionadas con multa de 10 000 000 a 50 000 000 de pesetas.
3. Las infracciones muy graves serán sancionadas con multa de 50 000 000 a 100 000 000 de pesetas.
4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.
5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.
6. En ningún caso podrá imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.
7. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 46. Infracciones de las Administraciones públicas.

1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las Administraciones públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.
2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas.
3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.
4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

Artículo 47. Prescripción.

1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.
3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.
4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.
5. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción.
6. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 48. Procedimiento sancionador.

1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título.
2. Las resoluciones de la Agencia de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa.

Artículo 49. Potestad de inmovilización de ficheros.

En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

Anexo VIII

Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal de España

*(*BOE *19 de enero de 2008)*

Título I

Disposiciones generales

Artículo 1. Objeto.

1. El presente reglamento tiene por objeto el desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
2. Asimismo, el capítulo III del título IX de este reglamento desarrolla las disposiciones relativas al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora, en aplicación de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, en el título VII de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, y en el título VIII de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 2. Ámbito objetivo de aplicación.

1. El presente reglamento será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.
2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.
4. Este reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

Artículo 3. Ámbito territorial de aplicación.

1. Se regirá por el presente reglamento todo tratamiento de datos de carácter personal:

   a) Cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que dicho establecimiento se encuentre ubicado en territorio español.
   Cuando no resulte de aplicación lo dispuesto en el párrafo anterior, pero exista un encargado del tratamiento ubicado en España, serán de aplicación al mismo las normas contenidas en el título VIII del presente reglamento.
   b) Cuando al responsable del tratamiento no establecido en territorio español le sea de aplicación la legislación española, según las normas de derecho internacional público.
   c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.
   En este supuesto, el responsable del tratamiento deberá designar un representante establecido en territorio español.

2. A los efectos previstos en los apartados anteriores, se entenderá por establecimiento, con independencia de su forma jurídica, cualquier instalación estable que permita el ejercicio efectivo y real de una actividad.

Artículo 4. Ficheros o tratamientos excluidos.

El régimen de protección de los datos de carácter personal que se establece en el presente reglamento no será de aplicación a los siguientes ficheros y tratamientos:

   a) A los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
   Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares.
   b) A los sometidos a la normativa sobre protección de materias clasificadas.

c) A los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

Artículo 5. Definiciones.

1. A los efectos previstos en este reglamento, se entenderá por:

a) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento.

b) Cancelación: procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo, deberá procederse a la supresión de los datos.

c) Cesión o comunicación de datos: tratamiento de datos que supone su revelación a una persona distinta del interesado.

d) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

e) Dato disociado: aquel que no permite la identificación de un afectado o interesado.

f) Datos de carácter personal: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

g) Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

h) Destinatario o cesionario: la persona física o jurídica, pública o privada u órgano administrativo al que se revelen los datos.
Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

i) Encargado del tratamiento: la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.
Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

j) Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que reali-

ce, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.

k) Fichero: todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

l) Ficheros de titularidad privada: los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

m) Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público, siempre que su finalidad sea el ejercicio de potestades de derecho público.

n) Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

ñ) Importador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

o) Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

p) Procedimiento de disociación: todo tratamiento de datos personales que permita la obtención de datos disociados.

q) Responsable del fichero o del tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

r) Tercero: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las

personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.
Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

s) Transferencia internacional de datos: tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

t) Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

2. En particular, en relación con lo dispuesto en el título VIII de este reglamento se entenderá por:

a) Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

b) Autenticación: procedimiento de comprobación de la identidad de un usuario.

c) Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

d) Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

e) Copia de respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

f) Documento: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

g) Ficheros temporales: ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

h) Identificación: procedimiento de reconocimiento de la identidad de un usuario.

i) Incidencia: cualquier anomalía que afecte o pudiera afectar la seguridad de los datos.

j) Perfil de usuario: accesos autorizados a un grupo de usuarios.

k) Recurso: cualquier parte componente de un sistema de información.

l) Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

m) Sistema de información: conjunto de ficheros, tratamientos, programas, soportes y, en su caso, equipos empleados para el tratamiento de datos de carácter personal.

n) Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

ñ) Soporte: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

o) Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

p) Usuario: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

Artículo 6. Cómputo de plazos.

En los supuestos en que este reglamento señale un plazo por días se computarán únicamente los hábiles. Cuando el plazo sea por meses, se computarán de fecha a fecha.

Artículo 7. Fuentes accesibles al público.

1. A efectos del artículo 3, párrafo j, de la Ley Orgánica 15/1999, se entenderá que sólo tendrán el carácter de fuentes accesibles al público:

   a) El censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.

   b) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica.

   c) Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.

   d) Los diarios y boletines oficiales.

   e) Los medios de comunicación social.

2. En todo caso, para que los supuestos enumerados en el apartado anterior puedan ser considerados fuentes accesibles al público, será preciso que su consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

Título II

Principios de protección de datos

Capítulo I

Calidad de los datos

Artículo 8. Principios relativos a la calidad de los datos.

1. Los datos de carácter personal deberán ser tratados de forma leal y lícita. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.
2. Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento.
3. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.
4. Sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
5. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.

   Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello.

   Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.

   En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviera el tratamiento de los datos deberá proceder a la rectificación y cancelación notificada.

   Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

   Lo dispuesto en este apartado se entiende sin perjuicio de las facultades que a los afectados reconoce el título III de este reglamento.
6. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Una vez cumplido el periodo al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

7. Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación.

Artículo 9. Tratamiento con fines estadísticos, históricos o científicos.

1. No se considerará incompatible, a los efectos previstos en el apartado 3 del artículo anterior, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos.

   Para la determinación de los fines a los que se refiere el párrafo anterior se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, Reguladora de la función estadística pública, la Ley 16/1985, de 25 junio, del Patrimonio histórico español y la Ley 13/1986, de 14 de abril de Fomento y coordinación general de la investigación científica y técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.

2. Por vía de excepción a lo dispuesto en el apartado 6 del artículo anterior, la Agencia Española de Protección de Datos o, en su caso, las autoridades de control de las comunidades autónomas podrán, previa solicitud del responsable del tratamiento y conforme al procedimiento establecido en la sección segunda del capítulo VII del título IX del presente reglamento, acordar el mantenimiento íntegro de determinados datos, atendidos sus valores históricos, estadísticos o científicos de acuerdo con las normas a las que se refiere el apartado anterior.

Artículo 10. Supuestos que legitiman el tratamiento o cesión de los datos.

1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello.
2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando:

   a) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes: El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezcan el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.

El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

b) Los datos objeto de tratamiento o de cesión figuren en fuentes accesibles al público y el responsable del fichero, o el tercero a quien se comuniquen los datos, tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

No obstante, las Administraciones públicas sólo podrán comunicar al amparo de este apartado los datos recogidos de fuentes accesibles al público a responsables de ficheros de titularidad privada cuando se encuentren autorizadas para ello por una norma con rango de ley.

3. Los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando:

a) Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario.

b) Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.

c) El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre.

4. Será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando:

a) La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso, la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

b) La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, al Ministerio Fiscal o a los Jueces o Tribunales o al Tribunal de Cuentas o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente.

c) La cesión entre Administraciones públicas cuando concurra uno de los siguientes supuestos:

- Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.
- Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.
- La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

5. Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre. En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

Artículo 11. Verificación de datos en solicitudes formuladas a las Administraciones públicas.

Cuando se formulen solicitudes por medios electrónicos en las que el interesado declare datos personales que obren en poder de las Administraciones públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la autenticidad de los datos.

Capítulo II

Consentimiento para el tratamiento de los datos y deber de información

Sección I. Obtención del consentimiento del afectado

Artículo 12. Principios generales.

1. El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal, salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes. La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.
2. Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.
3. Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.

Artículo 13. Consentimiento para el tratamiento de datos de menores de edad.

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En

el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.
3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.
4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso por los padres, tutores o representantes legales.

Artículo 14. Forma de recabar el consentimiento.

1. El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este artículo, salvo cuando la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos.
2. El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este reglamento y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.

   En particular, cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada o facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de modo claramente visible.
3. En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.
4. Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerarán ajustados al presente reglamento los procedimientos en los que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento, o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.
5. Cuando se solicite el consentimiento del interesado a través del procedimiento establecido en este artículo, no será posible solicitarlo nuevamente respec-

to de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

Artículo 15. Solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma.

Si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos.

En particular, se entenderá cumplido tal deber cuando se permita al afectado la marcación de una casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento.

Artículo 16. Tratamiento de datos de facturación y tráfico en servicios de comunicaciones electrónicas.

La solicitud del consentimiento para el tratamiento o cesión de los datos de tráfico, facturación y localización por parte de los sujetos obligados, o en su caso la revocación de aquél, según la legislación reguladora de las telecomunicaciones se someterá a lo establecido en su normativa específica y, en lo que no resulte contrario a la misma, a lo establecido en la presente sección.

Artículo 17. Revocación del consentimiento.

1. El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. En particular, se considerará ajustado al presente reglamento el procedimiento en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

   No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado.
2. El responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre.
3. Cuando el interesado hubiera solicitado del responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, éste deberá responder expresamente a la solicitud.
4. Si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios, en el plazo previsto en el apartado 2, para que éstos cesen en el tratamiento de los datos en caso de que aún lo mantuvieran, conforme al artículo 16.4 de la Ley Orgánica 15/1999, de 13 de diciembre.

Sección II. Deber de información al interesado

Artículo 18. Acreditación del cumplimiento del deber de información.

1. El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.
2. El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte de papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales.

Artículo 19. Supuestos especiales.

En los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre.

Capítulo III

Encargado del tratamiento

Artículo 20. Relaciones entre el responsable y el encargado del tratamiento.

1. El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente capítulo.

   El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

   No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.
2. Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo, deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.
3. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999,

de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.

Artículo 21. Posibilidad de subcontratación de los servicios.

1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.
2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización, siempre y cuando se cumplan los siguientes requisitos:

   a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

   Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

   b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

   c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.

   En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento.

3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior.

Artículo 22. Conservación de los datos por el encargado del tratamiento.

1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

   No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos, garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

Título III

Derechos de acceso, rectificación, cancelación y oposición

Capítulo I

Disposiciones generales

Artículo 23. Carácter personalísimo.

1. Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado.
2. Tales derechos se ejercitarán:

   a) Por el afectado, acreditando su identidad, del modo previsto en el artículo siguiente.
   b) Cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal, en cuyo caso será necesario que acredite tal condición.
   c) Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad del representado, mediante la aportación de copia de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquél.

   Cuando el responsable del fichero sea un órgano de las Administraciones públicas o de la Administración de Justicia, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado.
3. Los derechos serán denegados cuando la solicitud sea formulada por persona distinta del afectado y no se acreditase que la misma actúa en representación de aquél.

Artículo 24. Condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

1. Los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.
2. Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

3. El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

   No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.
4. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, podrá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la prestación de sus servicios o contratación de sus productos.
5. El responsable del fichero o tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado, aun cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud y que ésta contenga los elementos referidos en el párrafo 1 del artículo siguiente.

Artículo 25. Procedimiento.

1. Salvo en el supuesto referido en el párrafo 4 del artículo anterior, el ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero, que contendrá:

   a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.

   El párrafo anterior se entenderá sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos.

   b) Petición en que se concreta la solicitud.

   c) Dirección a efectos de notificaciones, fecha y firma del solicitante.

   d) Documentos acreditativos de la petición que formula, en su caso.

2. El responsable del tratamiento deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros.

3. En el caso de que la solicitud no reúna los requisitos especificados en el apartado primero, el responsable del fichero deberá solicitar la subsanación de los mismos.
4. La respuesta deberá ser conforme con los requisitos previstos para cada caso en el presente título.
5. Corresponderá al responsable del tratamiento la prueba del cumplimiento del deber de respuesta al que se refiere el apartado 2, debiendo conservar la acreditación del cumplimiento del mencionado deber.
6. El responsable del fichero deberá adoptar las medidas oportunas para garantizar que las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.
7. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición podrá modularse por razones de seguridad pública en los casos y con el alcance previsto en las leyes.
8. Cuando las leyes aplicables a determinados ficheros concretos establezcan un procedimiento especial para la rectificación o cancelación de los datos contenidos en los mismos, se estará a lo dispuesto en aquéllas.

Artículo 26. Ejercicio de los derechos ante un encargado del tratamiento.

Cuando los afectados ejercitasen sus derechos ante un encargado del tratamiento y solicitasen el ejercicio de su derecho ante el mismo, el encargado deberá dar traslado de la solicitud al responsable, a fin de que por el mismo se resuelva, a menos que en la relación existente con el responsable del tratamiento se prevea precisamente que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición.

Capítulo II

Derecho de acceso

Artículo 27. Derecho de acceso.

1. El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.
2. En virtud del derecho de acceso, el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento. No obstante, cuando razones de especial complejidad lo justifiquen, el responsable del fichero podrá solicitar del afectado la especificación de los ficheros respecto de los cuales quiera ejercitar el derecho de acceso, a cuyo efecto deberá facilitarle una relación de todos ellos.

3. El derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 28. Ejercicio del derecho de acceso.

1. Al ejercitar el derecho de acceso, el afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero:

   a) Visualización en pantalla.
   b) Escrito, copia o fotocopia remitida por correo, certificado o no.
   c) Telecopia.
   d) Correo electrónico u otros sistemas de comunicaciones electrónicas.
   e) Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

2. Los sistemas de consulta del fichero previstos en el apartado anterior podrán restringirse en función de la configuración o implantación material del fichero o de la naturaleza del tratamiento, siempre que el que se ofrezca al afectado sea gratuito y asegure la comunicación escrita si éste así lo exige.
3. El responsable del fichero deberá cumplir al facilitar el acceso lo establecido en el Título VIII de este Reglamento.

   Si tal responsable ofreciera un determinado sistema para hacer efectivo el derecho de acceso y el afectado lo rechazase, aquél no responderá por los posibles riesgos que para la seguridad de la información pudieran derivarse de la elección.

   Del mismo modo, si el responsable ofreciera un procedimiento para hacer efectivo el derecho de acceso y el afectado exigiese que el mismo se materializase a través de un procedimiento que implique un coste desproporcionado, surtiendo el mismo efecto y garantizando la misma seguridad el procedimiento ofrecido por el responsable, serán de cuenta del afectado los gastos derivados de su elección.

Artículo 29. Otorgamiento del acceso.

1. El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

   En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.
2. Si la solicitud fuera estimada y el responsable no acompañase a su comunicación la información a la que se refiere el artículo 27.1, el acceso se hará efectivo durante los diez días siguientes a dicha comunicación.

3. La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

Dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

Artículo 30. Denegación del acceso.

1. El responsable del fichero o tratamiento podrá denegar el acceso a los datos de carácter personal cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto.
2. Podrá también denegarse el acceso en los supuestos en que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.
3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

Capítulo III

Derechos de rectificación y cancelación

Artículo 31. Derechos de rectificación y cancelación.

1. El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.
2. El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento.

En los supuestos en que el interesado invoque el ejercicio del derecho de cancelación para revocar el consentimiento previamente prestado, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente reglamento.

Artículo 32. Ejercicio de los derechos de rectificación y cancelación.

1. La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.

En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso.
2. El responsable del fichero resolverá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la

solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de carácter personal del afectado, deberá igualmente comunicárselo en el mismo plazo.

3. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a rectificar o cancelar los datos.

La rectificación o cancelación efectuada por el cesionario no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 33. Denegación de los derechos de rectificación y cancelación.

1. La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.
2. Podrán también denegarse los derechos de rectificación o cancelación en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.
3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

Capítulo IV

Derecho de oposición

Artículo 34. Derecho de oposición.

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el

artículo 51 de este reglamento, cualquiera que sea la empresa responsable de su creación.

c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este reglamento.

Artículo 35. Ejercicio del derecho de oposición.

1. El derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento.

   Cuando la oposición se realice con base en la letra *a*) del artículo anterior, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.
2. El responsable del fichero resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

   En el caso de que no disponga de datos de carácter personal de los afectados, deberá igualmente comunicárselo en el mismo plazo.
3. El responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo previsto en el apartado 2 de este artículo.

Artículo 36. Derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos.

1. Los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.
2. No obstante, los afectados podrán verse sometidos a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

   a) Se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés. En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas en el apartado 1 y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.
   b) Esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

Título IV

Disposiciones aplicables a determinados ficheros de titularidad privada

Capítulo I

Ficheros de información sobre solvencia patrimonial y crédito

Sección 1. Disposiciones generales

Artículo 37. Régimen aplicable.

1. El tratamiento de datos de carácter personal sobre solvencia patrimonial y crédito, previsto en el apartado 1 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, se someterá a lo establecido, con carácter general, en dicha ley orgánica y en el presente reglamento.
2. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición en el caso de los ficheros a que se refiere el apartado anterior se rige por lo dispuesto en los capítulos I a IV del título III del presente reglamento, con los siguientes criterios:

   a) Cuando la petición de ejercicio de los derechos se dirigiera al responsable del fichero, éste estará obligado a satisfacer, en cualquier caso, dichos derechos.

   b) Si la petición se dirigiera a las personas y entidades a las que se presta el servicio, éstas únicamente deberán comunicar al afectado aquellos datos relativos al mismo que les hayan sido comunicados y a facilitar la identidad del responsable para que, en su caso, puedan ejercitar sus derechos ante el mismo.
3. De conformidad con el apartado 2 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, también podrán tratarse los datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés.

   Estos datos deberán conservarse en ficheros creados con la exclusiva finalidad de facilitar información crediticia del afectado y su tratamiento se regirá por lo dispuesto en el presente reglamento y, en particular, por las previsiones contenidas en la sección segunda de este capítulo.

Sección II. Tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés

Artículo 38. Requisitos para la inclusión de los datos.

1. Sólo será posible la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, siempre que concurran los siguientes requisitos:

a) Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o, tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero.

b) Que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

c) Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación.

2. No podrán incluirse en los ficheros de esta naturaleza datos personales sobre los que exista un principio de prueba que de forma indiciaria contradiga alguno de los requisitos anteriores.

   Tal circunstancia determinará asimismo la cancelación cautelar del dato personal desfavorable en los supuestos en que ya se hubiera efectuado su inclusión en el fichero.

3. El acreedor o quien actúe por su cuenta o interés estará obligado a conservar a disposición del responsable del fichero común y de la Agencia Española de Protección de Datos documentación suficiente que acredite el cumplimiento de los requisitos establecidos en este artículo y del requerimiento previo al que se refiere el artículo siguiente.

Artículo 39. Información previa a la inclusión.

El acreedor deberá informar al deudor, en el momento en que se celebre el contrato y, en todo caso, al tiempo de efectuar el requerimiento al que se refiere la letra *c* del apartado 1 del artículo anterior, que en caso de no producirse el pago en el término previsto para ello y cumplirse los requisitos previstos en el citado artículo, los datos relativos al impago podrán ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias.

Artículo 40. Notificación de inclusión.

1. El responsable del fichero común deberá notificar a los interesados respecto de los que hayan registrado datos de carácter personal, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos, informándole asimismo de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, en los términos establecidos por la Ley Orgánica 15/1999, de 13 de diciembre.
2. Se efectuará una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores.
3. La notificación deberá efectuarse a través de un medio fiable, auditable e independiente de la entidad notificante, que la permita acreditar la efectiva realización de los envíos.
4. En todo caso, será necesario que el responsable del fichero pueda conocer si la notificación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

No se entenderán suficientes para que no se pueda proceder al tratamiento de los datos referidos a un interesado las devoluciones en las que el destinatario haya rehusado recibir el envío.

5. Si la notificación de inclusión fuera devuelta, el responsable del fichero común comprobará con la entidad acreedora que la dirección utilizada para efectuar esta notificación corresponde a la contractualmente pactada con el cliente a efectos de comunicaciones y no procederá al tratamiento de los datos si la mencionada entidad no confirma la exactitud de este dato.

Artículo 41. Conservación de los datos.

1. Sólo podrán ser objeto de tratamiento los datos que respondan con veracidad a la situación de la deuda en cada momento concreto.

   El pago o cumplimiento de la deuda determinará la cancelación inmediata de todo dato relativo a la misma.
2. En los restantes supuestos, los datos deberán ser cancelados cuando se hubieran cumplido seis años contados a partir del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

Artículo 42. Acceso a la información contenida en el fichero.

1. Los datos contenidos en el fichero común sólo podrán ser consultados por terceros cuando precisen enjuiciar la solvencia económica del afectado. En particular, se considerará que concurre dicha circunstancia en los siguientes supuestos:

   a) Que el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida.
   b) Que el afectado pretenda celebrar con el tercero un contrato que implique el pago aplazado del precio.
   c) Que el afectado pretenda contratar con el tercero la prestación de un servicio de facturación periódica.

2. Los terceros deberán informar por escrito a las personas en las que concurran los supuestos contemplados en las letras *b* y *c* precedentes de su derecho a consultar el fichero.

   En los supuestos de contratación telefónica de los productos o servicios a los que se refiere el párrafo anterior, la información podrá realizarse de forma no escrita, correspondiendo al tercero la prueba del cumplimiento del deber de informar.

Artículo 43. Responsabilidad.

1. El acreedor o quien actúe por su cuenta o interés deberá asegurarse que concurren todos los requisitos exigidos en los artículos 38 y 39 en el momento de notificar los datos adversos al responsable del fichero común.
2. El acreedor o quien actúe por su cuenta o interés será responsable de la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión en

el fichero, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 44. Ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

1. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición se rige por lo dispuesto en los capítulos I a IV del título III de este reglamento, sin perjuicio de lo señalado en el presente artículo.
2. Cuando el interesado ejercite su derecho de acceso en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

    1. Si la solicitud se dirigiera al titular del fichero común, éste deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero.

        En este caso, el titular del fichero común deberá, además de dar cumplimiento a lo establecido en el presente reglamento, facilitar las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios.
    2. Si la solicitud se dirigiera a cualquier otra entidad participante en el sistema, deberá comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad y dirección del titular del fichero común para que pueda completar el ejercicio de su derecho de acceso.

3. Cuando el interesado ejercite sus derechos de rectificación o cancelación en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

    1. Si la solicitud se dirige al titular del fichero común, éste tomará las medidas oportunas para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte de la entidad en el plazo de siete días, procederá a la rectificación o cancelación cautelar de los mismos.
    2. Si la solicitud se dirige a quien haya facilitado los datos al fichero común, procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al titular del fichero común en el plazo de diez días, dando asimismo respuesta al interesado en los términos previstos en el artículo 33 de este reglamento.
    3. Si la solicitud se dirige a otra entidad participante en el sistema, que no hubiera facilitado al fichero común los datos, dicha entidad informará al afectado sobre este hecho en el plazo máximo de diez días, proporcionándole, además, la identidad y dirección del titular del fichero común para, que en su caso, puedan ejercitar sus derechos ante el mismo.

Capítulo II

Tratamientos para actividades de publicidad y prospección comercial

Artículo 45. Datos susceptibles de tratamiento e información al interesado.

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, así como quienes realicen estas actividades con el fin de comercializar sus propios productos o servicios o los de terceros, sólo podrán utilizar nombres y direcciones u otros datos de carácter personal cuando los mismos se encuentren en uno de los siguientes casos:

   a) Figuren en alguna de las fuentes accesibles al público a las que se refiere la letra j del artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, y el artículo 7 de este reglamento y el interesado no haya manifestado su negativa u oposición a que sus datos sean objeto de tratamiento para las actividades descritas en este apartado.
   b) Hayan sido facilitados por los propios interesados u obtenidos con su consentimiento para finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial, habiéndose informado a los interesados sobre los sectores específicos y concretos de actividad respecto de los que podrá recibir información o publicidad.

2. Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, deberá informarse al interesado en cada comunicación que se le dirija del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten, con indicación de ante quién podrán ejercitarse.

   A tal efecto, el interesado deberá ser informado de que sus datos han sido obtenidos de fuentes accesibles al público y de la entidad de la que hubieran sido obtenidos.

Artículo 46. Tratamiento de datos en campañas publicitarias.

1. Para que una entidad pueda realizar por sí misma una actividad publicitaria de sus productos o servicios entre sus clientes, será preciso que el tratamiento se ampare en alguno de los supuestos contemplados en el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre.
2. En caso de que una entidad contrate o encomiende a terceros la realización de una determinada campaña publicitaria de sus productos o servicios, encomendándole el tratamiento de determinados datos, se aplicarán las siguientes normas:

   a) Cuando los parámetros identificativos de los destinatarios de la campaña sean fijados por la entidad que contrate la campaña, ésta será responsable del tratamiento de los datos.

b) Cuando los parámetros fueran determinados únicamente por la entidad o entidades contratadas, dichas entidades serán las responsable del tratamiento.

c) Cuando en la determinación de los parámetros intervengan ambas entidades, serán ambas responsables del tratamiento.

3. En el supuesto contemplado en el apartado anterior, la entidad que encargue la realización de la campaña publicitaria deberá adoptar las medidas necesarias para asegurarse de que la entidad contratada ha recabado los datos cumpliendo las exigencias establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.
4. A los efectos previstos en este artículo, se consideran parámetros identificativos de los destinatarios las variables utilizadas para identificar el público objetivo o destinatario de una campaña o promoción comercial de productos o servicios que permitan acotar los destinatarios individuales de la misma.

Artículo 47. Depuración de datos personales.

Cuando dos o más responsables por sí mismos o mediante encargo a terceros pretendieran constatar sin consentimiento de los afectados, con fines de promoción o comercialización de sus productos o servicios y mediante un tratamiento cruzado de sus ficheros, quiénes ostentan la condición de clientes de una u otra o de varios de ellos, el tratamiento así realizado constituirá una cesión o comunicación de datos.

Artículo 48. Ficheros de exclusión del envío de comunicaciones comerciales.

Los responsables a los que el afectado haya manifestado su negativa a recibir publicidad podrán conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

Artículo 49. Ficheros comunes de exclusión del envío de comunicaciones comerciales.

1. Será posible la creación de ficheros comunes, de carácter general o sectorial, en los que sean objeto de tratamiento los datos de carácter personal que resulten necesarios para evitar el envío de comunicaciones comerciales a los interesados que manifiesten su negativa u oposición a recibir publicidad.

   A tal efecto, los citados ficheros podrán contener los mínimos datos imprescindibles para identificar al afectado.
2. Cuando el afectado manifieste ante un concreto responsable su negativa u oposición a que sus datos sean tratados con fines de publicidad o prospección comercial, aquél deberá ser informado de la existencia de los ficheros comunes de exclusión generales o sectoriales, así como de la identidad de su responsable, su domicilio y la finalidad del tratamiento.

   El afectado podrá solicitar su exclusión respecto de un fichero o tratamiento concreto o su inclusión en ficheros comunes de excluidos de carácter general o sectorial.
3. La entidad responsable del fichero común podrá tratar los datos de los interesados que hubieran manifestado su negativa u oposición al tratamiento de sus datos con fines de publicidad o prospección comercial, cumpliendo las

restantes obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento.

4. Quienes pretendan efectuar un tratamiento relacionado con actividades de publicidad o prospección comercial deberán previamente consultar los ficheros comunes que pudieran afectar a su actuación, a fin de evitar que sean objeto de tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa a ese tratamiento.

Artículo 50. Derechos de acceso, rectificación y cancelación.

1. El ejercicio de los derechos de acceso, rectificación y cancelación en relación con los tratamientos vinculados a actividades de publicidad y prospección comercial se someterá a lo previsto en los capítulos I a IV del título III de este reglamento.
2. Si el derecho se ejercitase ante una entidad que hubiese encargado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo otorgue al afectado su derecho en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

   Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 51. Derecho de oposición.

1. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

   La oposición a la que se refiere el párrafo anterior deberá entenderse sin perjuicio del derecho del interesado a revocar cuando lo estimase oportuno el consentimiento que hubiera otorgado, en su caso, para el tratamiento de los datos.
2. A tal efecto, deberá concederse al interesado un medio sencillo y gratuito para oponerse al tratamiento. En particular, se considerará cumplido lo dispuesto en este precepto cuando los derechos puedan ejercitarse mediante la llamada a un número telefónico gratuito o la remisión de un correo electrónico.
3. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a sus clientes o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, deberá concederse la posibilidad al afectado de ejercer su oposición a través de dichos servicios.

   No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar su oposición el

envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

En todo caso, el ejercicio por el afectado de sus derechos no podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

4. Si el derecho de oposición se ejercitase ante una entidad que hubiera encomendado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo atienda el derecho del afectado en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

Título V

Obligaciones previas al tratamiento de los datos

Capítulo I

Creación, modificación o supresión de ficheros de titularidad pública

Artículo 52. Disposición o acuerdo de creación, modificación o supresión del fichero.

1. La creación, modificación o supresión de los ficheros de titularidad pública sólo podrá hacerse por medio de disposición general o acuerdo publicados en el *Boletín Oficial del Estado* o *Diario Oficial* correspondiente.
2. En todo caso, la disposición o acuerdo deberá dictarse y publicarse con carácter previo a la creación, modificación o supresión del fichero.

Artículo 53. Forma de la disposición o acuerdo.

1. Cuando la disposición se refiera a los órganos de la Administración General del Estado o a las entidades u organismos vinculados o dependientes de la misma, deberá revestir la forma de orden ministerial o resolución del titular de la entidad u organismo correspondiente.
2. En el caso de los órganos constitucionales del Estado, se estará a lo que establezcan sus normas reguladoras.
3. En relación con los ficheros de los que sean responsables las comunidades autónomas, entidades locales y las entidades u organismos vinculados o dependientes de las mismas, las universidades públicas, así como los órganos de las comunidades autónomas con funciones análogas a los órganos constitucionales del Estado, se estará a su legislación específica.

4. La creación, modificación o supresión de los ficheros de los que sean responsables las corporaciones de derecho público y que se encuentren relacionados con el ejercicio por aquéllas de potestades de derecho público deberá efectuarse a través de acuerdo de sus órganos de gobierno, en los términos que establezcan sus respectivos Estatutos, debiendo ser igualmente objeto de publicación en el *Boletín Oficial del Estado* o *Diario Oficial* correspondiente.

Artículo 54. Contenido de la disposición o acuerdo.

1. La disposición o acuerdo de creación del fichero deberá contener los siguientes extremos:

   a) La identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos.
   b) El origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.
   c) La estructura básica del fichero mediante la descripción detallada de los datos identificativos y, en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.
   d) Las comunicaciones de datos previstas, indicando, en su caso, los destinatarios o categorías de destinatarios.
   e) Las transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos.
   f) Los órganos responsables del fichero.
   g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
   h) El nivel básico, medio o alto de seguridad que resulte exigible, de acuerdo con lo establecido en el título VIII del presente reglamento.

2. La disposición o acuerdo de modificación del fichero deberá indicar las modificaciones producidas en cualquiera de los extremos a los que se refiere el apartado anterior.
3. En las disposiciones o acuerdos que se dicten para la supresión de los ficheros se establecerá el destino que vaya a darse a los datos o, en su caso, las previsiones que se adopten para su destrucción.

Capítulo II

Notificación e inscripción de los ficheros de titularidad pública o privada

Artículo 55. Notificación de ficheros.

1. Todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de

la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.

2. Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible y, en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.
3. Cuando la obligación de notificar afecte a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, la notificación se realizará a la autoridad autonómica competente, que dará traslado de la inscripción al Registro General de Protección de Datos.

   El Registro General de Protección de Datos podrá solicitar de las autoridades de control de las comunidades autónomas el traslado al que se refiere el párrafo anterior, procediendo, en su defecto, a la inclusión de oficio del fichero en el Registro.
4. La notificación se realizará conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

Artículo 56. Tratamiento de datos en distintos soportes.

1. La notificación de un fichero de datos de carácter personal es independiente del sistema de tratamiento empleado en su organización y del soporte o soportes empleados para el tratamiento de los datos.
2. Cuando los datos de carácter personal objeto de un tratamiento estén almacenados en diferentes soportes, automatizados y no automatizados o exista una copia en soporte no automatizado de un fichero automatizado, sólo será precisa una sola notificación, referida a dicho fichero.

Artículo 57. Ficheros en los que exista más de un responsable.

Cuando se tenga previsto crear un fichero del que resulten responsables varias personas o entidades simultáneamente, cada una de ellas deberá notificar, a fin de proceder a su inscripción en el Registro General de Protección de Datos y, en su caso, en los Registros de Ficheros creados por las autoridades de control de las comunidades autónomas, la creación del correspondiente fichero.

Artículo 58. Notificación de la modificación o supresión de ficheros.

1. La inscripción del fichero deberá encontrarse actualizada en todo momento. Cualquier modificación que afecte al contenido de la inscripción de un fiche-

ro deberá ser previamente notificada a la Agencia Española de Protección de Datos o a las autoridades de control autonómicas competentes, a fin de proceder a su inscripción en el registro correspondiente, conforme a lo dispuesto en el artículo 55.

2. Cuando el responsable del fichero decida su supresión, deberá notificarla a efectos de que se proceda a la cancelación de la inscripción en el registro correspondiente.
3. Tratándose de ficheros de titularidad pública, cuando se pretenda la modificación que afecte a alguno de los requisitos previstos en el artículo 55 o la supresión del fichero deberá haberse adoptado, con carácter previo a la notificación, la correspondiente norma o acuerdo en los términos previstos en el capítulo I de este título.

Artículo 59. Modelos y soportes para la notificación.

1. La Agencia Española de Protección de Datos publicará mediante la correspondiente Resolución del Director los modelos o formularios electrónicos de notificación de creación, modificación o supresión de ficheros que permitan su presentación a través de medios telemáticos o en soporte papel, así como, previa consulta de las autoridades de protección de datos de las comunidades autónomas, los formatos para la comunicación telemática de ficheros públicos por las autoridades de control autonómicas, de conformidad con lo establecido en los artículos 55 y 58 del presente reglamento.
2. Los modelos o formularios electrónicos de notificación se podrán obtener gratuitamente en la página web de la Agencia Española de Protección de Datos.
3. El Director de la Agencia Española de Protección de Datos podrá establecer procedimientos simplificados de notificación en atención a las circunstancias que concurran en el tratamiento o el tipo de fichero al que se refiera la notificación.

Artículo 60. Inscripción de los ficheros.

1. El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución acordando, en su caso, la inscripción, una vez tramitado el procedimiento previsto en el capítulo IV del título IX.
2. La inscripción contendrá el código asignado por el Registro, la identificación del responsable del fichero, la identificación del fichero o tratamiento, la descripción de su finalidad y usos previstos, el sistema de tratamiento empleado en su organización, en su caso, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, y la indicación del nivel de medidas de seguridad exigible conforme a lo dispuesto en el artículo 81.

   Asimismo, se incluirán, en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales.

En el caso de ficheros de titularidad pública, también se hará constar la referencia de la disposición general por la que ha sido creado y, en su caso, modificado.

3. La inscripción de un fichero en el Registro General de Protección de Datos no exime al responsable del cumplimiento del resto de las obligaciones previstas en la Ley Orgánica 15/1999, de 13 de diciembre, y demás disposiciones reglamentarias.

Artículo 61. Cancelación de la inscripción.

1. Cuando el responsable del tratamiento comunicase, en virtud de lo dispuesto en el artículo 58 de este reglamento, la supresión del fichero, el Director de la Agencia Española de Protección de Datos, previa la tramitación del procedimiento establecido en la sección primera del capítulo IV del título IX, dictará resolución acordando la cancelación de la inscripción correspondiente al fichero.
2. El Director de la Agencia Española de Protección de Datos podrá, en ejercicio de sus competencias, acordar de oficio la cancelación de la inscripción de un fichero cuando concurran circunstancias que acrediten la imposibilidad de su existencia, previa la tramitación del procedimiento establecido en la sección segunda del capítulo IV del título IX de este reglamento.

Artículo 62. Rectificación de errores.

El Registro General de Protección de Datos podrá rectificar en cualquier momento, de oficio o a instancia de los interesados, los errores materiales, de hecho o aritméticos que pudieran existir en las inscripciones, de conformidad con lo dispuesto en el artículo 105 de la Ley 30/1992, de 26 de noviembre.

Artículo 63. Inscripción de oficio de ficheros de titularidad pública.

1. En supuestos excepcionales con el fin de garantizar el derecho a la protección de datos de los afectados y sin perjuicio de la obligación de notificación, se podrá proceder a la inscripción de oficio de un determinado fichero en el Registro General de Protección de Datos.
2. Para que lo dispuesto en el apartado anterior resulte de aplicación, será requisito indispensable que la correspondiente norma o acuerdo regulador de los ficheros que contengan datos de carácter personal haya sido publicado en el correspondiente diario oficial y cumpla los requisitos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.
3. El Director de la Agencia Española de Protección de Datos podrá, a propuesta del Registro General de Protección de Datos, acordar la inscripción del fichero de titularidad pública en el Registro, notificándose dicho acuerdo al órgano responsable del fichero.

   Cuando la inscripción se refiera a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, se comunicará a la referida autoridad de control autonómica para que proceda, en su caso, a la inscripción de oficio.

Artículo 64. Colaboración con las autoridades de control de las comunidades autónomas.

El Director de la Agencia Española de Protección de Datos podrá celebrar con los directores de las autoridades de control de las comunidades autónomas los convenios de colaboración o acuerdos que estime pertinentes, a fin de garantizar la inscripción en el Registro General de Protección de Datos de los ficheros sometidos a la competencia de dichas autoridades autonómicas.

Título VI

Transferencias internacionales de datos

Capítulo I

Disposiciones generales

Artículo 65. Cumplimiento de las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre.

La transferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

Artículo 66. Autorización y notificación.

1. Para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento, será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se otorgará en caso de que el exportador aporte las garantías a las que se refiere el artículo 70 del presente reglamento.

   La autorización se otorgará conforme al procedimiento establecido en la sección primera del capítulo V del título IX de este reglamento.

2. La autorización no será necesaria:

   a) Cuando el Estado en el que se encontrase el importador ofrezca un nivel adecuado de protección conforme a lo previsto en el capítulo II de este título.

   b) Cuando la transferencia se encuentre en uno de los supuestos contemplados en los apartados a a j del artículo 34 de la Ley Orgánica 15/1999, de 13 de diciembre.

4. En todo caso, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos, conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

Capítulo II

Transferencias a estados que proporcionen un nivel adecuado de protección

Artículo 67. Nivel adecuado de protección acordado por la Agencia Española de Protección de Datos.

1. No será precisa autorización del Director de la Agencia Española de Protección de Datos a una transferencia internacional de datos cuando las normas aplicables al Estado en que se encontrase el importador ofrezcan dicho nivel adecuado de protección a juicio del Director de la Agencia Española de Protección de Datos.

   El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

   Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se acordase que un determinado país proporciona un nivel adecuado de protección de datos serán publicadas en el *Boletín Oficial del Estado*.
2. El Director de la Agencia Española de Protección de Datos acordará la publicación de la relación de países cuyo nivel de protección haya sido considerado equiparable conforme a lo dispuesto en el apartado anterior.

   Esta lista se publicará y mantendrá actualizada asimismo a través de medios informáticos o telemáticos.

Artículo 68. Nivel adecuado de protección declarado por decisión de la Comisión Europea.

No será necesaria la autorización del Director de la Agencia Española de Protección de Datos para la realización de una transferencia internacional de datos que tuvieran por importador una persona o entidad, pública o privada, situada en el territorio de un Estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección.

Artículo 69. Suspensión temporal de las transferencias.

1. En los supuestos previstos en los artículos precedentes, el Director de la Agencia Española de Protección de Datos, en uso de la potestad que le otorga el artículo 37.1 f de la Ley Orgánica 15/1999, de 13 de diciembre, podrá acordar, previa audiencia del exportador, la suspensión temporal de la transferencia de datos hacia un importador ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes:

a) Que las autoridades de Protección de Datos del Estado importador o cualquier otra competente, en caso de no existir las primeras, resuelvan que el importador ha vulnerado las normas de protección de datos establecidas en su derecho interno.

b) Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad importadora de la transferencia y que las autoridades competentes en el Estado en que se encuentre el importador no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia Española de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados.

2. La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento. En estos casos, la decisión del Director de la Agencia Española de Protección de Datos será notificada a la Comisión Europea.

Capítulo III

Transferencias a estados que no proporcionen un nivel adecuado de protección

Artículo 70. Transferencias sujetas a autorización del Director de la Agencia Española de Protección de Datos.

1. Cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos.

   La autorización de la transferencia se tramitará conforme al procedimiento establecido en la sección primera del capítulo V del título IX del presente reglamento.

2. La autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

   A tal efecto, se considerará que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de junio de 2001, 2002/16/CE, de 27 de diciembre de 2001, y 2004/915/CE, de 27 de diciembre de 2004, o de lo que dispongan las Decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE.

3. En el supuesto contemplado en el apartado anterior, el Director de la Agencia Española de Protección de Datos podrá denegar o, en uso de la potestad que

le otorga el artículo 37.1 f de la Ley Orgánica 15/1999, de 13 de diciembre, suspender temporalmente, previa audiencia del exportador, la transferencia cuando concurra alguna de las circunstancias siguientes:

a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.
b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.
c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.
d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.
e) Que la transferencia o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.

Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se deniegue o suspenda una transferencia internacional de datos en virtud de las causas a las que se refiere este apartado serán notificadas a la Comisión de las Comunidades Europeas cuando así sea exigible.

4. También podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

En este caso, para que proceda la autorización del Director de la Agencia Española de Protección de Datos será preciso que las normas o reglas resulten vinculantes para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español.

En todo caso, la autorización del Director de la Agencia Española de Protección de Datos implicará la exigibilidad de lo previsto en las normas o reglas internas tanto por la Agencia como por los afectados cuyos datos hubieran sido objeto de tratamiento.

Título VII

Códigos tipo

Artículo 71. Objeto y naturaleza.

1. Los códigos tipo a los que se refiere el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, tienen por objeto adecuar lo establecido en la citada Ley

Orgánica y en el presente reglamento a las peculiaridades de los tratamientos efectuados por quienes se adhieren a los mismos.

A tal efecto, contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

2. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional y serán vinculantes para quienes se adhieran a los mismos.

Artículo 72. Iniciativa y ámbito de aplicación.

1. Los códigos tipo tendrán carácter voluntario.
2. Los códigos tipo de carácter sectorial podrán referirse a la totalidad o a parte de los tratamientos llevados a cabo por entidades pertenecientes a un mismo sector, debiendo ser formulados por organizaciones representativas de dicho sector, al menos en su ámbito territorial de aplicación, y sin perjuicio de la potestad de dichas entidades de ajustar el código tipo a sus peculiaridades.
3. Los códigos tipo promovidos por una empresa deberán referirse a la totalidad de los tratamientos llevados a cabo por la misma.
4. Las Administraciones públicas y las corporaciones de Derecho Público podrán adoptar códigos tipo de acuerdo con lo establecido en las normas que les sean aplicables.

Artículo 73. Contenido.

1. Los códigos tipo deberán estar redactados en términos claros y accesibles.
2. Los códigos tipo deben respetar la normativa vigente e incluir, como mínimo, con suficiente grado de precisión:

a) La delimitación clara y precisa de su ámbito de aplicación, las actividades a que el código se refiere y los tratamientos sometidos al mismo.
b) Las previsiones específicas para la aplicación de los principios de protección de datos.
c) El establecimiento de estándares homogéneos para el cumplimiento por los adheridos al código de las obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre.
d) El establecimiento de procedimientos que faciliten el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.
e) La determinación de las cesiones y transferencias internacionales de datos que, en su caso, se prevean, con indicación de las garantías que deban adoptarse.
f) Las acciones formativas en materia de protección de datos dirigidas a quienes los traten, especialmente en cuanto a su relación con los afectados.
g) Los mecanismos de supervisión a través de los cuales se garantice el cumplimiento por los adheridos de lo establecido en el código tipo, en los términos previstos en el artículo 74 de este reglamento.

3. En particular, deberán contenerse en el código:

   a) Cláusulas tipo para la obtención del consentimiento de los afectados al tratamiento o cesión de sus datos.
   b) Cláusulas tipo para informar a los afectados del tratamiento, cuando los datos no sean obtenidos de los mismos.
   c) Modelos para el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.
   d) Modelos de cláusulas para el cumplimiento de los requisitos formales exigibles para la contratación de un encargado del tratamiento, en su caso.

Artículo 74. Compromisos adicionales.

1. Los códigos tipo podrán incluir cualquier otro compromiso adicional que asuman los adheridos para un mejor cumplimiento de la legislación vigente en materia de protección de datos.
2. Además podrán contener cualquier otro compromiso que puedan establecer las entidades promotoras y, en particular, sobre:

   a) La adopción de medidas de seguridad adicionales a las exigidas por la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.
   b) La identificación de las categorías de cesionarios o importadores de los datos.
   c) Las medidas concretas adoptadas en materia de protección de los menores o de determinados colectivos de afectados.
   d) El establecimiento de un sello de calidad que identifique a los adheridos al código.

Artículo 75. Garantías del cumplimiento de los códigos tipo.

1. Los códigos tipo deberán incluir procedimientos de supervisión independientes para garantizar el cumplimiento de las obligaciones asumidas por los adheridos, y establecer un régimen sancionador adecuado, eficaz y disuasorio.
2. El procedimiento que se prevea deberá garantizar:

   a) La independencia e imparcialidad del órgano responsable de la supervisión.
   b) La sencillez, accesibilidad, celeridad y gratuidad para la presentación de quejas y reclamaciones ante dicho órgano por los eventuales incumplimientos del código tipo.
   c) El principio de contradicción.
   d) Una graduación de sanciones que permita ajustarlas a la gravedad del incumplimiento. Esas sanciones deberán ser disuasorias y podrán implicar la suspensión de la adhesión al código o la expulsión de la entidad adherida. Asimismo, podrá establecerse, en su caso, su publicidad.
   e) La notificación al afectado de la decisión adoptada.

3. Asimismo y sin perjuicio de lo dispuesto en el artículo 19 de la Ley Orgánica 15/1999, de 13 de diciembre, los códigos tipo podrán contemplar procedimientos para la determinación de medidas reparadoras en caso de haberse causado un perjuicio a los afectados como consecuencia del incumplimiento del código tipo.
4. Lo dispuesto en este artículo se aplicará sin perjuicio de las competencias de la Agencia Española de Protección de Datos y, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 76. Relación de adheridos.

El código tipo deberá incorporar como anexo una relación de adheridos, que deberá mantenerse actualizada, a disposición de la Agencia Española de Protección de Datos.

Artículo 77. Depósito y publicidad de los códigos tipo.

1. Para que los códigos tipo puedan ser considerados como tales a los efectos previstos en el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento, deberán ser depositados e inscritos en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos o, cuando corresponda, en el registro que fuera creado por las comunidades autónomas, que darán traslado para su inclusión al Registro General de Protección de Datos.
2. A tal efecto, los códigos tipo deberán ser presentados ante la correspondiente autoridad de control, tramitándose su inscripción, en caso de estar sometidos a la decisión de la Agencia Española de Protección de Datos, conforme al procedimiento establecido en el capítulo VI del título IX de este reglamento.
3. En todo caso, la Agencia Española de Protección de Datos dará publicidad a los códigos tipo inscritos, preferentemente a través de medios informáticos o telemáticos.

Artículo 78. Obligaciones posteriores a la inscripción del código tipo.

Las entidades promotoras o los órganos, personas o entidades que al efecto se designen en el propio código tipo tendrán, una vez que el mismo haya sido publicado, las siguientes obligaciones:

a) Mantener accesible al público la información actualizada sobre las entidades promotoras, el contenido del código tipo, los procedimientos de adhesión y de garantía de su cumplimiento y la relación de adheridos a la que se refiere el artículo anterior.

Esta información deberá presentarse de forma concisa y clara y estar permanentemente accesible por medios electrónicos.

b) Remitir a la Agencia Española de Protección de Datos una memoria anual sobre las actividades realizadas para difundir el código tipo y promover la adhesión a éste, las actuaciones de verificación del cumplimiento del código y sus resultados, las quejas y reclamaciones tramitadas y el curso que se les hubiera dado y cualquier otro aspecto que las entidades promotoras consideren adecuado destacar.

Cuando se trate de códigos tipo inscritos en el registro de una autoridad de control de una comunidad autónoma, la remisión se realizará a dicha autoridad, que dará traslado al registro General de Protección de Datos.

c) Evaluar periódicamente la eficacia del código tipo, midiendo el grado de satisfacción de los afectados y, en su caso, actualizar su contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento.

Esta evaluación deberá tener lugar, al menos, cada cuatro años, salvo que sea precisa la adaptación de los compromisos del código a la modificación de la normativa aplicable en un plazo menor.

d) Favorecer la accesibilidad de todas las personas, con especial atención a las que tengan alguna discapacidad o de edad avanzada a toda la información disponible sobre el código tipo.

Título VIII

De las medidas de seguridad en el tratamiento de datos de carácter personal

Capítulo I

Disposiciones generales

Artículo 79. Alcance.

Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cuál sea su sistema de tratamiento.

Artículo 80. Niveles de seguridad.

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

Artículo 81. Aplicación de los niveles de seguridad.

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.
2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

   a) Los relativos a la comisión de infracciones administrativas o penales.
   b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.
   c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.
   d) Aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e) Aquellos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f) Aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

   a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

   b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

   c) Aquellos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, bastará la implantación de las medidas de seguridad de nivel básico cuando:

   a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

   b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

Artículo 82. Encargado del tratamiento.

1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate a un encargado de tratamiento que preste sus servicios en los locales del primero, deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

   Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.
2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, aquél deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.
3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.

Artículo 83. Prestaciones de servicios sin acceso a datos personales.

El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Artículo 84. Delegación de autorizaciones.

Las autorizaciones que en este título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.

Artículo 85. Acceso a datos a través de redes de comunicaciones.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.

Artículo 86. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.

1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento, será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.
2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Artículo 87. Ficheros temporales o copias de trabajo de documentos.

1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81.
2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

Capítulo II

Del documento de seguridad

Artículo 88. El documento de seguridad.

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.
2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.
3. El documento deberá contener, como mínimo, los siguientes aspectos:

   a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.
c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes o, en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

   a) La identificación del responsable o responsables de seguridad.
   b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del periodo de vigencia del encargo.
6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

   En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.
7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.
8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Capítulo III

Medidas de seguridad aplicables a ficheros y tratamientos automatizados

Sección I. Medidas de seguridad de nivel básico

Artículo 89. Funciones y obligaciones del personal.

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.
   También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.
2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 90. Registro de incidencias.

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido o, en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Artículo 91. Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos, deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 92. Gestión de soportes y documentos.

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y

sólo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anexos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.
3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.
4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Artículo 94. Copias de respaldo y recuperación.

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos.
2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos, quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

   Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

Sección II. Medidas de seguridad de nivel medio

Artículo 95. Responsable de seguridad.

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Artículo 96. Auditoría.

1. A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

   Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.
2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.
3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tra-

tamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 97. Gestión de soportes y documentos.

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.
2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Artículo 98. Identificación y autenticación.

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 99. Control de acceso físico.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Artículo 100. Registro de incidencias.

1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.
2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Sección III. Medidas de seguridad de nivel alto

Artículo 101. Gestión y distribución de soportes.

1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido y que dificulten la identificación para el resto de personas.
2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte. Asimismo, se cifrarán los datos que contengan los dispositivos portátiles

cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Artículo 102. Copias de respaldo y recuperación.

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Artículo 103. Registro de accesos.

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
4. El periodo mínimo de conservación de los datos registrados será de dos años.
5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

   a) Que el responsable del fichero o del tratamiento sea una persona física.
   b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

   La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Artículo 104. Telecomunicaciones.

Cuando, conforme al artículo 81.3, deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Capítulo IV

Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados

Sección I. Medidas de seguridad de nivel básico

Artículo 105. Obligaciones comunes.

1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:

   a) Alcance.
   b) Niveles de seguridad.
   c) Encargado del tratamiento.
   d) Prestaciones de servicios sin acceso a datos personales.
   e) Delegación de autorizaciones.
   f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
   g) Copias de trabajo de documentos.
   h) Documento de seguridad.

2. Asimismo, se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:

   a) Funciones y obligaciones del personal.
   b) Registro de incidencias.
   c) Control de acceso.
   d) Gestión de soportes.

Artículo 106. Criterios de archivo.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Artículo 107. Dispositivos de almacenamiento.

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Artículo 108. Custodia de los soportes.

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Sección II. Medidas de seguridad de nivel medio

Artículo 109. Responsable de seguridad.

Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento.

Artículo 110. Auditoría.

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Sección III. Medidas de seguridad de nivel alto

Artículo 111. Almacenamiento de la información.

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.
2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Artículo 112. Copia o reproducción.

1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.
2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Artículo 113. Acceso a la documentación.

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.
2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Artículo 114. Traslado de documentación.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

Título IX

Procedimientos tramitados por la agencia española de protección de datos

Capítulo I

Disposiciones generales

Artículo 115. Régimen aplicable.

1. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el presente título, y supletoriamente, por la Ley 30/1992, de 26 de noviembre, del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
2. Específicamente serán de aplicación las normas reguladoras del procedimiento administrativo común al régimen de representación en los citados procedimientos.

Artículo 116. Publicidad de las resoluciones.

1. La Agencia Española de Protección de Datos hará públicas sus resoluciones, con excepción de las correspondientes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos y de aquellas por las que se resuelva la inscripción en el mismo de los códigos tipo, siempre que se refieran a procedimientos que se hubieran iniciado con posterioridad al 1 de enero de 2004, o que correspondan al archivo de actuaciones inspectoras incoadas a partir de dicha fecha.
2. La publicación de estas resoluciones se realizará preferentemente mediante su inserción en el sitio web de la Agencia Española de Protección de Datos, dentro del plazo de un mes a contar desde la fecha de su notificación a los interesados.
3. En la notificación de las resoluciones se informará expresamente a los interesados de la publicidad prevista en el artículo 37.2 de la Ley Orgánica 15/1999, de 13 de diciembre.
4. La publicación se realizará aplicando los criterios de disociación de los datos de carácter personal que a tal efecto se establezcan mediante Resolución del Director de la Agencia.

Capítulo II

Procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición

Artículo 117. Instrucción del procedimiento.

1. El procedimiento se iniciará a instancia del afectado o afectados, expresando con claridad el contenido de su reclamación y de los preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, que se consideren vulnerados.
2. Recibida la reclamación en la Agencia Española de Protección de Datos, se dará traslado de la misma al responsable del fichero, para que, en el plazo de quince días, formule las alegaciones que estime pertinentes.
3. Recibidas las alegaciones o transcurrido el plazo previsto en el apartado anterior, la Agencia Española de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y nuevamente del responsable del fichero, resolverá sobre la reclamación formulada.

Artículo 118. Duración del procedimiento y efectos de la falta de resolución expresa.

1. El plazo máximo para dictar y notificar resolución en el procedimiento de tutela de derechos será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la reclamación del afectado o afectados.
2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su reclamación por silencio administrativo positivo.

Artículo 119. Ejecución de la resolución.

Si la resolución de tutela fuese estimatoria, se requerirá al responsable del fichero para que, en el plazo de diez días siguientes a la notificación, haga efectivo el ejercicio de los derechos objeto de la tutela, debiendo dar cuenta por escrito de dicho cumplimiento a la Agencia Española de Protección de Datos en idéntico plazo.

Capítulo III

Procedimientos relativos al ejercicio de la potestad sancionadora

Sección I. Disposiciones generales

Artículo 120. Ámbito de aplicación.

1. Las disposiciones contenidas en el presente capítulo serán de aplicación a los procedimientos relativos al ejercicio por la Agencia Española de Protec-

ción de Datos de la potestad sancionadora que le viene atribuida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, en la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. No obstante, las disposiciones previstas en el artículo 121 y en la sección cuarta de este capítulo únicamente serán aplicables a los procedimientos referidos al ejercicio de la potestad sancionadora prevista en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 121. Inmovilización de ficheros.

1. En el supuesto previsto como infracción muy grave en la Ley Orgánica 15/1999, de 13 de diciembre, consistente en la utilización o cesión ilícita de los datos de carácter personal en la que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia Española de Protección de Datos podrá, en cualquier momento del procedimiento, requerir a los responsables de ficheros o tratamientos de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos.
2. El requerimiento deberá ser atendido en el plazo improrrogable de tres días, durante el cual el responsable del fichero podrá formular las alegaciones que tenga por convenientes en orden al levantamiento de la medida.
3. Si el requerimiento fuera desatendido, el Director de la Agencia Española de Protección de Datos podrá, mediante resolución motivada, acordar la inmovilización de tales ficheros o tratamientos, a los solos efectos de restaurar los derechos de las personas afectadas.

Sección II. Actuaciones previas

Artículo 122. Iniciación.

1. Con anterioridad a la iniciación del procedimiento sancionador se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación. En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos que pudieran justificar la incoación del procedimiento, identificar a la persona u órgano que pudiera resultar responsable y fijar las circunstancias relevantes que pudieran concurrir en el caso.
2. Las actuaciones previas se llevarán a cabo de oficio por la Agencia Española de Protección de Datos, bien por iniciativa propia o como consecuencia de la existencia de una denuncia o una petición razonada de otro órgano.
3. Cuando las actuaciones se lleven a cabo como consecuencia de la existencia de una denuncia o de una petición razonada de otro órgano, la Agencia Española de Protección de Datos acusará recibo de la denuncia o petición, pudiendo

solicitar cuanta documentación se estime oportuna para poder comprobar los hechos susceptibles de motivar la incoación del procedimiento sancionador.

4. Estas actuaciones previas tendrán una duración máxima de doce meses a contar desde la fecha en la que la denuncia o petición razonada a las que se refiere el apartado 2 hubieran tenido entrada en la Agencia Española de Protección de Datos o, en caso de no existir aquéllas, desde que el Director de la Agencia acordase la realización de dichas actuaciones.

   El vencimiento del plazo sin que haya sido dictado y notificado acuerdo de inicio del procedimiento sancionador producirá la caducidad de las actuaciones previas.

Artículo 123. Personal competente para la realización de las actuaciones previas.

1. Las actuaciones previas serán llevadas a cabo por el personal del área de la Inspección de Datos habilitado para el ejercicio de funciones inspectoras.
2. En supuestos excepcionales, el Director de la Agencia Española de Protección de Datos podrá designar para la realización de actuaciones específicas a funcionarios de la propia Agencia no habilitados con carácter general para el ejercicio de funciones inspectoras o a funcionarios que no presten sus funciones en la Agencia, siempre que reúnan las condiciones de idoneidad y especialización necesarias para la realización de tales actuaciones. En estos casos, la autorización indicará expresamente la identificación del funcionario y las concretas actuaciones previas de inspección a realizar.
3. Los funcionarios que ejerzan la inspección a la que se refieren los dos apartados anteriores tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

   Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 124. Obtención de información.

Los inspectores podrán recabar cuantas informaciones precisen para el cumplimiento de sus cometidos. A tal fin podrán requerir la exhibición o el envío de los documentos y datos y examinarlos en el lugar en que se encuentren depositados, como obtener copia de los mismos, inspeccionar los equipos físicos y lógicos, así como requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del fichero o ficheros sujetos a investigación, accediendo a los lugares donde se hallen instalados.

Artículo 125. Actuaciones presenciales.

1. En el desarrollo de las actuaciones previas se podrán realizar visitas de inspección por parte de los inspectores designados, en los locales ó sede del inspeccionado, o donde se encuentren ubicados los ficheros, en su caso. A tal efecto, los inspectores habrán sido previamente autorizados por el Director de la Agencia Española de Protección de Datos.

   Las inspecciones podrán realizarse en el domicilio del inspeccionado, en la sede o local concreto relacionado con el mismo o en cualquiera de sus lo-

cales, incluyendo aquellos en que el tratamiento sea llevado a cabo por un encargado.
La autorización se limitará a indicar la habilitación del inspector autorizado y la identificación de la persona u órgano inspeccionado.

2. En el supuesto contemplado en el apartado anterior, las inspecciones concluirán con el levantamiento de la correspondiente acta, en la que quedará constancia de las actuaciones practicadas durante la visita o visitas de inspección.
3. El acta, que se emitirá por duplicado, será firmada por los inspectores actuantes y por el inspeccionado, que podrá hacer constar en la misma las alegaciones o manifestaciones que tenga por conveniente.
En caso de negativa del inspeccionado a la firma del acta, se hará constar expresamente esta circunstancia en la misma. En todo caso, la firma por el inspeccionado del acta no supondrá su conformidad, sino tan sólo la recepción de la misma.
Se entregará al inspeccionado uno de los originales del acta de inspección, incorporándose el otro a las actuaciones.

Artículo 126. Resultado de las actuaciones previas.

1. Finalizadas las actuaciones previas, éstas se someterán a la decisión del Director de la Agencia Española de Protección de Datos.
Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.
2. En caso de apreciarse la existencia de indicios susceptibles de motivar la imputación de una infracción, el Director de la Agencia Española de Protección de Datos dictará acuerdo de inicio de procedimiento sancionador o de infracción de las Administraciones públicas, que se tramitarán conforme a lo dispuesto, respectivamente, en las secciones tercera y cuarta del presente capítulo.

Sección III. Procedimiento sancionador

Artículo 127. Iniciación del procedimiento.

Con carácter específico el acuerdo de inicio del procedimiento sancionador deberá contener:

a) Identificación de la persona o personas presuntamente responsables.
b) Descripción sucinta de los hechos imputados, su posible calificación y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción.
c) Indicación de que el órgano competente para resolver el procedimiento es el Director de la Agencia Española de Protección de Datos.
d) Indicación al presunto responsable de que puede reconocer voluntariamente su responsabilidad, en cuyo caso se dictará directamente resolución.

e) Designación de instructor y, en su caso, secretario, con expresa indicación del régimen de recusación de los mismos.

f) Indicación expresa del derecho del responsable a formular alegaciones, a la audiencia en el procedimiento y a proponer las pruebas que estime procedentes.

g) Medidas de carácter provisional que pudieran acordarse, en su caso, conforme a lo establecido en la sección primera del presente capítulo.

Artículo 128. Plazo máximo para resolver.

1. El plazo para dictar resolución será el que determinen las normas aplicables a cada procedimiento sancionador y se computará desde la fecha en que se dicte el acuerdo de inicio hasta que se produzca la notificación de la resolución sancionadora, o se acredite debidamente el intento de notificación.
2. El vencimiento del citado plazo máximo, sin que se haya dictado y notificado resolución expresa, producirá la caducidad del procedimiento y el archivo de las actuaciones.

Sección IV. Procedimiento de declaración de infracción de la ley orgánica 15/1999, de 13 de diciembre, por las administraciones públicas

Artículo 129. Disposición general.

El procedimiento por el que se declare la existencia de una infracción de la Ley Orgánica 15/1999, de 13 de diciembre, cometida por las Administraciones públicas será el establecido en la sección tercera de este capítulo.

Capítulo IV

Procedimientos relacionados con la inscripción o cancelación de ficheros

Sección I. Procedimiento de inscripción de la creación, modificación o supresión de ficheros

Artículo 130. Iniciación del procedimiento.

1. El procedimiento se iniciará como consecuencia de la notificación de la creación, modificación o supresión del fichero por el interesado o, en su caso, de la comunicación efectuada por las autoridades de control de las comunidades autónomas, a la que se refiere el presente reglamento.
2. La notificación se deberá efectuar cumplimentando los modelos o formularios electrónicos publicados al efecto por la Agencia Española de Protección de Datos, en virtud de lo dispuesto en el apartado 1 del artículo 59 de este reglamento.

Tratándose de la notificación de la modificación o supresión de un fichero, deberá indicarse en la misma el código de inscripción del fichero en el Registro General de Protección de Datos.

3. La notificación se efectuará en soporte electrónico, ya mediante comunicación electrónica a través de Internet mediante firma electrónica o en soporte informático, utilizando al efecto el programa de ayuda para la generación de notificaciones que la Agencia pondrá a disposición de los interesados de forma gratuita.

   Será igualmente válida la notificación efectuada en soporte papel cuando para su cumplimentación hayan sido utilizados los modelos o formularios publicados por la Agencia.

4. En la notificación, el responsable del fichero deberá declarar un domicilio a efectos de notificaciones en el procedimiento.

Artículo 131. Especialidades en la notificación de ficheros de titularidad pública.

1. Cuando se trate de la notificación de ficheros de titularidad pública, deberá acompañarse a la notificación una copia de la norma o acuerdo de creación, modificación o supresión del fichero a que hace referencia el artículo 52 del presente reglamento.

   Cuando el diario oficial en el que se encuentre publicada la citada norma o acuerdo sea accesible a través de Internet, bastará con indicar en la notificación la dirección electrónica que permita su concreta localización.

2. Recibida la notificación, si la misma no contuviera la información preceptiva o se advirtieran defectos formales, el Registro General de Protección de Datos requerirá al responsable del fichero para que complete o subsane la notificación. El plazo para la subsanación o mejora de la solicitud será de tres meses, en el caso de que se precise la modificación de la norma o acuerdo de creación del fichero.

Artículo 132. Acuerdo de inscripción o cancelación.

Si la notificación referida a la creación, modificación o supresión del fichero contuviera la información preceptiva y se cumplieran las restantes exigencias legales, el Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, acordará, respectivamente, la inscripción del fichero, asignando al mismo el correspondiente código de inscripción, la modificación de la inscripción del fichero o la cancelación de la inscripción correspondiente.

Artículo 133. Improcedencia o denegación de la inscripción.

El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución denegando la inscripción, modificación o cancelación cuando de los documentos aportados por el responsable del fichero se desprenda que la notificación no resulta conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.

La resolución será debidamente motivada, con indicación expresa de las causas que impiden la inscripción, modificación o cancelación.

Artículo 134. Duración del procedimiento y efectos de la falta de resolución expresa.

1. El plazo máximo para dictar y notificar resolución acerca de la inscripción, modificación o cancelación será de un mes.
2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá inscrito, modificado o cancelado el fichero a todos los efectos.

Sección II. Procedimiento de cancelación de oficio de ficheros inscritos.

Artículo 135. Iniciación del procedimiento.

El procedimiento de cancelación de oficio de los ficheros inscritos en el Registro General de Protección de Datos se iniciará siempre de oficio, bien por propia iniciativa o en virtud de denuncia, por acuerdo del Director de la Agencia Española de Protección de Datos.

Artículo 136. Terminación del expediente.

La resolución, previa audiencia del interesado, acordará haber lugar o no a la cancelación del fichero.

Si la resolución acordase la cancelación del fichero, se dará traslado de la misma al Registro General de Protección de Datos, para que proceda a la cancelación.

Capítulo V

Procedimientos relacionados con las transferencias internacionales de datos

Sección I. Procedimiento de autorización de transferencias internacionales de datos

Artículo 137. Iniciación del procedimiento.

1. El procedimiento para la obtención de la autorización para las transferencias internacionales de datos a países terceros a las que se refiere el artículo 33 de la Ley Orgánica 15/1999, de 13 de diciembre, y el artículo 70 de este reglamento se iniciará siempre a solicitud del exportador que pretenda llevar a cabo la transferencia.
2. En su solicitud, además de los requisitos legalmente exigidos, el exportador deberá consignar, en todo caso:

   a) La identificación del fichero o ficheros a cuyos datos se refiera la transferencia internacional, con indicación de su denominación y código de inscripción del fichero en el Registro General de Protección de Datos.

b) La transferencia o transferencias respecto de las que se solicita la autorización, con indicación de la finalidad que la justifica.

c) La documentación que incorpore las garantías exigibles para la obtención de la autorización, así como el cumplimiento de los requisitos legales necesarios para la realización de la transferencia, en su caso.

Cuando la autorización se fundamente en la existencia de un contrato entre el exportador y el importador de los datos, deberá aportarse copia del mismo, acreditándose asimismo la concurrencia de poder suficiente en sus otorgantes.

Si la autorización se pretendiera fundar en lo dispuesto en el apartado 4 del artículo 70, deberán aportarse las normas o reglas adoptadas en relación con el tratamiento de los datos en el seno del grupo, así como la documentación que acredite su carácter vinculante y su eficacia dentro del grupo. Igualmente deberá aportarse la documentación que acredite la posibilidad de que el afectado o la Agencia Española de Protección de Datos puedan exigir la responsabilidad que corresponda en caso de perjuicio del afectado o vulneración de las normas de protección de datos por parte de cualquier empresa importadora.

Artículo 138. Instrucción del procedimiento.

1. Cuando el Director de la Agencia Española de Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, de 26 de noviembre, la apertura de un periodo de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el *Boletín Oficial del Estado* del anuncio previsto en dicha Ley.
2. No será posible el acceso a la información del expediente en que concurran las circunstancias establecidas en el artículo 37.5 de la Ley 30/1992, de 26 de noviembre.
3. Transcurrido el plazo previsto en el apartado 1, en caso de que se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

Artículo 139. Actos posteriores a la resolución.

1. Cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la transferencia internacional de datos, se dará traslado de la resolución de autorización al Registro General de Protección de Datos, a fin de proceder a su inscripción.

   El Registro General de Protección de Datos inscribirá de oficio la autorización de transferencia internacional.
2. En todo caso, se dará traslado de la resolución de autorización o denegación de la autorización de la transferencia internacional de datos al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Artículo 140. Duración del procedimiento y efectos de la falta de resolución expresa.

1. El plazo máximo para dictar y notificar resolución será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud.
2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá autorizada la transferencia internacional de datos.

Sección II. Procedimiento de suspensión temporal de transferencias internacionales de datos

Artículo 141. Iniciación.

1. En los supuestos contemplados en el artículo 69 y en el apartado 3 del artículo 70, el Director de la Agencia Española de Protección de Datos podrá acordar la suspensión temporal de una transferencia internacional de datos.
2. En tales supuestos, el Director dictará acuerdo de inicio referido a la suspensión temporal de la transferencia. El acuerdo deberá ser motivado y fundarse en los supuestos previstos en este reglamento.

Artículo 142. Instrucción y resolución.

1. Se dará traslado del acuerdo al exportador, a fin de que en el plazo de quince días formule lo que a su derecho convenga.
2. Recibidas las alegaciones o cumplido el plazo señalado, el Director dictará resolución acordando, en su caso, la suspensión temporal de la transferencia internacional de datos.

Artículo 143. Actos posteriores a la resolución.

1. El Director de la Agencia Española de Protección de Datos dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el registro.

   El Registro General de Protección de Datos inscribirá de oficio la suspensión temporal de la transferencia internacional.
2. En todo caso, se dará traslado de la resolución al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo con lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Artículo 144. Levantamiento de la suspensión temporal.

1. La suspensión se levantará tan pronto como cesen las causas que la hubieran justificado, mediante resolución del Director de la Agencia Española de Protección de Datos, del que se dará traslado al exportador.
2. El Director de la Agencia Española de Protección de Datos dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el Registro.

El Registro General de Protección de Datos hará constar de oficio el levantamiento de la suspensión temporal de la transferencia internacional.

3. El acuerdo será notificado al exportador y al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26. 3 de la Directiva 95/46/CE.

Capítulo VI

Procedimiento de inscripción de códigos tipo

Artículo 145. Iniciación del procedimiento.

1. El procedimiento para la inscripción en el Registro General de Protección de Datos de los códigos tipo se iniciará siempre a solicitud de la entidad, órgano o asociación promotora del código tipo.
2. La solicitud, que deberá reunir los requisitos legalmente establecidos, habrá de acompañarse de los siguientes documentos:

   a) Acreditación de la representación que concurra en la persona que presente la solicitud.
   b) Contenido del acuerdo, convenio o decisión por la que se aprueba, en el ámbito correspondiente, el contenido del código tipo presentado.
   c) En caso de que el código tipo proceda de un acuerdo sectorial o una decisión de empresa, certificación referida a la adopción del acuerdo y legitimación del órgano que lo adoptó.
   d) En el supuesto contemplado en la letra anterior, copia de los estatutos de la asociación, organización sectorial o entidad en cuyo marco haya sido aprobado el código.
   e) En caso de códigos tipo presentados por asociaciones u organizaciones de carácter sectorial, documentación relativa a su representatividad en el sector.
   f) En caso de códigos tipo basados en decisiones de empresa, descripción de los tratamientos a los que se refiere el código tipo.
   g) Código tipo sometido a la Agencia Española de Protección de Datos.

Artículo 146. Análisis de los aspectos sustantivos del código tipo.

1. Durante los treinta días siguientes a la notificación o subsanación de los defectos, el Registro General de Protección de Datos podrá convocar a los solicitantes, a fin de obtener aclaraciones o precisiones relativas al contenido sustantivo del código tipo.
2. Transcurrido el plazo señalado en el apartado anterior, el Registro General de Protección de Datos elaborará un informe sobre las características del proyecto de código tipo.
3. La documentación presentada y el informe del Registro serán remitidos al Gabinete Jurídico, a fin de que por el mismo se informe acerca del cumplimiento de los requisitos establecidos en el Título VII de este Reglamento.

Artículo 147. Información pública.

1. Cuando el Director de la Agencia Española de Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, de 26 de noviembre, la apertura de un periodo de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el *Boletín Oficial del Estado* del anuncio previsto en dicha Ley.
2. No será posible el acceso a la información del expediente en que concurran las circunstancias establecidas en el artículo 37.5 de la Ley 30/1992, de 26 de noviembre.

Artículo 148. Mejora del código tipo.

Si durante la tramitación del procedimiento resultase necesaria la aportación de nuevos documentos o la modificación del código tipo presentado, la Agencia Española de Protección de Datos podrá requerir al solicitante, a fin de que en el plazo de treinta días introduzca las modificaciones que sean precisas, remitiendo el texto resultante a la Agencia Española de Protección de Datos.

Se declarará la suspensión del procedimiento en tanto el solicitante no dé cumplimiento al requerimiento.

Artículo 149. Trámite de audiencia.

En caso de que durante el trámite previsto en el artículo 148 se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

Artículo 150. Resolución.

1. Cumplidos los términos establecidos en los artículos precedentes, el Director de la Agencia resolverá sobre la procedencia o improcedencia de la inscripción del código tipo en el Registro General de Protección de Datos.
2. Cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la inscripción del código tipo, se dará traslado de la resolución al Registro General de Protección de Datos, a fin de proceder a su inscripción.

Artículo 151. Duración del procedimiento y efectos de la falta de resolución expresa.

1. El plazo máximo para dictar y notificar resolución será de seis meses, a contar desde la fecha de entrada de la solicitud en la Agencia Española de Protección de Datos.
2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el solicitante podrá considerar estimada su solicitud.

Artículo 152. Publicación de los códigos tipo por la Agencia Española de Protección de Datos.

La Agencia Española de Protección de Datos dará publicidad al contenido de los códigos tipo inscritos en el Registro General de Protección de Datos, utilizando para ello, con carácter preferente, medios electrónicos o telemáticos.

Capítulo VII

Otros procedimientos tramitados por la agencia española de protección de datos

Sección I. Procedimiento de exención del deber de información al interesado

Artículo 153. Iniciación del procedimiento.

1. El procedimiento para obtener de la Agencia Española de Protección de Datos la exención del deber de informar al interesado acerca del tratamiento de sus datos de carácter personal cuando resulte imposible o exija esfuerzos desproporcionados, prevista en el apartado 5 del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, se iniciará siempre a petición del responsable que pretenda obtener la aplicación de la exención.
2. En el escrito de solicitud, además de los requisitos recogidos en el artículo. 70 de la Ley 30/1992, de 26 de noviembre, el responsable deberá:

   a) Identificar claramente el tratamiento de datos al que pretende aplicarse la exención del deber de informar.
   b) Motivar expresamente las causas en que fundamenta la imposibilidad o el carácter desproporcionado del esfuerzo que implicaría el cumplimiento del deber de informar.
   c) Exponer detalladamente las medidas compensatorias que propone realizar en caso de exoneración del cumplimiento del deber de informar.
   d) Aportar una cláusula informativa que, mediante su difusión en los términos que se indiquen en la solicitud, permita compensar la exención del deber de informar.

Artículo 154. Propuesta de nuevas medidas compensatorias.

1. Si la Agencia Española de Protección de Datos considerase insuficientes las medidas compensatorias propuestas por el solicitante, podrá acordar la adopción de medidas complementarias o sustitutivas a las propuestas por aquél en su solicitud.
2. Del acuerdo se dará traslado al solicitante, a fin de que exponga lo que a su derecho convenga en el plazo de quince días.

Artículo 155. Terminación del procedimiento.

Concluidos los trámites previstos en los artículos precedentes, el Director de la Agencia dictará resolución, concediendo o denegando la exención del deber de informar. La resolución podrá imponer la adopción de las medidas complementarias a las que se refiere el artículo anterior.

Artículo 156. Duración del procedimiento y efectos de la falta de resolución expresa.

1. El plazo máximo para dictar y notificar resolución en el procedimiento será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud del responsable del fichero.
2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud por silencio administrativo positivo.

Sección II. Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos.

Artículo 157. Iniciación del procedimiento.

1. El procedimiento para obtener de la Agencia Española de Protección de Datos la declaración de la concurrencia en un determinado tratamiento de datos de valores históricos, científicos o estadísticos, a los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento, se iniciará siempre a petición del responsable que pretenda obtener la declaración.
2. En el escrito de solicitud, el responsable deberá:

   a) Identificar claramente el tratamiento de datos al que pretende aplicarse la excepción.
   b) Motivar expresamente las causas que justificarían la declaración.
   c) Exponer detalladamente las medidas que el responsable del fichero se propone implantar para garantizar el derecho de los ciudadanos.

3. La solicitud deberá acompañarse de cuantos documentos o pruebas sean necesarios para justificar la existencia de los valores históricos, científicos o estadísticos que fundamentarían la declaración de la Agencia.

Artículo 158. Duración del procedimiento y efectos de la falta de resolución expresa.

1. El plazo máximo para dictar y notificar resolución en el procedimiento será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud del responsable del fichero.
2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud.

Anexo IX

Legislación mexicana federal sobre delitos informáticos y en materia autoral

(Reformas publicadas en el **DOF** *del 17 de mayo de 1999)*

CÓDIGO PENAL FEDERAL

Título noveno

Revelación de secretos y acceso ilícito a sistemas y equipos de informática

Capítulo II

Acceso ilícito a sistemas y equipos de informática

Artículo 211 bis 1. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad se le impondrán de seis meses a dos años de prisión y de cien a trescientos días de multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días de multa.

Artículo 211 bis 2. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días de multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días de multa.

Artículo 211 bis 3. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

Artículo 211 bis 4. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6. Para los efectos de los artículos 211 bis 4 y 211 bis 5 anteriores, se entiende por instituciones que integran el sistema financiero las señaladas en el artículo 400 bis de este Código.

Artículo 211 bis 7. Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho.

Título vigesimosexto

De los delitos en materia de Derechos de Autor

Artículo 424. Se impondrán prisión de seis meses a seis años y de trescientos a tres mil días multa:

I. Al que especule en cualquier forma con los libros de texto gratuitos que distribuye la Secretaría de Educación Púb*lica;
II. Al editor, productor o grabador que a sabiendas produzca más números de ejemplares de una obra protegida por la *Ley Federal del Derecho de Autor* que los autorizados por el titular de los derechos;

III. A quien produzca, reproduzca, importe, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros protegidos por la *Ley Federal del Derecho de Autor* en forma dolosa, a escala comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.

Artículo 424 bis. Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

I. A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros protegidos por la *Ley Federal del Derecho de Autor* en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.

   Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior, o

II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

Artículo 424 ter. Se impondrá prisión de seis meses a seis años y de cinco mil a treinta mil días multa a quien venda a cualquier consumidor final en vías o en lugares públicos, en forma dolosa, con fines de especulación comercial, copias de obras, fonogramas, videogramas o libros a que se refiere la fracción I del artículo anterior.

Si la venta se realiza en establecimientos comerciales, o de manera organizada o permanente, se estará a lo dispuesto en el artículo 424 bis de este Código.

Artículo 425. Se impondrá prisión de seis meses a dos años o de trescientos a tres mil días multa al que a sabiendas y sin derecho explote con fines de lucro una interpretación o una ejecución.

Artículo 426. Se impondrá prisión de seis meses a cuatro años y de trescientos a tres mil días multa, en los casos siguientes:

I. A quien fabrique, importe, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal, y

II. A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal.

Artículo 427. Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa a quien publique a sabiendas una obra sustituyendo el nombre del autor por otro nombre.

Artículo 428. Las sanciones pecuniarias previstas en el presente título se aplicarán sin perjuicio de la reparación del daño, cuyo monto no podrá ser menor al

cuarenta por ciento del precio de venta al público de cada producto o de la prestación de servicios que impliquen violación a alguno o algunos de los derechos tutelados por la *Ley Federal del Derecho de Autor*.

Artículo 429. Los delitos previstos en este título se perseguirán por querella de parte ofendida, salvo el caso previsto en el artículo 424, fracción I, que será perseguido de oficio. En el caso de que los derechos de autor hayan entrado al dominio público, la querella la formulará la Secretaría de Educación Pública, considerándose como parte ofendida.

Anexo X

Regulación de los delitos informáticos en los ordenamientos jurídicos penales de las entidades federativas y el Distrito Federal (México)

AGUASCALIENTES

Legislación penal

Capítulo Decimosegundo

Tipos penales protectores de la confidencialidad

Artículo 80. La Violación de Correspondencia consiste en abrir o interceptar en forma dolosa una comunicación escrita, electrónica, magnética, óptica o informática que no esté dirigida al inculpado.

Al responsable de Violación de Correspondencia se le aplicarán de 3 a 6 meses de prisión y de 5 a 20 días multa, y al pago total de la reparación de los daños y perjuicios ocasionados.

Esta punibilidad no se aplicará si el responsable ejerce la patria potestad, tutela o custodia, y si la comunicación escrita se dirige a las personas bajo su tutela o guarda.

Capítulo Decimoséptimo

Tipos penales protectores del Fisco Estatal

Artículo 89. La Defraudación Fiscal consiste en:

[...]

XIII. Llevar dos o más libros similares o sistemas informáticos con distintos asientos o datos para registrar sus operaciones contables, fiscales o sociales;

XIV. Destruir, ordenar o permitir la destrucción total o parcial de los libros de contabilidad o sistemas informáticos previstos en la fracción anterior,

XV. Utilizar pastas o encuadernaciones de los libros a que se refiere la fracción XIII, para sustituir o cambiar las páginas foliadas, o alterar los sistemas informáticos de contabilidad que correspondan.

Título tercero

Actividad procesal

Capítulo primero

Artículo 228. Las promociones que se hagan por escrito deberán presentarse por triplicado o duplicado, según el caso, y estarán firmadas por su autor o llevarán su huella digital, pudiéndose ordenar su ratificación cuando se estime necesario; pero deberán ser siempre ratificadas si el que las hace no las firma por cualquier motivo.

Los documentos que se acompañen a las promociones deberán ser originales o con copia fotostática debidamente autorizada. En caso de utilización de respaldos informáticos o electrónicos, las promociones también podrán realizarse por ese medio.

Artículo 230. Los expedientes no podrán entregarse a los sujetos procesales interesados, los cuales podrán imponerse de ellos en la Secretaría del Tribunal o en la Agencia del Ministerio Público correspondiente. Esto no operará respecto del Ministerio Público o del Defensor de Oficio, en su caso, cuando se les dé vista para formular conclusiones, pero tal entrega se hará en las propias oficinas adscritas al tribunal correspondiente.

En caso de utilizar medios informáticos o electrónicos, sólo los sujetos procesales autorizados tendrán acceso a la información de tal medio, mediante la aplicación de los mecanismos de control existentes para el efecto.

BAJA CALIFORNIA

Código penal

Título tercero

Delitos contra la inviolabilidad del secreto y de los sistemas y equipos de informática

Capítulo I

Revelación del secreto

Artículo 175. Fue reformado por Decreto No. 161, publicado en el Periódico Oficial No. 24, de fecha 12 de junio de 1998, Sección I, Tomo CV, expedido por la H.

XV Legislatura, siendo Gobernador Constitucional del Estado el C. Lic. Héctor Terán Terán, 1995- 2001; fue reformado por Decreto No. 378, publicado en el Periódico Oficial No. 38, de fecha 14 de septiembre de 2007, Tomo CXIV, Sección IV, expedido por la H. XVIII Legislatura, siendo Gobernador Constitucional el C. Eugenio Elorduy Walther 2001-2007; para quedar vigente como sigue:

Artículo 175. Tipo y punibilidad. Al que sin consentimiento de quien tenga derecho a otorgarlo revele un secreto de carácter científico, industrial o comercial, o lo obtenga a través de medios electrónicos o computacionales, se le haya confiado, conoce o ha recibido con motivo de su empleo o profesión y obtenga provecho propio o ajeno se le impondrá prisión de uno a tres años y hasta cincuenta días multa, y, en su caso, suspensión de dos meses a un año en el ejercicio de su profesión; si de la revelación del secreto resulta algún perjuicio para alguien, la pena aumentará hasta una mitad más. Al receptor que se beneficie con la revelación del secreto se le impondrán de uno a tres años de prisión y hasta cien días multa.

Capítulo II

Pornografía y turismo sexual de personas menores de dieciocho años de edad o de quienes no tienen la capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo

Artículo 262. Fue reformado por Decreto No. 161, publicado en el Periódico Oficial No. 24, de fecha 12 de junio de 1998, Sección I, Tomo CV, expedido por la H. XV Legislatura, siendo Gobernador Constitucional del Estado el C. Lic. Héctor Terán Terán, 1995- 2001; fue reformado por Decreto No. 191, publicado en el Periódico Oficial No. 7, de fecha 17 de febrero de 2006, Tomo CXIII, expedido por la H. XVIII Legislatura siendo Gobernador Constitucional el C. Eugenio Elorduy Walther 2001-2007; fue reformado por Decreto No. 330, publicado en el Periódico Oficial No. 20, de fecha 11 de mayo de 2007, Sección I, Tomo CXIV, expedido por la Honorable XVIII Legislatura, siendo Gobernador Constitucional el C. Lic. Eugenio Elorduy Walter 2001-2007; para quedar vigente como sigue:

Artículo 262. Pornografía de personas menores de dieciocho años de edad o de quien no tiene la capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo. A quien procure, facilite, induzca, propicie, obligue o permita a una persona menor de dieciocho años de edad o quien no tiene la capacidad para comprender el significado del hecho o de quien no tiene la capacidad para resistirlo, a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de filmarlos, grabarlos, audiograbarlos, videograbarlos, describirlos, fotografiarlos o exhibirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, medios electrónicos o de cualquier otra naturaleza, se le aplicarán de siete a doce años de prisión y de mil a dos mil días multa.

BAJA CALIFORNIA SUR

Código penal

Libro segundo: delitos en particular

Título cuarto

Delitos contra la procuración y la administración de justicia

Capítulo IV

Robo y destrucción de documentos

Artículo 182. El robo o la destrucción dolosa de expedientes, constancias procesales y documentos que contengan obligación, liberación o transmisión de derechos que obren en los expedientes, archivos o cajas de seguridad de las instituciones encargadas de la procuración y administración de justicia o de la ejecución de penas y medidas de seguridad se castigará con pena de dos a doce años de prisión y multa hasta de doscientos días de salario.

La misma pena se aplicará a quien destruya, altere o copie indebidamente constancias, resoluciones o informes contenidos en memorias o archivos electrónicos pertenecientes a los órganos de procuración y administración de justicia o a las autoridades encargadas de la ejecución de penas.

Si el delito lo comete un servidor publico se le impondrá, además, la destitución y la inhabilitación para desempeñar otro empleo, cargo o comisión públicos por un término de hasta dos años.

Artículo 195. Se impondrá de uno a nueve años de prisión y multa de hasta cinco mil días de salario a quien, sin consentimiento de la persona o empresa autorizada y fuera de los casos de competencia federal:

I. Produzca, imprima, enajene, distribuya, altere o falsifique tarjetas, títulos o documentos utilizados para el pago de bienes y servicios o para la disposición de efectivo;
II. Adquiera, utilice o posea tarjetas, títulos o documentos para el pago de bienes y servicios, a sabiendas de que son alterados o falsificados;
III. Acceda ilegalmente a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo, y
IV. Adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes o servicios o para disposición de efectivo, así como información sustraída de esta forma.

Capítulo III

Lenocinio

Artículo 217. Al que explote a un menor mediante actos de prostitución o exhibicionismo se le impondrán de dos a nueve años de prisión y multa de cincuenta a doscientos días de salario.

Cuando los actos lascivos se realicen para videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, tendrá una pena de tres a diez años de prisión.

CAMPECHE

No existe regulación que tipifique alguna conducta.

COAHUILA

Código penal

(Adicionado, P.O. 1 de septiembre de 2006.)

Capítulo tercero

Delitos contra la seguridad en los medios informáticos

Artículo 281 bis. Sanciones y figuras típicas de los delitos contra la seguridad en los medios informáticos cometidos en perjuicio de particulares. Se aplicará prisión de tres meses a tres años y multa a quien:

I. Sin autorización para acceder a un sistema informático y con perjuicio de otro, conozca, copie, imprima, use, revele, transmita o se apodere de datos o información reservados, contenidos en el mismo;
II. Con autorización para acceder a un sistema informático y con perjuicio de otro, obtenga, sustraiga, divulgue o se apropie de datos o información reservados en él contenidos.

Si la conducta que en uno u otro caso se realiza es con el ánimo de alterar, dañar, borrar, destruir o de cualquier otra manera provocar la pérdida de datos o información contenidos en el sistema, la sanción será de cuatro meses a cuatro años de prisión y multa.

Artículo 281 bis 1. Circunstancias agravantes de los delitos anteriores. Las penas previstas en el artículo anterior se incrementarán en una mitad más:

I. Si el agente actuó con fines de lucro;
II. Si el agente accedió al sistema informático valiéndose de información privilegiada que le fue confiada en razón de su empleo o cargo, o como responsable de su custodia, seguridad o mantenimiento.

Artículo 281 bis 2. Sanciones y figuras típicas de los delitos contra la seguridad en los medios informáticos cometidos en perjuicio de una entidad pública. Se aplicará prisión de seis meses a seis años y multa a quien:

I. Sin autorización, acceda por cualquier medio a un sistema informático de una entidad pública de las mencionadas en el párrafo segundo del artículo 194, para conocer, copiar, imprimir, usar, revelar, transmitir o apropiarse de sus datos o información propios o relacionados con la institución;
II. Con autorización para acceder al sistema informático de una entidad pública de las mencionadas en el párrafo segundo del artículo 194, indebidamente copie, transmita, imprima, obtenga sustraiga, utilice, divulgue o se apropie de datos o información propios o relacionados con la institución.

Si la conducta que en uno u otro caso se realiza tiene la intención dolosa de alterar, dañar, borrar, destruir o de cualquier otra forma provocar la pérdida de los datos o información contenidos en el sistema informático de la entidad pública, la sanción será de uno a ocho años de prisión y multa.

Si el sujeto activo del delito es servidor público, se le sancionará, además, con la destitución del empleo, cargo o comisión e inhabilitación para ejercer otro hasta por seis años.

Artículo 281 bis 3. Circunstancias agravantes en los delitos anteriores. Las penas previstas en el artículo anterior se incrementarán en una mitad más:

I. Si el agente obró valiéndose de alguna de las circunstancias agravantes previstas en el artículo 290 bis 1;
II. Si el hecho constitutivo de delito fue cometido contra un dato o sistemas informáticos concernientes al régimen financiero de las entidades públicas que se mencionan en el artículo 194, o por funcionarios o empleados que estén a su servicio;
III. Si la conducta afectó un sistema o dato referente a la salud o seguridad pública o a la prestación de cualquier otro servicio público.

Artículo 281-bis 4. Norma complementaria en orden a la terminología propia de los delitos contra la seguridad de los medios informáticos. A los fines del presente capítulo, se entiende por:

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

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

Artículo 281-bis 4. Norma complementaria en orden a la terminología propia de los delitos contra la seguridad de los medios informáticos. A los fines del presente capítulo, se entiende por:

I. Sistema informático: todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos para generar, enviar, recibir, recuperar, procesar o almacenar información de cualquier forma o por cualquier medio;
II. Dato informático o información: toda representación de hechos, manifestaciones o conceptos, contenidos en un formato que puede ser tratado por un sistema informático.

(Reformado el primer párrafo, P.O. 1 de septiembre de 2006.)

Artículo 301. Sanciones y figura típica de pornografía infantil de menores e incapaces. Se aplicará prisión de siete a once años y multa, así como el decomiso de los objetos, instrumentos y productos del delito, incluyendo la destrucción de los materiales gráficos o grabados, a quien procure, obligue, facilite o induzca por cualquier medio o utilice a un menor de dieciocho años de edad, o a una persona sin capacidad de comprender el significado del hecho o de decidir conforme a esa comprensión, o que por cualquier circunstancia personal no pueda resistirlo, para realizar actos de exhibicionismo corporal, o sexuales, lascivos o pornográficos, con el propósito de videograbarlo, filmarlo, fotografiarlo o exhibirlo, por cualquier medio, con o sin fin de obtener un lucro. La misma sanción se impondrá a quien financie, elabore, reproduzca, comercialice, distribuya, arriende, exponga o publicite el material a que se refieren las conductas descritas.

(Reformado, P.O. 1 de septiembre de 2006.)

Las sanciones que señala este artículo serán de un tercio más del mínimo y máximo, si el corruptor es ascendiente del menor o incapaz, o si al ejecutar los actos ejercía cualquier forma de autoridad sobre aquéllos, lo mismo que si el delito se comete en perjuicio de un menor de doce años. En ambos supuestos; además, en su caso, se le privará de la patria potestad, tutela o guarda que ejerza y de todos los derechos sobre los bienes del ofendido.

Para los efectos de este Código se considera acto de pornografía toda representación realizada por cualquier medio de actividades obscenas sexuales, explícitas, reales o simuladas.

No constituyen pornografía infantil: las fotografías, videograbaciones, audiograbaciones o las imágenes fijas o en movimiento, impresas, plasmadas o que sean contenidas o reproducidas en medios magnéticos, electrónicos o de otro tipo y que constituyan recuerdos familiares, los programas preventivos, educativos o de cualquier índole que diseñen e impartan las instituciones públicas, privadas o sociales que tengan por objeto la educación sexual, educación sobre función reproductiva, la prevención de enfermedades de transmisión sexual o el embarazo de adolescentes.

COLIMA

Código penal

(Última reforma según decreto No. 159, aprobado el 10 de octubre de 2007.)

Artículo 10. Se califican como delitos graves, para todos los efectos legales, por afectar de manera importante valores fundamentales de la sociedad, los siguientes delitos previstos por este Código: REBELIÓN, tipificado por el artículo 104; los supuestos previstos por el artículo 108; FALSEDAD ANTE LA AUTORIDAD, establecido por el artículo 117; EVASIÓN DE PRESOS, conforme al segundo párrafo del artículo 121; PECULADO, tipificado por el artículo 131; DELITOS CONTRA LA SEGURIDAD VIAL Y LOS MEDIOS DE TRANSPORTE, establecidos en el segundo párrafo del artículo 145; CORRUPCIÓN DE MENORES, en su modalidad de procurar o facilitar de cualquier forma el consumo de algún tipo de estupefaciente, psicotrópico o vegetales que determine la *Ley General de Salud*, como ilegales, a un menor o de quien no tenga capacidad para comprender el significado del hecho, tipificado por el segundo párrafo del artículo 155, así como en su modalidad de EXPLOTACIÓN PORNOGRÁFICA, prevista por el artículo 157 bis, segundo párrafo, tratándose de la realización de acto de exhibicionismo corporal lascivo o sexual, con el objeto de videograbarlo, fotografiarlo o exhibirlo mediante anuncio impreso o electrónico; LENOCINIO, del numeral 161; HOMICIDIO, tipificado por los artículos 169, 170, 171, 172 tratándose del provocador, y las fracciones II y III del 173; LESIONES, conforme a los artículos 174, fracciones VI y VII, 175, 176, 177, 178, 179 y 183; HOMICIDIO Y LESIONES CULPOSAS, previstas en el artículo 184 bis; PRIVACIÓN DE LA LIBERTAD, previsto por el artículo 197; SECUESTRO, previsto por el artículo 199; VIOLACIÓN en todas sus formas y modalidades, que comprenden los artículos 206, 207, 208, 209 y 210; ROBO, respecto de los supuestos del inciso B) del artículo 227; los FRAUDES ESPECÍFICOS, previstos en las fracciones III, IV, V y VI del artículo 234; DAÑOS, tipificado por el artículo 238. Igualmente se consideran graves los delitos de TENTATIVA DE HOMICIDIO y SECUESTRO, así como la TENTATIVA DE ROBO, previsto por el inciso *b*) del artículo 227, y la TENTATIVA DE VIOLACIÓN, previsto por los artículos 206, 207, 208, 209 y 210; así como los DELITOS CONTRA EL AMBIENTE, previstos por los artículos 243 en su segundo párrafo y la fracción III del 244.

En tratándose de DELITOS DE LESIONES, se exceptúan de lo dispuesto por el párrafo anterior los casos previstos en los artículos 175, 176, 177 y 178, cuando las lesiones sean de las señaladas en las fracciones I y II del artículo 174.

Capítulo II

Corrupción de menores

(Reformado, P.O. 28 dic. de 2002.)

Artículo 157-bis. Al que explote a un menor o a quien no tenga capacidad para comprender el significado del hecho, con fines de lucro o para conseguir una

satisfacción de cualquier naturaleza, se le impondrá de dos años seis meses a ocho años de prisión y multa hasta por quinientas unidades.

Para los efectos de este artículo se tipifica como explotación de menor o de quien no tenga capacidad para comprender el significado del hecho, el permitir, inducir u obligar al sujeto pasivo, a la práctica de la mendicidad, o a realizar acto de exhibicionismo corporal, libidinoso o de naturaleza sexual, con el objeto de videograbarlo o fotografiarlo o exhibirlo mediante cualquier tipo de impreso o medio electrónico.

Capítulo III

Fraude

[...]

Artículo 234. Se considera fraude y se impondrá pena de uno a nueve años de prisión y multa hasta por 100 unidades, para el caso de las fracciones I y II, y de tres a nueve años de prisión y multa hasta por la misma cantidad en el caso de las fracciones III, IV, V y VI, en los siguientes casos:

[...]

III. Uso indebido de tarjetas y documentos de pago electrónico. Al que sin el consentimiento de su titular o de quien esté facultado para ello, haga uso de una tarjeta, título, documento o instrumento de pago electrónico, bien sea para disposición en efectivo o para el pago de bienes y servicios.

Igual pena se impondrá a quien teniendo el consentimiento de su titular o de quien esté facultado para ello, haga un uso indebido de tarjetas, títulos, documentos o instrumentos de pago electrónico, bien sea para el pago de bienes y servicios o para disposición en efectivo;

IV. Uso de tarjetas, títulos, documentos o instrumentos para el pago electrónico, falsos. Al que a sabiendas de que una tarjeta, título, documento o instrumento para el pago electrónico de bienes y servicios o para la disposición de efectivo, haga uso de él y obtenga un lucro indebido en perjuicio del titular de la tarjeta, título, documento o instrumento indubitable;

(Reformado mediante decreto No. 193, aprobado el 19 de abril de 2005.)

V. Acceso indebido a los equipos y sistemas de cómputo o electromagnéticos. Al que con el ánimo de lucro y en perjuicio del titular de una tarjeta, documento o instrumentos para el pago de bienes y servicios o para disposición en efectivo, acceda independientemente a los equipos y servicios de cómputo o electromagnéticos de las instituciones emisoras de los mismos, y

VI. Uso indebido de información confidencial o reservada de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición en efectivo. A quien obtenga un lucro en perjuicio del titular de una tarjeta, título, documento o instrumento para el pago electrónico de bienes y servicios o para la disposición de efectivo, mediante la utilización de información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir los mismos.

Si el sujeto activo es empleado o dependiente del ofendido, la pena corporal aumentará de cuatro años seis meses, la mínima, y de trece años seis meses la máxima.

CHIAPAS

Código penal

Título quinto

Delitos contra el honor

Capítulo I

Difamación

Artículo 164. La difamación consiste en comunicar dolosamente en forma escrita o verbal a una o más personas, a imputación que se hace a otra persona física o moral de un hecho cierto o falso, determinado o indeterminado, que pueda causarle deshonra, descrédito, perjuicio o afecte su reputación. Se sancionará al responsable con prisión de dos a cinco años y multa hasta de setenta y cinco días de salario.

Este delito se sancionará con prisión de tres a nueve años y de cien a mil días de multa.

[...]

Capítulo II

Calumnia

[...]

Artículo 168. Comete el delito de calumnia el que formule denuncia o querella respecto de una persona que sabe que no es la responsable o que no ha realizado el hecho determinado y calificado como delito.

[...]

Capítulo III

Disposiciones comunes para los capítulos precedentes

[...]

Artículo 173. Siempre que sea condenado el autor de una difamación o de una calumnia, si lo solicita la persona ofendida se publicará la sentencia en tres periódicos de circulación en la entidad, a costa de aquél. Cuando la infracción se cometa por conducto de algún medio de comunicación, los dueños, gerentes o directores de éste, sean o no infractores, estarán obligados a difundir la sentencia en la misma sección donde se publicó y si es un medio electrónico en el mismo horario y programa donde se dio a conocer, imponiéndoseles dos días de multa por cada día que pase sin hacerlo después de aquel en que se les notifique la sentencia.

[...]

Capítulo V

Fraude

Artículo 199. A quien engañando a alguien o aprovechándose del error en que éste se halla obtenga ilícitamente alguna cosa ajena o alcance un lucro indebido se le impondrán las siguientes sanciones:

I. Prisión de seis meses a dos años y multa hasta de cien días de salario cuando el valor de lo defraudado no exceda de doscientos días de salario;
II. Prisión de dos a cinco años y multa de cincuenta a noventa días de salario cuando el valor de lo defraudado fuere mayor de doscientos, pero no de mil días de salario, y
III. Prisión de cuatro a diez años y multa hasta de ciento ochenta días de salario si el valor de lo defraudado excede de mil días.

Artículo 200. Se aplicarán las mismas sanciones previstas en el artículo anterior:

[...]

XXIII. Al que para obtener algún beneficio para sí o para un tercero por cualquier medio acceda, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la institución.

Capítulo II

Corrupción de niños, niñas, adolescentes o incapacitados

[...]

Artículo 208 bis. Comete el delito de pornografía infantil el que procure, facilite o induzca por cualquier medio a un niño, niña o adolescente, con o sin su consentimiento, a realizar actos de exhibicionismo corporal pasivos o sexuales, con el objeto y fin de videograbarlo, fotografiarlo o exhibirlo mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro, y se le impondrán de cinco a diez años de prisión y de mil a dos mil días multa.

Al que filme, grabe, imprima actos de exhibicionismo corporal, lascivos o sexuales, en que participen uno o más niños, niñas o adolescentes, se le impondrá la pena de diez a catorce años de prisión y de quinientos a tres mil días multa. La misma pena se impondrá a quien con fines de lucro o sin él elabore, reproduzca, venda, arriende, exponga, publicite o difunda el material a que se refieren las acciones anteriores.

Para los efectos de este artículo, se entiende por pornografía infantil la representación sexualmente explícita de imágenes de niños, niñas o adolescentes.

[...]

Capítulo II

Falsificación de documentos en general

[...]

Artículo 262 bis. Se impondrán de tres a nueve años de prisión y de ciento cincuenta a cuatrocientos días multa al que sin consentimiento de quien esté facultado para ello:

I. Produzca, imprima, enajene, distribuya, altere o falsifique, aun gratuitamente tarjetas, títulos o documentos utilizados para el pago de bienes y servicios o para disposición de efectivo;
II. Adquiera, utilice, posea o detente indebidamente tarjetas, títulos o documentos para el pago de bienes y servicios, a sabiendas de que son alterados o falsificados;
III. Adquiera, utilice, posea o detente indebidamente tarjetas, títulos o documentos para el pago de bienes y servicios, sin consentimiento de quien esté facultado para ello;
IV. Altere los medios de identificación electrónicos de tarjetas, títulos o documentos para el pago de bienes y servicios, o
V. Acceda indebidamente a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos, para el pago de bienes y servicios o para disposición de efectivo.

Las mismas penas se impondrán a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos o documentos utilizados para el pago de bienes y servicios.

Si el sujeto activo es empleado o dependiente del ofendido, las penas se aumentarán en una mitad.

En el caso de que se actualicen otros delitos con motivo de las conductas a que se refiere este artículo, se aplicarán las reglas del concurso.

Título decimoquinto

Delitos de revelación de secretos y de acceso ilícito a sistemas y equipos de informática

Capítulo I

Revelación de secretos

Artículo 283. Se aplicará sanción de dos a cuatro años y multa de veinte a cuarenta días de salario al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado revele algún secreto o comunicación reservada, que conoce o ha recibido con motivo de su empleo, cargo o puesto.

Capítulo II

Acceso ilícito a sistemas de informática

Artículo 284 ter. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipo de informática protegidos por algún mecanismo o sistema de seguridad o que no tenga derecho de acceso a él se le impondrá una sanción de uno a cuatro años de prisión y de cuarenta a doscientos días multa.

Al que estando autorizado o tenga derecho de acceso a los sistemas o equipo de informática protegido por algún mecanismo o sistema de seguridad, indebidamente destruya, modifique o provoque pérdida de información que contengan los mismos, la pena prevista en el párrafo anterior se aumentará en una mitad.

Artículo 284 quáter. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistema o equipo de informática de alguna dependencia pública protegida por algún sistema o mecanismo de seguridad se le impondrá una sanción de dos a seis años de prisión y de doscientos a seiscientos días de multa.

Artículo 284 quínter. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de alguna dependencia pública protegida por algún sistema o mecanismo de seguridad se le impondrá pena de dos a cinco años de prisión y de cien a trescientos días multa.

Artículo 284 séxter. Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública indebidamente modifique, destruya o provoque pérdida de información que contengan se le impondrá prisión de tres a ocho años y de trescientos a ochocientos días multa.

Artículo 284 sépter. Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública indebidamente copie, transmita o imprima información que contengan se le impondrá de uno a cuatro años de prisión y de cien a trescientos días multa.

Artículo 284 ócter. Los delitos previstos en este título serán sancionados por querella de parte ofendida.

CHIHUAHUA

Código penal

Capítulo II

Pornografía con personas menores de edad o que no tienen la capacidad para comprender el significado del hecho

Artículo 185. Comete este delito:

I. Quien produzca, fije, grabe, videograbe, fotografíe o filme de cualquier forma imágenes o la voz de una persona menor de edad o de una persona que no tenga la capacidad para comprender el significado del hecho, sea en forma

directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas;

II. Quien reproduzca, publique, publicite, distribuya, difunda, exponga, envíe, transmita, importe, exporte o comercialice de cualquier forma imágenes o la voz de una persona menor de edad o de una persona que no tenga la capacidad para comprender el significado del hecho, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas;

III. Quien ofrezca, posea o almacene intencionalmente para cualquier fin imágenes o la voz de personas menores de edad o de personas que no tengan la capacidad de comprender el significado del hecho, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas.

Al autor de los delitos previstos en este artículo se le impondrá prisión de seis meses a seis años y quinientos a dos mil días multa.

A quien financie, dirija, administre o supervise cualquiera de las actividades anteriores con la finalidad de que se realicen las conductas previstas en las fracciones de este artículo se le impondrá pena de prisión de siete a once años y multa de mil a cuatro mil días.

[...]

Título decimocuarto

Delitos contra el patrimonio

Capítulo I

Robo

Artículo 208. A quien con ánimo de dominio y sin consentimiento de quien legalmente pueda otorgarlo se apodere de una cosa mueble ajena se le impondrá:

I. Cuando el valor de lo robado no exceda de quinientas veces el salario, se impondrán de seis meses a dos años de prisión y multa de treinta a cien veces el salario;

II. Cuando exceda de quinientas veces el salario, pero no de mil, la sanción será de dos a cuatro años de prisión y multa de cien a doscientas veces el salario;

III. Cuando exceda de mil veces el salario, la sanción será de cuatro a diez años de prisión y multa de doscientas a quinientas veces el salario.

Para estimar la cuantía del robo se atenderá al valor comercial de la cosa robada al momento del apoderamiento, pero si por alguna circunstancia no fuera estimable en dinero o si por su naturaleza no fuera posible fijar su valor, se aplicarán de seis meses a cinco años de prisión y multa de treinta a ochenta veces el salario.

En los casos de tentativa de robo, cuando no fuera posible determinar el monto, la pena será de seis meses a dos años de prisión.

Artículo 211. Además de las sanciones que correspondan conforme a los artículos anteriores, se aplicará prisión de seis meses a tres años cuando el robo:

[...]

VII. Recaiga en un expediente, documento o en cualquier información que se encuentre registrada o archivada en sistema o equipo de informática protegidos por algún mecanismo de seguridad, con afectación de alguna función pública.

Capítulo X

Daños

Artículo 238. Se aplicará prisión de seis meses a seis años al que deteriore o destruya expediente o documento de oficina o archivos públicos.

[...]

Las mismas penas se aplicarán al que destruya, altere o provoque pérdida de información contenida en sistema o equipo de informática de oficina o archivos públicos, protegidos por algún mecanismo de seguridad.

Podrá aumentarse la pena señalada hasta el doble, según la gravedad del daño que resulte, si no puede reponerse el expediente, la información a que se refiere el párrafo anterior, ni suplirse la falta del documento.

La misma pena señalada en el primer párrafo de este artículo se aplicará al que dolosamente cause destrucción o deterioro de un bien mueble o inmueble público o cultural del Estado.

Capítulo II

Violación de correspondencia

Artículo 326. A quien abra o intercepte una comunicación escrita que no esté dirigida a él se le impondrán de treinta a noventa días multa.

Los delitos previstos en este artículo se perseguirán por querella.

La misma sanción se impondrá en los casos en que la comunicación se encuentre registrada o archivada en sistemas o equipos de informática protegidos por algún mecanismo de seguridad.

DISTRITO FEDERAL

Código penal

Capítulo III

Pornografía

Artículo 187. Al que procure, promueva, obligue, publicite, gestione, facilite o induzca, por cualquier medio, a una persona menor de dieciocho años de edad

o persona que no tenga la capacidad de comprender el significado del hecho o de persona que no tiene capacidad de resistir la conducta a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de videograbarlos, audiograbarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, sistemas de cómputo, electrónicos o sucedáneos se le impondrán de siete a catorce años de prisión y de dos mil quinientos a cinco mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito, incluyendo la destrucción de los materiales mencionados.

[...]

Artículo 188. Al que almacene, compre o arriende el material a que se refiere el artículo anterior, sin fines de comercialización o distribución, se le impondrán de uno a cinco años de prisión y de cien a quinientos días multa

Título decimoquinto

Delitos contra el patrimonio

Capítulo III

Fraude

Artículo 231. Se impondrán las penas previstas en el artículo anterior, a quien:

[...]

XIV. Para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución, o

[...]

Capítulo VI

Extorsión

Artículo 236. Al que obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro causando a alguien un perjuicio patrimonial, se le impondrán de dos a ocho años de prisión y de cien a ochocientos días multa.

[...]

Asimismo, las penas se incrementarán en una mitad cuando se utilice como medio comisivo la vía telefónica, el correo electrónico o cualquier otro medio de comunicación electrónica.

Título vigesimocuarto

Delitos contra la fe pública

Capítulo I

Producción, impresión, enajenación, distribución, alteración o falsificación de títulos al portador, documentos de crédito públicos o vales de canje

Artículo 336. Se impondrán de tres a nueve años de prisión y de cien a cinco mil días multa al que, sin consentimiento de quien esté facultado para ello:

[...]

IV. Altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios;

V. Acceda a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo;

VI. Adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes o servicios o para disposición de efectivo, así como a quien posea o utilice la información sustraída, de esta norma, o

[...]

Código de Procedimientos Penales

Artículo 229. Cuando se trate de delito grave en el que haya concurrido violencia física, delito que atente contra la libertad y el normal desarrollo psicosexual o en aquellos en los que un menor aparezca como víctima o testigo, a petición de la víctima, testigo, del representante legal del menor o del Ministerio Público, el careo se llevará a cabo en recintos separados, con la ayuda de cualquier medio electrónico audiovisual, de tal manera que el procesado pueda cuestionar a la víctima o los testigos durante la audiencia sin confrontarlos físicamente.

DURANGO

Código penal

Subtítulo sexto

Delitos contra la fe pública

Capítulo primero

Falsificación de títulos al portador y documentos de crédito público

Artículo 235. Se impondrán de tres a nueve años de prisión y de cien a cinco mil días multa, al que, sin consentimiento de quien esté facultado para ello:

I. Produzca, imprima, enajene, distribuya, altere o falsifique tarjetas, títulos o documentos utilizados para el pago de bienes y servicios o para disposición de efectivo;

II. Adquiera, utilice, posea o detente tarjetas, títulos o documentos para el pago de bienes y servicios, a sabiendas de que son alterados o falsificados;

III. Adquiera, utilice, posea o detente tarjetas, títulos o documentos auténticos para el pago de bienes y servicios, sin consentimiento de quien esté facultado para ello;

IV. Altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios;

V. Acceda a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo;

VI. Adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes o servicios o para disposición de efectivo, así como a quien posea o utilice la información sustraída de esta forma, o

VII. A quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos o documentos utilizados para el pago de bienes y servicios, o de los titulares de dichos instrumentos o documentos.

Si el sujeto activo es empleado o dependiente del ofendido, las penas se aumentarán en una mitad.

Utilización de imágenes y/o voz de personas menores de edad o personas que no tienen la capacidad para comprender el significado del hecho para la pornografía

Artículo 206. Comete el delito de utilización de imágenes y/o voz de personas menores de edad o personas que no tienen la capacidad para comprender el significado del hecho para la pornografía el que realice las siguientes conductas:

I. Produzca, fije, grabe, videograbe, fotografíe o filme e imprima de cualquier forma imágenes, sonidos o la voz de una persona menor de edad o de una persona que no tenga la capacidad para comprender el significado del hecho o de resistirlo, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas;

[...]

II. Reproduzca, publique, ofrezca, publicite, almacene, distribuya, difunda, exponga, envíe, transmita, importe, exporte o comercialice de cualquier forma imágenes, sonidos o la voz de una persona menor de edad o de una persona que no tenga la capacidad para comprender el significado del hecho o de resistirlo, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas, y

III. Posea intencionalmente para cualquier fin imágenes, sonidos o la voz de personas menores de edad o de personas que no tengan la capacidad de comprender el significado del hecho o de resistirlo, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas

Título cuarto

Delitos contra el patrimonio

Capítulo primero

Robo

Artículo 418. Se equipara al robo y se castigará como tal:

[...]

IV. El apoderamiento material de los documentos que contengan datos de computadoras, o el aprovechamiento o utilización de dichos datos, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.

[...]

Capítulo segundo

Abigeato

[...]

Artículo 421. Se impondrá de cinco a doce años de prisión, además del decomiso de los instrumentos del delito considerándose como tales los vehículos, refrigeradores, sierras y demás instrumentos que hayan utilizado en la comisión del delito, al que:

I. Altere o elimine con planchas, alambres y argollas o remarque los fierros, las marcas de herrar, consistentes en letras, números y signos combinados entre si, así como la extracción de los dispositivos electrónicos de identificación, en ganado mayor o ganado menor;

[...]

ESTADO DE MÉXICO

Código penal

Título quinto

Delito contra el proceso electoral

Capítulo único

Artículo 322. A los responsables de los medios de comunicación electrónicos y escritos que en la actividad de su profesión, el día de la elección induzcan dolosa-

mente al electorado a votar en favor o en contra de un determinado partido o candidato o que con sus manifestaciones pretendan influir en la decisión del elector, se les aplicará una sanción de quinientos a mil días multa.

Subtítulo cuarto

Delitos contra el pleno desarrollo y la dignidad de la persona

Capítulo I

De las personas menores de edad y quienes no tienen la capacidad para comprender el significado del hecho

Artículo 204. Comete el delito contra las personas menores de edad y quienes no tienen la capacidad para comprender el significado del hecho al que por cualquier medio, obligue, procure, induzca o facilite a una persona menor de edad o quien no tenga la capacidad para comprender el significado del hecho o la capacidad de resistirlo, a realizar las siguientes conductas:

[...]

A quien permita directa o indirectamente el acceso a personas menores de edad a escenas, espectáculos, obras gráficas o audiovisuales de carácter pornográfico, incluyendo la información generada o comunicada por medios electrónicos o cualquier otra tecnología, se le aplicará prisión de seis meses a dos años y multa de cincuenta a trescientos días multa.

Subtítulo cuarto

Delitos contra la fe pública

Capítulo IV

Falsificación y utilización indebida de títulos al portador, documentos de crédito público y documentos relativos al crédito

Artículo 174. Se impondrán de cuatro a diez años de prisión y de ciento cincuenta a quinientos días de salario mínimo de multa al que:

I. Produzca, imprima, enajene aun gratuitamente, distribuya, altere o falsifique tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo, sin consentimiento de quien esté facultado para ello;
II. Adquiera, utilice, posea o detente indebidamente, tarjetas, títulos o documentos para el pago de bienes y servicios, a sabiendas de que son alterados o falsificados;
III. Adquiera, utilice, posea o detente indebidamente, tarjetas, títulos o documentos auténticos para el pago de bienes y servicios, sin consentimiento de quien esté facultado para ello;

IV. Altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios, y
V. Acceda indebidamente a los equipos de electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo.

GUANAJUATO

Código penal

Capítulo II

Violación de correspondencia

Artículo 231. Se aplicarán de diez días a dos años de prisión y de diez a cuarenta días multa a quien indebidamente:

I. Abra, intercepte o retenga una comunicación que no le esté dirigida, y
II. Accese, destruya o altere la comunicación o información contenida en equipos de cómputo o sus accesorios u otros análogos.

No se impondrá pena alguna a quienes ejerciendo la patria potestad o la tutela ejecuten cualquiera de las conductas antes descritas, tratándose de sus hijos menores de edad o de quienes se hallen bajo su guarda.

Se requerirá querella de parte ofendida cuando se trate de ascendientes y descendientes, cónyuges o concubinos, parientes civiles o hermanos.

Capítulo II

(Reformado en su denominacion, P.O. 13 de agosto de 2004.)

Falsificación de documentos o tarjetas o uso de documentos o tarjetas falsos

(Adicionado, P.O. 13 de agosto de 2004.)

Artículo 234-a. Se impondrá prisión de tres a nueve años y de cuarenta a doscientos días multa a quien:

[...]

II. Falsifique o altere tarjetas, títulos o documentos, que puedan ser utilizados para el pago de bienes o servicios;

III. Adquiera, utilice, posea o detente tarjetas, títulos o documentos para el pago de bienes o servicios, a sabiendas de que son falsificados o alterados;

IV. Adquiera, utilice, posea o detente tarjetas, títulos o documentos para el pago de bienes o servicios, sin consentimiento de quien esté facultado para ello;

V. Altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes o servicios;

VI. Adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos o documentos para el pago de bienes o servicios, así como a quien posea o utilice la información sustraída de esta forma.

Si el sujeto activo es empleado o dependiente del ofendido, las penas se aumentarán en una mitad.

Título quinto

De los delitos contra el desarrollo de las personas menores e incapaces

Capítulo único

(Reformada su denominación, P.O. 13 de agosto de 2004.)

Corrupción de menores e incapaces

Explotación sexual

Artículo 236. A quien por cualquier medio obligue, emplee, facilite o induzca a una persona menor de dieciocho años o incapaz, a fin de que realice actos de exhibicionismo sexual, con el objeto de que se le observe, muestre, fotografíe, filme, videograbe o de cualquier modo se generen u obtengan imágenes impresas o electrónicas, se le impondrán de seis a quince años de prisión y de quinientos a cinco mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito, incluyendo la destrucción de los materiales gráficos.

Artículo 236-b. Se impondrá de seis a quince años de prisión y de quinientos a cinco mil días multa a quien:

I. Venda, comercialice, reproduzca, distribuya, transporte, arriende, exponga, publicite, difunda o de cualquier otro modo trafique con el material a que se refiere el artículo 236;

[...]

GUERRERO

Código penal

Título X

(Reformada su denominación, P.O. 20 de abril de 1999.)

Delitos en contra de las personas en su patrimonio

Capítulo I

Robo

Artículo 163. Al que se apodere de una cosa mueble ajena, con ánimo de dominio, sin consentimiento de quien pueda otorgarlo conforme a la ley, se le aplicarán las siguientes penas:

I. De uno a dos años de prisión y de sesenta a cien días multa, cuando el valor de lo robado no exceda de cien veces el salario;
II. De dos a cinco años de prisión y de ciento veinte a cuatrocientos días multa, y cuando el valor de lo robado exceda de cien pero no de quinientas veces el salario, y
III. De cinco a once años de prisión y de trescientos a quinientos días multa, cuando el valor de lo robado exceda de quinientas veces el salario.

Artículo 165. Se impondrán las mismas penas previstas en el artículo 163 a quien:

[...]

II. Aprovechando energía eléctrica, algún fluido, programas computarizados, señales televisivas o de internet, sin consentimiento de la persona que legalmente pueda disponer y autorizar aquéllas.

Capítulo II

(Reformada su denominación, P.O. 17 de abril de 2007.)

Pornografía con utilización de imágenes y/o voz de personas menores de edad o de personas que no tienen la capacidad para comprender el significado del hecho

Artículo 217. Comete este delito:

I. Quien produzca, fije, grabe, fotografíe o filme de cualquier forma imágenes, sonidos o la voz de una persona menor de edad o personas con capacidades diferentes o de una persona que no tenga la capacidad para comprender el significado del hecho, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas;
II. Quien reproduzca, publique, ofrezca, publicite, distribuya, difunda, exponga, envíe, transmita, importe, exporte o comercialice de cualquier forma imágenes, sonidos o la voz de una persona menor de edad o personas con capacidades diferentes o de una persona que no tenga la capacidad para comprender el significado del hecho, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas;
III. Quien posea o almacene intencionalmente para cualquier fin, imágenes, sonidos o la voz de personas menores de edad o personas con capacidades diferentes o de personas que no tengan la capacidad de comprender el significando del hecho, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiestan actividades sexuales o eróticas, explícitas o no, reales o simuladas.

Al autor de los delitos previstos en las fracciones I y II se le impondrá la pena de siete a doce años de prisión y de mil a cuatro mil días multa. Al autor de los

delitos previstos en la fracción III se le impondrá la pena de seis a diez años de prisión y de mil a cuatro mil días multa.

Capítulo III

(Reformada su denominación, P.O. 17 de abril de 2007.)

Lenocinio y pornografía

[...]

Artículo 218 bis. Comete el delito de pornografía el que promueva, financie, elabore, reproduzca, distribuya, exhiba, venda, arriende, publique, transmita o difunda la representación material de personas en actos sexuales reales o simulados para la gratificación sexual de los usuarios o toda representación de las partes genitales con fines de depravación mediante libros, escritos, pinturas, impresos, anuncios, emblemas, fotografías, películas, audiograbación o videograbación, representaciones digitales computarizadas o por cualquier otro medio. Al que cometa este delito se le aplicarán de tres a ocho de prisión y de cien a trescientos días multa.

...

Título V

(Reformado con el capítulo que lo integra, P.O. 13 de febrero de 2004.)

Delitos electorales

Capítulo único

Artículo 290. Para los efectos de este Capítulo se entiende por:

I. Funcionarios electorales,

[...]

[...]

IV. Documentos públicos electorales, a las boletas electorales, las actas de la jornada electoral, las actas oficiales de instalación de casillas, de los escrutinios y cómputo, de las mesas directivas de casilla, los paquetes electorales y expedientes de casilla, las actas circunstanciadas de las sesiones de cómputo de los consejos locales y distritales, la de los cómputos de circunscripción plurinominal, la correspondencia que circule bajo franquicia del órgano estatal electoral, archivos electrónicos computarizados y, en general, todos los documentos utilizados y actas expedidas en el ejercicio de sus funciones por los órganos del Instituto Electoral del Estado.

Artículo 292. Se impondrá multa de diez a cien días de salario mínimo general vigente en el estado y prisión de seis meses a tres años a quien:

[...]

X. Introduzca o sustraiga de las urnas ilícitamente una o más boletas electorales, destruya o altere boletas o documentos electorales;

[...]

HIDALGO

Código penal

Capítulo IX

Daño en la propiedad

Artículo 221. Al que por cualquier medio destruya o deteriore una cosa ajena o propia, con perjuicio de otro se le impondrá la punibilidad prevista en el artículo 203 de este Código conforme al monto de lo dañado.

Capítulo II

Delitos electorales cometidos por particulares

Artículo 352. Se impondrá prisión de tres meses a cinco años y multa de treinta a cien días de salario mínimo general vigente en el estado a quien:

[...]

XXVII. Dentro de los ocho días previos a la elección y hasta la hora oficial del cierre de las casillas, publique o difunda por cualquier medio los resultados de encuestas o sondeos de opinión que den a conocer las preferencias de los ciudadanos

Artículo 353. Se impondrá prisión de seis meses a tres años y multa de cien a quinientos días de salario mínimo general vigente en el Estado a los ministros del culto religioso que por cualquier medio en el desarrollo de actos propios de su ministerio induzcan expresamente al electorado a la abstención a votar en favor o en contra de un candidato, partido político o coalición.

JALISCO

Código penal

Título quinto bis

Delitos contra el desarrollo de la personalidad

Capítulo II

Pornografía infantil

Artículo 142-D. Se impondrá una pena de tres a quince años de prisión y multa de quinientos a diez mil días de salario mínimo a la persona que incurra en las siguientes conductas:

I. Induzca, obligue o entregue a una persona menor de dieciocho años de edad o que no tenga capacidad para comprender el significado del hecho, con o sin su consentimiento, para que realice o simule actos de exhibicionismo corporal, de naturaleza sexual o lasciva, con el fin de producir imágenes o sonidos de dichos actos a través de fotografías, filmes, videos, revistas o cualquier otro medio impreso, electrónico o tecnológico, con o sin ánimo de lucro;

[...]

[...]

IV. Reproduzca, venda, compre, rente, exponga, publicite, difunda o envíe por cualquier medio con o sin ánimo de lucro las imágenes o sonidos señalados en la fracción I de este artículo.

Se impondrá una multa de cien a quinientos días de salario mínimo a quien posea una o más fotografías, filmes, grabaciones o cualquier otro material impreso o electrónico que contenga las imágenes o sonidos señalados en este artículo, cuando sea de su conocimiento el hecho de la posesión y de la minoría de edad de las personas que aparecen en las imágenes.

Si las conductas señaladas en este artículo son cometidas por servidores públicos valiéndose de la función que desempeña, por quien tenga parentesco consanguíneo o por afinidad hasta el cuarto grado o por quienes laboran en organismos públicos o privados dedicadas al cuidado y atención de personas menores de dieciocho años de edad o que no tengan capacidad para comprender el significado del hecho, la pena se aumentará en una tercera parte de la que corresponda y procederá en su caso la destitución del puesto, comisión o cargo público.

Capítulo IV

Prostitución infantil

[...]

Artículo 142-H. Comete el delito de promoción de la prostitución infantil quien promueva, publicite, invite, facilite o gestione por cualquier medio a persona o personas a que viajen con la finalidad de que sostengan prácticas sexuales con menores de dieciocho años de edad o con quien no tengan capacidad para comprender el significado del hecho; o para que éste o éstos viajen con esa finalidad, o financie cualquiera de las actividades antes descritas, y se le impondrá una pena de seis a diez años de prisión y de mil a tres mil días multa.

Título sexto

Revelación de secretos y la obtención ilícita de información electrónica

Capítulo II

La obtención ilícita de información electrónica

Artículo 143 bis. Al que sin autorización y de manera dolosa copie, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de

informática se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días de multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando el sujeto pasivo del delito sea una entidad pública o institución que integre el sistema financiero.

Título noveno

Falsedad

Capítulo VIII

Falsificación de medios electrónicos o magnéticos

Artículo 170 bis. Se impondrán de tres a nueve años de prisión y multa por el equivalente de doscientos a cuatrocientos días de salario mínimo general vigente en la época y área geográfica en que se cometa el delito al que, sin consentimiento de quien esté facultado para ello:

I. Produzca, imprima, enajene, distribuya, altere o falsifique, aun gratuitamente, adquiera, utilice, posea o detente, sin tener derecho a ello, boletos, contraseñas, fichas, tarjetas u otros documentos que no estén destinados a circular y sirvan exclusivamente para identificar a quien tiene derecho a exigir la prestación que en ellos se consigna, siempre que estos delitos no sean de competencia federal;
II. Altere, copie o reproduzca, indebidamente, los medios de identificación electrónica de boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I de este artículo;
III. Acceda, obtenga, posea o detente indebidamente información de los equipos electromagnéticos o sistemas de cómputo de las organizaciones emisoras de los boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I de este artículo, y los destine a alguno de los supuestos que contempla el presente artículo, y
IV. Adquiera, utilice, posea o detente equipos electromagnéticos o electrónicos para sustraer en forma indebida la información contenida en la cinta magnética de los boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I del artículo.

Capítulo VII

Secuestro

Artículo 194. Comete el delito de secuestro quien prive ilegalmente de la libertad a otro con la finalidad de obtener rescate o de causar daño o perjuicio. Por rescate se entiende todo aquello que entrañe un provecho indebido y a cuya realización se condiciona la libertad del plagiado. Al responsable de este delito se le impondrá

una pena de dieciocho a treinta y cinco años de prisión y multa por el importe de mil a dos mil días de salario mínimo.

I. Al responsable de secuestro se le sancionará con una pena de veinticinco a cuarenta años de prisión y multa por el importe de mil a tres mil días de salario mínimo y en su caso destitución, e inhabilitación del servidor público para desempeñar otro empleo, comisión o cargo público, cuando:

[...]

[...]

k) Para lograr sus propósitos se valga de redes o sistemas informáticos internacionales o de otros medios de alta tecnología, que impliquen marcada ventaja en el logro de su fin;

[...]

MICHOACÁN

Código penal

Título quinto

Delitos contra el libre desarrollo de la personalidad

Capítulo II

Pornografía y turismo sexual de personas menores de edad o de personas que no tienen capacidad para comprender el significado del hecho

(Reforma publicada en el Periódico Oficial del Estado el 24 de agosto de 2006.)

[...]

Artículo 164. Comete el delito de pornografía de personas menores de edad o de personas que no tienen capacidad para comprender el significado del hecho:

I. Quien induzca, procure, facilite o permita por cualquier medio a persona menor de edad o a persona que no tiene capacidad para comprender el significado del hecho a realizar actos sexuales o de exhibicionismo corporal, reales o simulados, de índole sexual, con el fin de grabarlos, videograbarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, sistemas de cómputo, medios electrónicos o de cualquier otra naturaleza, independientemente de que se logre la finalidad;

[...]

III. Quien reproduzca, ofrezca, almacene, distribuya, venda, compre, rente, exponga, publique, publicite, transmita, importe o exporte por cualquier medio las grabaciones, videograbaciones, fotografías o filmes a que se refieren las conductas descritas en la fracción II de este artículo, y

[...]

Título noveno

Delitos contra la fe pública

Capítulo II

Falsificación de documentos y uso de documentos falsos

(Adición publicada en el P.O. el 6 de julio de 2004.)

Artículo 203 bis. Se impondrán de tres a nueve años de prisión y multa de cien a cinco mil días de salario mínimo general vigente al que sin consentimiento de quien esté facultado para ello:

[...]

V. Adquiera o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes y servicios o disposición de efectivo, así como a quien posea o utilice la información sustraída de esta forma, o

[...]

MORELOS

Código penal

Título decimosegundo

Delitos contra la moral pública

Capítulo I

Ultrajes a la moral pública

Artículo 213. Se aplicará prisión de seis meses a tres años y de trescientos a quinientos días multa:

I. Al que ilegalmente fabrique, reproduzca o publique libros, escritos, imágenes u objetos obscenos y al que los exponga, distribuya o haga circular, y

II. Al que realice exhibiciones públicas obscenas por cualquier medio electrónico, incluyendo Internet, así como las ejecute o haga ejecutar por otro;

En caso de reincidencia, además de las sanciones previstas en este artículo, se ordenará la disolución de la sociedad o empresa.

[...]

Capítulo III

Corrupción de menores e incapaces

Artículo 213 quáter. Al que induzca, procure u obligue a un menor de edad o a quien no tenga la capacidad para comprender el significado del hecho a realizar

actos de exhibicionismo corporal, lascivos o sexuales, de prostitución, de consumo de narcóticos, a tener prácticas sexuales, a la práctica de la ebriedad o a cometer hechos delictuosos se le aplicarán de cinco a diez años de prisión y de cien a quinientos días multa. Se duplicará la sanción a la persona que cometa o consienta cualquiera de las conductas descritas, si fuere ascendiente, hermano, hermana, padrastro, madrastra, tutor, tutora o todo aquel que tenga sobre el menor el ejercicio de la patria potestad.

Si además del delito citado resultase cometido otro, se aplicarán las reglas de acumulación.

Al que procure, facilite o induzca por cualquier medio a un menor, o a un incapaz, a realizar actos de exhibicionismo corporal, lascivos o sexuales, con el objeto y fin de videograbarlo, fotografiarlo o exhibirlo mediante anuncios impresos o electrónicos, incluyendo la Internet, se le impondrán de seis a quince años de prisión y de cien a quinientos días multa. Se duplicará la sanción a la persona que cometa o consienta cualquiera de las conductas descritas, si fuere ascendiente, hermano, hermana, padrastro, madrastra, tutor, tutora o todo aquel que tenga sobre el menor el ejercicio de la patria potestad.

Al que filme, grabe o imprima los actos a que se refiere el párrafo anterior se le impondrá una pena de diez a catorce años de prisión y de doscientos cincuenta a mil días multa. La misma pena se impondrá a quien con fines de lucro, elabore, reproduzca, venda, arriende, exponga, publicite o difunda el material referido.

NAYARIT

Código penal

Esta legislación es omisa al describir alguna conducta delictiva.

NUEVO LEÓN

Código penal

Título tercero

Capítulo único

Violación de correspondencia

Artículo 178. Comete el delito de violación de correspondencia:

I. Quien abra indebidamente una comunicación escrita o que se encuentre en cualquier medio material o electrónico que no le esté dirigida, o
II. Quien indebidamente intercepte una comunicación escrita o que se encuentre en cualquier medio material o electrónico que no le esté dirigida, aunque la conserve cerrada y no se imponga de su contenido.

Al responsable de este delito se le impondrá una pena de prisión de tres días a seis meses y multa de cinco a cien cuotas.

Título quinto

Delitos contra la moral pública

[...]

Capítulo II

Corrupción de menores o de personas privadas de la voluntad y pornografía infantil

[...]

Artículo 201 bis. Comete el delito de pornografía infantil el que:

I. Induzca, incite, propicie, facilite u obligue a persona menor de edad a realizar actos de exhibicionismo corporal o de pornografía;

II. Videograbe, audiograbe, fotografíe o plasme en imágenes fijas o en movimiento a persona menor de edad realizando actos de exhibicionismo corporal o de pornografía;

III. Promueva, invite, facilite o gestione por cualquier medio la realización de actividades en las que se ofrezca la posibilidad de observar actos de exhibicionismo corporal o de pornografía, que estén siendo llevadas a cabo por persona menor de edad, o

[...]

Se entiende por actos de exhibicionismo corporal toda representación del cuerpo humano con fin lascivo sexual.

Se considera acto de pornografía toda representación realizada por cualquier medio de actividades lascivas sexuales explícitas, reales o simuladas.

Título séptimo

Delitos cometidos por servidores públicos

Capítulo VIII

Delitos cometidos en la custodia de documentos

Artículo 223. Se impondrán de seis meses a seis años de prisión, multa de treinta a trescientas cuotas y destitución e inhabilitación de seis meses a seis años para desempeñar un empleo, cargo o comisión públicos a los servidores públicos que:

[...]

[...]

VI. Teniendo su custodia, abrieren o consintieren abrir, sin la autorización correspondiente, papeles o documentos cerrados o cualquier otro medio de almacenamiento de información cuyo acceso no les esté permitido.

Título décimo

Falsedad

Capítulo I

Falsificación de títulos al portador, documentos de crédito público y relativos al crédito

[...]

Artículo 242-bis. Se impondrán de tres a nueve años de prisión y multa de ciento cincuenta a cuatrocientas cincuenta cuotas al que, sin consentimiento de quien esté facultado para ello, incurra en cualquiera de las siguientes conductas:

I. Produzca, reproduzca, introduzca al Estado, enajene, aun gratuitamente, o altere, tarjetas de crédito o de débito, o la información contenida en éstas, esqueletos de cheque o documentos utilizados para el pago de bienes y servicios o para disposición de efectivo;
II. Adquiera o utilice, con propósito de lucro indebido, cualquiera de los objetos a que se refiere la fracción anterior, a sabiendas de que son alterados o falsificados;
III. Posea o detente, sin causa legítima, cualquiera de los objetos a que se refiere la fracción I de este artículo;
IV. Altere los medios de identificación electrónica de cualquiera de los objetos a que se refiere la fracción I de este artículo, o
V. Acceda indebidamente a los equipos electromagnéticos de las instituciones emisoras de cualquiera de los objetos a que se refiere la fracción I de este artículo.

Las mismas penas se impondrán a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos o documentos utilizados para el pago de bienes y servicios.

Si el sujeto activo es funcionario o empleado del ofendido, las penas se aumentarán en una mitad.

Si además del delito previsto en este artículo resultare cometido otro, se aplicarán las reglas del concurso.

Libro segundo

Parte especial

Título decimoséptimo

Capítulo V

Explotación de personas socialmente desfavorecidas

[...]

Artículo 352. Los escritos, estampas, pinturas o cualquiera otra cosa que hubiere servido de medio para la injuria o la difamación se recogerán e inutilizarán, a menos que se trate de algún documento público o de uno privado que importe obligación, liberación o transmisión de derechos.

En tal caso, se hará en el documento una anotación sumaria de la sentencia pronunciada contra el acusado.

Artículo 352-bis. Se aumentará hasta la mitad de la pena a imponer por los delitos que resultaren cuando se efectúen mediante la utilización de la televisión, radio, prensa escrita o Internet.

Título decimonoveno

Delitos en relación con el patrimonio

Capítulo I

Robo

Artículo 364. Comete el delito de robo el que se apodere de una cosa mueble, ajena, sin el consentimiento de quien tenga derecho a disponer de ella.

Artículo 365. Se equipara al robo y se castigará como tal:

[...]

IV. El apoderamiento material de los documentos que contengan datos de computadoras, o el aprovechamiento o utilización de dichos datos, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.

Capítulo X

Reglas comunes para los capítulos precedentes

Artículo 408-bis. Cuando para cometer los delitos de robo, fraude, abuso de confianza, usura, chantaje o administración fraudulenta se utilicen tarjetas de crédito o débito, o cualquier medio o instrumento electrónico o bancario, la pena se aumentará hasta en una tercera parte de la que corresponda imponer.

Título vigesimosegundo

De los delitos por medios electrónicos

Artículo 427. A quien indebidamente accese a un sistema de tratamiento o de transmisión automatizado de datos, se le impondrán de 2 meses a 2 años de prisión y multa de 200 a 1 000 cuotas.

Artículo 428. A quien indebidamente suprima o modifique datos contenidos en el sistema, o altere el funcionamiento del sistema de tratamiento o de transmisión automatizado de datos, se le impondrán de 2 a 8 años de prisión y multa de 300 a 1 500 cuotas.

Artículo 429. A quien indebidamente afecte o falsee el funcionamiento de un sistema de tratamiento o de transmisión automatizada de datos se le impondrán de 2 a 8 años de prisión y multa de 350 a 2 000 cuotas.

OAXACA

Código penal

Título decimosegundo

Delitos contra la libertad, la seguridad y el normal desarrollo psicosexual

Capítulo I

Abuso y hostigamiento sexual, estupro y violación

Artículo 241. Comete el delito de abuso sexual quien sin consentimiento de una persona ejecute en ella o la haga ejecutar un acto sexual que no sea la cópula, o la obligue a observar cualquier acto sexual aun a través de medios electrónicos. Al responsable de tal hecho se le impondrán de dos a cinco años de prisión y multa de cincuenta a doscientos días de salario mínimo.

Capítulo II

Corrupción de menores, de incapaces y pornografía infantil

[...]

Artículo 195-bis. Comete el delito de pornografía infantil el que procure, facilite, obligue o induzca por cualquier medio a uno o a más menores de dieciocho años, con o sin su consentimiento, a realizar actos de exhibicionismo corporal, lascivos o sexuales, con la finalidad de videograbarlos, fotografiarlos exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro, y se le impondrán de cinco a diez años de prisión y multa de seiscientos a setecientos treinta días de salario mínimo.

PUEBLA

Código de defensa social

Capítulo séptimo

Delitos contra la moral pública, contra derechos de menores, incapaces o personas que no pudieren resistir y contra la dignidad de las personas

Sección primera

Ultrajes a la moral pública

Artículo 215. Al que ilegalmente fabricare, imprimiere, grabare, transportare, exhibiere, vendiere o hiciere circular por cualquier medio imágenes, libros, revistas,

escritos, fotografías, dibujos, carteles, videocintas, mecanismos u objetos lascivos, con implicaciones sexuales, se le aplicará prisión de treinta días a tres años y multa de diez a cien días de salario.

Sección segunda

Corrupción y pornografía de menores e incapaces o personas que no pudieren resistir

[...]

Artículo 224 bis.

Se deroga.

Artículo adicionado el 16 de agosto de 1999 y reformado el 30 de abril de 2004; se derogó por decreto publicado el 23 de marzo de 2007.

Expresaba: "Artículo 224 Bis. Al que procure, induzca, facilite o utilice a uno o más menores de dieciséis años o personas incapaces, con o sin su consentimiento, para realizar actos de exhibicionismo corporal lascivos o sexuales, con la finalidad de fotografiarlos, videograbarlos, filmarlos o exhibirlos, usando medios impresos o electrónicos, se le impondrá prisión de ocho a catorce años y multa de cien a mil doscientos días de salario.

Se entiende por pornografía infantil la representación sexualmente explícita de imágenes de personas menores de dieciséis años, y se equiparan a la misma los casos en que se incluya a una o varias personas incapaces de comprender las consecuencias del hecho en que intervienen".

Capítulo décimo

Falsedad

Sección primera

Falsificación de acciones, obligaciones y otros documentos de crédito público

[...]

Artículo 245-bis. Se impondrá prisión de tres a nueve años y multa de ciento cincuenta a cuatrocientos días de salario:

I. Al que produzca, imprima, enajene aun gratuitamente, distribuya o altere tarjetas, títulos, documentos o instrumentos utilizados para el pago de bienes y servicios o para disposición de efectivo, sin consentimiento de quien esté facultado para ello;

II. Al que adquiera, utilice o posea, tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo, a sabiendas de que son alterados o falsificados;

III. Al que adquiera, utilice, posea o detente indebidamente, tarjetas, títulos o documentos auténticos para el pago de bienes y servicios o para disposición de efectivo, sin consentimiento de quien esté facultado para ello;

IV. Al que adquiere, copie o falsifique los medios de identificación electrónica, cintas o dispositivos magnéticos de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo, y

V. Al que acceda indebidamente a los equipos y sistemas de cómputo o electromagnéticos de las Instituciones emisoras de tarjetas, títulos, documentos o instrumentos, para el pago de bienes y servicios o para disposición de efectivo.

Las mismas penas se impondrán a quien utilice indebidamente información confidencial o reservada de la Institución o persona que legalmente esté facultada para emitir tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo.

Si el sujeto activo es empleado o dependiente del ofendido, las penas aumentarán en una mitad.

(*Artículo adicionado el 6 de noviembre de 2000.*)

En caso de que se actualicen otros delitos con motivo de las conductas a que se refiere este artículo, se aplicarán las reglas del concurso.

Artículo 246. Si el infractor fuere funcionario o empleado público, además de las sanciones indicadas, se le destituirá de su empleo o cargo y se le inhabilitará hasta por diez años para obtener cualquier otro.

Capítulo decimoctavo

Delitos contra las personas en su patrimonio

Sección cuarta

Fraude

Artículo 404. Las mismas sanciones señaladas en el artículo anterior se impondrán:

[...]

XIX. Al que dolosamente y con el propósito de procurarse un lucro ilícito, para sí o para un tercero, dañe o perjudique el patrimonio de otro, mediante el uso indebido de mecanismos cibernéticos, que provoque o mantenga un error, sea presentando como ciertos hechos que no lo son, o deformando o disimulando hechos verdaderos, y

[...]

QUERÉTARO

Código penal

Capítulo II

Falsificación y uso indebido de documentos

Artículo 232-bis. Se impondrán de tres a nueve años de prisión y multa por el equivalente de doscientos a cuatrocientos días de salario mínimo general vigente

en la época en que se cometa el delito al que, sin consentimiento de quien esté facultado para ello:

I. Produzca, imprima, enajene, distribuya, altere o falsifique, aún gratuitamente, adquiera, utilice, posea o detente, sin tener derecho a ello, boletos, contraseñas, fichas, tarjetas de crédito o débito y otros documentos que no estén destinados a circular y sirvan exclusivamente para identificar a quien tiene derecho a exigir la prestación que en ellos se consignan u obtener cualquier beneficio.
II. Altere, copie o reproduzca, indebidamente, los medios de identificación electrónica de boletos, contraseñas, fichas u otros documentos a que se refiere la fracción I de este artículo.
III. Acceda, obtenga, posea, utilice o detente indebidamente información de los equipos electromagnéticos o sistemas de cómputo de las organizaciones emisoras de los boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I de este artículo o de módem o cualquier medio de comunicación remota y los destine a alguno de los supuestos que contempla el presente artículo, y
IV. Adquiera, utilice o detente equipos electromagnéticos, electrónicos o de comunicación remota para sustraer en forma indebida la información contenida en la cinta magnética de los boletos, contraseñas, fichas, tarjetas de crédito, tarjetas de débito u otros documentos a los que se refiere este artículo o de archivos de datos de las emisoras de los documentos.

Título décimo

Delito contra el patrimonio

Capítulo IV

Fraude

Artículo 193. Al que engañando a alguien o aprovechándose del error en que éste se halla se haga ilícitamente de alguna cosa o alcance un lucro indebido se le impondrán las siguientes penas:

I. Prisión de 3 meses a 4 años y hasta 180 días multa cuando el valor de lo defraudado no exceda de 600 veces el salario mínimo, y
II. Prisión de 4 a 10 años y de 180 hasta 500 días multa cuando el valor de lo defraudado exceda de 600 veces el salario mínimo.

Artículo 194. Se aplicarán las mismas penas previstas en el artículo anterior:

[...]

Si el sujeto activo es empleado, dependiente del ofendido o servidor público las penas se aumentarán en una mitad.

[...]

IX. Al que por sorteos, rifas, loterías, tandas, promesas de venta o por cualquier otro medio se quede en todo o en parte con las cantidades recibidas sin entregar la mercancía u objeto ofrecido;

[...]

QUINTANA ROO

Código penal

Título sexto

Delitos contra el patrimonio

Capítulo V

Fraude

Artículo 152. Comete el delito de fraude el que, engañando a alguien o aprovechándose del error en que éste se encuentra, obtenga alguna cosa ajena o alcance un lucro indebido para sí o para otro.

Se aplicará de seis meses a tres años de prisión y de veinticinco a doscientos días multa al que cometa el delito de fraude cuyo monto no exceda de mil días de salario mínimo general vigente en el Estado. Si excede de dicha cantidad, la sanción será de tres a doce años de prisión y de cincuenta hasta cuatrocientos días multa.

Artículo 153. Se impondrán las mismas penas previstas en el artículo anterior:

[...]

(Adicionada P.O. 29 de dic. de 2000.)

XV. Al que por medio de tarjetas, títulos o documentos falsos relacionados con instituciones bancarias o comerciales, o bien auténticos, pero adquiridos indebidamente y sin autorización de quien esté facultado para ello, haga el pago de cualquier bien o servicio u obtenga dinero en efectivo para sí o para otro. Si el sujeto activo es empleado o dependiente del ofendido, las penas aumentarán en una mitad más.

Título tercero

Delitos contra la fe pública

Capítulo II

Falsificación de documentos y uso de documentos falsos
(Adicionado P.O. 29 de dic.de 2000.)

Artículo 189-bis. Se impondrá hasta una mitad más de las penas previstas en el artículo anterior al que:

I. Produzca, imprima, enajene, aun gratuitamente, distribuya o altere tarjetas, títulos, documentos o instrumentos utilizados para el pago de bienes o servicios o para disposición en efectivo, sin consentimiento de quien esté facultado para ello;

II. Adquiera, posea o detente ilícitamente tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo a sabiendas de que son alterados o falsificados;

III. Copie o reproduzca, altere los medios de identificación electrónica, cintas o dispositivos magnéticos de documentos para el pago de bienes o servicios o para disposición en efectivo;

IV. Accese indebidamente los equipos y sistemas de cómputo o electromagnéticos de las instituciones emisoras de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo.

Las mismas penas se impondrán a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo.

Si el sujeto activo es empleado o dependiente del ofendido, las penas se aumentarán hasta en una mitad más.

En el caso de que se actualicen otros delitos con motivo de las conductas a que se refiere este artículo se aplicarán las reglas del concurso.

Título cuarto

Delitos contra el libre desarrollo de la personalidad

Capítulo I

Corrupción de personas menores de edad o de quienes no tienen capacidad para comprender el significado del hecho pornografía infantil

(Adicionado P.O. 20 de oct. de 2006.)

[...]

Artículo 192-bis. Comete el delito de pornografía infantil quien a persona menor de dieciocho años:

[...]

[...]

III. Promueva, invite, facilite o gestione por cualquier medio la realización de actividades en las que se ofrezca la posibilidad de observar actos de exhibicionismo corporal o de pornografía, que estén siendo llevadas a cabo por persona menor de dieciocho años de edad.

Comete también el delito de pornografía infantil el que, siendo mayor de edad, participe como activo o pasivo en los actos de exhibicionismo corporal o de pornografía realizados por persona menor de edad. Se entiende por actos de exhibicionismo corporal a toda representación del cuerpo humano, con fin lascivo sexual.

Se considera acto de pornografía a toda representación realizada por cualquier medio, de actividades lascivas sexuales explícitas, reales o simuladas. Las fotografías, videograbaciones, audiograbaciones o las imágenes fijas o en movimiento, impresas, plasmadas o que sean contenidas o reproducidas en medios magnéticos, electrónicos o de otro tipo y que constituyan recuerdos familiares; los programas preventivos, educativos o de cualquier índole que diseñen e impartan las instituciones públicas, privadas o sociales que tengan por objeto la educación sexual, educación sobre la función reproductiva, la prevención de enfermedades de transmisión sexual o de embarazo de adolescentes no constituyen pornografía infantil.

La sanción por el delito de pornografía infantil será de siete a veinte años de prisión y de 400 a 500 días multa. En todos los casos se aplicará también como pena el decomiso de objetos, instrumentos y productos del delito, respetando los derechos de terceros.

Artículo 192-ter. También se entenderá como pornografía infantil, aplicándose la misma pena establecida en el artículo anterior, al que:

I. Con o sin fines de lucro, fije, imprime o exponga de cualquier manera los actos de exhibicionismo corporal o de pornografía realizados por persona menor de dieciocho años de edad;

[...]

SAN LUIS POTOSÍ

Código penal

Fraude

Artículo 204. Comete el delito de fraude quien, engañando a otro o aprovechándose del error en que éste se encuentra, se hace ilícitamente de una cosa o alcanza un lucro indebido.

Artículo 205. Igualmente comete el delito de fraude, y se sancionará con las mismas penas, quien:

[...]

IX. Por sorteos, rifas, tandas, loterías, promesas de venta o por cualquier otro medio se queda en todo o en parte con las cantidades recibidas sin entregar la mercancía u objeto ofrecido;

[...]

SINALOA

Código penal

Título décimo

Delitos contra el patrimonio

Capítulo V

Delito informático

Artículo 217. Comete delito informático la persona que dolosamente y sin derecho:

I. Use o entre a una base de datos, sistema de computadores 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 computadora o los datos contenidos en la misma, en la base, sistema o red.

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

Título quinto

De los delitos electorales

Artículo 356. Se impondrán de cien a doscientos días multa y prisión de uno a cinco años al funcionario partidista, precandidato o candidato que:

(Ref. por Decreto número 504, de 27 de marzo del 2007, y publicado en el P.O. No. 039 de 30 de marzo de 2007.)

[...]

X. Emita cualquier expresión pública, impresa o por cualquier otro medio sobre un hecho determinado o indeterminado que calumnie, infame, injurie, difame o denigre a los ciudadanos, a las instituciones públicas, a las personas morales o a otros partidos políticos y sus candidatos, y

(Adic. Por Decreto número 504, de 27 de marzo del 2007, y publicado en el P.O. No. 039 de 30 de marzo de 2007.)

XI. Sin autorización del Consejo Estatal Electoral contrate en medios electrónicos o prensa, por sí o por interpósita persona, propaganda electoral en los procesos electorales.

(Adic. por Decreto número 504, de 27 de marzo del 2007, y publicado en el P.O. No. 039 de 30 de marzo de 2007.)

[...]

XVII. Contrate propaganda electoral en medios electrónicos o prensa a favor o en contra de algún partido político, coalición o candidato.

(Adic. por Decreto número 504, de 27 de marzo del 2007, y publicado en el P.O. No. 039 de 30 de marzo de 2007.)

SONORA

Código penal

Título vigésimo

Delitos en contra de las personas en su patrimonio

Capítulo IV

Fraude

Artículo 318. Se impondrán prisión de tres meses a ocho años y de diez a doscientos cincuenta días multa al que engañando a uno, o aprovechándose del error en que éste se encuentre, se haga ilícitamente de alguna cosa, o alcance un lucro indebido para sí o para otro.

Artículo 319. Se considerará como Fraude para los efectos de la sanción:

[...]

XI. Al que, por sorteos, rifas, loterías, promesas de venta o por cualquier otro medio se quede en todo o en parte con las cantidades recibidas, sin entregar la mercancía u objeto ofrecido.

TABASCO

Código penal

Título décimo

Delitos contra el patrimonio

Capítulo VI

Fraude

Artículo 191-bis. Se impondrán de tres a nueve años de prisión y de doscientos a quinientos días de multa al que:

I. En forma y sin autorización de quien esté facultado para ello adquiera, utilice, posea o detente tarjetas utilizadas en el comercio para obtener bienes o servicio, títulos o documentos que permitan el uso de éstas o sus bandas magnéticas.

La misma pena se aplicará si esas tarjetas, títulos, documentos o bandas magnéticas son falsos.

Si el sujeto activo es empleado o dependiente del ofendido, las penas se aumentarán en una mitad más, y

II. Sin consentimiento de quien esté facultado para ello, produzca, imprima, enajene aun gratuitamente o distribuya tarjetas utilizadas en el comercio para obtener bienes o servicios, títulos o documentos que permitan el uso de éstas o sus bandas magnéticas falsifique o altere esas tarjetas, bandas, títulos o documentos.

Si el sujeto activo es empleado o dependiente del ofendido, las penas se aumentarán en una mitad más.

Título decimoprimero

Delitos contra la seguridad de la comunicacion

Capítulo V

Violación de la comunicación privada

Artículo 316. Al que intervenga la comunicación privada de terceras personas, a través de medios eléctricos o electrónicos se le aplicará prisión de uno a cinco años.

Título decimotercero bis

Delitos contra la seguridad en los medios informáticos y magnéticos

Capítulo I

Acceso sin autorización

Artículo 326-bis. Al que intercepte, interfiera, reciba, use por cualquier medio sin la autorización debida o, excediendo la que tenga, una computadora personal, o un sistema de red de computadoras, un soporte lógico de programas de cómputo o base de datos, se le impondrán de veinte a cincuenta días de trabajo a favor de la comunidad y de veinte a treinta días multa.

Capítulo II

Daño informático

Artículo 326-bis 1. A quien sin autorización modifique, destruya o deteriore en forma parcial o total archivos, bases de datos o cualquier otro elemento intangible

contenido en computadoras personales, sistemas o redes de cómputos, soportes lógicos, o cualquier otro medio magnético, se le sancionará con penas de uno a cinco años de prisión y de cien a cuatrocientos días multa.

Cuando el activo tenga el carácter de encargado del manejo, administración o mantenimiento de los bienes informáticos dañados, las penas se incrementarán en una mitad más.

Capítulo III

Falsificación informática

Artículo 326-bis 2. Se impondrán penas de uno a cinco años de prisión al que copie o imite los originales de cualquier dato, archivo o elemento intangible contenido en una computadora personal o en un sistema de redes de computadoras, base de datos o soporte lógico, siempre que para ello se requiera autorización y no la obtenga.

Las mismas sanciones se aplicarán al que utilice o aproveche en cualquier forma los bienes informáticos falsificados, previstos en este Título.

Artículo 326-bis 3. Cuando los ilícitos previstos en este Título se cometan utilizando el equipo de cómputo de terceras personas, las penas se incrementarán en una mitad.

TAMAULIPAS

Código penal

Título quinto

Delitos contra la moral pública

Capítulo II

Corrupción, pornografía y prostitución sexual de menores e incapaces

Artículo 194-bis. Comete el delito de pornografía de menores de edad e incapaces:

I. El que obligue o induzca a uno o más menores de dieciocho años o incapaces a realizar actos de exhibicionismo corporal, lascivos, sexuales o pornográficos con la finalidad de grabarlos, videograbarlos, filmarlos, fotografiarlos o exhibirlos mediante anuncios impresos, electromagnéticos, electrónicos, o por vía internet, de telefonía o cualquier otra similar.

II. Toda persona que procure, permita o facilite por cualquier medio el que uno o más menores de dieciocho años con su consentimiento o sin él, o incapaces, realice cualquiera de los actos señalados en la fracción anterior con los mismos fines;

[...]

Para los efectos de este artículo, se entiende por pornografía de menores de edad o incapaces la representación, ejecución o simulación de actos sexuales, o desnudos corporales, en imágenes en que aparezcan menores de dieciocho años o incapaces.

Al responsable de los delitos señalados en las fracciones I, II y IV se le impondrá de ocho a doce años de prisión y multa de mil quinientos a dos mil quinientos días salario.

Artículo 194-ter. Comete el delito de prostitución sexual de menores e incapaces:

I. El que dentro del territorio del Estado publicite, facilite o gestione por cualquier medio a persona o personas para que se trasladen a cualquier lugar dentro de éste o fuera del mismo, con el propósito o fin de tener u obtener relaciones sexuales con menores de dieciocho años o incapaces;

[...]

Título decimonoveno

Delitos contra el patrimonio de las personas

Capítulo I

Robo

...

Artículo 400. Se sancionará con la pena del robo:

[...]

IV. El apoderamiento material de los documentos que contengan datos de computadoras o el aprovechamiento o utilización de dichos datos, sin consentimiento de la persona que legalmente pueda disponer de los mismos.

TLAXCALA

Código penal

(Reformada denominación, P.O. 28 de septiembre de 2007.)

Título sexto

Delitos contra el libre desarrollo de la personalidad

Capítulo II

Corrupción de menores

Artículo 166. Se aplicará prisión de seis meses a dos años y multa hasta de veinte días de salario al que procure o facilite la corrupción de un menor de die-

ciocho años, cualquiera que sea la naturaleza de la corrupción, con excepción de las conductas siguientes:

I. Quien induzca, procure, facilite o permita por cualquier medio la realización de actos eróticos o de exhibicionismo corporal, reales o simulados con el fin de grabarlos, videograbarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, sistemas de cómputo, medios electrónicos o de cualquier otra naturaleza;

VERACRUZ

Código penal

Título IV

Delitos contra la intimidad personal y la inviolabilidad del secreto

Capítulo III

Delitos informáticos

Artículo 181. Comete delito informático quien, sin derecho y con perjuicio de tercero:

I. Ingrese en una base de datos, sistema o red de computadoras para obtener, conocer, utilizar, alterar o reproducir la información en ellos contenida, o
II. Intercepte, interfiera, use, altere, dañe o destruya un soporte lógico o programa informático o la información contenida en el mismo o en la base, sistema o red.

Al responsable de este delito se le impondrán de seis meses a dos años de prisión y multa hasta de trescientos días de salario. Si se cometiere con fines de lucro, las penas se incrementarán en una mitad.

Capítulo V

Fraude

Artículo 216. A quien, engañando a alguien o aprovechándose del error en que se halle, obtenga para sí o para otro alguna cosa total o parcialmente ajena con ánimo de dominio, lucro o uso, o cause a otro un perjuicio patrimonial, se le sancionará con:

I. Trabajo en favor de la comunidad de uno a cuatro meses o multa hasta de cincuenta días de salario, cuando el valor de lo defraudado no exceda de cincuenta días de salario;

II. Prisión de seis meses a tres años y multa hasta de doscientos días de salario, cuando el valor de lo defraudado exceda de cincuenta pero no de trescientos días de salario;
III. Prisión de dos a cinco años y multa hasta de quinientos días de salario, cuando el valor de lo defraudado exceda de trescientos, pero no de setecientos cincuenta días de salario, o
IV. Prisión de cinco a doce años y multa hasta de setecientos días de salario, si el valor de lo defraudado excede de setecientos cincuenta días de salario.

Artículo 217. Las penas previstas en el artículo anterior se aplicarán a quien:

[...]

X. Por cualquier medio ingrese a sistemas o programas de informática de naturaleza financiera e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, con el propósito de obtener algún beneficio para sí o de un tercero.

Capítulo III

Falsificación de títulos y contra la fe pública

Artículo 280. Se impondrán de tres a nueve años de prisión y multa hasta de quinientos días de salario a quien:

I. Produzca, imprima, enajene o distribuya tarjetas, títulos o documentos falsos utilizados para el pago de bienes y servicios o para disposición en efectivo, o los adquiera, utilice, posea o detente a sabiendas de esa circunstancia, o
II. Adquiera, utilice, posea o detente tarjetas, títulos o documentos auténticos para el pago de bienes y servicios, sin consentimiento de quien esté facultado para ello.

YUCATÁN

Código penal

Título séptimo

Delitos contra la moral pública

Capítulo II

Corrupción de menores e incapaces, trata de menores y pornografía infantil

Artículo 211. Al que procure o facilite por cualquier medio que uno o más menores de dieciséis años, con o sin su consentimiento, los obligue o induzca a realizar actos de exhibicionismo corporal, lascivos o sexuales, con objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos,

con o sin el fin de obtener un lucro, se le impondrán de cinco a diez años de prisión y de cuatrocientos a quinientos días multa.

Título decimosexto

Falsedad

Capítulo II

Falsificación de documentos en general

Artículo 284-bis. Se impondrá de cuatro a diez años de prisión y de ciento cincuenta a quinientos días multa al que:

[...]
[...]
[...]

IV. Altere los medios de identificación electrónica de tarjetas bancarias o comerciales, documentos o pagarés en los que se asientan las operaciones que con ellas se realizan y vales para el pago de bienes o servicios, o

V. Acceda indebidamente a los equipos electrónicos de las instituciones emisoras de tarjetas bancarias o comerciales y vales para el pago de bienes o servicios o para disposición de efectivo, con el fin de utilizarlos u obtener información con fines indebidos...

ZACATECAS

Título sexto

Delitos contra la moral pública

Capítulo II

Corrupción de menores

Artículo 183-bis. También cometen el delito de corrupción de menores y se harán acreedores a las sanciones previstas:

I. Quienes vendan o alquilen a menores de edad material audiovisual clasificado como exclusivo para adultos;
II. Quienes propicien o permitan que menores de dieciocho años presencien, por medio de aparatos electrónicos, la exhibición de las cintas de vídeo a que se refiere la fracción anterior.
III. Quienes vendan o regalen a los menores de dieciocho años de edad, en la cantidad que fuere, cualquier tipo de droga, enervante o sustancia psicotrópica, cuya producción, transporte, trafico o comercio estén prohibidos en términos de la ley; introduzcan a su consumo, o empleen a los menores de edad para tales efectos.

Anexo XI

Ley de protección de datos personales del estado de Colima

(Publicada en el **Periódico Oficial** *del Estado de Colima el 21 de junio de 2003)*

CAPÍTULO I

Disposiciones generales

Artículo 1o. La presente Ley es de orden público e interés social, tiene por objeto reglamentar la fracción VI del artículo 1o. de la Constitución Política del Estado Libre y Soberano de Colima, a fin de proteger y garantizar los derechos de protección de los datos de carácter personal, como uno de los derechos humanos fundamentales.

Artículo 2o. La presente Ley será aplicable a los datos de carácter personal que sean registrados en cualquier soporte físico que permita su tratamiento, tanto por parte del sector público como privado dentro del Estado.

Se exceptúan de su aplicación:

I. Los archivos mantenidos por personas físicas para actividades exclusivamente personales o domésticas;
II. Los archivos que sean considerados como clasificados por la ley;
III. Los archivos establecidos para investigaciones penales. En este caso, el responsable del archivo deberá comunicar la existencia del mismo a la Comisión Estatal para el Acceso a la Información Pública, indicando sus características generales y su finalidad.

Artículo 3o. Para los efectos de la presente Ley se entenderá por:

I. Archivo: el conjunto de datos de carácter personal, correspondientes a un grupo de personas, independientemente de su forma de creación, almacenamiento, tratamiento o uso;

II. Archivo de acceso público: el archivo que puede ser consultado por cualquier persona que no esté impedida por una disposición legal, ya sea gratuitamente o mediante el pago de los derechos correspondientes;
III. Cesión de datos: la comunicación o transmisión de datos hacia una persona distinta del interesado;
IV. Consentimiento: la manifestación expresa, libre, inequívoca, específica e informada, mediante la cual el interesado consiente el tratamiento de datos personales de los que es titular;
V. Datos de carácter personal: los datos relativos a personas físicas o morales que de manera directa o indirecta puedan conectarse con una persona específica. Se incluyen a manera ilustrativa datos representados en forma de texto, imágenes, datos biométricos como la huella digital, datos sobre el DNA de las personas o cualquier otro que corresponda intrínsecamente a una persona determinada;
VI. Encargado del tratamiento: la persona física o moral que realice tratamiento de datos por cuenta y con autorización del responsable del archivo;
VII. Interesado o afectado: la persona física o moral cuyos datos de carácter personal se incorporen al archivo;
VIII. Proceso de disociación: el tratamiento de los datos personales de modo que los datos resultantes no puedan ser relacionados directamente con ninguna persona identificable;
IX. Responsable del archivo: la persona física o moral, pública o privada, encargada del tratamiento de los datos del archivo;
X. Tratamiento de datos: las operaciones y procesos, automatizados o manuales, relacionados con la recolección, captura, conservación, proceso, transmisión, interrelación, combinación, control y otros manejos de los datos;
XI. Ley: el presente ordenamiento;
XII. Comisión: la Comisión Estatal para el Acceso a la Información Pública, autoridad encargada de la aplicación del presente ordenamiento;
XIII. Unidad de salario: el equivalente a un día de salario mínimo general vigente en la entidad, y
XIV. Organismo público: los organismos autónomos, descentralizados, paramunicipales, fideicomisos y, en general, todo organismo público.

Capítulo II

De los datos de carácter personal

Artículo 4o. Para el manejo de los datos de carácter personal se seguirán los principios siguientes:

I. Sólo podrán obtenerse y ser sujetos de tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades expresas y legítimas para los que se hayan obtenido;

II. No podrán usarse para actividades incompatibles a los propósitos para los que fueron obtenidos. No se considerará un uso incompatible el tratamiento posterior para fines estadísticos, históricos o científicos;
III. Deberán ser correctos y actualizados, de modo que reflejen fielmente la situación del afectado;
IV. No podrán ser guardados de modo que se identifique al interesado una vez que dejen de ser necesarios o pertinentes para la finalidad que les dio origen o haya concluido el plazo de conservación a que obliguen las leyes. Los reglamentos correspondientes indicarán de manera expresa los casos de excepción en que se autorice la conservación íntegra de ciertos datos, en virtud del valor histórico, estadístico o científico que pudieran tener;
V. Deberá garantizarse el derecho de acceso por parte de los interesados para todos los archivos con datos que les correspondan;
VI. Los datos deberán obtenerse en todos los casos por medios lícitos que garanticen el respeto a las garantías individuales y, especialmente, de los derechos al honor y a la intimidad de la persona a la que conciernen. No deberán obtenerse por medios fraudulentos, desleales, ilícitos o engañosos;
VII. Previamente a su obtención, se deberá informar al interesado de manera completa y precisa sobre la existencia del archivo, su finalidad, el carácter obligatorio u optativo de la información que proporcione, las consecuencias del suministro de los datos o la negativa a hacerlo, la posibilidad de ejercer el derecho de acceso, rectificación, cancelación y oposición, así como la identidad y dirección del responsable del archivo;
VIII. Cuando se obtengan por parte de terceros, el responsable del archivo, a través de los mecanismos que defina el reglamento correspondiente, dentro de los 60 días naturales siguientes notificará al interesado después de haber dado de alta los datos, a menos que exista legislación al respecto que indique otra medida o se trate de procesos para fines históricos, estadísticos o científicos, o cuando los datos provengan de fuentes accesibles al público;
IX. Será necesario el consentimiento explícito e inequívoco del interesado para cualquier tratamiento de los datos de carácter personal. Se exceptúan los siguientes casos:

   a) Los previstos en la legislación;
   b) Cuando impliquen datos obtenidos para la realización de las funciones propias de la administración pública en su ámbito de competencia;
   c) Cuando se trate de los datos de las partes en contratos civiles, laborales, comerciales o administrativos;
   d) Cuando se trate de datos disponibles en fuentes de acceso público, y
   e) Cuando sean necesarios para el tratamiento médico del interesado.

X. El interesado podrá revocar el consentimiento mencionado en la fracción anterior cuando exista una causa justificada y no tendrá efectos retroactivos;
XI. Los servidores públicos, profesionales, trabajadores y otras personas que por razón de sus actividades tengan acceso a archivos o datos de carácter

personal estarán obligados a mantener la confidencialidad de los mismos y a no darlos a conocer a terceros. Esta obligación subsistirá aun después de finalizar las relaciones que les dieron acceso a los datos. La contravención a esta disposición será sancionada de conformidad con la legislación penal, y

XII. Los datos personales relativos a la salud podrán ser operados por los profesionales e instituciones de acuerdo con la legislación sanitaria, pero conservando la confidencialidad de los mismos de acuerdo con la presente Ley.

Artículo 5o. El responsable del archivo deberá establecer los mecanismos de seguridad que garanticen la confiabilidad y confidencialidad de los datos. El reglamento correspondiente establecerá las características mínimas de seguridad que deban tenerse en las instalaciones que manejen datos de carácter personal.

Artículo 6o. La cesión de los datos de carácter personal o su comunicación a terceros se regirá por lo siguiente:

I. Toda cesión o comunicación a terceros deberá contar con el consentimiento expreso del interesado, excepto cuando:

   a) La cesión haya sido autorizada en una ley;
   b) Se trate de datos disponibles en fuentes de acceso público;
   c) Sea necesario y esté previsto como parte de una relación jurídica;
   d) Esté dirigida a las autoridades de seguridad pública o penales y cuente con autorización judicial;
   e) Se trate de transferencias entre administraciones públicas;
   f) Sea transferida para fines históricos, estadísticos o científicos, y
   g) Se trate de datos sobre la salud y sean necesarios para atender una urgencia o para realizar estudios epidemiológicos;

II. El receptor de datos de carácter personal se obliga a acatar las disposiciones de la presente Ley;

III. Cuando la comunicación a terceros resulte de la prestación por parte de un tercero de servicios al responsable del archivo, el tercero en cuestión se considerará obligado a los términos de la presente Ley en las mismas condiciones que el responsable del archivo, y

IV. También queda obligado a acatar las disposiciones de la presente Ley quien obtenga los datos en virtud de liquidación, fusión, escisión u otro cambio en el caso de que los datos provengan de personas morales, o por herencia en el caso de provenir de personas físicas

Capítulo III

De la creación de protección de los datos personales

Artículo 7o. Las personas físicas o morales cuyos datos de carácter personal hayan sido integrados a un archivo tendrán los derechos siguientes, mismos que

podrán ejercerse a través de la acción de protección de datos personales o *Habeas Data*:

I. Solicitar y obtener gratuitamente información de sus datos de carácter personal y del origen de esos datos;
II. No verse sometidas a decisiones con efectos jurídicos o que le afecte, que se hayan basado exclusivamente en datos de carácter personal destinados a evaluar determinados aspectos de su personalidad;
III. Impugnar actos administrativos o decisiones privadas que solamente deriven de valoraciones de sus características y personalidad obtenidas de datos de carácter personal, en cuyo caso tendrán derecho de obtener información sobre los criterios de valoración usados. La valoración del comportamiento de un individuo basada en el tratamiento de datos de carácter personal sólo tendrá valor probatorio a petición del interesado;
IV. Solicitar y que se realicen gratuitamente las rectificaciones o cancelaciones de los datos de carácter personal que le correspondan y que no se apeguen a la presente Ley o que resulten inexactos o incompletos. El responsable del archivo deberá hacer efectivo este derecho dentro de los diez días hábiles siguientes al día en que se enteró de aquéllos, de conformidad con el reglamento correspondiente;
V. Recibir una indemnización proporcional al daño o lesión ocasionada en sus bienes o derechos, y
VI. Conocer gratuitamente el contenido del Registro de Protección de Datos un máximo de dos veces por año.

Artículo 8o. A quien se haya denegado los derechos consignados en la presente Ley podrá hacerlo del conocimiento de la Comisión, la que verificará la procedencia de la denuncia y dictará la resolución correspondiente dentro de un plazo máximo de 90 días naturales, contados a partir del día siguiente al de la presentación de aquélla.

Capítulo IV

De los archivos

Artículo 9o. Los archivos de datos de carácter personal que establezcan las administraciones públicas estatal y municipales, así como los organismos públicos se regirán por las siguientes disposiciones:

I. Sólo se crearán, modificarán o eliminarán archivos previa disposición del titular del Poder Ejecutivo, de los Presidentes Municipales o de los titulares de los organismos públicos, en su caso, publicadas en el *Periódico Oficial*;

II. La disposición deberá incluir:

a) La finalidad del archivo y los usos a los que se vaya a destinar;
b) Las personas o grupos a ser incluidos;

c) La obligatoriedad o carácter voluntario del suministro de la información;
d) Las características del proceso de obtención y del archivo, así como los tipos de datos de carácter personal a ser incluidos;
e) Las cesiones y comunicaciones de datos previstas;
f) El organismo responsable del archivo y, en su caso, donde pueden ejercerse los derechos de acceso, rectificación, cancelación y oposición;
g) Las medidas de seguridad aplicables y el nivel de protección exigible;
h) Cuando se trate de supresión de archivos, deberá indicarse el destino o, en su caso, las medidas a adoptarse para su destrucción;
i) Las reglas aplicables para posibles fusiones o correlación con otros archivos;

III. Sólo podrán comunicarse a otras instancias de las administraciones públicas estatal y municipales u organismos públicos cuando:

a) Se trate de la misma competencia, excepto cuando esté previsto en una ley;
b) Se hubiera previsto en la disposición de creación del archivo;
c) Una instancia de la administración u organismo público los procese para otra;
d) Exista una orden judicial para ello, y
e) El objeto sea el tratamiento con fines históricos, estadísticos o científicos.

IV. El Gobierno del Estado, los gobiernos municipales y el Instituto Electoral del Estado podrán integrar archivos sin consentimiento del interesado con nombres y apellidos, Clave Única del Registro de Población (CURP), domicilio, sexo, fecha y lugar de nacimiento de su población, para los siguientes efectos:

a) Comunicaciones respecto a las funciones que les competen;
b) Mantenimiento y operación de los registros públicos establecidos en la legislación;
c) Mantenimiento y operación del listado nominal para efectos electorales;
d) Padrones de contribuyentes, y
e) Control de vehículos y conductores.
En los casos anteriores, el organismo correspondiente cumplirá con los demás preceptos establecidos en la presente Ley.

V. No deberán integrarse datos derivados de diferentes archivos. Sin embargo, los datos indicados en la fracción anterior podrán obtenerse de un archivo existente para generar uno nuevo, creado conforme a la presente Ley,

VI. El cruce de datos entre archivos sólo podrá realizarse cuando exista la autorización expresa del interesado, cuando lo prevea la disposición de creación o modificación de los archivos involucrados o cuando exista una disposición expresa en la legislación;

VII. En el caso de archivos de instituciones de seguridad pública, se observará lo siguiente:

a) Cuando se trate de archivos de carácter administrativo que contengan datos de carácter personal, éstos se manejarán conforme a lo especificado en la presente Ley;

b) Los datos de carácter personal recogido con fines policiales podrán obtenerse sin el consentimiento de los interesados, pero estarán limitados a los supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la prevención de conductas delictivas. Deberán conservarse en archivos específicos para estos efectos y clasificarse por categorías de acuerdo con su confiabilidad. Sólo podrán obtenerse cuando sean absolutamente indispensables para los fines de una investigación concreta y se cancelarán cuando no sean necesarios para el objeto que motivó su almacenamiento;

c) Los responsables de archivos con datos de carácter personal registrados para fines policiales podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse, de la protección de derechos o libertades de terceros o de las necesidades de las investigaciones en proceso, y

d) Los datos de estos archivos podrán ser conocidos por mandato judicial en casos plenamente justificados o por disposición expresa de la ley.

VIII. Los responsables de archivos de carácter fiscal podrán negar el ejercicio de los derechos de los interesados cuando esto obstaculice la actuación de la autoridad durante el cumplimiento de sus funciones de recaudación;

IX. Se exceptúa de la obligatoriedad de autorización previa del interesado y su información previa a la obtención de los datos, cuando estas acciones impidan o dificulten gravemente el cumplimiento de las funciones de control y verificación de la autoridad, cuando afecte a la seguridad nacional o del Estado, a la seguridad pública o a la persecución de delitos o infracciones administrativas, y

X. Cuando se niegue a un afectado el ejercicio de los derechos aquí consignados, en virtud de las excepciones previstas, podrá ponerlo en conocimiento de la Comisión, la cual deberá asegurarse de la procedencia o improcedencia de la denegación.

Artículo 10. Los archivos de datos de carácter personal elaborados por particulares se regirán por las disposiciones siguientes:

I. Podrán crear archivos que contengan datos de carácter personal cuando sean necesarios para lograr los objetivos legítimos de la entidad titular, siempre que se respeten las disposiciones de la presente Ley;

II. Toda persona que cree un archivo de datos de carácter personal deberá notificarlo previamente a la Comisión. Los cambios en la finalidad del archivo, del responsable y del domicilio correspondiente deberán ser notificados a

dicha Comisión dentro de los sesenta días naturales siguientes a que se realicen;

III. Cuando se trate de investigaciones sobre genealogía, estudios biográficos y otras compilaciones de datos de carácter personal, deberá observarse lo previsto en la presente Ley para los interesados que se encuentren con vida al momento de la compilación;

IV. Cuando los interesados tengan más de 100 años de fallecidos, se considerará como un tratamiento de carácter histórico y queda exceptuado de la presente Ley, y

V. Cuando los interesados tengan menos de 100 años de haber fallecido, podrá generarse el archivo sin autorización de sus familiares, pero se requerirá de autorización previa de la Comisión para ceder los datos correspondientes; antes de emitir la autorización, dicha Comisión se asegurará de que los datos no afectan a los descendientes de los interesados.

Artículo 11. Se consideran fuentes de acceso público aquellos archivos o publicaciones que contengan listas de personas y que pertenezcan a alguna de las categorías siguientes:

I. Listas de miembros de asociaciones, colegios profesionales, clubes y otras agrupaciones;

II. Guías de servicios de telecomunicaciones.

Las fuentes a que se refiere este artículo podrán incluir el nombre, dirección, identificadores de comunicación y otros elementos esenciales para la finalidad del archivo. La incorporación de datos adicionales requerirá del consentimiento de los interesados, quienes podrán solicitar se les excluya.

Los interesados tienen derecho a solicitar gratuitamente que se indique que sus datos no pueden ser usados para fines de publicidad o prospección comercial y a que sus datos no sean divulgados si así lo desean.

Artículo 12. Quienes se dediquen a la prestación de servicios de información sobre crédito y solvencia económica que no queden incluidas en las sociedades previstas por la Ley para Regular las Sociedades de Información Crediticia podrán tratar datos de carácter personal sujetos a las disposiciones siguientes:

I. Deberán registrar el archivo ante la Comisión;

II. Sólo podrán usar datos obtenidos de fuentes de acceso público o suministrados con el consentimiento del interesado;

III. Para efectos de cumplimiento o incumplimiento de obligaciones monetarias, podrán utilizar datos suministrados por el acreedor. En este caso, el responsable del archivo notificará al interesado acerca de su inclusión, dentro de los treinta días naturales siguientes a la inclusión de los datos en el archivo, informándole del derecho que tiene para conocer la información registrada;

IV. A solicitud del interesado, el responsable del archivo le comunicará los datos que se tengan registrados, así como las evaluaciones o apreciaciones que hayan sido comunicadas a terceros durante los últimos seis meses y el nombre y dirección del tercero o terceros a quienes se hayan revelado los datos;

V. La transmisión de estos datos no se hará a terceros ajenos a las instituciones de seguros, banca, crédito y fianzas, salvo que se tenga la autorización del interesado, por mandato judicial o por disposiciones legales al respecto, y
VI. El archivo solamente contendrá los datos esenciales para determinar la solvencia económica de los interesados. Cuando estos datos sean adversos al interesado, sólo podrán ser conservados por un máximo de seis años desde su registro, siempre y cuando reflejen de manera veraz la situación del interesado.

Artículo 13. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, ventas a distancia, prospección comercial y otras actividades análogas también se regirán de acuerdo con las disposiciones siguientes:

I. Podrán usar datos de carácter personal que se encuentren en fuentes de acceso público o que hayan sido obtenidos con el consentimiento del interesado;
II. Cuando los datos hayan sido derivados de fuentes de acceso público, el interesado podrá solicitar que se le informe gratuitamente acerca de la fuente usada. También podrá solicitar que se le excluya.

Artículo 14. Los medios de comunicación podrán generar archivos de datos de carácter personal bajo las condiciones de la presente Ley. Sin embargo, no se considerarán datos de carácter personal aquellos difundidos por los medios de comunicación que no hayan violado las disposiciones de la presente Ley.

Capítulo V

De la comisión

Artículo 15. La Comisión será el organismo responsable de la tutela de los derechos consignados en la presente Ley.

Artículo 16. La Comisión tendrá las facultades siguientes:

I. Vigilar el cumplimiento de esta Ley, particularmente en lo relativo a los derechos de acceso, rectificación, oposición y cancelación de datos;
II. Emitir las autorizaciones y las instrucciones previstas por el presente ordenamiento;
III. Atender las peticiones y reclamaciones de los afectados, evaluarlas escuchando a los responsables de los archivos involucrados y dictar las medidas necesarias para adecuar el tratamiento a las disposiciones de la presente Ley. Podrá ordenar la cesación del tratamiento y la cancelación de archivos cuando no se ajusten a sus disposiciones e imponer las multas correspondientes;
IV. Informar a los ciudadanos acerca de sus derechos en materia de datos de carácter personal y asesorarles en la materia;
V. Expedir los reglamentos de la presente Ley;
VI. Elaborar y mantener el Registro de Protección de Datos, y
VII. Las demás que sean necesarias para el cumplimiento de las anteriores.

Capítulo VI

De las infracciones y sanciones

Artículo 17. Serán infracciones a la presente Ley:

I. No atender por motivos formales la solicitud que presente el interesado para rectificar o cancelar sus datos personales, cuando esto proceda legalmente;
II. Recabar datos de carácter personal sin proporcionar la información especificada en la presente Ley;
III. Crear archivos con datos de carácter personal de titularidad pública sin la publicación previa de la disposición correspondiente en el *Periódico Oficial* o, en el caso de los de titularidad privada, crearlos sin el registro correspondiente o con finalidad distinta a la indicada en el registro de que se trate;
IV. Obtener datos sin el consentimiento expreso del interesado cuando éste es requerido;
V. Incumplir los principios establecidos en el artículo 4o. de la presente Ley y detallados en el reglamento respectivo;
VI. Impedir, obstaculizar o negar el ejercicio de los derechos de los interesados indicados en la presente Ley;
VII. La violación del secreto de los datos;
VIII. No remitir las notificaciones establecidas en la presente Ley a la Comisión, obstruir las funciones de la misma y no acatar sus disposiciones;
IX. La obtención de datos personales de manera engañosa o fraudulenta;
X. Tratar los datos de manera ilegítima;
XI. La violación del secreto en el caso de los archivos de carácter policial, fiscal o de salud, y
XII. El impedimento, obstaculización o negativa sistemáticos al ejercicio de los derechos de los interesados indicados en la presente Ley.

Artículo 18. Las infracciones prescribirán a los tres años desde la última notificación enviada por la Comisión.

Artículo 19. Las infracciones a que se refiere el artículo 17 de la presente Ley se sancionarán con multa de:

I. 50 a 500 unidades de salario, en el caso de las fracciones I y II;
II. 300 a 1 000 unidades de salarios, en el caso de las fracciones III a VIII, y
III. 1 000 a 10 000 unidades de salario, en el caso de las fracciones IX a XII.

Artículo 20. Las sanciones se impondrán tomando en cuenta los siguientes elementos:

I. La naturaleza de los derechos personales afectados;
II. El volumen de los tratamientos efectuados;
III. Los beneficios obtenidos;

IV. El grado de intencionalidad;
V. La reincidencia, si la hubiere, y
VI. Los daños y perjuicios causados.

En el caso de las fracciones IX a XII del artículo 17 de la presente Ley, la Comisión podrá, además, suspender o cancelar la operación del archivo cuando existan circunstancias que atenten a un grupo importante de interesados.

Artículo 21. Las multas que imponga la Comisión tendrán el carácter de créditos fiscales, que hará exigible la Secretaría de Finanzas del Gobierno del Estado, por medio del procedimiento económico coactivo. Para tal efecto, la Comisión le turnará por oficio una copia certificada de la correspondiente resolución.

Artículo 22. Cuando las infracciones a la presente Ley hubieran sido cometidas en archivos bajo la responsabilidad de las administraciones públicas estatal y municipales así como organismos públicos, la Comisión notificará la resolución al jefe inmediato del responsable de archivo y a la Secretaría de la Contraloría del Gobierno del Estado, a la unidad de control municipal, o a la dependencia similar del organismo público, en su caso, las que procederán de acuerdo a la legislación estatal sobre responsabilidades de los funcionarios públicos y demás disposiciones aplicables.

Artículo 23. Las resoluciones de la Comisión podrán ser impugnadas ante el Tribunal de lo Contencioso-Administrativo.

Anexo XII

Ley de protección de datos personales para el estado y los municipios de Guanajuato

(Publicada en el **Periódico Oficial** *19 de mayo de 2006)*

Título primero

Disposiciones generales

Capítulo Único

De las disposiciones generales

Artículo 1. La presente ley es de orden público e interés general y tiene por objeto garantizar la protección de los datos personales en poder de los sujetos obligados a que se refiere este ordenamiento.

Artículo 2. Los sujetos obligados para la aplicación de esta ley son:

I. El Poder Legislativo;
II. El Poder Ejecutivo;
III. El Poder Judicial;
IV. Los Ayuntamientos;
V. Los organismos autónomos, y
VI. Cualquier otra dependencia o entidad estatal o municipal.

Artículo 3. Para efectos de este ordenamiento se entenderá por:

I. Archivo o banco de datos: El conjunto de datos personales obtenidos por los sujetos obligados, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización o acceso;

II. Bloqueo de datos: La identificación y reserva de datos con el fin de impedir su tratamiento;
III. Cesión de datos: La difusión, distribución, transferencia, interconexión o comercialización de datos personales contenidos en los archivos o bancos de datos de los sujetos obligados;
IV. Consentimiento del titular: La manifestación de voluntad expresa, ya sea por escrito o a través de medios electrónicos, mediante la cual acepta el tratamiento de sus datos personales;
V. Datos personales: La información concerniente a una persona física identificada o identificable, relativa a su origen racial o étnico, o que esté referida a sus características físicas, morales o emocionales, a su vida afectiva o familiar, domicilio, número telefónico, patrimonio, ideología, creencias o convicciones religiosas o filosóficas, su estado de salud físico o mental, sus preferencias sexuales, claves informáticas o cibernéticas, códigos personales encriptados u otras análogas; que se encuentre vinculada a su intimidad, entre otras;
VI. Fuentes accesibles al público: El archivo o banco de datos cuya consulta puede ser realizada por cualquier persona y que estén contenidos en medios como: censos, anuarios, archivos de prensa, bases de datos públicas, colecciones jurisprudenciales, directorios telefónicos, diarios, boletines oficiales u otros análogos;
VII. Instituto: El Instituto de Acceso a la Información Pública;
VIII. Titular: Toda persona física a la que conciernen los datos personales;
IX. Tratamiento de datos: Las operaciones y procedimientos sistemáticos, automatizados o no, que permiten a los sujetos obligados la obtención, corrección, cancelación o cesión de datos personales.
Se entiende por operaciones o procedimientos automatizados aquellos que se realizan a través de dispositivos electrónicos, digitales, ópticos o de cualquier otra tecnología, que son empleados por los sujetos obligados, y
X. Unidad de acceso: La unidad de acceso a la información pública de cada sujeto obligado.

Artículo 4. Se exceptúan de la regulación de la presente ley los archivos y bancos de datos que:

I. Tengan por objeto almacenar datos personales para su publicidad con carácter general y que se regulen por sus disposiciones específicas;
II. Se regulen por sus disposiciones específicas en atención a la naturaleza de sus funciones, y
III. Se conformen para la prevención, investigación y persecución de delitos, y conductas antisociales.

Artículo 5. En la integración del archivo o banco de datos, los sujetos obligados deberán adoptar las medidas técnicas y de organización necesarias que garanticen la seguridad en el tratamiento de datos y eviten su alteración, pérdida, inexactitud o acceso no autorizado, para lo cual atenderán a la normativa que regule su funcionamiento y organización.

Título segundo

Tratamiento de datos personales

Capítulo primero

De las obligaciones de los sujetos obligados

Artículo 6. Los sujetos obligados, en el tratamiento de datos, tendrán las siguientes obligaciones:

I. Contar con el consentimiento del titular para la obtención de sus datos personales, informándole previamente sobre la existencia y finalidad del archivo o banco de datos, así como el carácter obligatorio u optativo de proporcionarlos y las consecuencias de ello;
II. Adoptar los procedimientos adecuados para dar trámite a las solicitudes de informes, de corrección o cancelación de datos personales y, en su caso, para la cesión de los mismos; debiendo capacitar a los servidores públicos encargados de su atención y seguimiento;
III. Utilizar los datos personales únicamente cuando éstos guarden relación con la finalidad para la cual se hayan obtenido;
IV. Proceder a la cancelación de los datos personales cuando éstos dejen de ser necesarios para la finalidad para la cual se obtuvieron. No se considerará como finalidad distinta el tratamiento que con posterioridad se les dé con objetivos estadísticos o científicos, siempre que no puedan atribuirse a persona determinada o determinable, así como para fines históricos;
V. Permitir en todo momento al titular el ejercicio del derecho a conocer sobre sus datos personales, a solicitar su corrección o cancelación, así como a oponerse en los términos de esta ley a que los mismos sean cedidos;
VI. Actualizar los datos personales cuando haya lugar, debiendo corregir o completar de oficio aquellos que fueren inexactos o incompletos, respectivamente, a efecto de que coincidan con los datos presentes del titular.
Lo anterior sin perjuicio de las prerrogativas reconocidas al titular para solicitar la corrección o cancelación de los datos que le conciernen, y
VII. Las demás que se deriven de la presente ley o les señalen otros ordenamientos jurídicos aplicables.

Artículo 7. No se requerirá el consentimiento del titular para la obtención de sus datos personales, cuando:

I. En situaciones de urgencia, peligre la vida o la integridad personal o se requieran para la prestación de asistencia en salud;
II. Exista una orden jurisdiccional, y
III. Se obtengan por fuentes accesibles al público.

Artículo 8. Los servidores públicos que por razón de sus actividades tengan acceso a algún archivo o banco de datos están obligados a mantener la confiden-

cialidad de los mismos. Esta obligación subsistirá aun después de finalizar las relaciones que les dieron acceso al archivo o banco de datos.

Serán relevados de dicha obligación cuando medie resolución jurisdiccional o existan circunstancias que pudieran alterar o poner en riesgo la seguridad o la salud pública.

Capítulo segundo

De los derechos de los titulares

Artículo 9. El titular tendrá los siguientes derechos:

I. Solicitar y obtener gratuitamente informes de sus datos personales, así como la corrección y cancelación de los mismos contenida en archivos o bancos de datos de los sujetos obligados;
II. Obtener la corrección o, en su caso, la cancelación de los datos personales, cuando sea procedente;
III. Revocar el consentimiento otorgado a los sujetos obligados para la cesión de datos;
IV. Conocer la identidad de los terceros a quienes se hayan cedido sus datos, así como las razones que motivaron el pedimento de la misma;
V. Conocer del carácter obligatorio u optativo de su respuesta para la obtención de datos personales, así como de las consecuencias de la negativa a proporcionarlos, y
VI. Los demás que se deriven de la presente ley o le señalen otros ordenamientos jurídicos aplicables.

Capítulo tercero

De las solicitudes

Artículo 10. Sin perjuicio de lo que dispongan otras leyes, sólo el titular o su representante, previa acreditación, tendrán derecho a solicitar a la unidad de acceso lo siguiente:

I. Informes de los datos personales que le conciernan y que obren en archivo o banco de datos determinado, y
II. La corrección o cancelación de los datos personales que le conciernan, contenidos en archivo o banco de datos determinado.

Artículo 11. Las solicitudes previstas en el artículo anterior deberán contener como mínimo:

I. El nombre del solicitante y domicilio para recibir notificaciones, mismo que deberá estar ubicado en el lugar donde resida la unidad de acceso ante la que se presente la solicitud;

II. La descripción clara y precisa de lo solicitado, y
III. La modalidad en que el solicitante desee le sean entregados los informes a que se refiere la fracción I del artículo 10.

En la solicitud correspondiente se podrá señalar cualquier otro dato que facilite la localización de la información.

Al pedirse una corrección o cancelación de datos personales, se deberá anexar la documentación que acredite la veracidad de lo solicitado, cuando la naturaleza del dato personal permita contar con tal documentación.

Cuando el solicitante no proporcione la información suficiente para localizar los datos personales o ésta sea errónea, la unidad de acceso podrá requerirlo por única vez dentro de los diez días hábiles siguientes a la presentación de la solicitud, para que en un plazo de cinco días hábiles indique otros elementos o corrija la información que faciliten su localización. En el supuesto de que no cumpla con el requerimiento se desechará de plano su solicitud.

Dicho requerimiento interrumpirá los plazos establecidos en los artículos 12 y 13 de este ordenamiento.

Artículo 12. Los informes a que se refiere la fracción I del artículo 10 de esta ley deberán entregarse dentro de un plazo de veinte días hábiles posteriores a la recepción de la solicitud, los cuales deberán formularse de manera clara y sencilla, conteniendo de manera completa la información concerniente al titular. Los informes serán entregados en la forma en que consten los datos.

Cuando existan razones justificadas que impidan entregar los informes en el plazo señalado, la unidad de acceso deberá informarlas al solicitante, ampliándose el plazo hasta por diez días hábiles más.

Para el caso de que el titular haya fallecido, el albacea de su sucesión, previa acreditación de su carácter, podrá solicitar y recibir dichos informes.

Artículo 13. La solicitud de corrección o cancelación de los datos personales deberá ser tramitada y su resolución, fundada y motivada, será notificada por la unidad de acceso al solicitante de manera personal; lo anterior dentro de los treinta días hábiles posteriores a su recepción.

Artículo 14. La solicitud de cancelación de datos personales será improcedente cuando con ello se pueda alterar o poner en riesgo la seguridad o la salud pública, se afecten derechos de terceros o así lo disponga la ley.

Artículo 15. Durante el procedimiento que se siga para corregir o cancelar datos personales, la unidad de acceso podrá ordenar el bloqueo de los mismos en el archivo o banco de datos que los contengan. Lo anterior sin perjuicio del derecho del titular de solicitar información de sus datos almacenados.

Capítulo cuarto

De la cesión de datos personales

Artículo 16. Los sujetos obligados podrán realizar la cesión de datos cuando se cumplan las siguientes condiciones:

I. Que haya mediado el consentimiento expreso del titular, y
II. Que el uso que se les vaya a dar mantenga congruencia con la finalidad para la cual se obtuvieron.

El titular podrá revocar en cualquier momento el consentimiento otorgado para la cesión de datos, mediante aviso o notificación por escrito que realice ante el sujeto obligado.

Artículo 17. La cesión de datos no requerirá del cumplimiento de las condiciones previstas en el artículo anterior cuando:

I. En situaciones de urgencia, peligre la vida o la integridad personal o se requieran para la prestación de asistencia en salud;
II. Se entreguen por razones estadísticas, científicas o de interés general previstas en ley. En estos casos los sujetos obligados proporcionarán la información de tal manera que no puedan asociarse los datos personales con su titular;
III. Se transmitan entre sujetos obligados en términos de las leyes aplicables;
IV. Exista una orden jurisdiccional, y
V. El sujeto obligado contrate a terceros para la prestación de un servicio que requiera el tratamiento de datos. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquellos para los cuales se les hubieren transmitido.

Artículo 18. Cuando la cesión de datos se realice en los términos que prevé el artículo 16 de esta ley, el cesionario deberá proporcionar al sujeto obligado los siguientes datos y documentos:

I. En el caso de personas físicas: Nombre, edad, nacionalidad, número telefónico, así como original y copia de una identificación oficial y de un comprobante de su domicilio reciente para su cotejo, y
II. En tratándose de personas morales: Denominación o razón social, nacionalidad, número telefónico, así como copia certificada del acta constitutiva y del documento que acredite la personalidad del representante.

El cesionario deberá guardar confidencialidad de los datos personales obtenidos y por ningún motivo podrá realizar con terceros alguno de los actos comprendidos para la cesión de datos.

Artículo 19. Cuando los sujetos obligados hayan efectuado una cesión de datos, deberán informar a su titular la identidad del cesionario, así como las razones que motivaron el pedimento de la misma, dentro de los diez días hábiles siguientes al momento en que se haya hecho la cesión.

Artículo 20. No se considerará cesión de datos el acceso que un tercero tenga a los datos personales con motivo de la prestación de un servicio de mantenimiento o funcionamiento al archivo o banco de datos.

Título tercero

Autoridades

Capítulo primero

Del Instituto y sus atribuciones

Artículo 21. El Instituto como autoridad encargada de garantizar la protección de datos personales, además de las atribuciones que le confieren otras disposiciones legales, tendrá las siguientes:

I. Otorgar asesoría a las personas que lo requieran acerca del contenido y alcance de la presente ley;
II. Dictar, en el ámbito de su competencia, los lineamientos necesarios para garantizar el cumplimiento de esta ley;
III. Elaborar y mantener actualizado el Registro Estatal de Protección de Datos Personales de los archivos o bancos de datos de los sujetos obligados, y
IV. Procurar la conciliación de los intereses de los titulares con los de los sujetos obligados cuando éstos entren en conflicto con motivo de la aplicación de la presente ley.

Capítulo segundo

Del director general del Instituto y sus atribuciones

Artículo 22. El director general del Instituto, además de las atribuciones que le confieren otras disposiciones legales, tendrá las siguientes:

I. Conocer y resolver el recurso de queja;
II. Llevar un registro de las resoluciones que recaigan al recurso de queja que se tramite ante él, y
III. Coordinar y organizar el Registro Estatal de Protección de Datos Personales.

Título cuarto

Registro estatal de protección de datos personales

Capítulo único

Del Registro Estatal de Protección de Datos Personales

Artículo 23. El Instituto conformará el Registro Estatal de Protección de Datos Personales, el cual tendrá por objeto llevar un control sobre la existencia y finalidades de archivos o bancos de datos en poder de los sujetos obligados.

Para tal efecto, los sujetos obligados deberán proporcionar al Instituto dentro de los plazos y términos que se establezcan en sus lineamientos, la información relativa a sus archivos o bancos de datos, que a continuación se señala:

I. La ubicación;
II. Las características y finalidades, y
III. La cesión de datos que hayan realizado, indicando la identidad del cesionario. Cualquier modificación a la información proporcionada al Registro Estatal de Protección de Datos Personales deberá ser comunicada por el sujeto obligado dentro de los diez días hábiles siguientes a que haya tenido lugar, para su debida actualización.

Artículo 24. Toda persona tiene derecho de solicitar al Instituto información sobre la existencia y finalidades de archivos o bancos de datos en poder de los sujetos obligados.

Título quinto

Medios de impugnación

Capítulo único

Del recurso de queja

Artículo 25. El recurso de queja procederá en contra:

I. Del incumplimiento de entregar dentro del plazo que establece esta ley los informes de datos personales que le conciernan al titular, contenidos en archivos o bancos de datos;
II. Del incumplimiento de notificar dentro del plazo que establece esta ley el acto de corrección o cancelación de los datos personales solicitados, y
III. De la negativa de corregir o cancelar los datos personales.

Artículo 26. El titular o su representante podrán interponer el recurso de queja ante el director general del Instituto dentro de los quince días hábiles siguientes a la notificación o a la fecha en que tenga conocimiento de los supuestos contemplados en el artículo anterior.

Artículo 27. El escrito de interposición del recurso de queja deberá contener:

I. El nombre del recurrente;
II. El domicilio para recibir notificaciones, el cual deberá ubicarse en la sede del Instituto; de lo contrario se notificará por estrados;
III. La unidad de acceso ante la que se presentó la solicitud, señalando el domicilio de ésta;
IV. La fecha en que se le notificó o tuvo conocimiento del acto que origina su recurso, y

V. La exposición en forma clara y sucinta de los hechos relativos a la queja, así como los motivos por los cuales considera se le causan agravios con el tratamiento de sus datos.

Al escrito, el recurrente deberá acompañar los documentos en que funde su impugnación.

Artículo 28. Como medida preventiva, el director general del Instituto podrá ordenar el bloqueo de los datos personales contenidos en el archivo o banco de datos que sean motivo del recurso. Dicho bloqueo permanecerá hasta que se emita la resolución correspondiente.

Artículo 29. Una vez recibido el recurso de queja, se hará el emplazamiento a la unidad de acceso que corresponda, para que dentro de un plazo de siete días hábiles siguientes a éste rinda un informe justificado remitiendo las constancias relativas.

Ante la negación de la existencia del acto recurrido por parte de la unidad de acceso, se correrá traslado al recurrente para que en el plazo de tres días hábiles manifieste lo que a su interés convenga. En caso de no comprobar la existencia del acto impugnado se sobreseerá el recurso.

Artículo 30. Rendido el informe justificado o transcurrido el plazo señalado en el segundo párrafo del artículo anterior, el director general del Instituto resolverá el recurso de queja dentro de los diez días hábiles siguientes, confirmando, modificando o revocando el acto recurrido.

La resolución que recaiga al recurso de queja se notificará en forma personal al recurrente y por cualquier medio a la unidad de acceso que corresponda.

Si la resolución es favorable al recurrente, el director general del Instituto ordenará a la unidad de acceso que entregue los informes solicitados o realice la corrección o cancelación de los datos solicitados, en un plazo no mayor a cinco días hábiles.

Artículo 31. El director general del Instituto puede en todo momento y hasta antes de dictar resolución requerir todo tipo de información que considere necesaria para la resolución del recurso de queja.

Artículo 32. En la substanciación del recurso de queja, en lo no previsto por esta ley, se aplicará de manera supletoria la Ley de Justicia Administrativa del Estado de Guanajuato.

Título sexto

Infracciones y sanciones

Capítulo único

De las infracciones y sanciones

Artículo 33. Son infracciones a la presente ley por parte de los servidores públicos las siguientes:

I. Impedir u obstaculizar injustificadamente el ejercicio de los derechos del titular;
II. Incumplir con la entrega de informes dentro del plazo establecido en esta ley;
III. Notificar fuera del plazo que establece la presente ley el acto mediante el cual se efectúe, en su caso, la corrección o cancelación de los datos personales;
IV. Negar sin causa justificada la corrección o cancelación de datos personales;
V. Realizar la cesión de datos en contravención a lo dispuesto por esta ley;
VI. Violentar el principio de confidencialidad que deben guardar por disposición de esta ley;
VII. Realizar el tratamiento de datos contraviniendo las disposiciones que señala este ordenamiento, y
VIII. No atender el sentido de una resolución favorable para el recurrente, emitida con motivo de la interposición del recurso de queja.

Artículo 34. A los servidores públicos que incurran en las infracciones a que se refiere el artículo anterior se les impondrán las siguientes sanciones:

I. Amonestación, para los casos de las fracciones II y III;
II. Multa para los casos de las fracciones I, IV y VII, y
III. Destitución para los casos de las fracciones V, VI y VIII.

Artículo 35. Las sanciones previstas en el artículo anterior se aplicarán con base en el procedimiento y parámetros de las sanciones establecidos en la Ley de Responsabilidades Administrativas de los Servidores Públicos del Estado de Guanajuato y sus Municipios, sin perjuicio de la responsabilidad penal o civil en que pudieran incurrir los infractores.

Artículo 36. La facultad para fincar la responsabilidad administrativa prescribirá en el plazo de un año, contado a partir del día siguiente a aquel en que se haya cometido la infracción.

Dicha prescripción se interrumpirá por el inicio del procedimiento de responsabilidad administrativa.

Anexo XIII

Reglamento de protección de datos personales del municipio de Ocampo, Gto.

(Publicado en el **Periódico Oficial** *del Estado de Guanajuato el viernes 9 de noviembre de 2007)*

Capítulo I

Disposiciones generales

Artículo 1. El presente reglamento tiene por objeto establecer y regular los procedimientos para el trámite de las solicitudes de informes, corrección, y cancelación de datos personales, así como el procedimiento relativo para la cesión de datos personales.

Artículo 2. Para los efectos del presente reglamento se entenderá por:

I. Archivo, registro, base o banco de datos personales: indistintamente, designa [sic] al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso;
II. Archivos o bancos de datos personales físicos: conjunto ordenado de datos que para su tratamiento están contenidos en registros manuales, impresos;
III. Archivos o bancos de datos personales automatizados: conjunto ordenado de datos que para su manejo requiere de una herramienta tecnológica específica que permita su acceso, recuperación o tratamiento. Como son sonoros, magnéticos, visuales, holográficos u otro que la ciencia y la tecnología reconozca como tal [sic];
IV. Archivos o banco de datos personales mixtos: conjunto ordenado de datos que para su tratamiento se encuentran contenidos tanto en registros manuales como en aquellos en que se requiera una herramienta tecnológica que permita su acceso;

V. Cesión de datos: toda revelación de datos personales realizada a una persona u organismo distinta [sic] del interesado, por parte del sujeto obligado en los términos de la Ley de protección de datos personales;
VI. Consentimiento del Titular de los datos personales: se entenderá como aquel dado para la posible cesión de sus datos, y podrá ser por escrito o por medios electrónicos.
VII. Domicilio: se entenderá, para efectos de la Ley de Protección de Datos Personales por domicilio, el domicilio particular, atendiendo para su definición el domicilio en donde habita la persona Titular de los datos personales;
VIII. Informes de datos personales: relación de archivos o bancos de datos en que se contiene información del Titular, tipo de información contenida, naturaleza de la información y status [sic] de la misma precisándose si se han cancelado, corregido, modificado o cedido, proporcionando la información completa de la misma;
IX. Procedimientos de desvinculación: todo tratamiento de datos personales, de modo que la información que se obtenga no pueda atribuirse al titular de éstos, ni permitir por su estructura, contenido o grado de desagregación la identificación individual del mismo;
X. Ley: Ley de Protección de Datos Personales para el Estado y los Municipios de [sic] Estado de Guanajuato;
XI. Instituto: Instituto de Acceso a la Información Pública;
XII. Unidad de Acceso: Unidad de Acceso a la Información Pública Municipal;
XIII. Sujeto Obligado: H. Ayuntamiento; y
XIV. Titular: Toda persona física a la que conciernen los datos personales.

Artículo 3. Los datos personales no podrán tratarse automática ni manualmente en archivos o bases de datos accesibles al público, con las excepciones previstas en la Ley.

Artículo 4. Los datos personales no serán conservados en forma que permitan la identificación del interesado durante un periodo superior al necesario para la finalidad por la que fueron recabados.

Artículo 5. La excepción para la cancelación de los archivos o bases de datos y la decisión del mantenimiento de los datos será atendido [*sic*] a su valor histórico, estadístico o científico, de acuerdo con la regulación especifica.

Artículo 6. No se considera incompatible con la finalidad para la cual fueron recabados los datos personales en relación con el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

Artículo 7. En la integración de archivos o bancos de datos personales, se deberá indicar la siguiente información:

I. Finalidad de archivo o banco de datos personales y el uso previsto para el mismo.
II. Personas sobre las que pretende obtener datos personales o que resulten obligados a suministrarlos.
III. Procedimiento para la obtención de datos.
IV. Estructura básica del archivo.

V. Cesiones de datos personales y, en su caso, las cesiones de datos que se prevean.
VI. Los órganos de las administraciones responsables de los ficheros.
VII. Medidas de seguridad.

Capítulo II

Sobre el tratamiento de datos personales

Artículo 8. Cuando el servicio de tratamiento de datos personales es prestado por un tercero que ha sido contratado para tal fin, éstos no podrán utilizarse con un fin distinto al que figure en el contrato de servicios.

Artículo 9. Una vez que haya concluido la relación contractual, los datos personales deberán ser entregados al sujeto obligado del que se trate.

Artículo 10. Los datos personales que hayan sido tratados y no contengan valor histórico, científico o contable, deben ser cancelados teniendo en consideración los criterios que para la organización y conservación de archivos se hayan adoptado. Los que contengan esas características deberán atender a la desvinculación de los mismos.

Capítulo III

Del procedimiento

Artículo 11. El trámite de las solicitudes de informes, corrección y cancelación de datos personales, así como para la cesión de datos, se regirá por lo previsto en el presente reglamento, en los plazos y procedimientos establecidos en el mismo.

Artículo 12. Las solicitudes y los trámites para la obtención de informes, corrección o cancelación de datos personales contenidos en archivo o banco de datos del sujeto obligado estarán exentos de pago de acuerdo a lo establecido en la fracción I del artículo 9 de la Ley.

Artículo 13. Si el Titular o su representante desea solicitar informes, corrección o cancelación de sus datos vía electrónica deberá hacerla mediante el uso de firma electrónica certificada en los términos de la Ley sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios.

Artículo 14. Para este caso la Unidad de Acceso deberá dar entrada y trámite a las solicitudes mediante el mismo sistema.

Artículo 15. Para la acreditación del Titular o su representante, ante la Unidad de Acceso debe adjuntar los documentos que acrediten su personalidad.

Artículo 16. El sujeto obligado deberá elaborar un registro en formato libre, mediante el cual se relacione la solicitud de corrección o cancelación con los datos del documento oficial con el que se acredita la personalidad, los cuales podrán ser: pasaporte, cartilla de servicio militar, cédula profesional o credencial de elector.

Artículo 17. En todos los casos la Unidad de Acceso deberá corroborar la personalidad de los solicitantes para proceder a realizar, en definitiva, la corrección o cancelación de datos personales.

Capítulo IV

De las solicitudes de informes

Artículo 18. Es derecho de todo Titular el solicitar y obtener informes sobre sus datos personales que obran en archivos o bancos de datos del sujeto obligado.

Artículo 19. Este derecho lo ejercerá ante la Unidad de Acceso.

Artículo 20. Los datos mínimos que deberán contener las solicitudes son:

I. Nombre del solicitante (Titular o representante legal).
II. Domicilio para recibir notificaciones (lugar donde resida la Unidad de Acceso ante la que se presente la solicitud).
III. Descripción clara y precisa de los datos personales solicitados.
IV. Cualquier otro dato que facilite la localización de la información.
V. Modalidad en que el solicitante desee le sean entregados los informes.

Artículo 21. El plazo para entregar los informes de datos personales se hará dentro de los veinte días hábiles siguientes a la recepción de la solicitud, los cuales deberán formularse de manera clara y precisa, conteniendo de manera completa la información concerniente al titular, debiendo obtener la información total del titular en las diversas dependencias del sujeto obligado. Serán entregados en la forma en que consten los datos.

Artículo 22. La notificación correspondiente será enviada al solicitante por correo certificado con acuse de recibo, dentro de los veinte días hábiles siguientes a la recepción de la solicitud.

Artículo 23. La Unidad de Acceso podrá requerir al solicitante, por única vez dentro de los diez días hábiles siguientes a la presentación de la solicitud, para que en un plazo de cinco días hábiles indique otros elementos o corrija la información que facilite su localización. En el supuesto de que no cumpla con el requerimiento se desechará su solicitud. Dicho requerimiento interrumpirá los plazos establecidos en los artículos 21 y 22 de este ordenamiento.

Artículo 24. El titular de la Unidad de Acceso podrá ampliar el plazo de entrega del informe, siempre y cundo [*sic*] lo haga del conocimiento del solicitante; dicha ampliación no excederá de más de diez días hábiles.

Artículo 25. Las modalidades de entrega son:

I. Personalmente, o a través de su representante, en las instalaciones de la Unidad de Acceso, siendo requisito portar documentos que acrediten su personalidad.
II. Correo certificado con notificación.

Artículo 26. En caso de inexistencia de los datos solicitados se deberá informar que éstos no se encuentran en el archivo o banco de datos del sujeto obligado,

procurando orientar al particular sobre el sujeto obligado que probablemente posea dichos datos. La notificación de la resolución deberá enviarse por correo certificado con acuse de recibo al solicitante y le deberá indicar que puede interponer el recurso de queja ante la Dirección General del Instituto.

Capítulo V

De las solicitudes de corrección o cancelación de datos personales

Artículo 27. Es derecho de todo Titular el solicitar y obtener la cancelación de sus datos personales que obran en archivos o bancos de datos del sujeto obligado.

Artículo 28. La cancelación de datos personales procede cuando éstos dejen de ser necesarios para la finalidad para la cual se obtuvieron.

Artículo 29. En caso de que los archivos o bancos de datos revelen información para fines estadísticos, científicos o históricos, antes de la cancelación se procederá a eliminar los datos que puedan atribuirse a persona determinada o determinable para posteriormente respaldar la información o a sistematizarla a través de medios electrónicos de fácil consulta pública.

Artículo 30. El derecho de corrección de datos personales lo ejercerá el Titular o su representante legal, presentando su solicitud ante la Unidad de Acceso.

Artículo 31. Los datos mínimos que deberán contener las solicitudes son:

I. Nombre del solicitante (Titular o representante legal).
II. Domicilio para recibir notificaciones, que deberá estar ubicado en el lugar donde resida la Unidad de Acceso ante la que se presente la solicitud.
III. Descripción clara y precisa de los datos personales sobre los cuales se pide la corrección o cancelación.
IV. Cualquier otro dato que facilite la localización de la información.

Artículo 32. Anexar la documentación que acredite la veracidad de lo solicitado, cuando la naturaleza del dato personal permita contar con tal documentación.

Artículo 33. El Titular o su representante podrá presentar sus solicitudes de corrección o cancelación de datos personales a través de:

I. Formato.
II. Escrito libre.
III. Medios electrónicos certificados.
IV. Correo certificado con notificación.

Artículo 34. La Unidad de Acceso podrá requerir al solicitante, por única vez dentro de los diez días hábiles siguientes a la presentación de la solicitud, para que en un plazo de cinco días hábiles indique otros elementos o corrija la información que facilite su localización. En el supuesto de que no cumpla con el requerimiento se desechará su solicitud.

Artículo 35. La notificación interrumpirá el plazo para el trámite de la solicitud hasta que el solicitante corrija la misma y proporcione los elementos necesarios para su localización.

Artículo 36. Cuando se hayan satisfecho los requisitos de la solicitud, la Unidad de Acceso debe requerir de [*sic*] la Unidad Administrativa de que se trate para que remita dentro de los cinco días hábiles siguientes el documento o información concerniente a la solicitud de que se trate.

Artículo 37. La resolución de afirmativa de corrección la hará el titular de la Unidad de Acceso, fundada y motivada, misma que se hará del conocimiento del titular o su representante, y se deberá notificar al encargado del área donde se contengan los archivos o bancos de datos a fin de que se proceda a la corrección o cancelación de los datos personales, señalando en su caso cuáles son los datos correctos, o bien, cuáles de ellos tendrán que cancelarse, indicándole que en ambos supuestos deberá anexarse la resolución al documento correspondiente.

Artículo 38. La notificación de la resolución recaída a la solicitud de corrección o cancelación de datos deberá hacerse de manera personal dentro de los treinta días hábiles posteriores a la recepción de la solicitud. En caso de no cumplir dicho plazo, el Titular podrá interponer el recurso de queja ante la Dirección General del Instituto.

Artículo 39. En tanto se resuelve el sentido de la solicitud, el titular de la Unidad de Acceso podrá ordenar el bloqueo de los datos personales en el archivero o banco de datos.

Artículo 40. De resultar improcedente la corrección o cancelación de los datos personales, de igual manera la Unidad de Acceso debe notificar el acuerdo respectivo al solicitante expresando los motivos y fundamentos legales que haya tomado en consideración para tal efecto, dentro del mismo plazo al que se refiere el artículo 38. Debiendo orientar al solicitante sobre el medio de impugnación con el que cuenta de conformidad con el previsto en la Ley.

Artículo 41. En caso de que los servidores públicos, en ejercicio de sus atribuciones, detecten que hay datos personales inexactos, deberán de oficio actualizarlos en el momento en que tengan conocimiento de la inexactitud de los mismos, siempre que posean los documentos que justifiquen la actualización; posteriormente lo harán del conocimiento del titular de la Unidad de Acceso para que lo notifique al Titular.

Artículo 42. Una vez dictada la resolución en sentido afirmativo y realizado el tramite de corrección o cancelación deberá expedirse una constancia de ello a favor del Titular a fin de que conste el cumplimiento de de [*sic*] lo resuelto.

Capítulo VI

Atribuciones de la unidad de acceso a la información pública

Artículo 43. Las [*sic*] Unidad de Acceso en materia de protección de datos personales tendrá las siguientes atribuciones:

I. Recibir y tramitar las solicitudes de informe, corrección o cancelación de datos personales que obren en los archivos o bancos de datos del sujeto obligado.
II. Entregar o negar los informes requeridos, fundando y motivando su resolución en los términos de la Ley.

III. Proceder o no a la corrección o cancelación de datos personales, fundando y motivando su resolución en los términos de la Ley.
IV. Auxiliar a los Titulares en la elaboración de solicitudes de informes, corrección o cancelación de datos personales que obren en archivos o bancos de datos del sujeto obligado.
V. Realizar los trámites internos necesarios para localizar y, en su caso, entregar los informes, corregir o cancelar los datos personales.
VI. Efectuar las notificaciones al Titular o su representante de entrega de informes, corrección o cancelación de datos personales.
VII. Llevar un registro de las solicitudes de informes, corrección o cancelación de datos personales, sus resultados y tiempos de respuesta de las mismas.
VIII. Elaborar los formatos de solicitud, corrección o cancelación de datos personales.
IX. Informar trimestralmente al H. Ayuntamiento, o en cualquier momento a requerimiento de éste, sobre las solicitudes de informes, corrección o cancelación de datos personales recibidas y tramitadas.

Capítulo VII

De la cesión de los datos personales

Artículo 44. La cesión opera cuando el sujeto obligado que ha obtenido datos personales, cualquiera que sea la forma o modalidad de su creación o almacenamiento u organización, transfiera, distribuya, difunda, interconecte o comercialice los archivos o bancos de datos.

Artículo 45. Para llevar a cabo la cesión será indispensable el consentimiento expreso del Titular y que el uso que se les vaya a dar mantenga congruencia con la finalidad para la cual se obtuvieron, salvo en los casos de excepción previstos por la Ley.

Artículo 46. En caso de revocación de la cesión de datos personales por parte del Titular, deberá realizar los trámites internos para hacer del conocimiento de las áreas administrativas del sujeto obligado que posee el archivo o banco de datos.

Artículo 47. Los requisitos que deberá cubrir el cesionario de datos personales son los contenidos en el artículo 18 de la ley.

Artículo 48. En caso de llevarse a cabo la cesión de los datos personales se deberá informar al Titular de los datos personales de la identidad del cesionario, así como las razones que motivaron a cesión, dentro del término previsto por el artículo 19 de la Ley, mediante oficio suscrito por el responsable nombrado por el sujeto obligado.

Artículo 49. La cesión de datos puede comprender los datos personales del Titular, de varios Titulares o del total de Titulares que conforman el archivo o banco de datos. Debiéndose documentar la cesión de datos personales en cualquiera de los supuestos enunciados, de conformidad con lo previsto en el artículo 34 de este instrumento.

Artículo 50. El sujeto obligado, tratándose de cesión de datos personales, deberá documentar lo previsto en la fracción II del artículo 16 de la Ley, a fin de

sustentar que el uso que se les va a dar a los datos personales cedidos sea congruente con la finalidad para la que fueron obtenidos.

Artículo 51. Se formará el expediente respectivo en cada caso de cesión de datos con la documental que avale:

I. El consentimiento expreso del Titular, y
II. El sustento de la congruencia con la finalidad para la cual se obtuvieron.

Artículo 52. En el supuesto de que el Titular de los datos personales revoque el consentimiento otorgado para la cesión de datos, se deberá hacer la anotación correspondiente en el archivo o banco de datos, a fin de que se atienda a esa negativa y se observe por los servidores públicos que corresponda.

Artículo 53. El consentimiento del Titular de los datos personales se entenderá hecho sólo para la finalidad por la cual son recabados, debiéndose obtener el consentimiento en caso de que sus datos personales se obtengan en otro momento y con otra finalidad, no obstante que puedan englobarse en una sola herramienta tecnológica para su tratamiento.

Artículo 54. Al escrito que contenga la revocación del consentimiento otorgado para la cesión de datos personales por parte del Titular de los datos personales deberá recaer respuesta del responsable de la protección de datos personales.

Artículo 55. La revocación por parte del Titular de los datos personales al consentimiento otorgado para la cesión de los mismos surtiría efecto a partir de la fecha de la recepción del escrito correspondiente por parte del sujeto obligado, sin que pueda ser considerado en forma retroactiva.

Artículo 56. En los casos de excepción previstos por el artículo 17 de la Ley, se deberá dejar constancia documental de la fracción que se actualiza para poder realizar las cesiones sin necesidad del cumplimiento de las condiciones previstas para la cesión, haciéndose la anotación correspondiente en el propio sistema de Registro Estatal de Archivos o Banco de Datos.

Artículo 57. No será considerada como cesión la consulta de los datos personales que para el cumplimiento de las sesiones del Ayuntamiento se realice al interior del mismo.

Capítulo VIII

De la seguridad de los archivos y bancos de datos personales

Artículo 58. El Ayuntamiento adoptará las medidas técnicas y organizativas que garanticen la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado, con independencia de la naturaleza de los datos almacenados y los riesgos a quien [*sic*] estén expuestos.

Artículo 59. Los archivos o bancos de datos que contengan datos relativos a la ideología, religión, creencias, origen racial, salud o vida sexual deberán ser tratados protegiendo y/o encriptando los datos o utilizando cualquier otro medio que garantice que la información no será manipulada durante su transporte.

Artículo 60. El Ayuntamiento establecerá las medidas de índole técnica y organizativa para garantizar la seguridad que deben reunir los archivos automatizados, los centros de tratamiento, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado.

Artículo 61. Para proveer seguridad a los archivos y bancos de datos personales, el Ayuntamiento deberá adoptar, por lo menos, las medidas siguientes:

I. Designar a los responsables de mantener actualizado el Registro Estatal de Protección de Datos Personales;
II. La emisión de un manual de procedimientos sobre el manejo, mantenimiento, seguridad y protección de los archivos o bancos de datos personales, tomando como base lo dispuesto por el presente Reglamento;
III. Promover la difusión de la normatividad entre el personal involucrado en el manejo [sic] los archivos y bancos de datos personales.
IV. Elaborar un plan de capacitación en materia de seguridad de datos personales dirigido a los responsables y encargados.

Artículo 62. Al interior del Ayuntamiento, el responsable coordinará y supervisará las acciones de promoción del manejo, mantenimiento, seguridad y protección de los archivos o bancos de datos personales, así como la integridad, confiabilidad y disponibilidad de la información contenida en los mismos.

Artículo 63. La documentación generada para la implementación, administración y seguimiento de las medidas de seguridad administrativa, física y técnica tendrá el carácter de información reservada y será de acceso restringido, en los términos de la Ley de Acceso a la Información Pública para el Estado y los Municipios de Guanajuato.

Artículo 64. El encargado que tenga acceso a dicha documentación deberá evitar que ésta sea divulgada, a efecto de no comprometer la integridad, confiabilidad, confidencialidad y disponibilidad de los archivos o bancos de datos personales así como del contenido de éstos.

Artículo 65. El Ayuntamiento, además de las atribuciones que le confieren otras disposiciones legales, tendrá las siguientes:

I. Adoptar las medidas para el resguardo de los archivos o bancos de datos personales en soporte físico o automatizado, de manera que se evite su alteración, pérdida o acceso no autorizado;
II. Autorizar expresamente, en los casos en que no esté previsto por un instrumento jurídico, a encargados y usuarios llevar una relación actualizada de las personas que tengan acceso a los archivos o bancos de datos personales, y
III. Nombrar al responsable y encargados de los archivos y bancos de datos.

Artículo 66. Los archivos, estantes o medio que se utilice para almacenar los archivos no automatizados que contengan datos personales deberán encontrarse en áreas en las que el acceso esté protegido, es decir, cerrado, a fin de que se controle el acceso y se mantenga cerrado cuando no sea necesario acceder a la información contenida en los archivos.

En caso de imposibilidad de contar con el lugar físico adecuado, el responsable detallará las circunstancias y propondrá medidas alternativas, que permitan

proteger la información y se mantenga bajo resguardo e impedir que personal no autorizado tenga acceso a la misma.

Artículo 67. Para el cumplimiento de las atribuciones del Ayuntamiento que la Ley prevé, se deberá contar con:

I. Espacio suficiente y adecuado, que cumpla con las condiciones de seguridad establecidas en el presente Reglamento, destinados [sic] a almacenar medios de respaldo de archivos o bancos de datos personales;
II. Controlar el acceso físico a las instalaciones donde se encuentra el equipamiento que soporta la operación de los archivos o bancos de datos personales, debiendo registrarse para ello en una bitácora;
III. Realizar procedimientos de control, registro de asignación y baja de los equipos de cómputo a los usuarios que utilizan datos personales, considerando al menos las siguientes actividades:

   a) Si es asignación, configurarlo con las medidas de seguridad necesarias, tanto a nivel operativo como de infraestructura, y
   b) Verificar y llevar un registro del contenido del equipo para facilitar los reportes del usuario que lo recibe o lo entrega para su baja.

IV. Implantar procedimientos para el control de asignación y renovación de contraseñas de acceso a equipos de cómputo y a los archivos o bancos de datos personales;
V. Implantar medidas de seguridad para el uso de los dispositivos electrónicos y físicos de salida, así como para evitar el retiro no autorizado de los mismos fuera de las instalaciones de la entidad o dependencia, y
VI. En el caso de requerirse disponibilidad crítica de los datos, instalará [sic] y mantener el equipamiento de cómputo, eléctrico y de telecomunicaciones con la redundancia necesaria. Además realizar respaldos que permitan garantizar la continuidad de la operación.

Artículo 68. En relación con los aspectos de seguridad al utilizar la red de comunicación donde se transmitan datos personales, es necesario establecer:

I. Procedimientos de control de acceso a la red que consideren perfiles de usuario o grupos de usuarios para uso restringido a las funciones y programas de los archivos o bancos de datos personales;
II. Mecanismos de auditoría o rastreabilidad de operaciones que mantenga una bitácora para conservar un registro detallado de las acciones llevadas a cabo en cada acceso, ya sea autorizado o no, a los archivos o bancos de datos personales.
III. Las medidas de seguridad necesarias para el acceso a datos personales a través de la red de comunicación debe garantizar un nivel de seguridad óptimo equivalente al correspondiente al de los accesos en modo local.

Artículo 69. Se podrán atender las recomendaciones que sobre estándares mínimos de seguridad aplicable a los archivos o bancos de datos personales, en poder del Ayuntamiento, emita el Instituto.

Capítulo IX

De las infracciones y sanciones

Artículo 70. Son infracciones al presente Reglamento por parte de los servidores públicos las siguientes:

I. Impedir u obstaculizar injustificadamente el ejercicio de los derechos del Titular;
II. Incumplir con la entrega de informes dentro del plazo establecido en este Reglamento;
III. Notificar, fuera del plazo que establece el presente Reglamento, el acto mediante el cual se efectúe, en su caso, la corrección o cancelación de los datos personales;
IV. Negar, sin causa justificada, la corrección o cancelación de datos personales;
V. Realizar la cesión de datos en contravención a lo dispuesto por este Reglamento;
VI. Violentar el principio de confidencialidad que deben guardar por disposición de este Reglamento;
VII. Realizar el tratamiento de datos contraviniendo las disposiciones que señala este ordenamiento, y
VIII. No atender el sentido de una resolución favorable para el recurrente, emitida con motivo de la interposición del recurso de queja.

Artículo 71. A los servidores públicos que incurran en las infracciones a que [sic] refiere el artículo anterior se les impondrán las siguientes sanciones:

I. Amonestación, para los casos de las fracciones II y III;
II. Multa para los casos de las fracciones I, IV y VII, y
III. Destitución para los casos de las fracciones V, VI y VIII.

Artículo 72. Las sanciones previstas en el artículo anterior se aplicara [*sic*] con base en el procedimiento y parámetros de las sanciones establecidos en la Ley de Responsabilidades Administrativas de los Servidores Públicos del Estado de Guanajuato y sus Municipios, sin perjuicio de la responsabilidad penal o civil en que pudieran incurrir los infractores.

Artículo 73. La facultad para fincar la responsabilidad administrativa prescribirá en el plazo de un año, contado a partir del día siguiente a aquel en que se haya cometido la infracción.

Dicha prescripción se interrumpirá por el inicio del procedimiento de responsabilidad administrativa.

Anexo XIV

Decisiones judiciales en México respecto al valor probatorio de los documentos electrónicos

Registro No. 169027

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XVIII, Agosto de 2008
Página: 1209
Tesis: VIII.4o.28 C
Tesis Aislada
Materia(s): Civil

TARJETAS DE CRÉDITO. SUPUESTO EN EL QUE NO OPERA LA CARGA DE LA PRUEBA AL ACTOR CUANDO NIEGA HABER EFECTUADO LOS PAGOS Y DISPOSICIONES QUE DIERON ORIGEN A LOS CARGOS CUYA CANCELACIÓN DEMANDA. De los artículos 1194 y 1195 del Código de Comercio se advierte que la carga de la prueba queda definida de la siguiente manera: el que afirma está obligado a probar, por lo cual el actor debe probar su acción y el reo o demandado sus excepciones, y que por regla general, el que niega no está obligado a probar, pero excepcionalmente debe hacerlo cuando su negación envuelve la afirmación expresa de un hecho. Ahora bien, no se da ninguno de los anteriores supuestos para atribuirle la carga de la prueba al actor, cuando simplemente niega haber realizado los pagos y disposiciones que dieron origen a los cargos cuya cancelación demanda, pues la negativa de referencia, constituye una negativa lisa y llana, y no es correcto inferir que conlleva la afirmación de que fue el banco quien de manera arbitraria efectuó los cargos, pues implica la demostración de un hecho positivo por demás genérico y difícil de probar, ya que son las instituciones de crédito quienes, para seguridad de sus tarjetahabientes, deben conservar los registros y documentos a través de los cuales se cercioran que son ellos y no terceras personas quienes disponen del crédito previamente autorizado, considerando que, de conformidad con el artículo 77 de la Ley de Instituciones de Crédito, se encuentran obligadas a prestar seguridad a

sus cuentahabientes en la operación u operaciones que realicen, a fin de procurar brindarles una adecuada atención en ese servicio. Luego, si la institución de crédito demandada afirma que fue la parte actora quien dispuso del crédito utilizando los **medios electrónicos** autorizados, corresponde a dicha institución en un primer momento demostrar que el crédito se dispuso siguiendo los procedimientos autorizados y conforme a las políticas y normas de seguridad establecidas; por ejemplo, de ser el caso, vía telefónica mediante el número único de cliente y número confidencial de acceso al sistema de banca electrónica que sólo éste conoce, y de probarlo, quedará a cargo del tarjetahabiente la carga de demostrar que no fue él quien dispuso del crédito.

CUARTO TRIBUNAL COLEGIADO DEL OCTAVO CIRCUITO

Amparo directo 794/2007. Blanca Leticia Mondragón Cárdenas. 12 de junio de 2008. Unanimidad de votos. Ponente: Fernando Estrada Vásquez. Secretario: Pedro Guillermo Siller González Pico.

Registro No. 170349

Localización:
Novena Época
Instancia: Segunda Sala
Fuente: Semanario Judicial de la Federación y su Gaceta
XXVII, Febrero de 2008
Página: 530
Tesis: 2a./J. 24/2008
Jurisprudencia
Materia(s): Administrativa

DECLARACIÓN PRESENTADA A TRAVÉS DE MEDIOS ELECTRÓNICOS Y ACUSE DE RECIBO CON SELLO DIGITAL. LA CONSTANCIA IMPRESA O SU COPIA SIMPLE SON APTAS PARA ACREDITAR LA APLICACIÓN DE LOS PRECEPTOS LEGALES EN QUE AQUÉLLA SE SUSTENTÓ. De acuerdo con el artículo 31 del Código Fiscal de la Federación, los contribuyentes deben realizar pagos y presentar las declaraciones respectivas en documentos digitales a través de los **medios electrónicos** señalados por el Servicio de Administración Tributaria mediante reglas generales y este último, conforme al artículo 17-E del propio ordenamiento, por la misma vía remitirá el acuse de recibo que contenga el sello digital, consistente en la cadena de caracteres generada por la autoridad, la cual permita autenticar su contenido. De esa forma, si para cumplir con las indicadas obligaciones fiscales, por disposición legal, debe hacerse uso de una interconexión de redes informáticas, a través de la cual el contribuyente y las autoridades fiscales se transmiten información directamente desde computadoras, prescindiendo de constancias impresas, para valorar la información obtenida de dicha red, o sus copias simples, no debe acudirse a las

reglas aplicables en cuanto al valor probatorio de documentos impresos, sino a la regulación específica prevista en el artículo 210-A del Código Federal de Procedimientos Civiles, conforme al cual debe atenderse preponderantemente a la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si el contenido de la información relativa es atribuible a las personas obligadas y si está disponible para su ulterior consulta. Así, tratándose del cumplimiento de las obligaciones fiscales a través de **medios electrónicos**, el método por el cual se generan los documentos digitales está previsto en la ley y, además, el propio legislador y la autoridad administrativa, a través de reglas generales, han desarrollado la regulación que permite autenticar su autoría, de manera que su impresión o su copia simple son aptos para demostrar la aplicación de los preceptos legales que sirven de base a los diversos cálculos cuyo resultado se plasma en la declaración, siempre y cuando sea indudable que las correspondientes hipótesis normativas sustentan los resultados contenidos en ella.

Contradicción de tesis 261/2007-SS. Entre las sustentadas por el Tercer Tribunal Colegiado en Materia Administrativa del Primer Circuito y el Segundo Tribunal Colegiado en Materia Civil del Séptimo Circuito. 13 de febrero de 2008. Unanimidad de cuatro votos. Ausente: Sergio Salvador Aguirre Anguiano. Ponente: Mariano Azuela Güitrón. Secretario: Óscar F. Hernández Bautista.

Tesis de jurisprudencia 24/2008. Aprobada por la Segunda Sala de este Alto Tribunal, en sesión privada del trece de febrero de dos mil ocho.

Registro No. 171183

Localización:
Novena Época
Instancia: Segunda Sala
Fuente: Semanario Judicial de la Federación y su Gaceta
XXVI, Octubre de 2007
Página: 242
Tesis: 2a./J. 202/2007
Jurisprudencia
Materia(s): Administrativa

ESTADOS DE CUENTA INDIVIDUALES DE LOS TRABAJADORES. SU CERTIFICACIÓN POR PARTE DEL INSTITUTO MEXICANO DEL SEGURO SOCIAL TIENE VALOR PROBATORIO PLENO, POR LO QUE ES APTA PARA ACREDITAR LA RELACIÓN LABORAL ENTRE AQUÉLLOS Y EL PATRÓN. Los mencionados certificados, de conformidad con los artículos 3, 4 y 5, del Reglamento de la Ley del Seguro Social en Materia de Afiliación, Clasificación de Empresas, Recaudación y Fiscalización, independientemente de ser resultado de información presentada vía formato impreso o de aquella presentada a través de medios magnéticos, digitales, electrónicos, ópticos, magneto ópticos o de cualquier otra naturaleza (en donde se utilizó el número patronal de identificación **electrónica**, que hace las veces de sustituto de la **firma** autógrafa) tiene valor probatorio pleno, de conformidad con el artículo 46 de la Ley Federal de Procedimiento Contencioso Administrativo (equivalente al artícu-

lo 234, fracción I del Código Fiscal de la Federación), en relación con el diverso 63 del Código Fiscal de la Federación, aun cuando la parte patronal desconozca la relación laboral mediante su negativa lisa y llana. Por lo tanto, la certificación de los estados de cuenta individuales, es apta y suficiente para acreditar la relación laboral entre los trabajadores y el patrón, de manera que, no es necesario exigir el perfeccionamiento de ese tipo de constancias con la exhibición, por ejemplo, de los avisos de afiliación presentados por el patrón.

Contradicción de tesis 189/2007-SS. Entre las sustentadas por los Tribunales Colegiados en Materia Administrativa, Séptimo del Primer Circuito y Primero del Segundo Circuito. 10 de octubre de 2007. Cinco votos. Ponente: Margarita Beatriz Luna Ramos. Secretaria: Paula María García Villegas.

Tesis de jurisprudencia 202/2007. Aprobada por la Segunda Sala de este Alto Tribunal, en sesión privada del diecisiete de octubre de dos mil siete.

Registro No. 171270

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XXVI, Septiembre de 2007
Página: 2677
Tesis: I.15o.A.85 A
Tesis Aislada
Materia(s): Administrativa

TRANSMISIÓN TELEFÓNICA FACSIMILAR DE SOLICITUDES Y PROMOCIONES ANTE EL INSTITUTO MEXICANO DE LA PROPIEDAD INDUSTRIAL. EL ARTÍCULO 5o., ÚLTIMO PÁRRAFO, DEL REGLAMENTO DE LA LEY DE LA PROPIEDAD INDUSTRIAL QUE ADMITE ESA VÍA DE PRESENTACIÓN, NO VIOLA LOS PRINCIPIOS DE RESERVA DE LEY Y SUBORDINACIÓN JERÁRQUICA CONSAGRADOS EN EL NUMERAL 89, FRACCIÓN I, CONSTITUCIONAL. De la citada disposición reglamentaria se desprende que en las oficinas del Instituto Mexicano de la Propiedad Industrial pueden recibirse solicitudes o promociones por transmisión telefónica facsimilar, pero para que su presentación surta efectos jurídicos es necesario que al día hábil siguiente de haberse efectuado entreguen en la oficina respectiva del instituto el original de los escritos relativos y de sus anexos, acompañados del comprobante de pago de la tarifa que en su caso proceda y del acuse de recibo de la transmisión. Disposición que no rebasa la prevención establecida en los artículos 179, 180, 190 y 197 de la Ley de la Propiedad Industrial, y 69-C de la Ley Federal de Procedimiento Administrativo, relativa a que las citadas peticiones deberán presentarse por escrito, ya que esa vía simplifica y otorga un beneficio a los particulares, mientras que el vocablo "escrito" no es más que una reminiscencia de la tradición del derecho germano romanista, que impide que las solicitudes o promociones se realicen oralmente para otorgar seguridad jurídica a los peticionarios, pero que no significa que aquéllas no puedan presentarse por las

distintas vías de comunicación que la tecnología facilite, tales como correo ordinario o certificado, telégrafo, transmisión facsimilar, correo electrónico (e-mail), internet, mensajes instantáneos (win-pop), entre otros más, siempre y cuando los ordenamientos jurídicos así lo autoricen; luego, la mencionada disposición no altera la literalidad o forma escrita de las peticiones, sino sólo se refiere a una forma de envío y recepción de aquéllas, por lo que no viola los principios de reserva de ley y subordinación jerárquica consagrados en el numeral 89, fracción I, constitucional.

DÉCIMO QUINTO TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL PRIMER CIRCUITO

Amparo en revisión 380/2006. Colegio Anglo Americano de Coyoacán, S.A. de C.V. 27 de septiembre de 2006. Unanimidad de votos. Ponente: Armando Cortés Galván. Secretario: Edgar Genaro Cedillo Velázquez.

Registro No. 171467

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XXVI, Septiembre de 2007
Página: 2528
Tesis: I.4o.A.596 A
Tesis Aislada
Materia(s): Administrativa

ESTADOS DE CUENTA INDIVIDUALES DE LOS TRABAJADORES AFILIADOS AL INSTITUTO MEXICANO DEL SEGURO SOCIAL. PARA DETERMINAR SU VALOR PROBATORIO DEBEN EVALUARSE, ENTRE OTROS ASPECTOS, LOS REQUISITOS A QUE SE REFIERE EL SEGUNDO PÁRRAFO DEL ARTÍCULO 210-A DEL CÓDIGO FEDERAL DE PROCEDIMIENTOS CIVILES, APLICADO SUPLETORIAMENTE, EN CUANTO A LA INFORMACIÓN GENERADA QUE CONSTE EN MEDIOS ELECTRÓNICOS, ÓPTICOS O EN CUALQUIER OTRA TECNOLOGÍA. De los artículos 3, 4, 5 y 14 del Reglamento del Seguro Social en Materia de Afiliación, Clasificación de Empresas, Recaudación y Fiscalización se advierte, por una parte, que el patrón debe inscribir a sus trabajadores en el Instituto Mexicano del Seguro Social y comunicarle sus modificaciones salariales y bajas, ya sea presentando los formatos impresos autorizados, o bien, a través de medios magnéticos, digitales, electrónicos, ópticos, magneto ópticos o de cualquier otra naturaleza, debiendo utilizar, en este caso, el número patronal de identificación electrónica que le proporciona el citado instituto, como llave pública de sus sistemas criptográficos, con los mismos efectos que las leyes otorgan a los

documentos firmados autógrafamente y, por otra, que el aludido instituto podrá conservar en dichos medios la información presentada en formatos impresos. Por tanto, para que los estados de cuenta individuales, que son impresiones o registros de la información que obra en dispositivos magnéticos o electrónicos, tengan suficiente valor probatorio para acreditar la relación laboral entre el patrón y los trabajadores a que se refieren, es necesario evaluar, entre otros aspectos, los requisitos que exige el segundo párrafo del artículo 210-A del Código Federal de Procedimientos Civiles, aplicado supletoriamente, que son, en primer lugar, la fiabilidad del método en que se encuentre o almacene la información, es decir, donde se genere, comunique, reciba o archive; en segundo, de ser posible, que se atribuya el contenido de la información al patrón; y en tercero, que ésta sea accesible para su posterior consulta. Por consiguiente, debe acreditarse que efectivamente dicha información fue aportada por el patrón, ya sea conservando los formatos impresos autorizados o su resguardo en medios magnéticos o electrónicos, tal como lo señala el artículo 4 del citado reglamento, o bien, corroborar con el número patronal de identificación electrónica correspondiente (equivalente a la firma electrónica) que la información enviada por medios electrónicos fue efectivamente aportada por el patrón, pues en términos del invocado artículo 5, sólo los trámites en que se utilice ese número producirá los mismos efectos que los documentos firmados autógrafamente.

CUARTO TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL PRIMER CIRCUITO

Revisión fiscal 70/2007. Titular de la Jefatura de Servicios Jurídicos de la Delegación Sur del Distrito Federal del Instituto Mexicano del Seguro Social. 16 de mayo de 2007. Unanimidad de votos. Ponente: Jean Claude Tron Petit. Secretaria: Sandra Ibarra Valdez.

Registro No. 171757

Localización:
Novena Época
Instancia: Segunda Sala
Fuente: Semanario Judicial de la Federación y su Gaceta
XXVI, Agosto de 2007
Página: 638
Tesis: 2a. XCVII/2007
Tesis Aislada
Materia(s): Constitucional, Administrativo

FIRMA ELECTRÓNICA AVANZADA. EL HECHO DE QUE EL CÓDIGO FISCAL DE LA FEDERACIÓN NO ESTABLEZCA SU DEFINICIÓN NO VIOLA LA GARANTÍA DE LEGALIDAD. El artículo 17-D del Código Fiscal de la Federación establece que cuando las disposiciones fiscales obliguen a pre-

sentar documentos; éstos deberán ser digitales y contener una firma electrónica avanzada del autor, salvo los casos previstos en el propio precepto, y que para esos efectos deberá contarse con un certificado que confirme el vínculo entre un firmante y los datos de creación de una "firma electrónica avanzada", expedido por el Servicio de Administración Tributaria cuando se trate de personas morales y por un prestador de servicios de certificación autorizado por el Banco de México cuando se trate de personas físicas, mediante el cumplimiento de ciertos requisitos, entre ellos, el de la comparecencia del interesado o de su apoderado o representante legal en caso de personas morales, con la finalidad de acreditar su identidad. De lo anterior se concluye que no se viola la garantía de legalidad contenida en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, por el hecho de que el Código Fiscal de la Federación no establezca una definición particular de lo que debe entenderse por "firma electrónica avanzada", pues del indicado numeral 17-D se advierte el propósito perseguido con ésta, el cual, además de identificar al emisor de un mensaje como su autor legítimo, como si se tratara de una firma autógrafa, garantiza la integridad del documento produciendo los mismos efectos que las leyes otorgan a los documentos con firma autógrafa, teniendo el mismo valor probatorio; lo anterior, en razón de que la firma electrónica avanzada está vinculada a un certificado expedido por una autoridad, en este caso, por el Servicio de Administración Tributaria, en el que constan los datos del registro respectivo.

Amparo en revisión 262/2007. Radio XEAGS, S.A. de C.V. 13 de junio de 2007. Cinco votos. Ponente: Sergio Salvador Aguirre Anguiano. Secretario: Óscar Zamudio Pérez.

Registro No. 172004

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XXVI, Julio de 2007
Página: 2557
Tesis: I.8o.A.9 K
Tesis Aislada
Materia(s): Común

INTERÉS JURÍDICO EN EL AMPARO. LO TIENE EL QUEJOSO QUE RECLAMA DE LA PROCURADURÍA FEDERAL DEL CONSUMIDOR LA DIFUSIÓN EN MEDIOS ELECTRÓNICOS DE INFORMACIÓN DE SUS ESTABLECIMIENTOS QUE PERJUDIQUE SU IMAGEN COMERCIAL Y REPUTACIÓN. La imagen o reputación es un bien jurídico cuyo disfrute por parte de las personas está reconocido como un derecho subjetivo por el ordenamiento jurídico mexicano, entonces, es claro que asiste interés jurídico al quejoso que reclama de la Procuraduría Federal del Consumidor la difusión en medios electrónicos de información relacionada con la actividad comercial de sus establecimientos que perjudique su imagen comercial y reputación.

OCTAVO TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL PRIMER CIRCUITO

Amparo en revisión 39/2007. Servicio Lomas de Vista Hermosa, S.A. de C.V. y otras. 16 de febrero de 2007. Unanimidad de votos. Ponente: Adriana Leticia Campuzano Gallegos. Secretario: Sergio Padilla Terán.

Registro No. 172243

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XXV, Junio de 2007
Página: 1044
Tesis: XIX.2o.A.C.49 A
Tesis Aislada
Materia(s): Administrativa

COMPETENCIA PARA CONOCER DE UN JUICIO DE AMPARO PROMOVIDO CONTRA UNA LEY FISCAL FEDERAL CON MOTIVO DE SU PRIMER ACTO DE APLICACIÓN, CONSISTENTE EN LA DECLARACIÓN Y PAGO DE LA CONTRIBUCIÓN POR MEDIOS ELECTRÓNICOS. ANTE LA FALTA DE CERTEZA DEL DOMICILIO FISCAL DEL CONTRIBUYENTE, SE SURTE A FAVOR DEL JUEZ DE DISTRITO QUE PREVINO. Si con motivo de la presentación de una demanda de amparo contra una ley fiscal federal promovida respecto de su primer acto de aplicación, consistente en la declaración y pago de la contribución por medios electrónicos, no se tiene certeza del domicilio fiscal de la contribuyente persona moral quejosa, como referente para establecer la circunscripción territorial de la unidad administrativa del Servicio de Administración Tributaria al que se encuentren dirigidos la declaración y el pago mencionados, y así poder determinar la competencia legal del Juez de Distrito con jurisdicción en aquel domicilio (fiscal), tomando en consideración que en ningún asunto debe dejarse de resolver en términos del artículo 17 de la Constitución Política de los Estados Unidos Mexicanos y en atención al criterio establecido en la jurisprudencia 2a./J. 146/2002 emitida por la Segunda Sala de la Suprema Corte de Justicia de la Nación, publicada en el Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XVII, enero de 2003, página 324, de rubro: "COMPETENCIA PARA CONOCER DE UN JUICIO DE AMPARO PROMOVIDO CONTRA UNA LEY FISCAL FEDERAL CON MOTIVO DE SU PRIMER ACTO DE APLICACIÓN, CONSISTENTE EN LA DECLARACIÓN Y PAGO DE LA CONTRIBUCIÓN POR MEDIOS ELECTRÓNICOS. CORRESPONDE AL JUEZ DE DISTRITO QUE EJERCE JURISDICCIÓN EN EL LUGAR DEL DOMICILIO FISCAL DEL CONTRIBUYENTE.", resulta inconcuso que es el Juez de Distrito que previno en el conocimiento del asunto el competente para conocer de la citada demanda de amparo, sin perjuicio de que

durante el trámite del juicio se pueda insistir en la incompetencia, una vez que se obtenga la certeza del domicilio.

SEGUNDO TRIBUNAL COLEGIADO EN MATERIAS ADMINISTRATIVA Y CIVIL DEL DÉCIMO NOVENO CIRCUITO

Competencia 1/2006. Suscitada entre el Juzgado Noveno de Distrito en el Estado de Tamaulipas, con residencia en Tampico y el Juzgado Segundo de Distrito en Materia Administrativa del Estado de Nuevo León, con residencia en Monterrey. 31 de mayo de 2006. Unanimidad de votos. Ponente: José Luis Mendoza Pérez. Secretario: Gerónimo Luis Ramos García.

Registro No. 172698

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XXV, Abril de 2007
Página: 1489
Tesis: II.1o.A. J/19
Jurisprudencia
Materia(s): Administrativa

PRUEBAS EN EL JUICIO DE NULIDAD. LA CERTIFICACIÓN DE LOS ESTADOS DE CUENTA INDIVIDUALES DE LOS TRABAJADORES POR PARTE DEL INSTITUTO MEXICANO DEL SEGURO SOCIAL TIENE VALOR PROBATORIO PLENO Y, POR TANTO, ES APTA PARA ACREDITAR LA RELACIÓN LABORAL CUANDO SE CONTROVIERTE LA LEGALIDAD DE LAS CÉDULAS DE LIQUIDACIÓN DE CUOTAS OBRERO PATRONALES. La certificación de los estados de cuenta individuales de los trabajadores presentada por el Instituto Mexicano del Seguro Social en el juicio de nulidad en que se controvierte la legalidad de las cédulas de liquidación de cuotas obrero-patronales, tiene valor probatorio pleno en términos del artículo 234, fracción I, del Código Fiscal de la Federación; y por tanto, es apta para acreditar la relación laboral entre aquéllos y el patrón. Lo anterior, en virtud de haber sido expedida con base en las facultades derivadas de los artículos 3, 4 y 5 del Reglamento de la Ley del Seguro Social en Materia de Afiliación, Clasificación de Empresas, Recaudación y Fiscalización, de los cuales se advierte que el mencionado organismo conservará la información presentada por los patrones y demás sujetos obligados, ya sea en formatos impresos o a través de medios magnéticos, digitales, electrónicos, ópticos, magneto ópticos o de cualquier otra naturaleza, de los cuales podrá expedir certificaciones que producirán idénticos efectos a aquellos que las leyes otorgan a los documentos firmados autógrafamente. En consecuencia, si la actora niega lisa y llanamente la relación laboral y el instituto

demandado exhibe la certificación de los estados de cuenta individuales correspondientes, dicha negativa queda desvirtuada, por lo que es innecesario exigir el perfeccionamiento de ese tipo de constancias, con la exhibición, por ejemplo, de los avisos de afiliación presentados por el patrón.

PRIMER TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL SEGUNDO CIRCUITO

Amparo directo 340/2006. Distribuidora Malsa, S.A. de C.V. 30 de noviembre de 2006. Unanimidad de votos. Ponente: Eugenio Reyes Contreras. Secretaria: Olga Lidia Treviño Berrones.

Amparo directo 406/2006. Car Lop de México, S.A. 25 de enero de 2007. Unanimidad de votos. Ponente: Rodolfo Castro León. Secretario: Luis Miguel Domínguez López.

Amparo directo 183/2006. Industrial Aceitera, S.A. de C.V. 1o. de febrero de 2007. Unanimidad de votos. Ponente: José Guillermo Zárate Granados. Secretario: Hugo Mundo Valenzuela.

Registro No. 173071

Localización:
Novena Época
Instancia: Primera Sala
Fuente: Semanario Judicial de la Federación y su Gaceta
XXV, Marzo de 2007
Página: 30
Tesis: 1a./J. 27/2007
Jurisprudencia
Materia(s): Común

CONSTANCIAS ENVIADAS POR FAX ENTRE LOS ÓRGANOS DEL PODER JUDICIAL DE LA FEDERACIÓN. SI ESTÁ CERTIFICADA LA HORA Y FECHA DE SU RECEPCIÓN, ASÍ COMO EL ÓRGANO QUE LAS REMITE POR EL SECRETARIO DE ACUERDOS DEL TRIBUNAL JUDICIAL QUE LAS RECIBE, TIENEN PLENO VALOR PROBATORIO. El artículo 210-A del Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo en términos de lo previsto en el diverso artículo 2o. de esta Ley, reconoce como medios de prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología, y establece que su fuerza probatoria está sujeta a la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta. Ahora bien, entre los medios de comunicación electrónica se encuentra el denominado fax, que es un medio de transmisión de datos que emplea la red telefónica, por el cual se envía un documento que se reci-

be por el destinatario en copia fotostática; de ahí que las constancias transmitidas por este medio, entre los órganos del Poder Judicial de la Federación, si están certificadas por el secretario de Acuerdos del tribunal judicial al que se transmite el mensaje, sobre la hora y fecha de recepción del fax y la persona del órgano jurisdiccional federal que lo remitió, tienen pleno valor probatorio, por ser confiable el medio en que fueron comunicadas dichas constancias, ya que tiene un grado de seguridad similar al de la documentación consignada en papel, además de que es identificable la persona a quien se atribuye su contenido y pueden verificarse tanto el origen de la documentación como su texto; pues en la actualidad los citados órganos se encuentran comunicados electrónicamente, por distintos medios, lo que permite corroborar los datos del fax recibido.

Reclamación 180/2000. Bardomiano Olvera Morán, su sucesión. 24 de enero de 2001. Unanimidad de cuatro votos. Ausente: Olga Sánchez Cordero de García Villegas. Ponente: Olga Sánchez Cordero de García Villegas; en su ausencia hizo suyo el asunto Juan N. Silva Meza. Secretario: José Luis Vázquez Camacho.

Incidente de inejecución 33/2006. Johnson Matthey de México, S.A. de C.V. 8 de febrero de 2006. Cinco votos. Ponente: José Ramón Cossío Díaz. Secretario: Roberto Lara Chagoyán.

Incidente de inejecución 12/2006. Sergio Efrén Rebolledo Hernández. 1o. de marzo de 2006. Cinco votos. Ponente: Olga Sánchez Cordero de García Villegas. Secretaria: Mariana Mureddu Gilabert.

Incidente de inejecución 113/2006. Ernesto Javier González González. 19 de abril de 2006. Cinco votos. Ponente: Olga Sánchez Cordero de García Villegas. Secretaria: Mariana Mureddu Gilabert.

Incidente de inejecución 534/2006. Luis Ángel Gallardo Rubio. 29 de noviembre de 2006. Cinco votos. Ponente: José de Jesús Gudiño Pelayo. Secretario: Jesús Antonio Sepúlveda Castro.

Tesis de jurisprudencia 27/2007. Aprobada por la Primera Sala de este Alto Tribunal, en sesión de veintiocho de febrero de dos mil siete.

Registro No. 173175

Localización:
Novena Época
Instancia: Segunda Sala
Fuente: Semanario Judicial de la Federación y su Gaceta
XXV, Febrero de 2007
Página: 736
Tesis: 2a./J. 15/2007
Jurisprudencia
Materia(s): laboral

SEGURO SOCIAL. EL VALOR PROBATORIO DE LA PRUEBA DE INSPECCIÓN SOBRE LA CÉDULA BASE DE DATOS COMPUTARIZADA DE LOS TRABAJADORES PARA ACREDITAR SU ANTIGÜEDAD GENÉRICA, QUEDA AL PRUDENTE ARBITRIO DE LA AUTORIDAD JURISDICCIONAL. La cédula base de datos forma parte de un sistema compu-

tarizado que el Instituto Mexicano del Seguro Social emplea para registrar las contrataciones del trabajador, su tiempo de servicios, sus licencias o incapacidades, sus ausencias y, en general, su historial como empleado en diversos cargos, de manera que si en el juicio se ofrece la prueba de inspección sobre dicha cédula, queda al prudente arbitrio de la autoridad jurisdiccional su valoración, no sólo de su contenido, sino también de su autenticidad (pues incluso puede acontecer que también por medios electrónicos se capture la firma del trabajador); por tanto, su alcance probatorio dependerá de las objeciones de las partes y de los elementos de prueba que puedan avalar, desvirtuar o reforzar la información que sirvió de base para almacenar el historial de aquél, como pueden ser los documentos que deba conservar el patrón en términos del artículo 804 de la Ley Federal del Trabajo o algún otro medio probatorio. Por otra parte, si el elemento sobre el que versa la prueba de inspección no es objetado, ello no tiene como consecuencia que ésta tenga valor probatorio pleno, aunque constituirá un indicio cuyo valor será determinado por la autoridad al apreciarlo, en relación con las demás pruebas y atendiendo a su contenido, del que pueda desprenderse con claridad la información sobre los hechos que pretende probar la oferente.

Contradicción de tesis 222/2006-SS. Entre las sustentadas por el Segundo Tribunal Colegiado en Materias Penal y de Trabajo del Décimo Noveno Circuito, el entonces Primer Tribunal Colegiado del Décimo Noveno Circuito, ahora Primer Tribunal Colegiado en Materias Penal y de Trabajo del citado circuito y el Tribunal Colegiado del Décimo Séptimo Circuito. 7 de febrero de 2007. Cinco votos. Ponente: Margarita Beatriz Luna Ramos. Secretaria: Estela Jasso Figueroa.

Tesis de jurisprudencia 15/2007. Aprobada por la Segunda Sala de este Alto Tribunal, en sesión privada del catorce de febrero de dos mil siete.

Registro No. 173930

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XXIV, Noviembre de 2006
Página: 1039
Tesis: VIII.5o.1 A
Tesis Aislada
Materia(s): Administrativa

DERECHO DE PETICIÓN. SU EJERCICIO A TRAVÉS DE INTERNET ESTÁ TUTELADO POR EL ARTÍCULO 8o. CONSTITUCIONAL, SIEMPRE QUE LA AUTORIDAD A QUIEN SE FORMULE LA PETICIÓN PREVEA INSTITUCIONALMENTE ESA OPCIÓN Y SE COMPRUEBE QUE LA SOLICITUD ELECTRÓNICA FUE ENVIADA. Del artículo 8o. de la Constitución Política de los Estados Unidos Mexicanos se advierte que los funcionarios y empleados públicos están obligados a respetar el ejercicio del derecho de petición, siempre que se formule por escrito, de manera pacífica y respetuosa, el cual por seguridad jurídica está condicionado a que la solicitud se haga median-

te escrito en sentido estricto, pues de no ser así la autoridad no estaría obligada a dar contestación; sin embargo, el rápido avance de los medios electrónicos como el internet, constituye en los últimos años, un sistema mundial de diseminación y obtención de información en diversos ámbitos, incluso, del gobierno, ya que en la actualidad en el país diversas autoridades han institucionalizado la posibilidad legal de que algunas gestiones los ciudadanos las puedan realizar a través de ese medio, en pro de la eficiencia y el valor del tiempo, lo que evidentemente no previó el Constituyente en la época en que redactó el referido texto constitucional, pues su creación se justificó únicamente en evitar la venganza privada y dar paso al régimen de autoridad en la solución de los conflictos, obvio, porque en aquel momento no podía presagiarse el aludido avance tecnológico. En esa virtud, de un análisis histórico progresivo, histórico teleológico y lógico del numeral 8o. de la Carta Magna, se obtiene que a fin de salvaguardar la garantía ahí contenida, el derecho de petición no sólo puede ejercerse por escrito, sino también a través de documentos digitales, como serían los enviados por internet, en cuyo caso la autoridad a quien se dirija estará obligada a dar respuesta a lo peticionado, siempre que institucionalmente prevea esa opción dentro de la normatividad que regula su actuación y se compruebe de manera fehaciente que la solicitud electrónica fue enviada.

QUINTO TRIBUNAL COLEGIADO DEL OCTAVO CIRCUITO

Amparo en revisión 182/2006. Wyatt Hidalgo Vegetables, S.A. de C.V. 31 de agosto de 2006. Unanimidad de votos. Ponente: Hugo Alejandro Bermúdez Manrique. Secretaria: Dulce Gwendolyne Sánchez Elizondo.

Registro No. 174038

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XXIV, Octubre de 2006
Página: 1496
Tesis: XXI.2o.P.A.32 K
Tesis Aislada
Materia(s): Común

PRUEBA DE INSPECCIÓN. DEBE DESECHARSE CUANDO LOS PUNTOS PROPUESTOS PARA SU DESAHOGO PUEDAN SER COMPROBADOS A TRAVÉS DE LA DOCUMENTAL, ENTENDIDA COMO LA INFORMACIÓN GENERADA O COMUNICADA QUE CONSTE EN MEDIOS ELECTRÓNICOS O EN CUALQUIER OTRA TECNOLOGÍA, QUE PUEDE SER REPRODUCIDA, NO SOLAMENTE EN PAPEL SINO TAMBIÉN EN ALGÚN DISQUETE O DISCO ÓPTICO. La base de datos

existente en el sistema de cómputo de alguna dependencia oficial, constituye, en sentido amplio, una documental, atendiendo a que el artículo 210-A del Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo, por disposición de su artículo 2o., segundo párrafo, señala que se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología. En ese contexto, resulta correcto desechar la prueba de inspección cuando los puntos materia de su desahogo tienen como propósito demostrar hechos susceptibles de ser comprobados a través de la prueba documental, entendida ésta como la información que puede ser reproducida, no exclusivamente en papel, sino también en algún disquete o disco óptico, en el cual se logre grabar la información solicitada por el quejoso para efectos de exhibirlos como prueba en el juicio de amparo, de conformidad con el artículo 152 de la Ley de Amparo.

SEGUNDO TRIBUNAL COLEGIADO EN MATERIAS PENAL Y ADMINISTRATIVA DEL VIGÉSIMO PRIMER CIRCUITO

Queja 39/2006. Inversiones Raf, S.A. de C.V. 29 de junio de 2006. Unanimidad de votos. Ponente: Martiniano Bautista Espinosa. Secretario: Mario Alejandro Nogueda Radilla.

Registro No. 176863

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XXII, Octubre de 2005
Página: 2471
Tesis: I.7o.A.410 A
Tesis Aislada
Materia(s): Administrativa

RECIBO DE PAGO ELECTRÓNICO. VALOR PROBATORIO DE LA DOCUMENTAL IMPRESA CORRESPONDIENTE. El artículo 210-A del Código Federal de Procedimientos Civiles reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología, condicionando su valor a la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada, y en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta. De esta manera, el legislador, ante los avances de la tecnología, contempló la posibilidad de que en los juicios seguidos ante los tribunales se exhibieran y valoraran elementos probatorios distintos a los convencionales, tales como testimoniales, periciales, documentos, entre otros; consecuentemente, la información generada por la vía electrónica (internet, comercio electrónico y

análogos), tiene un respaldo legislativo, a efecto de crear seguridad jurídica en los usuarios de tales servicios. Así, la valoración del material probatorio en comento no debe sujetarse a las reglas convencionales de justipreciación, sino al apartado específico del numeral en estudio; de esta manera, un recibo de pago de impuestos realizado electrónicamente no carece, por tal circunstancia, de eficacia probatoria, ya que lo que se habrá de tomar en consideración, en su momento, son los datos que corroboren su fiabilidad, como son el código de captura y sello digital, y no elementos ajenos a la naturaleza de los documentos electrónicos, tales como si se trata del original de una impresión.

SÉPTIMO TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL PRIMER CIRCUITO

Amparo en revisión 328/2005. María Alejandra Carrillo Gómez. 24 de agosto de 2005. Unanimidad de votos. Ponente: F. Javier Mijangos Navarro. Secretario: Carlos Alfredo Soto Morales.

Registro No. 177866

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XXII, Julio de 2005
Página: 1498
Tesis: XV.4o.4 L
Tesis Aislada
Materia(s): laboral

PRUEBAS DE AUDIO Y VIDEOGRABACIÓN EN EL JUICIO LABORAL. ATENDIENDO A SU NATURALEZA, SU DESECHAMIENTO POR NO ACOMPAÑARSE EN SU OFRECIMIENTO LOS ELEMENTOS NECESARIOS PARA SU DESAHOGO CONSTITUYE UNA VIOLACIÓN A LAS LEYES DEL PROCEDIMIENTO. Si bien es cierto que el artículo 780 de la Ley Federal del Trabajo establece la obligación de ofrecer las pruebas acompañadas de todos los elementos necesarios para su desahogo, también lo es que tratándose de la prueba consistente en casetes, uno de audio y otro de video, resulta improcedente que la autoridad laboral la deseche con base en que al ser ofertada no se exhibieron los instrumentos electrónicos necesarios para su práctica, ya que, en todo caso, debe conminar a su oferente para que el día y hora que fije para su desahogo, allegue los medios con los que pueda llevarse a cabo su reproducción, pues dada su naturaleza, resultaría ilógico pretender que al escrito de ofrecimiento deban acompañarse, además de los respectivos casetes, un audiorreproductor, una videorreproductora y un aparato de televisión, mecanismos que estarían en poder de la responsable durante todo el tiempo que transcurra hasta su diligenciación, lo

cual sería oneroso para el oferente; consecuentemente, si la prueba es desechada, ello constituye una violación a las reglas del procedimiento que afecta las defensas del oferente y trasciende al resultado del fallo.

CUARTO TRIBUNAL COLEGIADO DEL DÉCIMO QUINTO CIRCUITO

Amparo directo 132/2005. Mario Gutiérrez Tapia y otros. 26 de mayo de 2005. Unanimidad de votos. Ponente: Inosencio del Prado Morales. Secretario: Herminio Armando Domínguez Zúñiga.

Registro No. 178929

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XXI, Marzo de 2005
Página: 1205
Tesis: II.1o.A.21 K
Tesis Aislada
Materia(s): Común

PRUEBAS EN EL AMPARO. PARA EL DESAHOGO DE LAS RELACIONADAS CON MEDIOS ELÉCTRICOS O ELECTRÓNICOS NO ES ADMISIBLE LA IMPOSICIÓN DE CARGA ESPECÍFICA A SU OFERENTE PARA VALORAR SU ADMISIBILIDAD. Además de los medios clásicos o tradicionales de prueba, la rápida evolución de la técnica ha creado nuevos métodos probatorios antaño insospechados que, en parte, debido a su constante innovación y dadas las particularidades que cada uno de ellos pueden presentar, no han sido regulados en detalle por el legislador, pero la posibilidad de aportarlos como elementos de convicción está prevista tanto en el artículo 150 de la Ley de Amparo como en los artículos 93, 188, 189, 210-A y 217 del Código Federal de Procedimientos Civiles supletorio de aquélla. En razón de ello, el juzgador deberá determinar en cada caso concreto y según sus propias características, la forma más conveniente para el desahogo y valoración de tales medios de convicción; sin embargo, el legislador en ningún caso previó que las peculiaridades de tales probanzas tuvieran como efecto imponer cargas específicas a los quejosos, como sería el caso de solicitar a éstos que aportaran algún tipo de aparato (como televisión o videocasetera), a fin de que se valorara la admisibilidad de su prueba, ya que no es posible tener la certeza de que los quejosos cuenten con la posibilidad real y material de aportar tales aparatos eléctricos o electrónicos, y dado que el juicio de garantías constituye una defensa del gobernado frente a actos arbitrarios de la autoridad, no resulta aceptable que su acceso se haga depender de la posibilidad de disponer de determinados bienes materiales. Por ello, se estima que la imposición a los quejosos de tal carga afecta el derecho a probar y, por ello, implica violación a las leyes del procedimiento.

PRIMER TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL SEGUNDO CIRCUITO

Amparo en revisión 480/2004. Sebastián Pallares Robles y otros. 25 de noviembre de 2004. Unanimidad de votos. Ponente: Salvador Mondragón Reyes. Secretaria: Sonia Rojas Castro.

Registro No. 180113

Localización:
Novena Época
Instancia: Segunda Sala
Fuente: Semanario Judicial de la Federación y su Gaceta
XX, Noviembre de 2004
Página: 129
Tesis: 2a. XCIV/2004
Tesis Aislada
Materia(s): Constitucional, Administrativa

PAGO DE CONTRIBUCIONES POR MEDIOS ELECTRÓNICOS. LOS ARTÍCULOS 20, SÉPTIMO PÁRRAFO Y 31, SEGUNDO PÁRRAFO, DEL CÓDIGO FISCAL DE LA FEDERACIÓN QUE LO PREVÉN, NO INFRINGEN EL ARTÍCULO 28 DE LA CONSTITUCIÓN FEDERAL (LEGISLACIÓN VIGENTE EN 2002). El hecho de que los mencionados preceptos establezcan que el pago de las contribuciones en moneda nacional se efectúe mediante transferencia electrónica de fondos a favor de la Tesorería de la Federación, de conformidad con las reglas de carácter general que señale la Secretaría de Hacienda y Crédito Público, no infringen el artículo 28 de la Constitución Política de los Estados Unidos Mexicanos, pues el pago así realizado no demerita la estabilidad del poder adquisitivo de la moneda nacional que el referido precepto constitucional encomienda al Banco de México, ya que dicha transferencia se efectúa precisamente en esa moneda, según el primer párrafo del artículo 20 del Código Fiscal de la Federación. Además, la indicada transferencia electrónica de fondos sólo constituye uno de los medios de pago de las contribuciones, cuyo establecimiento se hizo con el fin de simplificar y reforzar los procedimientos administrativos a través de los cuales los contribuyentes cumplen sus obligaciones y ejercen sus derechos, aprovechando los avances tecnológicos, sin que la autoridad pierda la información ni el control.

Amparo en revisión 470/2004. De Silva y Zamora, S.C. 1o. de octubre de 2004. Unanimidad de cuatro votos. Ausente: Margarita Beatriz Luna Ramos. Ponente: Genaro David Góngora Pimentel. Secretaria: Blanca Lobo Domínguez.

Registro No. 180341

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito

Fuente: Semanario Judicial de la Federación y su Gaceta
XX, Octubre de 2004
Página: 2352
Tesis: IV.3o.A.16 A
Tesis Aislada
Materia(s): Administrativa

IMPUESTO SUSTITUTIVO DEL CRÉDITO AL SALARIO. LA COPIA CERTIFICADA POR NOTARIO PÚBLICO DE LA IMPRESIÓN DE LA CONSTANCIA DE RECEPCIÓN DEL PAGO PROVISIONAL DEL IMPUESTO DE REFERENCIA OBTENIDA DE INTERNET, ES IDÓNEA PARA TENER POR DEMOSTRADO EL ACTO DE APLICACIÓN DE LA NORMA QUE LO ESTATUYE. El artículo 31 del Código Fiscal de la Federación permite que los contribuyentes obligados a presentar pagos provisionales mensuales, declaraciones o avisos previstos en las disposiciones fiscales, realicen sus trámites administrativos a través de **medios electrónicos**, en los casos y reuniendo los requisitos que establezca la Secretaría de Hacienda y Crédito Público, mediante reglas de carácter general. Por tanto, la copia certificada aportada al juicio de amparo, con el fin de acreditar el pago provisional del impuesto sustitutivo del crédito al salario, así como el consecuente acto de aplicación del numeral que estatuye dicho impuesto, en que se asienta por el notario público que constituye "una copia fiel y correcta sacada de su copia de internet que tuvo a la vista", debe considerarse como copia certificada sacada del documento auténtico tipo copia emitido por el sistema de internet vía impresión del propio particular, debido a que ésta constituye la naturaleza inherente a la impresión que se obtiene de las constancias de recepción de declaraciones y pagos provisionales expedidas por la red electrónica de la Secretaría de Hacienda y Crédito Público, que constituye el único documento que puede obtener quien opta por realizar su pago de esa forma legalmente autorizada, cuya autenticidad no se encuentra asociada a quién, con qué y en qué tipo de papel se imprime la constancia de recepción de la declaración efectuada vía internet, sino a los datos inherentes a la cadena original y al sello digital que en ellos se asienta a efecto de validar la operación efectuada. Entonces, si acorde con el artículo 203 del Código Federal de Procedimientos Civiles, de aplicación supletoria a la materia de amparo: "El documento proveniente de un tercero sólo prueba a favor de la parte que quiere beneficiarse con él y contra su colitigante cuando éste no lo objeta ..."; por consiguiente, al no haber sido tal documento objetado oportunamente por las autoridades hacendarias, no es posible poner en duda su autenticidad y contenido, por lo que resulta idóneo para acreditar el acto de aplicación del impuesto reclamado en el juicio de garantías.

TERCER TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL CUARTO CIRCUITO

Amparo en revisión 153/2004. Villa Tours, S.A. de C.V. 29 de abril de 2004. Unanimidad de votos. Ponente: Jorge Meza Pérez. Secretaria: Marina Chapa Cantú.

Registro No. 180608

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XX, Septiembre de 2004
Página: 1790
Tesis: VII.2o.C.5 A
Tesis Aislada
Materia(s): Administrativa

INTERÉS JURÍDICO DEL CONTRIBUYENTE. PARA ACREDITARLO EN EL AMPARO ES SUFICIENTE LA COPIA FOTOSTÁTICA SIMPLE DEL ACUSE DE RECIBO OBTENIDO DE LA RED DE INTERNET, AL CUMPLIRSE CON LAS OBLIGACIONES FISCALES A TRAVÉS DE ESA VÍA. De lo dispuesto por el artículo 31 del Código Fiscal de la Federación, y de la regla número 2.14.1 de la Resolución Miscelánea Fiscal para 2002, se concluye que al tener el contribuyente la posibilidad de rendir declaraciones vía internet, la copia fotostática simple del acuse de recibo obtenida mediante esa vía, es suficiente para acreditar su interés jurídico en el amparo promovido contra la inconstitucionalidad de los preceptos legales que regulan dicha materia, toda vez que la constancia de referencia es el único documento que puede obtener al realizar su pago de esa forma, siendo el contenido de la misma lo que interesa, pues al utilizarse los medios electrónicos para el cumplimiento de las obligaciones fiscales, la información relativa sólo puede enviarse a través de documentos digitales, entendiéndose por éstos, aquellos mensajes de datos que contienen información o escritura generada, enviada, recibida o archivada por medios de dicha índole, ópticos o de cualquier otra tecnología y, por tanto, el único medio previsto para autentificar y acreditar que dichos documentos fueron recibidos por la autoridad debida es el acuse de recibo enviado por la misma vía con el sello digital correspondiente, a través del cual se identifica a la dependencia que recibió el documento, sustituyendo a la firma autógrafa y produciendo los mismos efectos que las leyes otorgan a los documentos respectivos, teniendo el mismo valor probatorio, según lo establece la diversa regla general 2.16 de la resolución multicitada, el cual se materializa a través de la cadena de caracteres (conjunto de letras, números y símbolos) asignada por el banco o el Servicio de Administración Tributaria al presentarse las declaraciones o pagos, según se trate, a través de un documento digital. Por ende, ni aun su primera impresión podría refutarse como original, sino únicamente como una reproducción de la información proporcionada por el contribuyente en la dirección electrónica de las instituciones de crédito autorizadas, así como de los de identificación de la operación realizada a través de ese medio electrónico y mientras no sean objetadas por las autoridades hacendarias, no es posible, por razones de seguridad jurídica, poner en duda su autenticidad y contenido. Consecuentemente, se colige, que al existir regulación específica sobre la manera de cumplir con las obligaciones fiscales, no es válido aplicar las normas que rigen en materias de naturaleza diversa, en las cuales a las copias fotostáticas

simples se les otorga el carácter de mero indicio, pues en la especie lo trascendente es demostrar que se presentó la declaración y se efectuó el pago por concepto del impuesto, lo cual se logra con la exhibición de la multicitada documental en la que aparecen los datos suficientes para identificar si se aplicaron o no los dispositivos legales reclamados.

SEGUNDO TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL SÉPTIMO CIRCUITO

Amparo en revisión 673/2003. Materiales Aceros Tucán, S.A. de C.V. 29 de abril de 2004. Mayoría de votos. Disidente y Ponente: Agustín Romero Montalvo. Secretaria: Maura Lidia Rodríguez Lagunes.

Nota: Esta tesis contendió en la contradicción 261/2007-SS resuelta por la Segunda Sala, de la que derivó la tesis 2a./J. 24/2008, que aparece publicada en el Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XXVII, febrero de 2008, página 530, con el rubro: "DECLARACIÓN PRESENTADA A TRAVÉS DE MEDIOS ELECTRÓNICOS Y ACUSE DE RECIBO CON SELLO DIGITAL. LA CONSTANCIA IMPRESA O SU COPIA SIMPLE SON APTAS PARA ACREDITAR LA APLICACIÓN DE LOS PRECEPTOS LEGALES EN QUE AQUÉLLA SE SUSTENTÓ."

Registro No. 180799

Localización:
Novena Época
Instancia: Segunda Sala
Fuente: Semanario Judicial de la Federación y su Gaceta
XX, Agosto de 2004
Página: 418
Tesis: 2a./J. 102/2004
Jurisprudencia
Materia(s): Constitucional, Administrativa

RENTA. A LA OBLIGACIÓN DE PRESENTAR DECLARACIONES POR MEDIOS ELECTRÓNICOS, PREVISTA EN EL ARTÍCULO 86, FRACCIÓN X, DE LA LEY DEL IMPUESTO RELATIVO, VIGENTE A PARTIR DEL 1o. DE ENERO DE 2002, NO LE SON APLICABLES LOS PRINCIPIOS DE JUSTICIA FISCAL. La Suprema Corte de Justicia de la Nación ha establecido que los principios de proporcionalidad y equidad tributarias previstos en el artículo 31, fracción IV, de la Constitución Política de los Estados Unidos Mexicanos, están dirigidos a las contribuciones en sí mismas consideradas y a sus elementos esenciales, tales como sujeto, objeto, base y tasa o tarifa, sin que sea factible hacer extensivos dichos principios a las obligaciones formales a cargo de los contribuyentes. En ese sentido, la obligación a cargo de determinados contribuyentes de presentar declaraciones por medios electrónicos, contenida en

el artículo 86, fracción X, de la Ley del Impuesto sobre la Renta, vigente a partir del 1o. de enero de 2002, en tanto que sólo determina un procedimiento para la presentación de las declaraciones, constituye una obligación formal, cuya finalidad consiste en que la autoridad pueda comprobar el correcto cumplimiento de las obligaciones de los gobernados de contribuir al gasto público, por lo que debe concluirse que a la mencionada obligación no le son aplicables los mencionados principios constitucionales.

Amparo en revisión 1643/2003. Profud, S.A. de C.V. 27 de febrero de 2004. Unanimidad de cuatro votos. Ponente: Guillermo I. Ortiz Mayagoitia. Secretaria: María Dolores Omaña Ramírez.

Amparo en revisión 333/2004. Constructora Indemetales, S.A. de C.V. 28 de mayo de 2004. Cinco votos. Ponente: Margarita Beatriz Luna Ramos. Secretario: Gustavo Eduardo López Espinoza.

Amparo en revisión 718/2004. Corning Mexicana, S.A. de C.V. 23 de junio de 2004. Cinco votos. Ponente: Margarita Beatriz Luna Ramos. Secretaria: Hilda Marcela Arceo Zarza.

Amparo en revisión 686/2004. Teycon, S.A. de C.V. 25 de junio de 2004. Unanimidad de cuatro votos. Ponente: Guillermo I. Ortiz Mayagoitia; en su ausencia hizo suyo el asunto Margarita Beatriz Luna Ramos. Secretaria: Lourdes Margarita García Galicia.

Amparo en revisión 544/2004. Indalum, S.A. de C.V. 9 de julio de 2004. Unanimidad de cuatro votos. Ausente: Guillermo I. Ortiz Mayagoitia. Ponente: Sergio Salvador Aguirre Anguiano. Secretario: Óscar Zamudio Pérez.

Tesis de jurisprudencia 102/2004. Aprobada por la Segunda Sala de este Alto Tribunal, en sesión privada del seis de agosto de dos mil cuatro.

Registro No. 181356

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XIX, Junio de 2004
Página: 1425
Tesis: I.7o.T.79 L
Tesis Aislada
Materia(s): laboral

CORREO ELECTRÓNICO TRANSMITIDO POR INTERNET, OFRECIDO COMO PRUEBA EN EL JUICIO LABORAL. VALOR PROBATORIO. El artículo 776 de la Ley Federal del Trabajo establece que son admisibles en el proceso todos los medios de prueba que no sean contrarios a la moral y al derecho, entre ellos, aquellos medios aportados por los descubrimientos de la ciencia; consecuentemente, es permisible ofrecer el correo **electrónico** transmitido por internet, que constituye un sistema mundial de diseminación y obtención de información en diversos ámbitos. Por otra parte, dada su naturaleza y la falta de firma de la persona a la que se le imputa un correo **electrónico**, ello trae como

consecuencia que no se tenga la certeza de que aquel a quien se atribuye su envío a través de la red sea quien efectivamente lo emitió y dirigió al oferente, por lo que si es objetado no puede perfeccionarse mediante la ratificación de contenido y firma, de conformidad con el artículo 800 del mismo ordenamiento legal, que dispone que cuando un **documento** que provenga de tercero ajeno a juicio resulta impugnado, deberá ser ratificado en su contenido y firma por el suscriptor. De lo que se sigue que ese medio de prueba por sí solo carece de valor probatorio ante la imposibilidad de su perfeccionamiento, además, si dicho correo **electrónico** no es objetado, ello no trae como consecuencia que tenga valor probatorio pleno, aunque sí constituirá un indicio, cuyo valor será determinado por la Junta al apreciarlo con las demás pruebas que obren en autos.

SÉPTIMO TRIBUNAL COLEGIADO EN MATERIA DE TRABAJO DEL PRIMER CIRCUITO

Amparo directo 2397/2004. María de Lourdes Liceaga Escalera. 25 de marzo de 2004. Unanimidad de votos. Ponente: María Yolanda Múgica García. Secretario: Eduardo Sánchez Mercado.

Registro No. 181546

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XIX, Mayo de 2004
Página: 1784
Tesis: I.13o.T.82 L
Tesis Aislada
Materia(s): laboral

INFONAVIT. EL ESTADO DE CUENTA DEL FONDO DE AHORRO DEL DERECHOHABIENTE, CERTIFICADO POR EL GERENTE DE SERVICIOS LEGALES DEL INSTITUTO, ES IDÓNEO PARA ACREDITAR LAS APORTACIONES PATRONALES A FAVOR DEL TRABAJADOR, SALVO PRUEBA EN CONTRARIO. De lo establecido por los artículos 30 de la Ley del Instituto del Fondo Nacional de la Vivienda para los Trabajadores, y 3o., fracciones I y XXII, y 11 de su reglamento interior, se advierte que esta entidad pública tiene el carácter de organismo fiscal autónomo, y que en términos de la ley que lo rige, así como del Código Fiscal de la Federación, cuenta con facultades de comprobación, entre otras, para requerir a los patrones la exhibición de libros y registros electrónicos o de cualquier otra naturaleza, así como los medios utilizados para procesar la información que integre su contabilidad, incluyendo nóminas de salarios y plantillas de personal, avisos, declaraciones, documentos y demás información necesaria para determinar la existencia o no de la relación laboral y la que permita establecer de manera presuntiva el monto de las aportaciones, así como el

pago de salarios a las personas a su servicio, vinculados con las obligaciones que a cargo de dichos patrones establecen la Ley Federal del Trabajo, la Ley del Instituto del Fondo Nacional de la Vivienda para los Trabajadores, el Código Fiscal de la Federación y sus disposiciones reglamentarias aplicables. Ahora bien, dentro de las facultades del gerente de servicios legales del instituto se encuentra la consistente en certificar documentos en los que consten los actos y operaciones para su remisión a las autoridades, lo cual conduce a concluir que el estado de cuenta del fondo de ahorro certificado, es el documento oficial de control e información utilizado para la determinación del monto de las aportaciones correspondientes al derechohabiente, reflejado en los registros que obran en el Instituto del Fondo Nacional de la Vivienda para los Trabajadores; por tanto, los datos que contenga este documento son idóneos para acreditar los extremos referidos, sin que sea necesario que se exhiba otro tipo de constancias, dado que es precisamente el estado de cuenta del fondo de ahorro el documento en el que se asientan los datos correspondientes. Además, dada la trascendencia fiscal que pudiera derivarse de la información en él contenida, sería difícil que los datos ahí registrados fueran alterados, lo que, desde luego, no impide la posibilidad de que el trabajador pueda desvirtuarlos con prueba en contrario.

DÉCIMO TERCER TRIBUNAL COLEGIADO EN MATERIA DE TRABAJO DEL PRIMER CIRCUITO

Amparo directo 3873/2004. Gabriel Domínguez Pérez. 18 de marzo de 2004. Unanimidad de votos. Ponente: José Manuel Hernández Saldaña. Secretaria: Margarita Jiménez Jiménez.

Amparo directo 4013/2004. Francisco Hernández Juárez. 18 de marzo de 2004. Unanimidad de votos. Ponente: Héctor Landa Razo. Secretario: Juan de Dios González-Pliego Ameneyro.

Registro No. 182400

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XIX, Enero de 2004
Página: 1533
Tesis: XVII.2o.P.A.16 A
Tesis Aislada
Materia(s): Administrativa

IMPUESTO SUSTITUTIVO DEL CRÉDITO AL SALARIO. LA CONSTANCIA DE RECEPCIÓN Y PAGO VÍA INTERNET PUEDE ACREDITAR EL PRIMER ACTO DE APLICACIÓN CUANDO DE LA MISMA SE DERIVE FEHACIENTEMENTE QUE SE ENTERÓ EL MONTO EQUI-

VALENTE AL CRÉDITO AL SALARIO MENSUAL A QUE SE REFIERE EL ARTÍCULO 115 DE LA LEY DEL IMPUESTO SOBRE LA RENTA. Tratándose de contribuyentes obligados a presentar declaraciones de pagos mensuales provisionales o definitivos por concepto de contribuciones federales como el impuesto sobre la renta y el impuesto sustitutivo del crédito al salario, a través de medios electrónicos como internet, la constancia de recepción de la declaración y pago que se efectúa a través de tal vía es el único documento que se puede obtener por ese medio, para acreditar que se efectuó dicha operación y, por tanto, es apto para acreditar el acto de aplicación tratándose de amparo contra leyes sin embargo, ello debe considerarse así cuando de dicha constancia se desprenda el tipo de operación que se realizó, de tal manera que se evidencie la aplicación de la norma impugnada, pero no es posible otorgar plena validez probatoria al citado documento para demostrar la aplicación de la norma o normas impugnadas, en el caso de que del mismo no se desprenda fehacientemente el concepto o conceptos por los cuales se hace el pago o entero, como cuando sólo se advierte que se efectuó un pago complementario por concepto de "ISR retenciones por salario", sin que aparezca claramente que ese pago complementario corresponde precisamente al entero del monto equivalente al crédito al salario mensual, calculado conforme a la tabla contenida en el artículo 115 de la Ley del Impuesto sobre la Renta, por lo que en tal caso el quejoso está obligado a adminicular dicho documento con diversos medios probatorios, a fin de demostrar fehacientemente que se ubicó en la hipótesis de las normas impugnadas y, por ende, su interés jurídico cuando se promueve el juicio de amparo con motivo del primer acto de aplicación.

SEGUNDO TRIBUNAL COLEGIADO EN MATERIAS PENAL Y ADMINISTRATIVA DEL DÉCIMO SÉPTIMO CIRCUITO

Amparo en revisión 181/2003. V Impulsora Comercial, S.A. de C.V. 16 de octubre de 2003. Unanimidad de votos. Ponente: Ángel Gregorio Vázquez González. Secretaria: Natalia López López.

Véase: Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XVI, septiembre de 2002, página 1351, tesis I.7o.A.183 A, de rubro: "DECLARACIONES FISCALES PRESENTADAS POR MEDIOS ELECTRÓNICOS (VÍA INTERNET). EL PRIMER ACTO DE APLICACIÓN SE ACREDITA CON ACUSE DE RECEPCIÓN QUE CONTENGA LOS DATOS REFERENTES A LA HORA, FECHA, FOLIO Y TIPO DE OPERACIÓN, TRANSMITIDO POR LA AUTORIDAD CORRESPONDIENTE."

Nota: Por ejecutoria de fecha 28 de enero de 2005, la Segunda Sala declaró sin materia la contradicción de tesis 149/2004-SS en que participó el presente criterio.

Registro No. 182439

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito

Fuente: Semanario Judicial de la Federación y su Gaceta
XIX, Enero de 2004
Página: 1492
Tesis: I.1o.A.120 A
Tesis Aislada
Materia(s): Administrativa

CONTRIBUCIONES. LA COPIA SIMPLE DEL COMPROBANTE DE PAGO POR MEDIOS ELECTRÓNICOS OBTENIDA MEDIANTE IMPRESORA, FAX O CUALQUIER OTRO MEDIO ANÁLOGO ES APTA PARA ACREDITAR EL ACTO DE APLICACIÓN DEL ARTÍCULO TERCERO TRANSITORIO DE LA LEY DEL IMPUESTO SOBRE LA RENTA VIGENTE EN EL AÑO DOS MIL TRES. Del artículo 31, segundo párrafo, del Código Fiscal de la Federación y de la regla 2.9.17. de la Resolución Miscelánea Fiscal vigente en febrero del año dos mil tres se desprende que cuando los contribuyentes realicen el cumplimiento de sus deberes fiscales por medios electrónicos, no es obligatorio que presenten la declaración correspondiente en las formas aprobadas por la Secretaría de Hacienda y Crédito Público, en virtud de que los contribuyentes podrán presentar la declaración en las citadas formas para obtener el sello o impresión de la máquina registradora, lo que significa que se está en presencia de una facultad o derecho del gobernado que puede o no ejercer y no de un deber; en igual forma, es una facultad de éste obtener copia certificada de las declaraciones presentadas por medios electrónicos. Ahora bien, el pago de contribuciones por medios electrónicos constituye un instrumento para facilitar el cumplimiento de las obligaciones fiscales de los gobernados y la pronta y eficaz recaudación, cuya forma de operar implica que los causantes tengan una clave de acceso al sistema tributario cuando realicen pagos por transferencia electrónica, en tanto que la institución financiera proporcionará el sello digital. El concepto del "equivalente funcional" entre los documentos consignados en papel y aquellos consignados por vía electrónica tiene por objeto establecer una serie de características numéricas y criptográficas que identifican a la persona y aprobar la información que aparece en el mensaje, de ahí que la reproducción de la información mediante impresora, fax o cualquier otro medio análogo, que naturalmente se reduce a copia simple, no significa, en modo alguno, que carezcan de valor probatorio para demostrar el acto de aplicación del artículo tercero transitorio de la Ley del Impuesto sobre la Renta, vigente en el año dos mil tres, reclamado, por el simple hecho de que consten en copia simple, antes bien, son confiables partiendo de la base de los fines del artículo 31 del ordenamiento citado, que sirvió de fundamento para generar la información electrónica, en virtud de que la seguridad de la operación se encuentra en la clave digital que es original, adminiculada con los demás datos como son el registro federal de contribuyentes, la fecha de pago, el número de cuenta, el número de operación, el periodo, el impuesto y la cantidad que se paga y, en todo caso, el fisco federal, de no estar de acuerdo con su contenido, está en posibilidad de impugnarlo, y si no lo hizo, tal omisión se traduce en su aceptación tácita para todos los efectos legales, porque la presentación de una declaración escrita para obtener el sello oficial en original o la impresión en ella de la máquina registradora, después de haber realizado el pago o cumplimiento

de obligaciones fiscales por medios electrónicos, es una facultad o derecho del gobernado que puede o no ejercer a su juicio, porque no se trata de un deber, una obligación. Por tanto, la fuerza probatoria deriva de la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser exigida para su ulterior consulta, de conformidad con lo dispuesto por el artículo 210-A del Código Federal de Procedimientos Civiles, aplicado supletoriamente en términos del artículo 2o. de la Ley de Amparo, y no de la aplicación dogmática de una regla general de que las copias simples carecen, por sí mismas, de valor, por el hecho de que el sello digital se encuentra en una copia simple obtenida de impresora, fax, entre otros, ya que los avances tecnológicos, a nivel mundial, trajeron como resultado que el legislador introdujera los medios electrónicos para crear, modificar, extinguir o cumplir obligaciones, según se advierte de los artículos 31 del código tributario, 89 a 114 del Código de Comercio, 188 y 210-A del Código Federal de Procedimientos Civiles, entre otros ordenamientos, que establecen excepciones a la regla general citada. Por consiguiente, si al realizar el pago provisional del impuesto sustitutivo del crédito al salario que le corresponde, el acuse referido es el único documento que obtuvo el particular al realizar su pago de esa forma, es claro que si las autoridades hacendarias no lo objetaron, por razones de lealtad procesal, de probidad y buena fe frente al Juez, quien debe evitar que se trastoquen dichos valores, debe considerarse apto y suficiente para demostrar el pago de referencia y, por ende, el acto concreto de aplicación de la norma tildada de inconstitucional y su interés jurídico para cuestionarla; con mayor razón si la quejosa, en el escrito de demanda, manifestó bajo protesta de decir verdad que la copia simple en la que consta la firma electrónica, es real, sin perjuicio de las responsabilidades que le pudieran resultar, en el supuesto de que llegara a faltar a la verdad, sobre todo si se toma en cuenta que la autoridad fiscal se abstuvo de cuestionar la veracidad de la firma electrónica, no obstante que cuenta con la base de datos que contiene los sellos digitales y las firmas electrónicas.

PRIMER TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL PRIMER CIRCUITO

Amparo en revisión 354/2003. Cierres Best de México, S.A. de C.V. 10 de octubre de 2003. Unanimidad de votos. Ponente: Julio Humberto Hernández Fonseca. Secretario: José de Jesús Alcaraz Orozco.

Amparo en revisión 437/2003. Nutrical, S.A. de C.V. 15 de octubre de 2003. Unanimidad de votos. Ponente: Julio Humberto Hernández Fonseca. Secretario: José de Jesús Alcaraz Orozco.

Véase: Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XVI, septiembre de 2002, página 1351, tesis I.7o.A.183 A, de rubro: "DECLARACIONES FISCALES PRESENTADAS POR MEDIOS ELECTRÓNICOS (VÍA INTERNET). EL PRIMER ACTO DE APLICACIÓN SE ACREDITA CON ACUSE DE RECEPCIÓN QUE CONTENGA LOS DATOS REFERENTES A LA HORA, FECHA, FOLIO Y TIPO DE OPERACIÓN, TRANSMITIDO POR LA AUTORIDAD CORRESPONDIENTE."

Registro No. 182803

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XVIII, Noviembre de 2003
Página: 997
Tesis: VI.2o.A.62 A
Tesis Aislada
Materia(s): Administrativa

PAGOS PROVISIONALES MENSUALES. PARA ACREDITARLOS BASTA CON QUE EL CONTRIBUYENTE EXHIBA LA CONSTANCIA DE RECEPCIÓN DEL DISCO MAGNÉTICO (DISQUETE) QUE UTILIZÓ, SELLADO POR LA INSTITUCIÓN BANCARIA AUTORIZADA (INTERPRETACIÓN DEL ARTÍCULO 31, PÁRRAFO SEGUNDO, DEL CÓDIGO FISCAL DE LA FEDERACIÓN, VIGENTE EN MIL NOVECIENTOS NOVENTA Y NUEVE). De la interpretación integral de ese precepto se colige que los contribuyentes obligados a realizar pagos provisionales mensuales, de conformidad con las leyes fiscales, en lugar de utilizar las formas de declaración a que se refiere el párrafo primero del artículo 31 en mención, deberán presentar las declaraciones correspondientes a través de medios electrónicos, en los términos que señale la Secretaría de Hacienda y Crédito Público con reglas de carácter general, de ahí que deba estimarse que no es obligatorio presentar la declaración relativa a las formas aprobadas por esa secretaría, ya que claramente dispone dicho numeral que "Adicionalmente, los contribuyentes podrán presentar la declaración correspondiente en las formas aprobadas por la citada dependencia, para obtener el sello o impresión de la máquina registradora de la oficina autorizada que reciba el pago ...", mas no que deban hacerlo de manera ineludible; en tal virtud, si por una parte, para determinar el crédito fiscal impugnado, la autoridad demandada se apoya en forma esencial en el hecho de que el particular no realiza el pago provisional mensual normal del periodo relativo, por no encontrarse registrado tal pago en la base de datos de la administración local respectiva, en tanto que, por otra parte, dicho proceder fue considerado legal por la Sala, bajo el argumento de que la demandante no demostró que hizo ese pago, al resultar insuficiente el acuse de recibo del disquete, con sello de recepción de la institución bancaria, porque tuviera que hacerlo "adicionalmente" en la forma aprobada por la Secretaría de Hacienda y Crédito Público, es de concluir que la determinación del crédito obedeció a que el gobernado omitió presentar la declaración de pago provisional mensual en el "formato oficial de pago provisional" con el sello de recepción por la institución bancaria autorizada y no sólo a través de un medio electrónico, lo cual no es obligatorio, dado que esto último es suficiente, acorde con el artículo 31, párrafo segundo, del Código Fiscal de la Federación.

SEGUNDO TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL SEXTO CIRCUITO

Amparo directo 39/2002. Comercializadora Reforma de Puebla, S.A. de C.V. 28 de febrero de 2002. Unanimidad de votos. Ponente: Omar Losson Ovando. Secretaria: Rosa Iliana Noriega Pérez.

Registro No. 182830

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XVIII, Noviembre de 2003
Página: 976
Tesis: IV.3o.C.20 C
Tesis Aislada
Materia(s): Civil

INCIDENTE DE REPOSICIÓN DE AUTOS. CARECEN DE VALIDEZ LAS RESOLUCIONES O ACTUACIONES JUDICIALES OBTENIDAS DE LOS ARCHIVOS ELECTRÓNICOS O DE LOS SISTEMAS DE CÓMPUTO DE LOS ÓRGANOS JURISDICCIONALES (LEGISLACIÓN DEL ESTADO DE NUEVO LEÓN). Si bien es cierto que el artículo 37, párrafo tercero, del código adjetivo civil del Estado de Nuevo León faculta a los Jueces para investigar de oficio la existencia de las piezas de autos desaparecidas, valiéndose para ello de todos los medios que no sean contrarios a la moral o al derecho, también lo es que las resoluciones o actuaciones obtenidas de los archivos electrónicos o sistemas de cómputo que se utilizan en los órganos jurisdiccionales no deben ser tomados en cuenta para ese efecto, en virtud de que carecen de validez legal al faltar las firmas correspondientes de los funcionarios judiciales que intervinieron en su confección, tal como lo exige el último párrafo del numeral 51 del invocado código procesal; por tanto, es inconcuso que el instructor, al conceder eficacia a los instrumentos de referencia, viola las garantías de legalidad y seguridad jurídica contenidas en el artículo 16 de la Constitución General de la República.

TERCER TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL CUARTO CIRCUITO

Amparo en revisión 589/2002. Ricardo Javier Hinojosa González. 17 de marzo de 2003. Unanimidad de votos. Ponente: Sergio García Méndez. Secretario: Jerónimo Villanueva Acosta.

Registro No. 183903

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XVIII, Julio de 2003
Página: 1045
Tesis: I.3o.C.429 C
Tesis Aislada
Materia(s): Civil

CLAVE DIGITAL. SU UTILIZACIÓN PRUEBA EL RECONOCIMIENTO DEL MEDIO DIGITAL PARA CELEBRAR OPERACIONES Y UTILIZAR SERVICIOS PROPORCIONADOS POR LAS INSTITUCIONES DE CRÉDITO. El artículo 52 de la Ley de Instituciones de Crédito dispone que las instituciones de crédito pueden celebrar sus operaciones y prestar servicios con el público por medios electrónicos, ópticos o de cualquier otra tecnología, sujetando tales actividades a lo que se pacte en el contrato respectivo; conforme a ello el empleo de la clave digital acredita el consentimiento del usuario para celebrar la operación previamente solicitada con la institución de crédito, pues constituye un acceso personalizado a esos medios expresados a través de cifras, signos, códigos, barras u otros atributos numéricos que permiten asegurar la procedencia y veracidad de su autoría, que constituye un medio de identificación del usuario y es la base para determinar la responsabilidad correspondiente a su uso.

TERCER TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL PRIMER CIRCUITO

Amparo directo 4143/2003. Ingeniería y Consultoría en Presfuerzo, S.A. de C.V. 22 de abril de 2003. Unanimidad de votos. Ponente: Neófito López Ramos. Secretario: José Luis Evaristo Villegas.

Registro No. 184947

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XVII, Febrero de 2003
Página: 1024
Tesis: III.2o.T.1 A
Tesis Aislada
Materia(s): Administrativa

COMPETENCIA. DEBE CONOCER DE LA DEMANDA DE GARANTÍAS EL JUEZ DE DISTRITO DEL LUGAR EN QUE SE EFECTUÓ LA DECLARACIÓN DEL IMPUESTO VÍA INTERNET, RESPECTO DE LA APLICACIÓN DE UNA LEY TILDADA DE INCONSTITUCIONAL. Si el contribuyente, con motivo de sus obligaciones fiscales, a través de una institución bancaria realiza transferencia electrónica de fondos, en el lugar de su domicilio, en favor de la autoridad tributaria correspondiente, que tiene su domicilio en diverso lugar y circuito de amparo al de aquél, conforme al artículo 36 de la Ley de Amparo, el primer acto de aplicación de la ley autoaplicativa señalada como inconstitucional se da en el lugar en que se hace la operación relativa y no en el lugar de residencia de la autoridad, toda vez que la declaración respectiva aconteció precisamente en el lugar en el que el gobernado debió dar cumplimiento a sus obligaciones. Consecuentemente, para conocer de la demanda de amparo indirecto, resulta ser competente el Juez de Distrito del lugar en que se haya hecho el pago del impuesto vía internet.

SEGUNDO TRIBUNAL COLEGIADO EN MATERIA DE TRABAJO DEL TERCER CIRCUITO

Competencia 13/2002. Suscitada entre el Juzgado Primero de Distrito en Materia Administrativa en el Estado de Jalisco y el Juzgado Noveno de Distrito en Materia Administrativa en el Distrito Federal. 4 de octubre de 2002. Unanimidad de votos. Ponente: Hugo Gómez Ávila. Secretaria: María Guadalupe de Jesús Mejía Pulido.

Véase: Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XVII, enero de 2003, página 324, tesis 2a./J. 146/2002, de rubro: "COMPETENCIA PARA CONOCER DE UN JUICIO DE AMPARO PROMOVIDO CONTRA UNA LEY FISCAL FEDERAL CON MOTIVO DE SU PRIMER ACTO DE APLICACIÓN, CONSISTENTE EN LA DECLARACIÓN Y PAGO DE LA CONTRIBUCIÓN POR MEDIOS ELECTRÓNICOS. CORRESPONDE AL JUEZ DE DISTRITO QUE EJERCE JURISDICCIÓN EN EL LUGAR DEL DOMICILIO FISCAL DEL CONTRIBUYENTE.".

Nota: Por ejecutoria de fecha 28 de enero de 2005, la Segunda Sala declaró sin materia la contradicción de tesis 149/2004-SS en que participó el presente criterio.

Registro No. 185231

Localización:
Novena Época
Instancia: Segunda Sala
Fuente: Semanario Judicial de la Federación y su Gaceta
XVII, Enero de 2003
Página: 324
Tesis: 2a./J. 146/2002

Jurisprudencia
Materia(s): Administrativa

COMPETENCIA PARA CONOCER DE UN JUICIO DE AMPARO PROMOVIDO CONTRA UNA LEY FISCAL FEDERAL CON MOTIVO DE SU PRIMER ACTO DE APLICACIÓN, CONSISTENTE EN LA DECLARACIÓN Y PAGO DE LA CONTRIBUCIÓN POR MEDIOS ELECTRÓNICOS. CORRESPONDE AL JUEZ DE DISTRITO QUE EJERCE JURISDICCIÓN EN EL LUGAR DEL DOMICILIO FISCAL DEL CONTRIBUYENTE. Conforme al artículo 36 de la Ley de Amparo si el acto reclamado en un juicio de garantías requiere ejecución material, será competente el Juez de Distrito que ejerza jurisdicción en el lugar donde dicho acto deba tener ejecución, trate de ejecutarse, se ejecute o se haya ejecutado. Ahora bien, si se reclama en un juicio de amparo indirecto una ley fiscal federal con motivo de su primer acto de aplicación, consistente en la declaración y pago de la contribución en ella establecida, efectuados a través de medios electrónicos, debe considerarse competente para conocer del juicio el Juez de Distrito que ejerza jurisdicción en el lugar del domicilio fiscal del contribuyente, el cual coincide con la circunscripción territorial de la unidad administrativa del Servicio de Administración Tributaria a la que se entienden dirigidos la declaración y el pago relativos, por ser aquel en que tuvo ejecución el acto de aplicación y producirá sus consecuencias de control y fiscalización autoritarios, pues el criterio general establecido en la legislación fiscal para efectos de vinculación del contribuyente al cumplimiento de sus obligaciones fiscales es el de su domicilio fiscal, que se precisa en el artículo 10 del Código Fiscal de la Federación, y en relación con el cual se realiza su control por la unidad administrativa regional en cuya circunscripción se ubica. Lo anterior es así, pues si bien es cierto que formalmente la declaración presentada por medios electrónicos se dirige, en general, al Servicio de Administración Tributaria, el cual, conforme al artículo 4o. de la Ley que lo regula tiene su domicilio en la Ciudad de México, donde se ubican sus oficinas centrales, también lo es que la introducción de los medios electrónicos como vía para el cumplimiento de las obligaciones fiscales sólo tuvo por finalidad el simplificar a los contribuyentes tal cumplimiento, pero no modificar el criterio del domicilio fiscal como lugar de vinculación de los contribuyentes a dicho cumplimiento, ni el régimen de distribución de facultades entre los órganos que conforman tal dependencia bajo el criterio de desconcentración para el logro de una administración tributaria accesible, eficiente y cercana a los contribuyentes, por lo que la declaración y el pago relativos deben entenderse dirigidos a la unidad administrativa que ejerce el control sobre el contribuyente; además, considerar que la ejecución del acto tuvo lugar en la Ciudad de México por encontrarse en ella el domicilio del Servicio de Administración Tributaria sería sustentar un criterio contrario al principio de expeditez en la administración de justicia que consagra el artículo 17 de la Constitución Política de los Estados Unidos Mexicanos, toda vez que llevaría a concentrar en los Juzgados de Distrito que ejercen jurisdicción en tal entidad los juicios promovidos contra leyes fiscales cuando el avance tecnológico computacional tiende a que la mayoría de los contribuyentes cumpla sus obligaciones a través de medios electrónicos.

Contradicción de tesis 133/2002-SS. Entre las sustentadas por el Primer y Tercer Tribunales Colegiados en Materia Administrativa del Segundo Circuito. 22 de noviembre de 2002. Unanimidad de cuatro votos. Ausente: Sergio Salvador Aguirre Anguiano. Ponente: Mariano Azuela Güitrón. Secretaria: Lourdes Ferrer Mac Gregor Poisot.

Tesis de jurisprudencia 146/2002. Aprobada por la Segunda Sala de este Alto Tribunal, en sesión privada del nueve de diciembre de dos mil dos

Registro No. 186038

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XVI, Septiembre de 2002
Página: 1351
Tesis: I.7o.A.183 A
Tesis Aislada
Materia(s): Administrativa

DECLARACIONES FISCALES PRESENTADAS POR MEDIOS ELECTRÓNICOS (VÍA INTERNET). EL PRIMER ACTO DE APLICACIÓN SE ACREDITA CON ACUSE DE RECEPCIÓN QUE CONTENGA LOS DATOS REFERENTES A LA HORA, FECHA, FOLIO Y TIPO DE OPERACIÓN, TRANSMITIDO POR LA AUTORIDAD CORRESPONDIENTE. Para acreditar el primer acto de aplicación y, por ende, el interés jurídico del gobernado para acudir al juicio de amparo a reclamar una ley, basta con la exhibición de la constancia de recepción de la declaración y pago correspondiente, presentada a través de los medios electrónicos, específicamente en la página del Servicio de Administración Tributaria de la red respectiva que contenga los datos relativos a la hora, fecha, folio y tipo de operación, para considerarse acreditado el acto de aplicación de las normas reclamadas en el juicio de garantías, toda vez que las constancias de referencia son el único documento que se puede obtener para demostrar el cumplimiento de las obligaciones fiscales por esa vía, de conformidad con lo dispuesto en el artículo 31, párrafo segundo, del Código Fiscal de la Federación y la regla número 2.10.7. de la miscelánea fiscal vigente para el año dos mil uno.

SÉPTIMO TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL PRIMER CIRCUITO

Amparo en revisión 1067/2002. Servicios Monte Blanco, S.A. de C.V. 22 de mayo de 2002. Unanimidad de votos. Ponente: David Delgadillo Guerrero. Secretaria: María del Rocío Sánchez Ramírez.

Nota: Por ejecutoria de fecha 28 de enero de 2005, la Segunda Sala declaró inexistente la contradicción de tesis 149/2004-SS en que participó el presente criterio.

Registro No. 186243

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XVI, Agosto de 2002
Página: 1306
Tesis: V.3o.10 C
Tesis Aislada
Materia(s): Civil

INFORMACIÓN PROVENIENTE DE INTERNET. VALOR PROBATORIO. El artículo 188 del Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo, en términos de lo previsto en el diverso artículo 2o. de este ordenamiento legal, dispone: "Para acreditar hechos o circunstancias en relación con el negocio que se ventila, pueden las partes presentar fotografías, escritos o notas taquigráficas, y, en general, toda clase de elementos aportados por los descubrimientos de la ciencia."; asimismo, el diverso artículo 210-A, párrafo primero, de la legislación que se comenta, en lo conducente, reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquiera otra tecnología; ahora bien, entre los medios de comunicación electrónicos se encuentra "internet", que constituye un sistema mundial de diseminación y obtención de información en diversos ámbitos y, dependiendo de esto último, puede determinarse el carácter oficial o extraoficial de la noticia que al efecto se recabe, y como constituye un adelanto de la ciencia, procede, en el aspecto normativo, otorgarle valor probatorio idóneo.

TERCER TRIBUNAL COLEGIADO DEL QUINTO CIRCUITO

Amparo en revisión 257/2000. Bancomer, S.A., Institución de Banca Múltiple, Grupo Financiero. 26 de junio de 2001. Unanimidad de votos. Ponente: Epicteto García Báez.

Registro No. 186637

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XVI, Julio de 2002
Página: 1270
Tesis: II.3o.A.13 A
Tesis Aislada
Materia(s): Administrativa

CONFLICTO DE COMPETENCIA ENTRE JUECES DE DISTRITO. CORRESPONDE CONOCER DEL JUICIO DE AMPARO QUE SE PROMUEVA EN CONTRA DE UNA LEY TRIBUTARIA, CON MOTIVO DE UN ACTO DE APLICACIÓN, AL JUEZ DE DISTRITO QUE RESIDE EN EL LUGAR EN EL QUE SE RECIBIÓ LA DECLARACIÓN, CUANDO ÉSTA SE PRESENTA POR MEDIOS ELECTRÓNICOS Y NO EXISTE EVIDENCIA DEL LUGAR DE DONDE SE ENVIÓ. Conforme a lo dispuesto por los artículos 20 y 31 del Código Fiscal de la Federación, que prevén el empleo de medios electrónicos para la presentación de las declaraciones, los contribuyentes obligados a presentar pagos provisionales mensuales, de conformidad con las leyes fiscales respectivas, deberán efectuar el pago de sus contribuciones mediante transferencia electrónica de fondos a favor de la Tesorería de la Federación, de conformidad con las reglas de carácter general que al efecto expida la Secretaría de Hacienda y Crédito Público, y en lugar de utilizar las formas que al efecto apruebe dicha secretaría, deberán presentar, a través de medios electrónicos, las declaraciones establecidas en las disposiciones fiscales que señale la propia secretaría, mediante reglas de carácter general, y cumplir los requisitos que se establezcan en dichas reglas para tal efecto; sin embargo, adicionalmente los contribuyentes podrán presentar las declaraciones correspondientes en las formas aprobadas por la citada dependencia, para obtener el sello o impresión de la máquina registradora de la oficina autorizada que reciba el documento de que se trate, debiendo cumplir los requisitos que dicha secretaría señale mediante reglas de carácter general. Por otra parte, en términos de las Reglas 2.10.7 y 2.10.19, de la Resolución Miscelánea Fiscal para el año dos mil, publicada en el *Diario Oficial de la Federación* el seis de marzo del año dos mil y prorrogada su vigencia hasta el seis de marzo del año dos mil dos, por publicación en el mismo órgano de difusión oficial del dos de marzo del año dos mil uno, que regulan los pagos provisionales y la presentación de declaraciones mediante medios electrónicos, se considera que un contribuyente ha cumplido la obligación de presentar la declaración por medios electrónicos, cuando ésta y el pago coincidan en la fecha y en la cantidad manifestada y enterada, y se tomará como fecha de presentación de declaración aquella en que el Servicio de Administración Tributaria reciba la información correspondiente, la que acusará recibo utilizando la misma vía. Conforme al procedimiento indicado, se considera que la aplicación de las disposiciones fiscales respectivas se dan cuando el Servicio de Administración Tributaria recibe el pago del impuesto y la declaración enviados por el medio electrónico que se utilice, que deben coincidir en la fecha y en la cantidad manifestada y enterada, según lo estimó la Suprema Corte de Justicia de la Nación en un asunto análogo, que dio origen a la tesis número P. XVII/2001, publicada en el Semanario Judicial de la Federación y su Gaceta, Tomo XIV, octubre de 2001, Novena Época, Pleno, de rubro: "CONSOLIDACIÓN FISCAL. LA CONSTANCIA DE RECEPCIÓN DEL PAGO PROVISIONAL DEL IMPUESTO SOBRE LA RENTA EN RELACIÓN CON EL RESULTADO DE LOS ESTADOS CONSOLIDADOS DE LAS SOCIEDADES CONTROLADORAS, OBTENIDA DE LA RED DE INTERNET, ACREDITA EL ACTO DE APLICACIÓN DE LOS ARTÍCULOS 57-E, 57-K, 57-N Y 57-Ñ DE LA LEY DE LA MATERIA, VIGENTES A PARTIR DEL PRIMERO DE ENERO DE MIL NOVECIENTOS NOVENTA Y NUEVE,

PARA EFECTOS DEL JUICIO DE AMPARO.". Por tanto, si de las pruebas exhibidas por la quejosa con la demanda de amparo, consistentes en los acuses de recibo, se advierte que efectuó los pagos provisionales del impuesto sobre la renta mediante declaraciones presentadas por un medio electrónico (internet), que fueron recibidas por la Administración General de Recaudación del Servicio de Administración Tributaria de la Secretaría de Hacienda y Crédito Público, que tiene su sede en la Ciudad de México, Distrito Federal, y no existe evidencia del lugar donde se envió la declaración por el medio electrónico utilizado, es en esa ciudad en donde se actualizó el acto de aplicación de la ley y, por tanto, con fundamento en el artículo 36 de la Ley de Amparo, en esta hipótesis en particular, el competente para conocer de la demanda de garantías lo es el Juez de Distrito en Materia Administrativa en el Distrito Federal.

TERCER TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL SEGUNDO CIRCUITO

Competencia 1/2002. Suscitada entre el Juez Primero de Distrito en el Estado de México, con residencia en Naucalpan y el Juez Octavo de Distrito "A" en Materia Administrativa en el Distrito Federal. 4 de abril de 2002. Unanimidad de votos. Ponente: Manuel de Jesús Rosales Suárez. Secretario: Marco Quintana Vargas.

Notas: Por ejecutoria de fecha 22 de noviembre de 2002, la Segunda Sala declaró inexistente la contradicción de tesis 118/2002-SS en que participó el presente criterio.

Esta tesis contendió en la contradicción 133/2002-SS resuelta por la Segunda Sala, de la que derivó la tesis 2a./J. 146/2002, que aparece publicada en el Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XVII, enero de 2003, página 324, con el rubro: "COMPETENCIA PARA CONOCER DE UN JUICIO DE AMPARO PROMOVIDO CONTRA UNA LEY FISCAL FEDERAL CON MOTIVO DE SU PRIMER ACTO DE APLICACIÓN, CONSISTENTE EN LA DECLARACIÓN Y PAGO DE LA CONTRIBUCIÓN POR MEDIOS ELECTRÓNICOS. CORRESPONDE AL JUEZ DE DISTRITO QUE EJERCE JURISDICCIÓN EN EL LUGAR DEL DOMICILIO FISCAL DEL CONTRIBUYENTE."

Nota: Esta tesis fue superada por contradicción

Registro No. 188651

Localización:
Novena Época
Instancia: Pleno
Fuente: Semanario Judicial de la Federación y su Gaceta
XIV, Octubre de 2001
Página: 20
Tesis: P. XVII/2001

Tesis Aislada
Materia(s): Constitucional, Administrativa

CONSOLIDACIÓN FISCAL. LA CONSTANCIA DE RECEPCIÓN DEL PAGO PROVISIONAL DEL IMPUESTO SOBRE LA RENTA EN RELACIÓN CON EL RESULTADO DE LOS ESTADOS CONSOLIDADOS DE LAS SOCIEDADES CONTROLADORAS, OBTENIDA DE LA RED DE INTERNET, ACREDITA EL ACTO DE APLICACIÓN DE LOS ARTÍCULOS 57-E, 57-K, 57-N Y 57-Ñ DE LA LEY DE LA MATERIA, VIGENTES A PARTIR DEL PRIMERO DE ENERO DE MIL NOVECIENTOS NOVENTA Y NUEVE, PARA EFECTOS DEL JUICIO DE AMPARO. De una interpretación armónica y sistemática de lo dispuesto en el artículo 31, párrafo segundo, del Código Fiscal de la Federación y en la regla número 2.10.13. de la Resolución Miscelánea Fiscal para 1998, se desprende que las sociedades controladoras que consolidan sus resultados para efectos fiscales, tienen la obligación legal de presentar sus pagos provisionales mensuales y la declaración anual del ejercicio fiscal de que se trate, a través de medios electrónicos. Ahora bien, si una sociedad controladora, en cumplimiento de las obligaciones fiscales antes precisadas, presenta sus declaraciones y pago correspondiente a través de esos medios, la prueba consistente en la constancia de recepción de la declaración provisional, que obtuvo de la red de internet, sí puede considerarse como idónea para acreditar el acto de aplicación de las normas reclamadas en el juicio de garantías, toda vez que la constancia de referencia es el único documento que puede obtener la sociedad que realiza su pago de esa forma. Por consiguiente, si tal documento no es objetado oportunamente por las autoridades hacendarias, no es posible, por razones de seguridad jurídica, poner en duda su autenticidad y contenido, sin que obste a lo anterior el hecho de que en el mencionado artículo 31, párrafo segundo, se establezca que: "... Adicionalmente, los contribuyentes podrán presentar la declaración correspondiente en las formas aprobadas por la citada dependencia, para obtener el sello o impresión de la máquina registradora de la oficina autorizada que reciba el pago ...", pues del propio numeral se advierte que no es obligatorio para los contribuyentes presentar la declaración correspondiente en las formas aprobadas por la Secretaría de Hacienda y Crédito Público.

Amparo en revisión 1825/99. Industrias Electrolux, S.A, de C.V. y coags. 9 de agosto de 2001. Unanimidad de diez votos. Ausente: José Vicente Aguinaco Alemán. Ponente: Guillermo I. Ortiz Mayagoitia. Secretaria: Lourdes Margarita García Galicia.

El Tribunal Pleno, en su sesión privada celebrada hoy veinte de septiembre en curso, aprobó, con el número XVII/2001, la tesis aislada que antecede; y determinó que la votación es idónea para integrar tesis jurisprudencial. México, Distrito Federal, a veinte de septiembre de dos mil uno

Registro No. 189515

Localización:
Novena Época

Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XIII, Junio de 2001Página: 677
Tesis: VII.1o.A.T.48 A
Tesis Aislada
Materia(s): Administrativa

AUTORIDADES ADUANERAS. SON COMPETENTES PARA VERIFICAR EL CUMPLIMIENTO DE LAS REGULACIONES Y RESTRICCIONES NO ARANCELARIAS DE MERCANCÍA DE IMPORTACIÓN, EN EL PUNTO DE SU ENTRADA O SALIDA, PREVISTAS EN LA NOM-015/1-SCFI/SSA-1994. La correcta interpretación de los artículos 36, fracción I, inciso c), de la Ley Aduanera y 26 de la Ley de Comercio Exterior, el primero de los cuales establece: "Artículo 36. Quienes importen o exporten mercancías están obligados a presentar ante la aduana, por conducto de agente o apoderado aduanal, un pedimento en la forma oficial aprobada por la secretaría. En los casos de las mercancías sujetas a regulaciones y restricciones no arancelarias cuyo cumplimiento se demuestre a través de medios electrónicos, el pedimento deberá incluir la firma electrónica que demuestre el descargo total o parcial de esas regulaciones o restricciones. Dicho pedimento se deberá acompañar de: I. En importación: ... c) Los documentos que comprueben el cumplimiento de las regulaciones y restricciones no arancelarias a la importación, que se hubieran expedido de acuerdo con la Ley de Comercio Exterior, siempre que las mismas se publiquen en el *Diario Oficial de la Federación* y se identifiquen en términos de la fracción arancelaria y de la nomenclatura que les corresponda conforme a la tarifa de la Ley del Impuesto General de Importación.", y el segundo prescribe: "Artículo 26. En todo caso, la importación, circulación o tránsito de mercancías estarán sujetos a las normas oficiales mexicanas de conformidad con la ley de la materia. ... La secretaría determinará las normas oficiales mexicanas que las autoridades aduaneras deban hacer cumplir en el punto de entrada de la mercancía al país. ...", permite establecer que las autoridades aduaneras son competentes para verificar el cumplimiento de las obligaciones no arancelarias al levantar el acta de inicio de procedimiento administrativo y reconocimiento aduanero de mercancías que ingresan al país, a que se refiere la Norma Oficial Mexicana NOM-015/1-SCFI/SSA-1994, "Seguridad e información comercial en juguetes-seguridad de juguetes y artículos escolares. Límites de biodisponibilidad de metales en artículos recubiertos con pinturas y tintas. Especificaciones químicas y métodos de prueba".

PRIMER TRIBUNAL COLEGIADO EN MATERIAS ADMINISTRATIVA Y DE TRABAJO DEL SÉPTIMO CIRCUITO

Amparo directo 88/2001. Alfredo Deschamps Blanco. 5 de abril de 2001. Unanimidad de votos. Ponente: Eliel E. Fitta García. Secretaria: Nilvia Josefina Flota Ocampo

Registro No. 190520

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XIII, Enero de 2001
Página: 1699
Tesis: I.5o.C.90 C
Tesis Aislada
Materia(s): Civil

CONTRATO DE INTERMEDIACIÓN BURSÁTIL NO DISCRECIONAL. MEDIOS A TRAVÉS DE LOS CUALES PUEDEN PROBARSE LAS INSTRUCCIONES QUE LOS INVERSIONISTAS DAN A LAS CASAS DE BOLSA PARA QUE REALICEN OPERACIONES AUTORIZADAS POR LA LEY. De conformidad con lo dispuesto en los artículos 90 y 91, fracciones I, II, V y VIII de la Ley del Mercado de Valores, las operaciones celebradas por la casa de bolsa con su clientela inversionista y por cuenta de la misma, se regirán por las previsiones contenidas en los contratos de intermediación bursátil, en los cuales el cliente confiere un mandato general para que por su cuenta, la casa de bolsa realice las operaciones autorizadas por la ley, contratos que pueden pactarse bajo dos modalidades diferentes, una de manera no discrecional, en la que la casa de bolsa, en el desempeño de su encargo, actuará conforme a las instrucciones del cliente que reciba el apoderado para celebrar operaciones con el público, y la otra, cuando en el contrato se pacte el manejo discrecional de la cuenta. Cuando el contrato bursátil se pacta bajo la modalidad no discrecional, las instrucciones del cliente para la ejecución de operaciones concretas o movimientos en la cuenta del mismo, podrán hacerse de manera escrita, verbal o telefónica, debiendo precisarse en todo caso el tipo de operación o movimiento, así como el género, especie, clase, emisor, cantidad, precio y cualquier otra característica para identificar los valores materia de cada operación o movimiento en la cuenta, pudiendo convenir el uso de carta, telégrafo, télex, telefax, o cualquier otro medio electrónico, de cómputo o telecomunicaciones para el envío, intercambio o, en su caso, la confirmación de las órdenes de la clientela inversionista, precisándose las claves de identificación recíproca, las que sustituirán la firma autógrafa, por lo que las constancias documentales o técnicas en donde aparezcan producirán los mismos efectos que las leyes otorgan a los documentos suscritos por las partes y tendrán igual valor probatorio. De lo establecido en los anteriores dispositivos legales, se infiere que las instrucciones que los inversionistas dan a la casa de bolsa para realizar operaciones autorizadas por la ley, tratándose de contratos de intermediación bursátil en los que se pacte un manejo de la cuenta no discrecional, sólo pueden probarse con las constancias documentales o técnicas en las que consten dichas instrucciones y la firma autógrafa o electrónica correspondiente, o bien, con las constancias que al efecto se hayan pactado en el contrato respectivo.

QUINTO TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL PRIMER CIRCUITO

Amparo directo 565/2000. Efraín y Marco Antonio Dávalos Padilla. 13 de octubre de 2000. Unanimidad de votos. Ponente: Efraín Ochoa Ochoa. Secretario: Salvador Martínez Calvillo

Registro No. 921309

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Apéndice (actualización 2002)
Tomo I, Const., P.R. TCC
Página: 467
Tesis: 237
Tesis Aislada
Materia(s): Constitucional

CONFLICTO DE COMPETENCIA ENTRE JUECES DE DISTRITO. CORRESPONDE CONOCER DEL JUICIO DE AMPARO QUE SE PROMUEVA EN CONTRA DE UNA LEY TRIBUTARIA, CON MOTIVO DE UN ACTO DE APLICACIÓN, AL JUEZ DE DISTRITO QUE RESIDE EN EL LUGAR EN EL QUE SE RECIBIÓ LA DECLARACIÓN, CUANDO ÉSTA SE PRESENTA POR MEDIOS ELECTRÓNICOS Y NO EXISTE EVIDENCIA DEL LUGAR DE DONDE SE ENVIÓ. Conforme a lo dispuesto por los artículos 20 y 31 del Código Fiscal de la Federación, que prevén el empleo de medios electrónicos para la presentación de las declaraciones, los contribuyentes obligados a presentar pagos provisionales mensuales, de conformidad con las leyes fiscales respectivas, deberán efectuar el pago de sus contribuciones mediante transferencia electrónica de fondos a favor de la Tesorería de la Federación, de conformidad con las reglas de carácter general que al efecto expida la Secretaría de Hacienda y Crédito Público, y en lugar de utilizar las formas que al efecto apruebe dicha secretaría, deberán presentar, a través de medios electrónicos, las declaraciones establecidas en las disposiciones fiscales que señale la propia secretaría, mediante reglas de carácter general, y cumplir los requisitos que se establezcan en dichas reglas para tal efecto; sin embargo, adicionalmente los contribuyentes podrán presentar las declaraciones correspondientes en las formas aprobadas por la citada dependencia, para obtener el sello o impresión de la máquina registradora de la oficina autorizada que reciba el documento de que se trate, debiendo cumplir los requisitos que dicha secretaría señale mediante reglas de carácter general. Por otra parte, en términos de las Reglas 2.10.7 y 2.10.19, de la Resolución Miscelánea Fiscal para el año dos mil, publicada en el *Diario Oficial de la Federación* el seis de marzo del año dos mil y prorrogada su vigencia hasta el seis de marzo del año dos mil dos, por publicación en el mismo órgano de difusión oficial del dos de marzo del año dos mil uno, que regulan los pagos

provisionales y la presentación de declaraciones mediante medios electrónicos, se considera que un contribuyente ha cumplido la obligación de presentar la declaración por medios electrónicos, cuando ésta y el pago coincidan en la fecha y en la cantidad manifestada y enterada, y se tomará como fecha de presentación de declaración aquella en que el Servicio de Administración Tributaria reciba la información correspondiente, la que acusará recibo utilizando la misma vía. Conforme al procedimiento indicado, se considera que la aplicación de las disposiciones fiscales respectivas se dan cuando el Servicio de Administración Tributaria recibe el pago del impuesto y la declaración enviados por el medio electrónico que se utilice, que deben coincidir en la fecha y en la cantidad manifestada y enterada, según lo estimó la Suprema Corte de Justicia de la Nación en un asunto análogo, que dio origen a la tesis número P. XVII/2001, publicada en el Semanario Judicial de la Federación y su Gaceta, Tomo XIV, octubre de 2001, Novena Época, Pleno, de rubro: "CONSOLIDACIÓN FISCAL. LA CONSTANCIA DE RECEPCIÓN DEL PAGO PROVISIONAL DEL IMPUESTO SOBRE LA RENTA EN RELACIÓN CON EL RESULTADO DE LOS ESTADOS CONSOLIDADOS DE LAS SOCIEDADES CONTROLADORAS, OBTENIDA DE LA RED DE INTERNET, ACREDITA EL ACTO DE APLICACIÓN DE LOS ARTÍCULOS 57-E, 57-K, 57-N Y 57-Ñ DE LA LEY DE LA MATERIA, VIGENTES A PARTIR DEL PRIMERO DE ENERO DE MIL NOVECIENTOS NOVENTA Y NUEVE, PARA EFECTOS DEL JUICIO DE AMPARO." Por tanto, si de las pruebas exhibidas por la quejosa con la demanda de amparo, consistentes en los acuses de recibo, se advierte que efectuó los pagos provisionales del impuesto sobre la renta mediante declaraciones presentadas por un medio electrónico (internet), que fueron recibidas por la Administración General de Recaudación del Servicio de Administración Tributaria de la Secretaría de Hacienda y Crédito Público, que tiene su sede en la Ciudad de México, Distrito Federal, y no existe evidencia del lugar donde se envió la declaración por el medio electrónico utilizado, es en esa ciudad en donde se actualizó el acto de aplicación de la ley y, por tanto, con fundamento en el artículo 36 de la Ley de Amparo, en esta hipótesis en particular, el competente para conocer de la demanda de garantías lo es el Juez de Distrito en Materia Administrativa en el Distrito Federal.

TERCER TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL SEGUNDO CIRCUITO

Competencia 1/2002. Suscitada entre el Juez Primero de Distrito en el Estado de México, con residencia en Naucalpan y el Juez Octavo de Distrito "A" en Materia Administrativa en el Distrito Federal. 4 de abril de 2002. Unanimidad de votos. Ponente: Manuel de Jesús Rosales Suárez. Secretario: Marco Quintana Vargas.

Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XVI, julio de 2002, página 1270, Tribunales Colegiados de Circuito, tesis II.3o.A. 13 A.

Notas: Por ejecutoria de fecha 22 de noviembre de 2002, la Segunda Sala declaró inexistente la contradicción de tesis 118/2002 en que participó el presente criterio.

Esta tesis contendió en la contradicción 133/2002-SS resuelta por la Segunda Sala, de la que derivó la tesis 2a./J. 146/2002, que aparece publicada en el Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XVII, enero de 2003, página 324, con el rubro: "COMPETENCIA PARA CONOCER DE UN JUICIO DE AMPARO PROMOVIDO CONTRA UNA LEY FISCAL FEDERAL CON MOTIVO DE SU PRIMER ACTO DE APLICACIÓN, CONSISTENTE EN LA DECLARACIÓN Y PAGO DE LA CONTRIBUCIÓN POR MEDIOS ELECTRÓNICOS. CORRESPONDE AL JUEZ DE DISTRITO QUE EJERCE JURISDICCIÓN EN EL LUGAR DEL DOMICILIO FISCAL DEL CONTRIBUYENTE."

Nota: Esta tesis fue superada por contradicción

Registro No. 921310

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Tomo I, Const., P.R. TCC
Página: 471
Tesis: 238
Tesis Aislada
Materia(s): Constitucional

DECLARACIONES FISCALES PRESENTADAS POR MEDIOS ELECTRÓNICOS (VÍA INTERNET). EL PRIMER ACTO DE APLICACIÓN SE ACREDITA CON ACUSE DE RECEPCIÓN QUE CONTENGA LOS DATOS REFERENTES A LA HORA, FECHA, FOLIO Y TIPO DE OPERACIÓN, TRANSMITIDO POR LA AUTORIDAD CORRESPONDIENTE. Para acreditar el primer acto de aplicación y, por ende, el interés jurídico del gobernado para acudir al juicio de amparo a reclamar una ley, basta con la exhibición de la constancia de recepción de la declaración y pago correspondiente, presentada a través de los medios electrónicos, específicamente en la página del Servicio de Administración Tributaria de la red respectiva que contenga los datos relativos a la hora, fecha, folio y tipo de operación, para considerarse acreditado el acto de aplicación de las normas reclamadas en el juicio de garantías, toda vez que las constancias de referencia son el único documento que se puede obtener para demostrar el cumplimiento de las obligaciones fiscales por esa vía, de conformidad con lo dispuesto en el artículo 31, párrafo segundo, del Código Fiscal de la Federación y la regla número 2.10.7. de la miscelánea fiscal vigente para el año dos mil uno.

SÉPTIMO TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL PRIMER CIRCUITO

Amparo en revisión 1067/2002. Servicios Monte Blanco, S.A. de C.V. 22 de mayo de 2002. Unanimidad de votos. Ponente: David Delgadillo Guerrero. Secretaria: María del Rocío Sánchez Ramírez.

Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XVI, septiembre de 2002, página 1351, Tribunales Colegiados de Circuito, tesis I.7o. A.183 A.

Nota: Por ejecutoria de fecha 28 de enero de 2005, la Segunda Sala declaró inexistente la contradicción de tesis 149/2004-SS en que participó el presente criterio.

Registro No. 922125

Localización:
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Apéndice (actualización 2002)
Tomo IV, Civil, P.R. TCC
Página: 113
Tesis: 44
Tesis Aislada
Materia(s): Civil

INFORMACIÓN PROVENIENTE DE INTERNET. VALOR PROBATORIO. El artículo 188 del Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo, en términos de lo previsto en el diverso artículo 2o. de este ordenamiento legal, dispone: "Para acreditar hechos o circunstancias en relación con el negocio que se ventila, pueden las partes presentar fotografías, escritos o notas taquigráficas, y, en general, toda clase de elementos aportados por los descubrimientos de la ciencia." Asimismo, el diverso artículo 210-A, párrafo primero, de la legislación que se comenta, en lo conducente, reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquiera otra tecnología; ahora bien, entre los medios de comunicación electrónicos se encuentra "internet", que constituye un sistema mundial de diseminación y obtención de información en diversos ámbitos y, dependiendo de esto último, puede determinarse el carácter oficial o extraoficial de la noticia que al efecto se recabe, y como constituye un adelanto de la ciencia, procede, en el aspecto normativo, otorgarle valor probatorio idóneo.

TERCER TRIBUNAL COLEGIADO DEL QUINTO CIRCUITO

Amparo en revisión 257/2000. Bancomer, S.A., Institución de Banca Múltiple, Grupo Financiero. 26 de junio de 2001. Unanimidad de votos. Ponente: Epicteto García Báez.

Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XVI, agosto de 2002, página 1306, Tribunales Colegiados de Circuito, tesis V.3o.10 C.

Glosario

Consultable en http.//www.pandasecurity.com/spain/homeusers/security-info/glossary/

A

Acceso de escritura/Permiso de escritura. Operación o derecho asociado a un usuario o a un programa para escribir en un disco o en cualquier otro dispositivo de almacenamiento informático.

Acción directa. Categoría o tipo de virus específico.

ActiveX. Tecnología utilizada, entre otras cosas, para dotar a las páginas web de mayores funcionalidades, como animaciones, video, navegación tridimensional, etc. Los controles ActiveX son pequeños programas que se incluyen dentro de estas páginas. Lamentablemente, por ser programas, pueden ser el objetivo de algún virus.

Actualizar/Actualización. Los antivirus evolucionan continuamente hacia versiones más potentes y adaptadas a las nuevas tecnologías empleadas por los virus. Para no quedar obsoletos, detectan todos los nuevos virus que surgen a diario. Para ello, cuentan con el denominado Archivo de Identificadores de Virus. Este fichero incluye todas las características que identifican a cada uno de los virus, haciendo posible detectarlos y actuar en consecuencia. La incorporación de la última versión de dicho fichero y de otros al antivirus es lo que se conoce como actualización.

Administrador. Persona o programa encargado de gestionar, realizar el control, conceder permisos, etc., de todo un sistema informático o red de computadoras.

Administrador de servicios. Applet con el que cuenta Windows XP/2000/NT, encargado de administrar (configurar y controlar) los servicios del sistema.

ADSL (Asymmetric Digital Subscriber Line). Tipo de conexión a internet y clase de módem que se caracterizan por su elevada velocidad.

Adware. Programas que muestran publicidad utilizando cualquier tipo de medio, por ejemplo, ventanas emergentes, banners, cambios en la página de inicio o de búsqueda del navegador, etc. Puede instalarse con el consentimiento del usuario y su plena conciencia, pero en ocasiones no es así. Lo mismo ocurre con el conocimiento o falta del mismo acerca de sus funciones.

Algoritmo. La definición formal de algoritmo es: "conjunto ordenado de operaciones que permite hallar la solución de un problema".

Alias. Cada virus tiene asignado un determinado nombre y sin embargo, muchas veces es más fácil reconocerlo por alguna de sus características más destacadas. En estos casos, el virus cuenta además con un segundo nombre (a modo de nombre de pila) que hace referencia a dicha característica. Dicho nombre es lo que se conoce como alias de un virus. Por ejemplo, el virus CIH se conoce con alias Chernobyl.

Análisis heurístico. Método, estrategia o técnica empleada para hacer más fácil la resolución de problemas. Aplicado al mundo informático, se entiende como una técnica utilizada para detectar virus que en ese momento son desconocidos.

ANSI (American National Standards Institute). Estándar definido y establecido en materia de informática.

Anti-Debug/Antidebugger. Conjunto de técnicas que los virus emplean para evitar ser investigados.

Antivirus/Programas antivirus. Programas que permiten analizar la memoria, las unidades de disco y otros elementos de una computadora, en busca de virus.

API (Application Programming Interface). Propiedad mediante la cual los programas pueden solicitar peticiones para ser atendidos o utilizar un servicio del sistema operativo y de otros programas.

Applets Java/Java Applets. Pequeños programas que se pueden incluir en algunas páginas web, con la finalidad de aportar más y mejores funcionalidades a dichas páginas.

Archivo de identificadores de virus. Fichero que permite a los antivirus detectar a los virus. También es conocido con el nombre de Fichero de firmas.

Armouring. Técnica que utilizan los virus para esconderse e impedir ser detectados por los antivirus.

ASCII. (American Standard Code for Information Interchange). Código estándar definido y establecido para representar los caracteres (letras, números, signos de puntuación, caracteres especiales, etc.) de forma numérica.

ASP (Active Server Page). Tipo de páginas web que permiten ser personalizadas a medida de las características y necesidades del usuario visitante. Además, también hace referencia a Application Service Provider. Es decir, proveedor de servicios de aplicaciones.

Ataque dirigido. Ataques realizados normalmente de manera silenciosa e imperceptible, cuyo objetivo es una persona, empresa o grupos de ambas. No son ataques masivos, porque su objetivo no es alcanzar al mayor número posible de computadoras. Su peligro estriba en que son ataques personalizados, diseñados especialmente para engañar a las potenciales víctimas.

Atributos. Determinadas características que se asocian y determinan el tipo de fichero y directorio.

Autoencriptación. Operación mediante la cual un virus codifica —cifra— parte de su contenido, o éste en su totalidad. Esto, en el caso de los virus, dificulta el estudio de su contenido.

Autofirma. Texto o contenido que se introduce automáticamente cuando se crea un nuevo mensaje de correo electrónico.

B

Backdoor/Puerta trasera. Programa que se introduce en la computadora y establece una puerta trasera a través de la cual es posible controlar el sistema afectado sin conocimiento por parte del usuario.

Bandeja de acceso rápido en Windows (Quick Launch). Zona próxima al menú o botón Inicio de Windows, donde se encuentran diversos iconos que dan un acceso rápido y directo a determinados elementos y/o programas, correo electrónico, internet, al antivirus, etc. En inglés se conoce como Quick Launch.

Bandeja de entrada. Carpeta existente en los programas de correo electrónico que contiene todos los mensajes que se han recibido.

Bandeja de sistema, en Windows. Zona situada en la Barra de tareas de Windows (habitualmente en la parte inferior derecha de la pantalla y junto al reloj del sistema), que muestra diversos iconos para configurar opciones del sistema, visualizar el estado de la protección antivirus, etc. En inglés se conoce como System Tray.

Banner. Anuncio mostrado en una página web sobre un determinado producto o servicio propio o ajeno a la página y que, al ser pulsado, lleva al sitio del anunciante.

Barra de estado. Sección inferior que aparece en las ventanas de algunos programas de Windows con información sobre el estado del programa o de los ficheros con los que se trabaja.

Barra de tareas de Windows. Barra que aparece en la sección inferior de la pantalla cuando se trabaja en Windows. Esta barra contiene, entre otras cosas, el botón Inicio de Windows, el reloj del sistema, iconos que representan cada uno de los programas residentes en la memoria en ese momento y botones de acceso rápido que permiten la ejecución inmediata de ciertos programas.

Barra de título. Área que aparece en la sección superior de las ventanas de Windows. En ella, se muestra generalmente el nombre del programa al que corresponde la ventana y el título del fichero con el que se está trabajando.

Base de datos. Conjunto de ficheros que contienen datos y los programas que gestionan la estructura y la forma en la que éstos se almacenan, así como la forma en la que deben relacionarse entre sí. Algunos ejemplos de sistemas de bases de datos son: Access, Oracle, SQL, Parados, dBase, etcétera.

BBS (Bulleting Board System). Sistema o servicio —utilizado en internet— que permite a los usuarios —mediante una suscripción previa— leer y responder a los mensajes que otros usuarios han escrito (en un foro de debate o grupo de noticias, por ejemplo).

BHO (Browser Helper Object). Plugin que se ejecuta automáticamente junto con el navegador de internet, y extiende sus funciones. Algunos se emplean con fines maliciosos, por ejemplo, monitorear las páginas web visitadas.

BIOS (Basic Input/Output System). Conjunto de programas que permite arrancar la computadora (parte del sistema de arranque).

Bit (Binary digit). Es la unidad más pequeña de la información digital con la que trabajan las computadoras (sistemas informáticos).

Bomba lógica. Programa, en principio de apariencia normal e inofensiva, que puede actuar provocando acciones dañinas, al igual que cualquier otro virus.

Boot/Master Boot Record (MBR). También conocido como Sector de arranque, es el área o la sección de un disco donde se almacena información sobre sus características y la capacidad del disco para arrancar la computadora.

Bot. Contracción de la palabra robot. Es un programa que permite que el sistema sea controlado remotamente sin el conocimiento ni consentimiento del usuario.

Bot herder (propietario de bots). Persona o grupo propietario que controla las redes de bot. También se le llama "bot master" o "zombie master".

Botnet. Red o grupo de computadoras zombies, controlados por el propietario de los bots. El propietario de las redes de bots da instrucciones a los zombies. Estas órdenes pueden incluir la propia actualización del bot, la descarga de una nueva amenaza, el mostrar publicidad al usuario o el lanzar ataques de denegación de servicio, entre otras.

Bucle. Conjunto de comandos u órdenes que un programa realiza de forma, en un número concreto y reiterado de ocasiones.

Buffer. Memoria intermedia utilizada para guardar temporalmente la información que se transfiere entre diferentes dispositivos informáticos (o entre los componentes de un mismo sistema informático).

Bug. Este término se emplea para indicar un fallo o error en un programa informático. Cuando uno de ellos tiene errores, se dice que tiene bugs.

Bus. Canal de comunicación entre los diferentes componentes de una computadora (señales de datos, de direcciones de control, etcétera).

Byte. Unidad que mide la cantidad de información, el tamaño y la capacidad de almacenamiento. Un byte equivale a 8 bits.

C

Cabecera (de un fichero). Parte de un fichero donde se guarda información sobre éste y su ubicación.

Caché. Pequeña sección correspondiente a la memoria de una computadora.

Cadena/Cadena de caracteres. Es una consecución de caracteres de texto, dígitos numéricos, signos de puntuación, caracteres especiales o espacios en blanco consecutivos.

Categoría/Tipo. No todos los virus son iguales. Éstos pueden ser agrupados por características concretas que conforman un tipo concreto de virus.

Cavity. Técnica utilizada por algunos virus y gusanos para dificultar su localización. Aplicando dicha técnica consiguen no variar el tamaño de cada uno de los ficheros infectados o afectados (utilizan solamente las cavidades del fichero afectado).

Chat/Chat IRC/Chat ICQ. Conversaciones escritas en internet, en tiempo real.

Cifrado/Autocrifrado. Técnica utilizada por algunos virus que se codifican a sí mismos (o parte de ellos), para tratar de evitar a los antivirus.

Cilindro. Sección de un disco que se puede leer por completo en una sola operación.

Clave del Registro de Windows. Secciones del Registro de Windows en las cuales se almacenan determinados valores correspondientes a la configuración de la computadora.

Cliente. Sistema informático (computadora) que solicita ciertos servicios y recursos de otra computadora (denominado servidor), al que está conectada en red.

Cluster. Varios sectores consecutivos de un disco.

CMOS (Complementary Metal Oxide Semiconductor). Sección de la memoria de una computadora en la que se guarda la información y los programas que permiten arrancar la computadora (BIOS).

Código. Contenido de los ficheros de un virus —código del virus, escrito en un determinado lenguaje de programación—. También hace referencia a los sistemas de representación de información. En sentido estricto, puede definirse como conjunto de normas sistemáticas que regulan unitariamente una materia determinada, o combinación de signos que tiene un determinado valor dentro de un sistema establecido.

Compañía/Virus de compañía/Spawning. Tipo de virus que no se incluye dentro de otros programas, sino que se asocia a ellos.

Comprimido/Comprimir/Compresión/Descomprimir. La compresión de ficheros es una operación por la que un fichero, o un grupo de ellos, se incluye dentro de otro que los contiene a todos, ocupando menos espacio.

Condición de activación (Trigger). Condiciones bajo las cuales un virus se activa o comienza a realizar sus acciones en la computadora infectada.

Constructor de virus. Programa malicioso que permite crear nuevos virus sin necesidad de tener conocimientos de programación, mediante una interfaz a través de la cual se eligen las características del malware creado, tipo, efectos, archivos que infectará, encriptación, polimorfismo, etcétera.

Contraseña. Cadena de caracteres con la que se restringe o permite el acceso, de ciertos usuarios, a un determinado lugar o fichero. El ejemplo más habitual es la contraseña de una tarjeta de crédito.

Control remoto. Acceso a la computadora de un usuario (con su consentimiento, o sin él), desde otra computadora que se encuentra en otro lugar. Dicho acceso puede suponer una amenaza, si no es realizado convenientemente, o con buenas intenciones.

Cookie. Fichero de texto que, en ocasiones, se envía a un usuario cuando éste visita una página web. Su objetivo es registrar la visita del usuario y guardar cierta información al respecto.

Cracker. Persona interesada en saltarse la seguridad de un sistema informático.

CRC (número o código CRC). Código numérico asociado de forma única a cada uno de los ficheros. Es como el número de pasaporte de dicho fichero.

Crimeware. Todo aquel programa, mensaje o documento utilizado para obtener beneficios económicos fraudulentamente, perjudicando al usuario afectado o a terceras partes de forma directa o indirecta.

CVP (Content Vectoring Protocol). Protocolo desarrollado en 1996 por Check Point que permite integrar una protección antivirus en un servidor firewall.

D

DdoS/Denegación de servicios distribuida. Ataque de Denegación de servicios (DoS) realizado al mismo tiempo desde varias computadoras contra un servidor.

Debug/Debugger/Desensamblaje. Herramienta informática con la que se puede leer el código fuente en el que están escritos los programas.

Derechos de administrador. Conjunto de acciones u operaciones que sólo uno o varios usuarios concretos pueden realizar dentro de una red de computadoras.

Descarga/Download. Acción por la cual se obtienen ficheros de internet (de páginas web o de lugares FTP dispuestos para este fin).

Desinfección. Acción que realizan los antivirus cuando detectan a un virus y lo eliminan.

Detección actualizada. Fecha en que se actualizó por última vez la detección de un malware dentro del Archivo de Identificadores de Virus.

Dialer. Programa que suele ser utilizado para redirigir, de forma maliciosa, las conexiones mientras se navega por internet. Su objetivo es colgar la conexión telefónica que se está utilizando en ese momento (la que permite el acceso a internet, mediante el marcado de un determinado número de teléfono) y establecer otra, marcando un número de teléfono de tarifa especial. Esto supondrá un notable aumento del importe en la factura telefónica.

Directorio/Carpeta. Divisiones, secciones (no físicas) mediante las cuales se estructura y organiza la información contenida en un disco. Los términos carpeta y directorio hacen referencia al mismo concepto. Pueden contener ficheros y otros directorios (subdirectorios o subcarpetas).

Directorio raíz. Carpeta o directorio principal (más importante) de un disco.

Disco de emergencia/Disco de rescate. Disquete que permite analizar la computadora sin utilizar el antivirus que se encuentra instalado en ella, sino con lo que se conoce como el antivirus en línea de comandos.

Disco de inicio, de sistema o de arranque. Disco (disquete, CD-ROM o disco duro) con el que es posible arrancar la computadora.

DNS (Sistema de Nombres de Dominio). Sistema que facilita la comunicación entre computadoras conectadas a una red (o a internet), su localización, etc., asignando nombres (cadenas de texto más comprensibles) a las direcciones IP de cada una de ellas.

Los servidores DNS son las computadoras en las que se relacionan, administran y gestionan todos esos nombres (de dominio) y se relacionan con sus correspondientes direcciones IP.

DoS/Denegación de servicios. Ataque causado en ocasiones por los virus que evita al usuario la utilización de ciertos servicios (del sistema operativo, de servidores web, etcétera).

Driver/Controlador. Programa, conocido como controlador, que permite la gestión de los dispositivos conectados a la computadora (generalmente, periféricos como impresoras, unidades de CD-ROM, etcétera).

Dropper. Fichero ejecutable que contiene varios tipos de virus en su interior.

E

EICAR. European Institute of Computer Anti-Virus Research. Institución informática que ha creado un método para evaluar la fiabilidad y el comportamiento de los antivirus, el test EICAR.

Elementos eliminados. Carpeta existente en los programas de correo electrónico que contiene todos los mensajes que se han borrado o eliminado (los que no se han borrado de manera definitiva). En el caso de borrar el mensaje de un virus, es conveniente acceder a esta carpeta y eliminarlo también en ella.

Elementos enviados. Carpeta existente en los programas de correo electrónico, que contiene todos los mensajes que se han enviado a otros destinatarios.

ELF —ficheros— (Executable and Linking Format). Ficheros ejecutables (programas), propios del sistema operativo Unix/Linux.

Empaquetar. Operación por la cual un grupo de ficheros (o uno solo) se incluyen dentro de otro fichero, ocupando así menos espacio. El empaquetado es similar a la compresión de ficheros, pero es más común llamarlo así en sistemas Unix/Lunix.

La diferencia entre empaquetado y compresión es la herramienta con que se realiza la operación. Por ejemplo, la herramienta tar se utiliza para empaquetar, mientras que la herramienta zip o gzip —WinZip— se utiliza para comprimir.

En circulación. Se dice que un virus está en circulación cuando se están realizando detecciones de él, en cualquier parte del mundo, durante un periodo.

EPO (Entry Point Obscuring). Técnica para infectar programas mediante la cual un virus intenta ocultar su punto de entrada para evitar ser detectado. El virus, en lugar de tomar el control y realizar sus acciones al principio del programa (de su utilización o ejecución), permite el correcto funcionamiento de éste hasta un cierto momento en el que comienza a actuar.

Escanear —puertos, direcciones IP—. Acción por la cual se chequean los puertos de comunicaciones y/o las direcciones IP de una computadora, para localizarlos y obtener información sobre su estado. En ocasiones, puede considerarse un ataque o amenaza.

Escritorio de Windows. Área principal de Windows que aparece al arrancar la computadora. Desde ella se accede a todas las herramientas, utilidades y programas instalados en la computadora, mediante iconos de acceso directo, opciones de menú existentes en el botón Inicio de Windows, la Barra de tareas de Windows, etcétera.

Estación/Puesto/Workstation. Es una de las computadoras conectada a una red local que utiliza los servicios y los recursos existentes en dicha red. Por lo general, no presta servicios al resto de computadoras de la red como lo hacen los servidores.

Estadísticas. Un malware tiene estadísticas asociadas cuando su porcentaje de infección está entre los 50 malware más activos.

Estafa o timo (scam). Fraude destinado a conseguir que una persona o grupo de personas entreguen dinero bajo falsas promesas de beneficios económicos (viajes, vacaciones, premios de lotería, etcétera).

Excepciones. Técnica utilizada por los antivirus para la detección de virus.

Exploit. Técnica o programa que aprovecha un fallo o hueco de seguridad —una vunerabilidad— existente en un determinado protocolo de comunicaciones, sistema operativo o herramienta informática.

Explorador de Windows. Programa o aplicación disponible en Windows que permite gestionar los ficheros disponibles en la computadora. Es de gran utilidad para visualizar estructuras de directorios de forma organizada.

Extensión. Ficheros que se representan asignándoles un nombre y una extensión, separados entre sí por un punto. NOMBRE.EXTENSIÓN. El fichero puede tener cualquier NOMBRE, pero la EXTENSIÓN (si existe) tendrá como máximo 3 caracteres. Dicha extensión es la que indica el formato o tipo de fichero (texto, documento de Word, imagen, sonido, base de datos, programa, etcétera).

F

Familia/Grupo. Existen virus con nombres muy parecidos y características similares, incluso idénticas. Estos grupos de virus, que tienen hermanos, conforman lo que se denomina una familia de virus. Cada uno de ellos, en lugar de denominarse hermanos, se llaman variantes de la familia o del virus original (el que apareció primero, el padre).

FAT (File Allocation Table). Sección de un disco en la que se define la estructura y las secciones del citado disco. Además en ella se guardan las direcciones para acceder a los ficheros que el disco contiene.

Fecha de aparición. Fecha en la que se tuvo la primera noticia de la existencia de un virus concreto.

Fecha de detección. Fecha en la que se incluyó la detección de un determinado malware dentro del Archivo de Identificadores de Virus.

Fichero/Archivo/Documento. Información que se encuentra en un soporte de almacenamiento informático, textos, documentos, imágenes, bases de datos, ficheros de sonido, hojas de cálculo, etc. Se identifica por un nombre, un punto y una extensión (indica de qué tipo es el fichero).

Ficheros de proceso por lotes (Batch). Ficheros que tienen extensión BAT y que permiten automatizar operaciones.

Ficheros SCR. Este tipo de ficheros tienen extensión SCR y pueden ser salvapantallas de Windows o ficheros cuyo contenido es lenguaje Script.

Firewall/Cortafuegos. Su traducción literal es muro de fuego, también conocido a nivel técnico como cortafuegos. Es una barrera o protección que permite a un sistema salvaguardar la información al acceder a otras redes, como por ejemplo internet.

FireWire. Tipo de canal de comunicaciones externo caracterizado por su elevada velocidad de transferencia, empleado para conectar computadoras y periféricos a otra computadora.

Firma/Identificador. Se trata del número de pasaporte de un virus. Es decir, una cadena de caracteres (números, letras, etc.) que representa de forma inequívoca a un virus.

Flooder. Programa que envía el mismo mensaje o texto de manera reiterada y masiva, pretendiendo así producir un efecto de saturación, colapso o inundación (de ahí su nombre, inundador) en sistemas de correo como MSN Messenger.

Formateo/Formatear. Dar formato a una unidad de disco, eliminando todo su contenido.

Freeware. Es todo aquel software, legalmente distribuido, de forma gratuita.

FTP (File Transfer Protocol). Es un mecanismo que permite la transferencia de ficheros a través de una conexión TCP/IP.

G

Gateway. Computadora que permite las comunicaciones entre distintos tipos de plataformas, redes, computadoras o programas. Para lograrlo traduce los distintos protocolos de comunicaciones que éstos utilizan. Es lo que se conoce como pasarela o puerta de acceso.

GDI (Graphics Device Interface). Sistema (Interfaz de Dispositivos para Gráficos,) que permite al sistema operativo Windows mostrar presentaciones en pantalla y en las impresoras.

Groupware. Sistema que permite a los usuarios de una red local (LAN) la utilización de todos los recursos de ésta como programas compartidos, accesos a internet, intranet y a otras áreas, correo electrónico, firewalls, proxys, etcétera.

Grupo de noticias. Uno de los servicios de internet, mediante el cual varias personas se conectan para discutir e intercambiar información sobre temas concretos de interés común.

Gusano (Worm). Programa similar a un virus que, a diferencia de éste, solamente realiza copias de sí mismo, o de partes de él.

H

Hacker. Persona que accede a una computadora de forma no autorizada e ilegal.

Hardware. Término que hace referencia a cada uno de los elementos físicos de un sistema informático (pantalla, teclado, ratón, memoria, discos duros, microprocesador, etcétera).

Herramienta de hacking. Programa que puede ser utilizado por un hacker para causar perjuicios a los usuarios de una computadora (pudiendo provocar el control de la computadora afectada, obtención de información confidencial, chequeo de puertos de comunicaciones, etcétera).

Hijacker. Literalmente, secuestrador. Cualquier programa que cambia la configuración del navegador, para hacer que su página de inicio, búsqueda, etc., apunte a otro sitio distinto del indicado por el usuario.

Hoax. No es un virus, sino falsos mensajes de alarma (bromas o engaños) sobre virus que no existen.

Host. Este término se refiere a una computadora que actúa como fuente de información.

HTTP (HyperText Transfer Protocol). Sistema de comunicación que permite la visualización de páginas web desde un navegador.

I

IFS (Instalable File System). Sistema que se encarga de gestionar las transferencias de información de entrada y de salida, correspondientes a un grupo de dispositivos informáticos (de la red o de otras redes) y ficheros.

IIS (Internet Information Server). Servidor de Microsoft (Internet Information Server), destinado a la publicación, mantenimiento y gestión de páginas y portales web.

IMAP (Internet Message Access Protocol). Sistema de comunicación que permite el acceso a los mensajes de correo electrónico.

In The Wild. Lista oficial en la que se enumeran mensualmente los virus que más incidencias han ocasionado (los más extendidos).

Índice de peligrosidad. Valor calculado que permite medir lo peligroso que puede llegar a ser un virus.

Infección. Acción que realizan los virus, consistente en introducirse en la computadora o en áreas concretas de ésta y en determinados ficheros.

Interfaz/Interface. Es el sistema que permite a los usuarios dialogar (comunicarse e interactuar) con la computadora y el software que éste tiene instalado. A su vez, este software (programas) se comunica mediante un sistema de interfaz con el hardware de la computadora.

Interrupción. Señal mediante la cual se consigue hacer una pausa momentánea en las labores que lleva a cabo el cerebro de la computadora (el microprocesador).

IP (Internet Protocol)/TCP-IP. La IP es la dirección o código que identifica exclusivamente a cada una de las computadoras existentes. El protocolo TCP/IP es el sistema utilizado para la interconexión de dichas computadoras, sin provocar conflictos de direcciones. Se utiliza en internet.

IRC (Chat IRC). Son conversaciones escritas a través de internet (en las que además pueden transferirse ficheros), conocidas vulgarmente como chat.

ISP (Internet Service Provider). Proveedor de acceso a internet que además ofrece una serie de servicios relacionados con internet (Proveedor de Servicios Internet).

J

Java. Lenguaje de programación que permite generar programas independientes de la plataforma, es decir, que pueden ejecutarse en cualquier sistema operativo o hardware (lenguaje multiplataforma).

JavaScript. Lenguaje de programación que aporta características dinámicas (datos variables en función del tiempo y el modo de acceso, interactividad con el usuario, personalización, etc.) a las páginas web escritas en lenguaje HTML.

Joke. No es un virus, sino bromas de mal gusto que tienen por objeto hacer pensar a los usuarios que han sido afectados por un virus.

K

Kernel. Núcleo, parte más importante o centro del sistema operativo.

Keylogger (Capturador de teclado). Programa que recoge y guarda una lista de todas las teclas pulsadas por un usuario. Dicho programa puede hacer pública la lista, permitiendo que terceras personas conozcan estos datos: lo que ha escrito el usuario afectado (información introducida por teclado, contraseñas, texto escrito en documentos, mensajes de correo, combinaciones de teclas, etcétera).

L

Ladrón de contraseñas. Programa que obtiene y guarda datos confidenciales, como las contraseñas de acceso de un usuario (utilizando keyloggers u otros medios). Dicho programa puede hacer pública esta información, permitiendo que terceras personas puedan utilizarla en perjuicio del usuario afectado.

LAN (Local Area Network). Red de área local o grupo de computadoras conectadas entre sí dentro de una zona geográfica pequeña (generalmente en una misma ciudad, población o edificio).

Lenguaje de programación. Conjunto de instrucciones, órdenes, comandos y reglas que permite la creación de programas.

Las computadoras entienden señales eléctricas (valores 0 o 1). Los lenguajes permiten al programador indicar lo que debe hacer un programa, sin tener que escribir largas cadenas de ceros y unos, sino palabras (instrucciones) más comprensibles por las personas.

Librería de enlace dinámico (DLL). Tipo especial de fichero, con extensión DLL.

Libreta de direcciones. Fichero con extensión WAB donde se almacenan datos de contacto de otros usuarios, como la dirección de correo electrónico (entre otros).

Lista de tareas. Relación —listado— de todos los programas y procesos que se encuentran activos (en funcionamiento), en un determinado momento (generalmente en el sistema operativo Windows).

M

Macro. Secuencia de instrucciones u operaciones que definimos para que un programa (por ejemplo, Word, Excel, PowerPoint o Access) las realice de forma automática y secuencial. Por ser programas pueden verse afectadas por los virus. Los virus que utilizan las macros para realizar infecciones se denominan virus de macro.

Malware. Cualquier programa, documento o mensaje, susceptible de causar perjuicios a los usuarios de sistemas informáticos. MALicious softWARE.

Mapeo/Mapear/Mapeada. Acción por la cual se asigna una letra a una unidad de disco, que se encuentra compartida en una red de computadoras, como si se tratase de un disco más de la computadora.

MAPI. Messaging Application Program Interface. Sistema empleado para que los programas puedan enviar y recibir correo electrónico mediante un sistema de mensajería concreto.

Máscara (de red o de dirección). Número —de 32 bits— que identifica la dirección IP de una red concreta. Esto permite que el protocolo de comunicaciones conocido como TCP/IP pueda saber si una dirección IP asociada a una computadora pertenece a una red o a otra.

Menú contextual. Listado de definiciones que se pueden seleccionar cuando se pulsa con el botón secundario del ratón (generalmente el derecho) sobre un determinado elemento o área de la ventana de un programa. Dichas opciones suelen estar escogidas dentro de un contexto, es decir, seleccionadas para acceder directamente a determinadas áreas del programa.

Método de infección. Es una de las características más importantes de un virus. Se trata de cada una de las operaciones que el virus realiza para llevar a cabo su infección en la computadora afectada.

Método de propagación. Es una de las características más importantes de un virus. Se trata de cada una de las operaciones que el virus realiza para transmitirse a otras computadoras.

Microprocesador/Procesador. Corazón electrónico e integrado de una computadora o sistema informático, popularmente conocido como Pentium (I, II, III, IV,...), 486, 386, etcétera.

Se trata del chip (pastilla o circuito integrado —CI— de silicio, con elementos electrónicos microscópicos —transistores, resistencias etc.—) que gobierna todas y cada una de las operaciones que se realizan en el sistema.

MIME (Multipurpose Internet Mail Extensions). Extensiones Multipropósito del Correo Internet. Es el conjunto de especificaciones que permite intércambiar texto y ficheros con juegos de caracteres diferentes (entre computadoras con idiomas diferentes, por ejemplo).

Módem. Elemento físico (un periférico), también conocido como MOdulador DEMmodulador, que se utiliza para convertir las señales eléctricas (analógicas y digitales). Su objetivo es facilitar la comunicación entre computadoras y otros tipos de equipos. Su utilidad más habitual, en la actualidad, es conectar las computadoras a internet.

Módulo. En términos informáticos, consiste en el conjunto o agrupación de macros existentes dentro de un documento de Word, o una hoja de cálculo de Excel, etcétera.

MSDE (Microsoft Desktop Engine). Servidor para el almacenamiento de datos, compatible con SQL Server 2000.

MS-DOS (Disk Operating System). Sistema operativo, anterior a Windows, en el que se trabaja escribiendo órdenes para todas las operaciones que se desean realizar.

MTA (Message Transfer Agent). Sistema organizado de correo electrónico que se encarga de recibir los mensajes desde diversos lugares y distribuirlos entre los usuarios. Los MTA también transfieren los mensajes a otros servidores de correo. Exchange, sendmail, qmail y Postfix son ejemplos de MTA.

Multipartite. Propiedad que caracteriza a determinados virus avanzados. Éstos realizan infecciones utilizando combinaciones de técnicas de infección que otros tipos de virus emplean en exclusiva.

Mutex. Técnica utilizada por algunos virus (un mutex) para controlar el acceso a recursos (programas u otros virus) y evitar que más de un proceso utilice el mismo recurso al mismo tiempo.

Esto dificulta la detección por parte de los antivirus. Los virus que utilizan mutex pueden incluir otros virus en su interior, al igual que lo hacen otros tipos de virus como, por ejemplo, los polimórficos.

N

Navegador. Un navegador web o navegador de internet es el programa que permite visualizar los contenidos de las páginas web en internet. También se

conoce con el nombre de browser. Algunos ejemplos de navegadores web o browsers son: Internet Explorer, Netscape Navigator, Opera, etcétera.

Nivel de daños/Daño potencial/Perjuicio. Valor que indica el grado de efectos que el virus puede producir en una computadora afectada. Este dato se emplea para el cálculo del Índice de peligrosidad.

Nivel de propagación/Nivel de distribución. Valor que indica qué tan rápido se puede extender o se ha extendido el virus por todo el mundo. Este dato se emplea para el cálculo del Índice de peligrosidad.

Nombre común. Nombre por el que se conoce vulgarmente a un virus.

Nombre técnico. Nombre real de un virus, utilizado, además, para indicar su tipo o clase.

Nuke (ataque). Caída o pérdida de la conexión de red, provocada de forma intencionada por alguna persona. La computadora sobre la que se realiza un nuke, además puede quedar bloqueada.

Nuker. Persona o programa que realiza una operación de nuke, provocando el bloqueo de una computadora o impidiendo que ésta pueda acceder a la red donde está conectada.

O

Objeto OLE (Object Linking and Embedding). Estándar que permite la incrustación y vinculación de objetos (imágenes, clips de video, sonido MIDI, animaciones, etc.) dentro de ficheros (documentos, bases de datos, hojas de cálculo, etc.). También hace posible la inclusión de controles ActiveX y la comunicación entre ellos.

Ocultamiento/Ocultación / Stealth. Técnica utilizada por algunos virus para intentar pasar desapercibidos ante los ojos del usuario afectado y de algunos antivirus (de forma temporal).

P

P2P (Peer to peer). Programas —o conexiones de red— empleados para prestar servicios a través de internet (intercambio de ficheros, generalmente), que los virus y otros tipos de amenazas utilizan para distribuirse. Algunos ejemplos de estos programas son KaZaA, Emule, eDonkey, etcétera.

País de origen. Indica el país o zona geográfica en la que apareció o se tuvo constancia de la existencia de un virus, por primera vez.

Papelera de reciclaje. Sección o carpeta del disco duro en la que se guardan los ficheros que se han borrado (siempre que no se hayan eliminado definitivamente).

Parámetro. Dato variable que indica a un programa informático cómo debe comportarse en cada situación.

Parche de seguridad. Conjunto de ficheros adicionales al software original de una herramienta o programa informático, que sirven para solucionar sus posibles carencias, vulnerabilidades o defectos de funcionamiento.

Partición. Una de las áreas en las que se puede dividir el disco duro de una computadora para que el sistema operativo pueda reconocerla como si se tratara de

otro disco duro. Cada partición de un disco duro puede contener un sistema operativo diferente.

Payload. Efectos producidos por un virus.

PDA (Personal Digital Assistant). Computadora portátil de tamaño muy reducido (de bolsillo), que tiene su propio sistema operativo, lleva programas instalados y permite intercambiar información con computadoras convencionales, internet, etc. Algunas de las más conocidas son Palm y PocketPC entre otras.

PE (Portable ejecutable). El término PE (Portable ejecutable) hace referencia al formato de ciertos programas.

Phishing. Consiste en el envío masivo de mensajes que, aparentando provenir de fuentes fiables, intentan conseguir que el usuario proporcione datos confidenciales. El caso más típico de phishing es el envío de correos electrónicos que se hacen pasar por procedentes de una entidad bancaria online, para conseguir que el usuario introduzca sus contraseñas en una página web falseada.

Pista. Sección circular existente en cualquier tipo de disco de almacenamiento informático.

Plantilla/Plantilla global. Fichero que determina las características iniciales que debe tener un documento, antes de comenzar a trabajar con él.

Plataforma. Hace referencia a un sistema operativo, que funciona en equipos informáticos concretos y bajo unas determinadas condiciones (tipos de programas instalados, etcétera).

Plugin. Equipo o programa que añade nuevas funciones a un determinado sistema ya existente.

Polimórfico/Polimorfismo. Técnica que utilizan algunos virus para cifrar (codificar) su firma de forma diferente en cada ocasión y además las instrucciones para realizar dicho cifrado.

Política de privacidad. Documento que especifica los procedimientos, reglas y prácticas de seguridad de datos que realiza una empresa, con las que garantiza el mantenimiento de la integridad, confidencialidad y disponibilidad de la información que recoge de sus clientes y de otros interesados titulares de datos, de conformidad con la legislación vigente, las necesidades de seguridad informática y objetivos de negocio que persiga.

POP (Post Office Protocol). Protocolo para recibir y obtener los mensajes de correo electrónico.

Prepending. Técnica para infectar ficheros que incluye el código de un virus al principio del fichero infectado. Esto asegura la activación del virus cuando se utiliza o abre el fichero afectado.

Programa. Elementos que permiten realizar operaciones concretas de forma automática (generalmente ficheros con extensión EXE o COM).

Programa espía. Programas que recopilan datos sobre los hábitos de navegación, preferencias y gustos del usuario. Dichos datos son transmitidos a los propios fabricantes o a terceros, cabiendo la posibilidad de que sean almacenados de alguna manera para ser posteriormente recuperados. El Spyware puede ser

instalado en el sistema por numerosas vías, a veces sin que medie consentimiento expreso del usuario, así como con su conocimiento o falta del mismo respecto a la recopilación y/o uso de los datos ya mencionados. El spyware puede ser instalado con el consentimiento del usuario y su plena conciencia, pero en ocasiones no es así. Lo mismo ocurre con el conocimiento de la recogida de datos y la forma en que son posteriormente utilizados.

Programa potencialmente no deseado (PUP). Programa que se instala sin el consentimiento consciente del usuario y realiza acciones o tiene características que pueden menoscabar el control del usuario sobre su privacidad, confidencialidad, uso de recursos de la computadora, etcétera.

Protección contra escritura. Técnica mediante la cual se permite la lectura del contenido de un disco u otros dispositivos de almacenamiento, pero se impide la escritura de contenido en él (por ejemplo, guardar ficheros).

Protección permanente. Análisis continuo que algunos antivirus realizan sobre todos los ficheros que intervienen en cualquier tipo de operación (realizada por el usuario o por el propio sistema operativo). También es conocido como centinela o residente.

Protección proactiva. Capacidad de proteger la computadora de malware desconocido basándose en su comportamiento, y sin necesidad de disponer de un archivo de identificadores de virus que deba ser periódicamente actualizado.

Protocolo. Sistema, reglas y conjunto de normas que establece, gobierna y permite la comunicación entre dispositivos informáticos (la transferencia de datos).

Proxy. Servidor proxy actúa como un intermediario entre una red interna (por ejemplo, una intranet) y una conexión externa a internet. De esta forma, se puede compartir una conexión para recibir ficheros desde servidores web.

Puerto de comunicaciones/Puerto. Punto de acceso a una computadora o medio a través del cual tienen lugar las transferencias de información (entradas/salidas), de la computadora con el exterior y viceversa (vía TCP/IP).

R

RAM (Random Access Memory). Memoria principal de la computadora donde se colocan todos los ficheros cuando se utilizan y todos los programas cuando se ejecutan.

RDSI (Red Digital de Servicios Integrados). Uno de los tipos de conexiones de red, utilizados para la transmisión digital de cualquier tipo de información (datos, voz, imágenes, etcétera).

Red. Grupo de computadoras o dispositivos informáticos conectados entre sí a través de cable, línea telefónica, ondas electromagnéticas (microondas, satélite, etc.), con la finalidad de comunicarse y compartir recursos entre ellos. Internet es una inmensa red a la cual están conectadas otras subredes y a la cual también se conectan millones de computadoras.

Redireccionar. Acceder a una determinada dirección mediante otra.

Referencia/Salto/Link/Hiperenlace. Estos términos hacen referencia al mismo concepto. Se trata de elementos o secciones dentro de una página web (texto,

imágenes botones, etc.), que permiten el acceso a otra página o área dentro de la misma página, cuando se hace clic sobre ellos.

Registro de Windows (Registry). Fichero que almacena todos los valores de configuración e instalación de los programas que se encuentran instalados y de la propia definición del sistema operativo Windows.

Registro Online. Sistema mediante el cual se permite la inscripción (o registro) a través de internet, como usuario de un determinado producto y/o servicio (en este caso, un programa y sus servicios asociados). Para realizar un registro, es necesario contar con un código de activación o de registro, facilitado previamente por el fabricante del programa. Después de registrarse, se podrá utilizar dicho programa y los servicios que incluye, mediante un nombre de usuario y contraseña (facilitados por el fabricante).

Reinicio. Acción por la cual la computadora se apaga momentáneamente y se vuelve a encender de inmediato.

Renombrar. Acción por la cual se da un nuevo nombre a un fichero, directorio u otro elemento del sistema informático.

Réplica. Entre otras acepciones, se trata de la acción por la cual los virus se propagan o hacen copias de sí mismos, con el único objetivo de realizar posteriores infecciones.

Residente/Virus residente. Se denomina fichero o programa residente a todo aquel fichero que se coloca en la memoria de la computadora, de forma permanente, controlando las operaciones realizadas en el sistema.

Riesgo de seguridad. Todo aquello que puede ser utilizado con fines malintencionados para causar perjuicios a los usuarios de una computadora. Por ejemplo, un programa dedicado a crear virus o troyanos.

Ring. Sistema de estados correspondiente a los niveles de privilegio sobre las operaciones que se pueden realizar en el microprocesador, su protección y funcionamiento. Existen varios niveles. Ring0 (administrador), Ring1 y Ring2 (administrador con menos privilegios), Ring3 (usuario).

Robo de identidad. Obtención de información confidencial del usuario, como contraseñas de acceso a diferentes servicios, con el fin de que personas no autorizadas puedan utilizarla para suplantar al usuario afectado.

ROM (Read Only Memory). Tipo de memoria en la que no se puede escribir de forma normal, pero que mantiene su contenido de forma permanente (éste no se borra si desaparece la alimentación eléctrica).

Rootkit. Programa diseñado para ocultar objetos como procesos, archivos o entradas del Registro de Windows (incluyendo los propios normalmente). Este tipo de software no es malicioso en sí mismo, pero es utilizado por los piratas informáticos para esconder evidencias y utilidades en los sistemas previamente comprometidos. Existen ejemplares de malware que emplean rootkits con la finalidad de ocultar su presencia en el sistema en el que se instalan.

Rutina. Secuencia invariable de instrucciones, que forma parte de un programa y se puede utilizar repetidamente.

S

Salvapantallas/Protector de pantalla. Programa que muestra animaciones en la pantalla de la computadora. Su objetivo es que la imagen de la pantalla

no quede fija —por ejemplo, cuando la computadora lleva un rato sin utilizarse—, para evitar que ésta se queme. Actualmente son utilizados más por razones estéticas o incluso de seguridad.

Script/Virus de Script. Término que hace referencia a todos aquellos ficheros o secciones de código escritas en algún lenguaje de programación, como Visual Basic Script (VBScript), JavaScript, etcétera.

Sector. Sección de un disco de almacenamiento informático.

Servicio. Conjunto de prestaciones que una computadora o sistema informático facilita a otros sistemas informáticos o a otras computadoras que están conectadas a ella.

Servicios del sistema. Son aplicaciones que normalmente se inician de manera autónoma al poner en marcha el sistema y se cierran, también de manera autónoma, al cerrar el sistema. Los servicios del sistema llevan a cabo tareas fundamentales como, por ejemplo, mantener en funcionamiento el servidor SQL o el detector de servicios Plug&Play.

Servidor. Sistema informático (computadora) que presta ciertos servicios y recursos (de comunicación, aplicaciones, ficheros, etc.) a otras computadoras (denominadas clientes), las cuales están conectadas en red a ella.

Shareware. Versiones de evaluación de un producto software, de uso gratuito, que sirven básicamente para probar el producto antes de adquirirlo de manera definitiva.

Síntomas de infección. Cada una de las acciones o efectos que un virus puede realizar cuando ha producido su infección y además las condiciones de activación (si éste cuenta con ellas).

Sistema operativo (S.O.). Conjunto de programas y ficheros que permiten la utilización de la computadora.

SMTP (Simple Mail Transfer Protocol). Protocolo que se utiliza en internet para el envío (exclusivamente) de correo electrónico.

Sobrepasamiento/Tunneling. Técnica que utilizan algunos virus para impedir la protección antivirus.

Sobrescritura. Acción por la cual un determinado programa o un virus escribe encima del contenido de un fichero, haciendo que se pierda su contenido original y que éste ya no se pueda recuperar.

Software. Ficheros, programas, aplicaciones y sistemas operativos que nos permiten trabajar con la computadora o sistema informático. Se trata de los elementos que hacen funcionar al hardware.

Spam. Correo electrónico no solicitado, normalmente con contenido publicitario, que se envía de forma masiva. Este tipo de mensajes pueden causar graves molestias y provocar pérdidas de tiempo y recursos.

Spammer. Programa que permite el envío masivo de mensajes de correo electrónico con contenido publicitario y la consiguiente recepción masiva de éstos. Puede ser también empleado para el envío masivo de amenazas tales como gusanos y troyanos.

Spear phishing. Utiliza las técnicas del phishing pero se trata de un ataque dirigido lanzado contra un objetivo concreto. El autor que origina este tipo de ataque nunca recurrirá al spam para conseguir una avalancha masiva de datos personales de los usuarios. El hecho de que sea dirigido y no masivo implica

una más rigurosa elaboración para lograr mayor credibilidad, y la utilización más sofisticada de ingeniería social.

SQL (Structured Query Language). Lenguaje de Consulta Estructurado. Es un lenguaje de programación estándar, destinado a la gestión, administración y comunicación de bases de datos, muy utilizado en la web (por ejemplo, Microsoft SQL Server, MySQL, etcétera).

Subtipo. Cada uno de los subgrupos en los que se divide un tipo. En este caso, grupo de virus o amenazas con características y/o comportamientos comunes, incluida dentro de un tipo o categoría.

T

Tabla de particiones. Área de un disco que contiene información correspondiente a cada una de las secciones o áreas —particiones— en las que está dividido éste.

Terminador de procesos. Programa que finaliza las acciones o procesos que se encuentren en funcionamiento (activos) en una computadora, pudiendo provocar riesgos de seguridad.

Trackware. Es todo programa que realiza el seguimiento de las acciones que realiza el usuario mientras navega por internet (páginas visitadas, banners que pulsa, etc.) y crea un perfil que utiliza con fines publicitarios.

Troyano bancario. Programa malicioso, que utilizando diversas técnicas, roba información confidencial a los clientes de banca y/o plataformas de pago online.

Troyano/Caballo de Troya. En sentido estricto, un troyano no es un virus, aunque se considere como tal. Realmente se trata de un programa que llega de manera encubierta a la computadora, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario afectado. La historia mitológica El Caballo de Troya ha inspirado su nombre.

TSR (Terminate and Stay Resident). Característica que permite a determinados programas permanecer en memoria, después de haberse ejecutado.

U

UPX (Ultimate Packer for eXecutables). Herramienta de compresión de ficheros que además permite ejecutar los programas que están comprimidos con dicha utilidad, sin necesidad de descomprimirlos.

URL (Uniform Resource Locator). Dirección a través de la cual se accede a las páginas web en internet (o a otras computadoras).

V

Vacunación. Técnica antivirus que permite almacenar información sobre los ficheros, con el fin de detectar posibles infecciones de éstos, posteriormente.

Variante. Versión modificada de un virus original, que puede infectar de forma similar o distinta y realizar las mismas acciones u otras.

Vector de interrupciones. Técnica utilizada para que una computadora gestione correctamente las interrupciones que se solicitan al microprocesador. Así se facilita al microprocesador la dirección de memoria a la que debe acceder para dar servicio a dicha interrupción.

Ventana emergente. Ventana que aparece repentinamente, por regla general, cuando el usuario selecciona una opción con su ratón o pulsa una tecla de función especial.

Virus. Programas que se pueden introducir en las computadoras y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.

Virus de boot. Virus que afecta al sector de arranque de los discos de almacenamiento.

Virus de enlace. Tipo de virus que modifica la dirección donde se almacena un fichero, sustituyéndola por la dirección donde se encuentra un virus (en lugar del fichero original). Esto provoca la activación del virus cuando se utiliza el fichero afectado.

Después de producirse la infección, es imposible trabajar con el fichero original.

Virus de macro. Virus que afecta a las macros contenidas en documentos de Word, hojas de cálculo de Excel, presentaciones de PowerPoint, etcétera.

Vista previa. Característica por la cual los programas de correo electrónico permiten visualizar el contenido de los mensajes, sin necesidad de abrirlos.

Volumen. Partición de un disco duro, o una referencia a un disco duro completo. Este término se emplea mucho en las redes de computadoras donde existen unidades de disco compartidas.

Vulnerabilidades. Fallos o huecos de seguridad detectados en algún programa o sistema informático que los virus utilizan para propagarse e infectar.

W

WAN (Wide Area Network). Red de área extensa, o grupo de computadoras conectadas entre sí, pero distantes geográficamente. La conexión se realiza mediante línea telefónica, radioenlaces o vía satélite).

WINS (Windows Internet Name Service). Servicio que gestiona los nombres asociados a las computadoras de una red y, por tanto, el acceso y la posibilidad de trabajar con cada una de ellas. Una computadora contiene la base de datos con las direcciones en formato IP (por ejemplo, 125.15.0.32) y los nombres comunes asignados a cada computadora de la red (por ejemplo, SERVIDOR1).

WSH (Windows Scripting Host). Sistema que permite el funcionamiento de ficheros de proceso por lotes y el acceso a funciones de Windows, mediante lenguajes de programación como Visual Basic Script y Java Script (lenguajes de script).

X

XOR (OR-Exclusive). Operación que muchos virus utilizan para cifrar su contenido.

Z

Zip. Formato correspondiente a los ficheros comprimidos con la herramienta WinZip.

Zombie. Computadora controlada mediante la utilización de bots.

Zoo (virus de zoo). Virus que no están extendidos y que solamente se pueden encontrar en determinados lugares, como laboratorios, donde son analizados para conocer mejor sus características y las técnicas que emplean.

Fuentes consultables recientes fundamentalmente en castellano referidas al derecho informático

1. Davara Rodríguez, Miguel Ángel, *Anuario de derecho de las tecnologías de la información y las comunicaciones* (TIC), 2006 (trabajos doctrinales especializados, boletines de actualidad, reseñas de interés jurídico, glosario de términos, preguntas más frecuentes, normativa jurisprudencia y otras informaciones de interés), Fundación Vodafone y Davara & Davara Asesores Jurídicos, Madrid, 2006.
2. _____, *Guía práctica de protección de datos para abogados*, DaFeMa, Madrid, 2004.
3. _____, *La protección de datos personales en el sector de las telecomunicaciones*, Fundación Airtel, Universidad Pontificia Comillas de Madrid y Davara & Davara Asesores Jurídicos, Madrid, 2000.
4. _____, *La seguridad en las transacciones electrónicas: la firma electrónica*, Fundación Vodafone, Univesidad Pontificia Comillas de Madrid y Davara & Davara Asesores Jurídicos, Madrid, 2005.
5. _____, *La transposición de la directiva sobre la privacidad y las comunicaciones electrónicas*, Fundación Vodafone, Universidad Pontificia Comillas de Madrid y Davara & Davara Asesores Jurídicos, Madrid, 2004.
6. _____, *Manual de derecho informático*, Aranzadi, 7a. ed., 2005.
7. Del Peso Navarro, Emilio, *Servicios de la sociedad de la información* (Comercio electrónico y protección de datos), Ediciones Díaz de Santos, Madrid, 2004.
8. _____, Miguel Ángel Ramos González y Margarita del Peso Ruiz, *El documento de seguridad* (Análisis técnico y jurídico. Modelo), Ediciones Díaz de Santos, Madrid, 2004.
9. _____, Miguel Ángel Ramos González, Margarita del Peso Ruiz, *Nuevo Reglamento de Protección de Datos de Carácter Personal* (Medidas de seguridad), Ediciones Díaz de Santos, Madrid, 2008.
10. Fernández Rodríguez, José Julio, *Defensa e Internet,* Actas del I Congreso sobre Seguridad, Defensa e Internet, Universidad Santiago de Compostela, Santiago de Compostela, marzo 2004.
11. _____, *Gobierno Electrónico. Un desafío en Internet* (Implicaciones jurídicas), Fundación Universitaria de Derecho, Administración y Política, S.C., 2004.

12. Fernández Rodríguez, José Julio, *Lo público y lo privado en Internet* (Intimidad y libertad de expresión en la Red), Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, Serie doctrina jurídica núm. 154, México, 2004.
13. _____, Joseph Maria Reniu I. Vilamala, Jordi Barrat I Esteve y Rosa María Fernández Rivera, *Voto electrónico*, Estudio comparado en una aproximación jurídico-política (desafíos y posibilidades), Fundación Universitaria de Derecho, Administración y Política, S.C., Instituto Electoral y de Participación Ciudadana de Coahuila e Instituto Electoral de Querétaro, 2007.
14. Delpiazzo E., Carlos y María José Viega, *Lecciones de Derecho Telemático*, Fundación de Cultura Universitaria, Uruguay, Montevideo, 2004.
15. Grün Ernesto, *Una visión sistémica y cibernética del derecho en el mundo globalizado del siglo XXI*, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, Serie doctrina jurídica núm. 98, México, 2006, 1a. ed., Buenos Aires, 2006.

Clásicos

16. Bell, Daniel, *El Advenimiento de la Sociedad Post-Industrial*, Alianza, Madrid, 2001.
17. Castells, Manuel, *La Galaxia Internet*, Plaza & Janés, Madrid, 2001.
18. Lessig, Lawrence, *Code version 2.0*, Basic Books, Nueva York, 2006.
19. Masuda Yoneji, *La Sociedad Informatizada como Sociedad Post-Industrial*, Tecnos, Madrid, 1984.
20. McLuhan, Marshall, *La Galaxia Gutenberg. Génesis del homo typographicus*, Círculo de Lectores, Barcelona, 1998.
21. McLuhan, Marshall y Bruce R. Powers, *La Aldea Global*, Gedisa, Barcelona, 1990.
22. Negroponte, Nicholas, *El Mundo Digital. Un futuro que ya ha llegado*, Ediciones B, Barcelona, 1999.
23. Postman, Neil, *Technopoly, The surrender of culture to technology*, Vintage Books, Nueva York, abril de 2003.
24. _____, *Tecnópolis: la rendición de la cultura a la tecnología*, Círculo de Lectores, Barcelona, 1994.
25. Roszak, Theodore, *El Culto a la Información. Un tratado sobre alta tecnología, inteligencia artificial y el verdadero arte de pensar*, Gedisa, Barcelona, septiembre de 2005.
26. Toffler, Alvin, *La Tercera Ola*, Plaza & Janés, Barcelona, 1999.
27. Toffler, Alvin Toffler, *El Cambio del Poder*, Plaza & Janés, Barcelona, 1992.
28. Wiener, Norbert, *Cibernética o el control y comunicación en animales y máquinas*, Tusquets Editores, Barcelona, 1998.

Comercio electrónico

29. Alonso Conde, Ana Belén, *Comercio Electrónico: Antecedentes, Fundamentos y Estado Actual*, Dykinson y Universidad Rey Juan Carlos (Servicio de Publicaciones), Madrid, 2004.

30. Arias Pou, María, *Manual Práctico de Comercio Electrónico*, La Ley, Madrid, 2006.
31. _____, *Manual Práctico de Comercio Electrónico*, La Ley, Madrid, 2006.
32. Aspis Analía, Ileana, Carla Pertusi y Hugo Gonzalo Nieva, *Comercio Electrónico. e-Commerce*, Errepar, Buenos Aires, 2006.
33. Basso Cerda, Osvaldo y Claudio Barroilhet Acevedo, *Conocimiento de Embarque Electrónico*, Librotecnia, Santiago, mayo de 2005.
34. Brandt Graterol, Leopoldo, *Páginas Web. Condiciones, políticas y términos legales*, Legis, Caracas, octubre de 2001.
35. Cavanillas Múgica, Santiago y otros, *Turismo y Comercio Electrónico. La promoción y contratación on line de servicios turísticos*, Comares, Granada, 2001.
36. Devoto Mauricio, *Comercio Electrónico y Firma Digital. La regulación del ciberespacio y las estrategias globales*, La Ley, Argentina, 2001.
37. Dreyzin de Klor, Adriana y Diego P. Fernández Arroyo, *DeCita 5/6.2006: Internet, comercio electrónico y sociedad de la información*, Fundação Boiteux, Zavalia, 2006.
38. García Más, Francisco Javier, *Comercio y Firma Electrónicos. Análisis jurídico de los servicios de la Sociedad de la Información*, Lex Nova, Valladolid, 2004 (2a. ed.).
39. GECTI (Grupo de Estudios en Internet, Comercio Electrónico & Telecomunicaciones e Informática, Facultad de Derecho de la Universidad de los Andes), *Comercio Electrónico,* Legis Bogotá, 2005.
40. Gómez Segade, José Antonio, *Comercio Electrónico en Internet*, Marcial Pons, Madrid, 2001.
41. González Gómez, Pedro Manuel, *Equiparación del Comercio Electrónico en el Derecho Civil*, Nova Tesis Editorial Jurídica, Rosario, 2006.
42. González Malabia, Sergio, *Tutela Judicial del Comercio Electrónico,* Tirant lo Blanch, Valencia, 2004.
43. Hance, Olivier, *Leyes y Negocios en Internet*, McGraw-Hill, México, 1996.
44. Hocsman, Heriberto Simón, *Negocios en Internet*, Astrea, Buenos Aires, 2005.
45. Huarag Guerrero, Enrico, *Derecho Comercial Informático,* Universidad Ricardo Palma, Universitaria, Lima, 2004.
46. Iasoni, Marie, *Comercio Electrónico, Aspectos Legales: Un desafío para el Derecho peruano*, Portocarrero, Lima, 2002.
47. Inmaculada, Higueras, *Valor Comercial de la Imagen. Aportaciones del right of publicy estadounidense al derecho a la propia imagen.* Universidad de Navarra (EUNSA), Pamplona, marzo de 2001.
48. J. Briceño C., Francisco (comp.), *Aspectos Legales del Comercio Electrónico*, Cámara Venezolana de Comercio Electrónico, Caracas, 2004.
49. Jijena Oddo, Hernan, Renato Jijena Leiva, *Comercio, Facturas y Factoring Electrónico,* Análisis de la ley núm. 19.983, Lexis Nexos, Santiago, 2008.

50. Juanes, Norma, *Comercio Electrónico y Seguridad de las Transacciones*, Advocatus, Argentina, 2003.
51. Lorenzetti, Ricardo Luis y Carlos Alberto Soto Coaguila (dirs.) *Comercio Electrónico* (vol. III), ARA Editores (Lima); Temis (Bogotá), Lima, julio de 2003.
52. Moro Almaraz, María Jesús (dir.) *Autores, Consumidores y Comercio Electrónico*, Colex, Madrid, 2004.
53. Peña Valenzuela, Daniel (comp.), *Sociedad de la Información Digital: perspectivas y alcances*, Universidad Externado de Colombia, Bogotá, 2007.
54. _____, *Aspectos Legales de Internet y del Comercio Electrónico*, Dupré, Colombia, 2001.
55. Per Bro, Narciso Cerpa y otros, *Building Society Through E-Commerce: e-Government, e-Business and e-Learning*, Collecter LatAM Conference, Santiago, 2003.
56. Illescas Ortiz, Rafael (dir.) e Isabel Ramos H. (coord.), *Derecho del Comercio Electrónico*, La Ley-Actualidad, Madrid, 2001.
57. Rengifo García, Ernesto y otros, *Comercio Electrónico*, Universidad Externado de Colombia, Bogotá, 2002 (2a. ed.).
58. Ribas Alejandro, Xavier, *Aspectos Jurídicos del Comercio Electrónico en Internet*, Aranzadi, Cizur Menor Navarra, 2003 (2a. ed.).
59. Sandoval López, Ricardo *Derecho del Comercio Electrónico*, Jurídica de Chile, Santiago, 2003.
60. Rico Carrillo, Mariliana, *Comercio Electrónico, Internet y Derecho*, Legis, Caracas, 2005 (2a, ed.).
61. Rincón Cárdenas, Erick, *Manual de Derecho de Comercio Electrónico y de Internet*, Centro Editorial Universidad del Rosario, Bogotá, 2006.
62. _____, *Tratamiento Jurídico del Comercio Electrónico en el Marco de los Procesos de Integración Comercial: Especial referencia al Tratado de Libre Comercio*, Centro Editorial Universidad del Rosario, Bogotá, 2005.
63. Rodríguez de las Heras Ballell, Teresa, *El Régimen Jurídico de los Mercados Electrónicos Cerrados (e-Marketplaces)*, Marcial Pons, Madrid, 2006.
64. Rodríguez Gladys, Stella, *El Comercio Electrónico (E-commerce) bajo el Marco de la OMC y la CNUDMI*, Jurídicas Rincón, Venezuela, 2004.
65. Rodríguez Sau, Carlos y Raúl Rubio Velásquez, *Todo sobre la LSSI y de Comercio Electrónico*, Experiencia, Barcelona, 2002.
66. S. Rippe, I. Creimer *et al.*, *Comercio Electrónico. Análisis jurídico multidisciplinario*, B de F. Buenos Aires, 2003.
67. Sanjuán y Muñoz, Enrique (dir.), *Incorporación de las Nuevas Tecnologías en el Comercio: Aspectos Legales*, Consejo General del Poder Judicial, Madrid, España, 2006.
68. Triana Sandoval Alonso (comp.), *El Comercio Electrónico*, Leyer, Bogotá, 2007.
69. Viviana Sarra, Andrea, *Comercio Electrónico y Derecho. Aspectos jurídicos de los negocios en Internet*, Astrea, Buenos Aires, 2001.

Derecho a la intimidad e informática

70. Galán Juárez, Mercedes, *Intimidad. Nuevas dimensiones de un viejo derecho*, Centro de Estudios Ramón Areces, Madrid, 2005.
71. Gómez Martínez, Carlos (dir.), *Derecho a là Intimidad y Nuevas Tecnologías*, Consejo General del Poder Judicial, Madrid, 2004.
72. Jesús Morant, Vidal, *Protección Penal de la Intimidad frente a las Nuevas Tecnologías*, Editorial Práctica de Derecho, Valencia, 2003.
73. Rebolledo Delgado, Lucrecio, *El Derecho Fundamental a la Intimidad.* 2a. ed., Dykinson, Madrid, 2005.

Derecho informático

74. Cabanellas de las Cuevas, Guillermo (dir.), Ángel Montes de Oca (coord.), Keith Aoki, Kory D. y otros, *Derecho de Internet*, Heliasta, Argentina, 2004.
75. Castañeda González, Alberto (coord.), *Derecho Tecnológico. Respuestas legales a nuevos retos*, Experiencia, Barcelona, 2004.
76. Davara Rodríguez, Miguel Ángel, *Manual de Derecho Informático*, Aranzadi, Cizur, España, 2007 (9a. ed.).
77. Do Livro Usina, Ribeiro do Valle, Regina (org.), *E-dicas: o Direito na Sociedade da Informacao*, São Paulo, 2005.
78. Fernández Delpech, Horacio, *Internet: Su Problemática Jurídica*, Abeledo-Perrot, Buenos Aires, 2004 (2a. ed.).
79. García Barrera, Myrna Elia, *Derecho de las Nuevas Tecnologías*, Instituto de Investigaciones Jurídicas, UNAM, México, 2008.
80. F. Gállego Higueras, Gonzalo, *Código de Derecho Informático y de las Nuevas Tecnologías*, Civitas Madrid, 2003.
81. Penadés, Javier Plaza, (coord.), *Cuestiones Actuales de Derecho y Tecnologías de la Información y la Comunicación (TICs)*, Aranzadi, Cizur Menor, Navarra, 2006.
82. López Zamora, Paula, *El Ciberespacio y su Ordenación*, Difusión Jurídica y Temas de Actualidad, Madrid, 2006.
83. Minardi Paesani, Liliana, *Direito e Internet. Liberdade de informacao, privacidade e responsabalidade civil*, Atlas, São Paulo, 2006 (3a. ed.).
84. P. F. Tuzio, Alejandro (dir.) y Pablo A. Palazzi (coord.), *Derecho Informático (Jurisprudencia Argentina, 2005-II | Número especial)*, LexisNexis, Buenos Aires, mayo de 2005.
85. _____, Lucas F. Tamagno (colab.), *Derecho Informático (Jurisprudencia Argentina 2007-II | Número especial)*, LexisNexis, Buenos Aires, mayo de 2007.
86. Peguera Poch, Alberto Miquel (coord.) y otros, *Derecho y Nuevas Tecnologías*, UOC, Barcelona, enero de 2005.
87. Pinochet Cantwell, Francisco José, *El Derecho de Internet*, Editorial de Derecho, Santiago de Chile, 2006.
88. Rico Carrillo, Mariliana (coord.), *Derecho de las Nuevas Tecnologías*, La Rocca, Argentina, 2007.

89. Rojo Villada, Pedro Antonio, *Sociedad Global y Nuevas Tecnologías de la Información. Los retos de la comunicación social ante la liberación del mercado europeo*, Universidad Católica San Antonio de Murcia, Murcia, 2007.
90. Saavedra López, Modesto (dir.), *Derecho y Nuevas Tecnologías. Revista de la Facultad de Derecho de la Universidad de Granada núm. 8 (monográfica)*, Universidad de Granada-Tirant lo Blanch, Granada, 2005.
91. Salas Carceller, Antonio (dir.), *La Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico*, Consejo General del Poder Judicial, Madrid, 2007.
92. Suñé Llinás, Emilio (coord.) y otros, *Tratado de Derecho Informático (Volumen II). Servicios de la Sociedad de la Información e Innovación Jurídica*, Servicio de Publicaciones, Facultad de Derecho, Universidad Complutense de Madrid, Madrid, 2006.
93. Téllez Valdés, Julio y otros, *Temas de Derecho Informático*, Secretaría de Gobernación, Dirección General de Compilación y Consulta del Orden Jurídico Nacional, México, junio de 2006.
94. Velázquez Bautista, Rafael, *100 Interrog@ntes Fundamentales en Derecho de Tecnologías de la Información y las Comunicaciones (T.I.C.)*, COLEX, Madrid, 2004.

Firma electrónica

95. Apolonia Martínez Nadal, *Comentarios a la Ley 59/2003 de Firma Electrónica*, Civitas, Madrid, 2004.
96. Bibiana, Luz Clara, *Ley de Firma Digital – Comentada*, Nova Tesis Editorial Jurídica, Rosario, 2006.
97. Diego Cruz Rivero, Marcial, *Eficacia Formal y Probatoria de la Firma Electrónica*, Pons, Madrid, 2006.
98. Diego Cruz Rivero, *La Firma Electrónica Reconocida. Análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, Consejo General del Notariado, Madrid, 2006.
99. Jesús Ignacio Fernández, Domingo, *La Firma Electrónica. Aspectos de la Ley 59/2003, de 19 de diciembre*, Reus, Madrid, 2006.
100. Saleme Murad, Marcelo A. *Firma Digital. Ley 25.506 y Normativa Vigente. Guía práctica del tratamiento jurídico de la firma digital en la Argentina. Ad Hoc*, Buenos Aires, 2004.
101. Micó Giner, Javier, *La Firma Electrónica de Notarios y Registradores y el Documento Público Electrónico*, Tirant lo Blanch, Valencia, 2007.
102. Rubio Velázquez, Raúl, Carlos Rodríguez Sau y Ramiro Muñoz Muñoz, *La Firma Electrónica. Aspectos legales y técnicos*, Experiencia, Barcelona, 2004.

Internet

103. *100 Perversiones en la Red. Las patologías de Internet y su tratamiento*, Giorgio Nardone y Federica Cagnoni, RBA Libros, Barcelona, mayo de 2003.

104. *Comunicación Pública en Internet*, Luis M. González de la Garza, Creaciones Copyright, Madrid, 2004.
105. *Consecuencias Sociales del Uso de Internet*, James E. Katz y Ronald E. Rice, UOC, Barcelona, 2006.
106. *El Control de Internet. Poder y autoridad en los mercados electrónicos*, Josep Ibáñez, Los Libros de la Catarata, Madrid, 2005.
107. *Etnografía Virtual*, Christine Hine, UOC, Barcelona, 2004.
108. *Gobernanza de Internet. Asuntos, actores y brechas*, Jovan Kurbalija, Eduardo Gelbstein, DiploFoundation, Sociedad para el Conocimiento Mundial (GKP), Génova, 2005.
109. L. Dreyfus, Hubert, *Acerca de Internet*, UOC, Barcelona, 2003.
110. *Internet y Libertad. Ampliación tecnológica de la esencia humana*, María Asunción Gutiérrez López, Comunicacióon Social Ediciones y Publicaciones Sevilla, 2005.
111. *Internet y Pobreza*, Bernardo Sorj y Luis Eduardo Guedes, Ediciones TRILCE en coedición con UNESCO, Montevideo, 2006.
112. *Internet y Sistema Judicial en América Latina. Reglas de Heredia*, Carlos G. Gregorio (coord.) y Sonia Navarro Solano (coord.), Ad-Hoc, Buenos Aires, 2004.
113. *Internet, Columna Vertebral de la Sociedad de la Información*, Octavio Islas y Claudia Benassini, LIX Legislatura de la H. Cámara de Diputados; Instituto Tecnológico y de Estudios Superiores de Monterrey; Miguel Ángel Porrúa Librero-Editor, México, julio de 2005.
114. *Justicia e Internet. Una filosofía del Derecho para el mundo virtual*, Anna Mancini, Buenos Books America, Nueva York, 2004.
115. *La Red es de Todos. Cuando los movimientos sociales se apropian de la red*, Victor Marí Sáez (coord.), Popular, Madrid, 2004.
116. *Libertad en Internet. La red y las libertades de expresión e información*, Lorenzo Cotino Hueso (coord.), Tirant lo Blanch, Valencia, 2007.
117. *Los Enlaces en Internet. Propiedad intelectual e industrial y responsabilidad de los prestadores*, Juan Francisco Ortega Díaz, Aranzadi, Cizur Menor, Navarra, 2006.
118. *Más Allá de Internet: la Red Universal Digital. X-Economía y nuevo entorno tecnosocial*, Fernando Sáez Vacas, Centro de Estudios Ramón Areces, Madrid, 2004.
119. Pablo García Mexía, (dir) *Principios de Derecho de Internet* (2a. ed.), Tirant lo Blanch, Valencia, 2005.
120. Jijena Leiva, Renato, Pablo Andrés Palazzi y Julio Téllez Valdés, *El derecho y la sociedad de la información: la importancia de Internet en el mundo actual*, Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Estado de México y Miguel Ángel Porrúa, librero-editor, México, septiembre de 2003.

Nombres de dominio

121. *Conflictos entre Signos Distintivos y Nombres de Dominio en Internet*, Fernando Carbajo Cascón, Aranzadi, Cizur Menor, Navarra, septiembre de 2002 (2a. ed.).

122. *Marcas Comerciales y Nombres de Dominio*, Rodrigo Moretti Oyarzún Librotecnia, Santiago, 2007.
123. *Marcas versus Nombres de Dominio en Internet*, Isabel Ramos Herranz Iustel, Madrid, 2004.
124. *Nombres de Dominio*, Ezequiel María Zabale; María Karina Arreche, Nova Tesis Editorial Jurídica, Rosario, enero de 2006.

Protección de datos personales

125. *Aspectos Prácticos de la Protección de Datos de las Personas Físicas*, Antonio María Rubio Navarro, J. M. Bosch, Barcelona, 2004.
126. *Auditoría de la Protección de Datos*, Jordi Velasco Dobaño; Luis Velasco Massip, Bosch, Barcelona, abril de 2005.
127. *Data Protection Law (2a. ed.)*, David I. Bainbridge, XPL Publishing Hertfordshire, Reino Unido, 2005 (2a. ed.).
128. *Datos de Salud y Datos Genéticos. Su protección en la Unión Europea y en España*, Javier Sánchez-Caro; Fernando Abellán, Comares, Granada, 2004.
129. *Derecho de Autodeterminación Informativa*, Mercedes Muñoz Campos y Hannia Soto Arroyo, Editorial Jurídica Continental, San José, 2005.
130. *Derechos Fundamentales y Protección de Datos Genéticos*, Susana Álvarez González, Dykinson, Madrid, 2007.
131. *El Dato Personal Terapéutico*, Francisco Almodóvar Navalón European Pharmaceutical Law Group, Madrid, mayo de 2005.
132. *El Derecho a la Protección de Datos Personales en la Sociedad de la Información*, Ana Isabel Herrán Ortiz, Universidad de Deusto, Bilbao, España, 2003.
133. *El Derecho al Acceso y Control de Datos o Información y su Protección en Venezuela*, Gustavo Marín García, Fundación Estudios de Derecho Administrativo (FUNEDA), Caracas, 2005.
134. *El Derecho Fundamental a la Protección de Datos Personales en Europa*, Mónica Arenas Ramiro, Tirant lo Blanch, Valencia, 2006.
135. *Estudio Práctico sobre la Protección de Datos de Carácter Personal* (2a. ed.), Cristina Almuzara Almaida (coord.); Fanny Coudert; Ana Marzo Portera; Yolanda Navalpotro Navalpotro, Lex Nova, Valladolid, 2007 (2a. ed.).
136. *Estudios de Protección de Datos de Carácter Personal en el Ámbito de la Salud*, Santiago Ripol Carulla (ed.); Jordi Bacaria Martrus (coord.)Agèencia Catalana de Protecció de Dades, Marcial Pons, Madrid, 2006.
137. *Estudios sobre Administraciones Públicas y Protección de Datos Personales. I encuentro entre agencias autonómicas de protección de datos personales*, Antonio Troncoso Reigada, Agencia de Protección de Datos de la Comunidad de Madrid, Madrid, julio de 2006.
138. *Guía Práctica de Protección de Datos para Ayuntamientos*, Miguel Ángel Davara Rodríguez, El Consultor de los Ayuntamientos y Juzgados, Madrid, 2006.

139. *Guía Práctica sobre Protección de Datos de Carácter Personal para Abogados*, Alfonso Ortega Giménez; Manuel Badenes Cazorla; Alejandro Macho-Quevedo Pérez-Victoria; Ana Marzo Portera, Difusión Jurídica, España, 2008.
140. *Informática y Libertades. La protección de datos personales y su regulación en Francia y España*, Teresa García-Berrio Hernández, Universidad de Murcia, Murcia, 2003.
141. *Informes Comerciales*, Pablo A. Palazzi, Astrea, Buenos Aires, 2007.
142. *Internet, Privacidad y Datos Personales*, Víctor Drummond Reus, Madrid, 2004.
143. *Introducción a la Protección de Datos*, Lucrecio Rebollo Delgado; Mercedes Serrano Pérez, Dykinson, Madrid, 2006.
144. *La Auditoría de Seguridad en la Protección de Datos de Carácter Personal*, Ana Marzo Portera y Alejandro Macho-Quevedo Pérez-Victoria, Experiencia, Barcelona, 2004.
145. *La Cesión de Datos Personales*, Jessica Matus Arenas y Alejandro Montecinos García, Lexis Nexis, Santiago, 2006.
146. *La Privacidad Electrónica*, Luis Ángel Ballesteros Moffa, Tiranto Lo Blanch, Valencia, 2006.
147. La Protección de Datos en la Administración Local, Jesús Fuentetaja Pastor; Sara Medina González, Iustel, España, 2008.
148. *La Protección de Datos en la Gestión de Empresas*, Ana Marzo Portera (dir.); Fernando M. Ramos Suárez (dir.), Aranzadi, Cizur Menor, Navarra, 2004.
149. *La Protección de Datos en los Centros de Enseñanza. Recomendaciones para cumplir el régimen jurídico*, Elena Pérez Gómez; Antonio Sánchez-Crespo López, Aranzadi, Cizur Menor, Navarra, 2007.
150. *La Protección de Datos Personales en el Sector de las Comunicaciones Electrónicas*, Miguel Ángel Davara Rodríguez, Universidad Pontificia Comillas, Madrid, 2003.
151. *La Protección de Datos Personales y el Derecho a la Vida Privada. Régimen jurídico, jurisprudencia y derecho comparado*, Pedro Anguita Ramírez, Jurídica de Chile, Santiago, 2007.
152. *La Protección de los Datos Personales en la Argentina*, Pablo Andrés Palazzi, Errepar, Buenos Aires, 2004.
153. *La Protección Jurídica de los Datos Genéticos de Carácter Personal*, Pilar Nicolás Jiménez, Comares, Bilbao-Granada, 2006.
154. *La Protección Penal de los Datos Sanitarios. Especial referencia al secreto profesional médico*, María del Carmen Gómez Rivero, Comares, Granada, 2007.
155. *La Red Iberoamericana de Protección de Datos. Declaraciones y Documentos*, José Luis Piñar Mañas, M. A. Montull Cremades, Tirant lo Blanch, Madrid, 2006.
156. *La Transposición de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas*, Autor: Miguel Ángel Davara Rodríguez, Fundación Vodafone, Madrid, 2004.

157. *La Tutela de la Unión Europea al Contribuyente en el Intercambio de Información Tributaria*, Fernando Fernández Marín, Atelier, España, 2007.
158. *Manual de Protección de Datos para Abogados*, Miguel Ángel Davara Rodríguez, Aranzadi, Cizur Menor, Navarra, 2006.
159. *Manual Práctico de Protección de Datos*, Antonio Ruiz Carrillo, Bosch, Barcelona, febrero de 2005.
160. *Memorias del Foro sobre Protección de Datos Personales y Regulación Legal del Habeas Data*, Defensoría del Pueblo, Bogotá, 2004.
161. *Privacy Handbook. Guidelines, exposures, policy implementation, and international issues*, Albert J. Marcella Jr.; Carol Stucki, John Wiley and Sons, Nueva Jersey, 2003.
162. *Protección de Datos de Carácter Personal en Iberoamérica*, José Luis Piñar Mañas, Tirant lo Blanch, Valencia, 2005.
163. *Protección de Datos de Carácter Personal*, Oscar R. Puccinelli, Astrea, Buenos Aires, 2004.
164. *Protección de Datos Personales en Uruguay y el Mercosur*, Carlos E. Delpiazzo; Maricarmen Pascale; Daniela Peña; Flavia Meleras; Andrés Saravia, Fundación de Cultura Universitaria, Montevideo, noviembre de 2005.
165. *Protección de Datos Personales y Derechos de los Extranjeros Inmigrantes*, Ángeles Solanes Corella y María Belén Cardona Rubert, Tirant lo Blanch, Valencia, 2005.
166. *Publicidad Registral y Derecho a la Privacidad. Una necesaria conciliación*, Emilio Guichot, Colegio de Registradores de la Propiedad y Mercantiles de España, Madrid, 2006.
167. *Seguridad, Privacidad, Confidencialidad. El desafío de la protección de datos personales*, Emilio Aced Félez; Rubén Amato; Orual Andina; Marcelo Bauzá; Rubén Berriolo; Joël Boyer; Carlos Delpiazzo; Eduardo Fernández; Virginia Galeano; Eduardo Giorgi; Silvia Liebaug; Jutta Limbach; Jorge Marabotto; Álvaro Margolis; Addy Mazz; Emilie Passemard; Alberto Pérez Pérez; José Luis Puig; María de los Ángeles Salgado; Luis Scotto; Rodolfo Uicich; Rosario Viana, TRILCE, Montevideo, 2004.
168. *The Digital Person. Technology and privacy in the information age*, Daniel J. Solove, New York University Press, Nueva York, 2004.
169. *Tratamiento de Datos Personales en el Ámbito Sanitario: Intimidad "versus" Interés Público*, Noelia de Miguel Sánchez, Tiranto lo Blanch, Valencia, 2004.
170. *Tratamiento de Datos Personales y Derechos Fundamentales*, Ana Garriga Domínguez, Dykinson, Madrid, 2004.

Software

171. *El Contrato para la Elaboración de Programas de Ordenador. Contrato de desarrollo de software*, Pere Soler Matutes; Il.lustre Col. legi Oficial d'Enginyeria en Informàtica de Catalunya, Aranzadi, Cizur Menor, Navarra, 2003.

172. *El Derecho y la Industria Informática*, Diego Martín Buitrago Botero, Señal, Medellín, 2002.
173. *Internet, Hackers y Software Libre*, Carlos Gradin (comp.); John Gilmore; Eric Hughes; Christian Ferrer; Eric Hughes; Jaromil; Bill Joy, Jonas Löwgren; Steven Mizrach; Thomas Pynchon; Eric Raymond; Richard Stallman; Bruce Sterling; Miquel Vidal; Marilina Winik, Fantasma, Buenos Aires, 2004.
174. *La Dimensión Jurídica del Software. Naturaleza, tutela jurídica, contratos y responsabilidad*, Christian Hess Araya, IJSA, San José, junio de 2004 (2a. ed.)
175. *La Pastilla Roja. Software libre y revolución digital*, Alfredo Romeo Molina, Juan Tomás García Molina y Cristóbal Prieto Rodríguez, Edit Lin, Madrid, 2003.
176. *La Siempre Conflictiva Relación del Trabajador Intelectual y un Apunte Específico para el Creador de "Software"*, José Gustavo Rodríguez Hidalgo y Henar Álvarez Cuesta, Universidad de León, León, España, 2004.
177. *Licencias de Uso No Personalizadas de Programas de Ordenador. Shrink-wrap, click-wrap y otras formas de distribución de software*, Juan Pablo Aparicio Vaquero, Comares, Granada, 2004.
178. *Los Videojuegos. Qué son y cómo nos afectan*, Ricardo Tejeiro Salguero y Manuel Pelegrina del Río, Ariel, Barcelona, 2003.
179. *Problemática Jurídica del Software Libre*, Martín Carranza TorresLexis Nexis, Buenos Aires, 2004.
180. Sobre Software Libre. Compilación de ensayos sobre software libre, Vicente Matellán Olivera, Jesús M. González Barahona, Pedro de las Heras Quirós y Gregorio Robles Martínez (eds.), Dykinson, Madrid, 2004.
181. *Software Libre: empresa y administración en España y Cataluña*, Meritxell Roca, UOC, Barcelona, 2007.

Teletrabajo

182. Alarcón Caracuel, Manuel Ramón y Ricardo Esteban Legarreta (coords.), *Nuevas Tecnologías de la Información y la Comunicación y Derecho del Trabajo*, Bomarzo, Alicante, 2004.
183. Algar Jiménez, Carmen, *El Derecho Laboral ante el Reto de las Nuevas Tecnologías*, Grupo Difusión, 2007.
184. Aragón, Jorge; Alicia Durán; Fernando Rocha; Jesús Cruces, *Las Relaciones Laborales y la Innovación Tecnológica en España*, Los Libros de la Catarata, Madrid, 2005.
185. Arias Domínguez, Ángel y Francisco Rubio Sánchez, *El Derecho de los Trabajadores a la Intimidad*, Aranzadi, Cizur Menor, Navarra, 2007.
186. Del Rey Guanter, Salvador (dir.) y Manuel Luque Parra (coord.), *Relaciones Laborales y Nuevas Tecnologías*, La Ley, Madrid, 2005.
187. Durante Calvo, Marco, *El Teletrabajo. Nuevas formas de trabajo a través de la telemática*, IJSA, San José, 2003.
188. Felio José Bauza Martorell, *Régimen Jurídico de la Videovigilancia*, Marcial Pons, Madrid, 2004.

189. Fernández Delpech, Horacio, *Esquemas de Derecho Laboral y de Derecho Informático*, Universidad Libros, Buenos Aires, marzo de 2006.
190. Izquierdo Carbonero, Francisco Javier, *El Teletrabajo*, Difusión Jurídica y Temas de Actualidad, Madrid, 2006.
191. Jeffery, Mark; Javier Thibault Aranda; Ángel Jurado (coords.), y otros, *Tecnología Informática y Privacidad de los Trabajadores*, Cizur Menor, Navarra, 2003.
192. Juri Sabag, Ricardo, *El Teletrabajo. La nueva forma de trabajo*, Lexis Nexos, Santiago, 2006.
193. *La Protección de Datos de Carácter Personal en los Centros de Trabajo*, Farriolsi Solá, Antoni (dir.-coord.), Cinca, Madrid, 2006.
194. Marín Alonso, Inmaculada, *El Poder de Control Empresarial sobre el Uso del Correo Electrónico en la Empresa. Su limitación en base al secreto de las comunicaciones*, Tirant lo Blanch, Valencia, 2005.
195. Oliveira Rocha, Marcelo, *Direito do Trabalho e Internet*, Livraria e Editora, Universitaria de Directo, São Paulo, 2005.
196. Oviedo, María Natalia, *Control Empresarial sobre los "e-mails" de los Dependientes*, Hammurabi, Buenos Aires, 2004.
197. Piñar Mañas, José Luis (dir.), *Protección de Datos de Carácter Personal en Iberoamérica*, Tirant lo Blanch, Valencia, 2005.
198. Roig Batalla, Antonio; Carolina Gala Durán; Daniel Martínez Fons; José Muñoz, Lorente, *El Uso Laboral y Sindical del Correo Electrónico e Internet en la Empresa. Aspectos constitucionales, penales y laborales*, Tirant lo Blanch, Valencia, 2007.
199. Roqueta Buj, Remedios, *Uso y Control de los Medios Tecnológicos de Información y Comunicación en la Empresa*, Tirant lo Blanch, Valencia, 2005.
200. Thibault Aranda, Javier, *Control Multimedia de la Actividad Laboral*, Tirant lo Blanch, Valencia, 2006.
201. Ulrich Beck, *Un Nuevo Mundo Feliz. La precariedad del trabajo en la era de la globalización*, Paidós, Barcelona, 2007.

Índice analítico

Los números de página seguidos por una *n* indican notas

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U