

MANUAL CHILENO DE DERECHO INFORMÁTICO

Documentos Preparatorios

Lección: Derechos Fundamentales y Sociedad en Red

Autor: Lorena Donoso Abarca

Correo electrónico: ldonoso [ARROBA] icdt.cl

Versión: 0.1

Queda totalmente prohibida la reproducción total o parcial de este texto, en cualquier soporte mecánico o digital sin el consentimiento expreso y por escrito de su autor.

Derechos Humanos y Sociedad en Red

Sumario: Derechos Humanos y Derechos Fundamentales en la sociedad en Red; Derechos Fundamentales, Orden Público y Tecnologías; Afectación de los Derechos Humanos por las tecnologías de la información y las comunicaciones; Nueva sociedad, nuevos Derechos Humanos?; Libertad Informática o autodeterminación informativa como un Derecho Humano emergente en la sociedad en Red. Situación Chilena

Derechos Humanos y Derechos Fundamentales en la sociedad en Red.

La sociedad informatizada ha surgido y se ha desarrollado en la última centuria, la que ha estado marcada por el desarrollo de los derechos fundamentales y del Estado Social Democrático. Siendo así, el desarrollo tecnológico deben tener como referente estos derechos como marco teórico al que debe circunscribirse y que de alguna manera encausa su avance.

No pretendemos hacer un análisis pormenorizado de la historia de los Derechos Fundamentales, pero creemos necesario al menos distinguir entre Derechos Humanos, Derechos Fundamentales y Garantías Constitucionales, pues éstos son conceptos básicos a la hora de enfrentar el tema que nos ocupa.

La historia de los derechos humanos, es relativamente reciente, es una idea patrimonio del Estado Moderno, en su concepción más amplia, acuñada y teorizada por Maquiavello y Bodin. Entre las características del nuevo modelo destacan la legalidad de la función pública, la pluralidad de los órganos constitucionales, la división de poderes, la justicia constitucional y administrativa, y la consagración de una esfera de libertades. Producto de este nuevo orden de cosas, la persona se reposiciona frente al gobernante, ahora no “sometido” sino

“reconocido” como un sujeto con el cual se generan relaciones recíprocas "derecho-deber", entre los cuales se destacan los derechos subjetivos públicos, que la persona puede hacer valer en contra del gobernante. Es así como la forma clásica de las declaraciones de derechos a fines del siglo XVIII y principios del Siglo XIX, consisten en la afirmación de la existencia de los Derechos del Hombre contra todo absolutismo político, constituyendo en sí mismas un diseño básico de la estructura del Estado.

Frente a estos Derechos del Hombre, los Derechos Fundamentales se constituyen como derechos subjetivos previamente identificados, en cuanto encuentran reconocimiento en las Constituciones y en la medida en que de este reconocimiento se derive alguna consecuencia jurídica. En Sentido amplio, se entiende por tales a todos y cada uno de los derechos reconocidos en la norma fundamental (La Constitución) y no necesariamente aquellos que se encuentran en el capítulo de garantías fundamentales.

Ahora bien, las garantías fundamentales buscan otorgar la fuerza constitucional a los derechos individuales así garantizados, a fin de protegerlos incluso contra el legislador. En este aspecto, respecto de los derechos garantizados se establece una relación jurídica entre el ciudadano y el Estado, en el sentido que al ser reconocidos en la Constitución, gozan de permanencia e imprescriptibilidad, además de su tutela judicial y el respeto de su contenido esencial por el legislador.

Visto desde una óptica humanista, los derechos fundamentales son aquellos aspectos que emanan de la dignidad humana, a cuyo respecto existe un consenso social amplio en cuanto a la necesidad de resguardarlos incluso contra los poderes a los que la sociedad les ha conferido alguno de los poderes del Estado. De este modo, la Constitución comprende principios filosófico/políticos que sirven de soporte al tipo de organización que se ha dado el Estado, importantes por representar la parte ideológica de las Constituciones en la cual se consagran los Derechos Humanos, ya sea expresa o tácitamente, lo que sirve de límite a los órganos de poder y a los de los propios asociados.

A su vez, en paralelo se encuentran las garantías que debe acatar el Estado en bien de la comunidad y sus asociados, de manera tal que sin ellas no hay organización posible ni Derechos Humanos efectivos; tales garantías constituyen instrumentos de control para la permanencia de la Constitución y progreso de la comunidad establecida.

Es en este sentido que se ha considerado que las garantías fundamentales representan los valores ético-culturales admitidos formalmente por la sociedad. De su parte, serán Derechos Humanos, cuando su reconocimiento como tales sea común a la generalidad de las sociedades que se desenvuelven en el marco de los Estados de Derecho.

Los instrumentos de control para resguardar el orden en que se sustentan son: el **control de constitucionalidad**, que busca hacer efectivo el principio de primacía constitucional, columna vertebral del Estado Democrático de Derecho; el **control de legalidad**, dirigido a los órganos aplicadores del Derecho y el "**control social**", dirigido a la conducta de los particulares, que entra en funciones cuando se lesiona o pone en peligro normas básicas de la organización, tales como los "derechos humanos", control que corresponde al Derecho Penal como instrumento garantizador de la convivencia pacífica en una organización establecida.

Esta explicación resulta importante porque las tecnologías de la información y las comunicaciones han impactado tanto en la concepción de los Derechos Humanos, como de los Derechos y Garantías Fundamentales, en tanto que su desarrollo nos ha impuesto analizar la forma como se venían configurando y en algunos casos, incluso cuestionar su contenido esencial, como veremos más adelante.

No entraremos en el análisis de las generaciones de derecho, no obstante en el estudio de cada una de las garantías fundamentales que serán objeto de tratamiento en esta fase de nuestro estudio haremos algunas referencias a esta materia, en lo que respecta a cada derecho en específico.

Asimismo, no realizaremos un análisis pormenorizado respecto de las tecnologías a que nos referiremos en cada caso, no sólo por las complejidades técnicas sino por la extensión que significaría emprender esta tarea. Baste en este punto señalar que existen tecnologías que apoyan los procesos comunicacionales / informacionales, que son aquellas que sirven para recolectar, sistematizar y distribuir información entre emisores y receptores, otras que apoyan los procesos decisorios, básicamente a través de procesos de análisis de información y emisión de informes de resultado, que pueden decir relación con análisis de documentos y emisión de reportes, hasta el procesamiento de muestras biológicas y emisión de informes técnicos, pasando por sistemas que permiten generar prototipos de dictámenes, en base a la información ingresada y algoritmos de análisis de los mismos y otras que permiten gestionar procesos de la más diversa índole, como los complejos sistemas que manejan las cámaras de seguridad de una ciudad, o las que gestionan los sistemas de cobro de los estacionamientos, por sólo mencionar algunos o, finalmente, los sistemas tecnológicos de apoyo al control laboral de cumplimiento de obligaciones laborales de los trabajadores de una empresa.

En el empleo de cada uno de estos sistemas y otros muchos que por tiempo y espacio no mencionamos, puede haber afectaciones a derechos, las que podrán ser legítimas o no. Lo importante es adquirir las nociones básicas que permitan en cada caso discernir cuál es el límite de la aplicación y/o implementación de estas tecnologías. Desde nuestra óptica, estimamos que la esencia de los derechos fundamentales es precisamente este límite y esto es lo que llamaremos “orden público tecnológico”, para los efectos de nuestro estudio.

Derechos Fundamentales, Orden Público y Tecnologías

En general, mucho se ha dicho sobre el orden público, sobre todo en lo que se refiere al orden público económico, en tanto normas de ordenación de los mercados y de las relaciones entre los actores económicos. En este contexto, el orden público ha sido entendido por la jurisprudencia como el conjunto de principios y normas jurídicas que organizan la economía de un país y facultan a la autoridad para regularla [CAP STGO-1992].

Aplicando este criterio a la materia que nos ocupa en este acápite diremos que el orden público agrupa al conjunto de normas y principios que regulan las tecnologías de la información y las comunicaciones en tanto interactúan con los derechos fundamentales y con las bases de la institucionalidad. Entendemos que lo que respecta a las tecnologías insertas en los procesos económicos, entendemos queda comprendido en el concepto tradicional de orden público tecnológico.

Siguiendo nuestra analogía, entendemos que si una norma integra el orden público tecnológico, habrá de interpretarse conforme al método aplicable al orden público y por tanto, parafraseando lo dicho por nuestros tribunales, en relación con el orden público económico, debe ser interpretado y aplicado con sujeción a los valores que moldean la institucionalidad política, social y económica proclamada en la Constitución. Así, debe entenderse que el propósito perseguido por el constituyente al consagrar la disposición de que se trata, es el de enfatizar el derecho protegido a través de la respectiva garantía constitucional, para evitar que se impida o perturbe arbitrariamente su ejercicio, en la medida que su titular respete las

normas legales que la regulan [CSUP-1999]. En este sentido entonces, las normas sobre derechos fundamentales deben servir como un límite a la aplicación de las tecnologías, pero también pueden ser la clave de bóveda para propiciar su desarrollo. Son dos caras de la misma moneda, que trataremos de esbozar en las próximas páginas.

Afectación de los Derechos Humanos por las tecnologías de la información y las comunicaciones.

El fenómeno tecnológico, con su aptitud para manejar grandes volúmenes de información estructurada, de su gestión y transmisión más allá de las fronteras de un país determinado, con las posibilidades de modelación de aspectos que antes eran insospechados, tales como la vida, gracias al desarrollo de la investigación genómica, que permite diseñar, planificar o incluso extinguirla.

Recordemos que Gracias al desarrollo de las tecnologías y al trabajo mancomunado (en Red) de muchos científicos fue posible descifrar el Código Genético de las personas, y con ello descifrar las relaciones filiales y aspectos relativos con las predisposiciones a ciertos males o enfermedades. Más tarde, en este mismo campo, fue posible descifrar las huellas de ADN, que permiten identificar a una persona, haciéndola única e irrepetible.

Estos avances han sido profusamente aplicados para diversas finalidades que impactan los derechos de las personas, tanto en materia de reconocimiento de paternidad, en el primero de ellos, como en la identificación de personas con finalidades de interés criminal.

Otro aspecto relevante es que las actuales sociedades se desarrollan “enredadas”, en el sentido que las distintas plataformas se encuentran ya interconectadas y en condiciones de inter-operar de manera transparente para los usuarios. Ello promueve nuevos desafíos, adicionales a los ya advertidos en la época de la eclosión de la convergencia tecnológica propiciada por la digitalización de las redes y servicios. Entre estos desafíos están aquellos que dicen relación con la protección de la información de las personas que circula, se almacena y/o procesa en esas redes. A este respecto, ha sido necesario configurar y reconocer un nuevo derecho fundamental, a la protección de los datos personales, como un derecho independiente de otros derechos fundamentales. Así lo ha reconocido la Carta de Derechos Fundamentales de Europa, de 2010.

Frente a esta evidencia se ha generado todo un movimiento legislativo y doctrinal, tendente a evidenciar la necesaria relación existente entre el avance de las tecnologías de la información y las comunicaciones en las sociedades modernas y la efectiva protección de las garantías fundamentales.

El objeto de esta lección es realizar un sucinto estudio acerca de la configuración de los derechos fundamentales generalmente reconocidas como susceptibles de verse afectadas por el fenómeno informático, a fin de determinar su sentido y alcance y mecanismos de protección ideados por el legislador para garantizar su vigencia efectiva. Como método de trabajo, y para los solos efectos de ordenar el discurso, seguiremos el orden que ha establecido la Constitución Chilena para las garantías fundamentales, para luego hacer referencia a la Transparencia, consagrada como derecho constitucional, en las bases de nuestra institucionalidad.

Para nuestro análisis tomaremos algunos derechos que ya pueden ser considerados como tradicionales, sin que ello signifique que no reconozcamos la importancia de los demás. A su

respecto nos referiremos a de qué manera las TICs los afectan y de qué manera su contenido esencial limita y/o modela el desarrollo tecnológico.

1.- El Derecho a la Vida y las Tecnologías de la Información y las Comunicaciones.

Las Tecnologías de la información y las comunicaciones han impactado la esencia misma de la vida. Al descifrarse el código genético se ha generado una serie de desarrollos que rayan en una afectación esencial del derecho a la vida, en tanto que permiten, generar vida humana, seleccionar los “mejores” ejemplares para privilegiarlos con el derecho a desarrollarse en un extremo, pasando por las posibilidades de generar órganos de reemplazo, para el caso de requerirlos una persona o incluso, en el otro extremo, contribuir al término de la existencia humana.

Al respecto, es importante destacar que no obstante el desarrollo tecnológico puede alcanzar límites insospechados, las comunidades científicas han propiciado que se adopten acuerdos internacionales para ponerle coto cuando ello entrañe atentar contra la esencia del derecho a la vida.

Es en este sentido que el Convenio de Oviedo (1996) protege la vida embrionaria, prohibiendo el uso de embriones humanos para experimentación, y la Declaración Universal sobre Genoma Humano y Derechos Humanos (1997) fija los principios que deben regir en la investigación genómica, a saber:

- a) **Dignidad**, en tanto que en este campo se debe procurar siempre la preeminencia del ser humano y la no discriminación;
- b) **Libertad**, de la cual deriva el consentimiento libre e información, la protección al vulnerable y el derecho a saber (y a no saber);
- c) **Adecuación/Razonabilidad**, que impone que se generen protocolos de investigación aprobados por comités éticos-científicos, además de que se prevean mecanismos de reparación de los daños directos, producidos por la investigación en la persona y el principio de confidencialidad;
- d) finalmente el principio de **justicia**, conforme al cual los Estados deben instar la cooperación Científica /cultural y el reconocimiento de las “identidades culturales”.

Un tercer instrumento relevante en esta materia es la Declaración sobre Datos Genéticos Humanos, de la Unesco (2003), que precisa los principios de la Declaración de 1997, en relación al uso de los datos genéticos, otorgándoles el carácter de datos sensibles y consagrando los derechos que a su respecto les corresponden a sus titulares:

- a) Derecho de Acceso del titular;
- b) Confidencialidad / reserva /secreto, en cuanto a la identidad del titular de la muestra, la muestra propiamente tal y el consentimiento expreso e informado del afectado por el tratamiento de datos de esta naturaleza, sin perjuicio de establecer excepciones, fundadas en un interés público importante, previsto en una ley interna compatible con la legislación internacional de los derechos humanos;
- c) Temporalidad del almacenamiento;

- d) Exactitud, fiabilidad, calidad y seguridad de esos datos y del tratamiento de las muestras biológicas y
- e) Tratamiento de acuerdo a la finalidad

Estas normas vienen a complementar la protección que ya habían dado a la vida y a la Dignidad Humana en la primera generación de derechos, básicamente a través del Código de Núremberg (1947) y la Declaración Universal de Derechos Humanos (1948) y en la Segunda Generación, en el Pacto Internacional de Derechos Civiles y Políticos (1969), que ya reconocían como derechos humanos que ninguna persona fuera sometida a torturas ni a penas o tratos crueles, inhumanos o degradantes, así como que el derecho a que no fueran sometido sin su libre consentimiento a experimentos médicos o científicos.

Demás está señalar que la Constitución Chilena no se ha adaptado a las nuevas exigencias de la protección del derecho a la vida, que surge a partir de la evidente capacidad exponencial de los sistemas tecnológicos. No se ha incorporado a nivel constitucional la protección de la vida embrionaria a cuyo respecto “no se espera que exista”, por cuanto no se ha implantado sino que se encuentra en un laboratorio, monitorizado por complejos sistemas de información, tampoco se ha adoptado una decisión a nivel constitucional, respecto de si avanzaremos hacia la creación de vida humana “de diseño”, claramente posible a través del empleo de estas tecnologías.

2.- La Igualdad ante la ley

La igualdad fue reconocida en el Pacto Internacional de Derechos Civiles y Políticos (1966) en su artículo 3, en los términos siguientes: *“Los Estados Partes en el presente Pacto se comprometen a garantizar a hombres y mujeres la igualdad en el goce de todos los derechos civiles y políticos enunciados en el presente Pacto”*. De su parte, la Convención Americana de Derechos Humanos (1969), la reconoce en su artículo 1, como una de las principales obligaciones de los Estados.

En la sociedad en Red se advierten ciertas ventajas comparativas que gozan aquellos que se han conectado, respecto de quienes no. En este sentido, estimamos que la actualización de esta garantía fundamental impone que se reconozca el derecho de las personas a acceder a los servicios de este nuevo modelo social y que se dé un igual trato jurídico a los servicios en línea, respecto de aquellos que se prestan en los entornos desconectados, de una parte y por otra se dé igual trato económico a las actividades en línea, respecto de aquellas que se desarrollan en los métodos tradicionales.

En la primera de las esferas, en la segunda generación de derechos fundamentales se construyó el servicio universal y acceso universal a las telecomunicaciones, que de acuerdo a lo que postula la Unión Internacional de Telecomunicación, se erigen como manifestaciones expresas del derecho que toda persona tiene a comunicarse, que ameritan por tanto la elevación de estos imperativos a la categoría de una garantía individual.

En cuanto al alcance de la protección, se han mencionado los siguientes:

- Conjunto definido de servicios asequible a todos los ciudadanos, condicionados por dos aspectos esenciales, cuales son: a) el estado de la Técnica y b) el avance social y económico de una sociedad determinada

- Otras obligaciones de servicio público complementarias de la institución anterior (Guías, números de emergencia).
- Implantación de servicios adicionales o complementarios de telecomunicaciones
- Derecho al uso compartido de infraestructuras de telecomunicaciones, básicamente por cuanto: a) Minimizan el impacto urbanístico y medioambiental de dichas infraestructuras y b) Facilitan la introducción de la competencia en el mercado de las telecomunicaciones

Entre los instrumentos internacionales de derechos humanos que han ayudado a la construcción del servicio y acceso universal como una manifestación de la igualdad ante la ley, están la Declaración sobre Acceso Universal a las Comunicaciones Básicas y Servicios de Información, del Comité Administrativo de las Naciones Unidas (1995), que dispone que “Los Estados deben velar porque los nuevos servicios de sistemas y de Datos informatizados que se ofrezcan al público en general sean desde un comienzo accesibles a las personas con discapacidad, o se adapten para hacerlos accesibles a ellas”.

Ahora bien, estas garantías, de una parte imponen a los Estados no generar beneficios a quienes actúan a través de medios tecnológicos, que rompan el equilibrio de la igualdad ante la ley, pero a la vez promover aquellos desarrollos e implementaciones tecnológicas que contribuyan a bajar las barreras de la desigualdad. Este último es el caso de las normas que tienen a equiparar las condiciones de las personas con necesidades especiales, que requieren que los sistemas propios de la sociedad en red contemplen funcionalidades que les ayuden a servirse de sus beneficios, tales como controles de voz para las personas con hipoacusia, lectores a viva voz de texto en pantallas, para las personas ciegas, entre otros. Así se ha reconocido en el Art. 5 de las Normas Uniformes sobre la igualdad de oportunidades para las personas con discapacidad, aprobadas por la Asamblea General de las Naciones Unidas, mediante Resolución 48/96, de 20 de diciembre de 1993, en el Cuadragésimo Octavo Período de Sesiones, en que se acordó lo siguiente: "los estados deben elaborar estrategias para que los servicios de información y documentación sean accesibles a los diferentes grupos con incapacidad"...

Hoy en día ya algunos países, en derecho comparado, consagran a como una garantía Fundamental el acceso a Internet. Es el caso de Finlandia, Costa Rica y Perú, por mencionar algunos, en los cuales, ya sea por vía de consagración legal o por decisión jurisprudencial, consideran que el acceso a Internet merece alcanzar este reconocimiento. En Chile, de su parte, existe un proyecto de ley que busca este mismo objetivo.

3.- Igualdad ante la justicia

La garantía fundamental del artículo 19 N° 3 de la constitución se funda en la necesidad de asegurar a todas las personas, que tengan iguales posibilidades de defender sus derechos a través de los medios que establece la ley para la resolución de conflictos de intereses de relevancia jurídica.

Cuando nos aproximamos a esta garantía desde las tecnologías de la información y las comunicaciones debemos necesariamente hacer referencia a los siguientes aspectos, que integra lo que se ha dado en llamar e-justicia:

- a) Tecnologías de la información en apoyo de los procesos asociados al ejercicio de derechos de las partes, ya sea para la consulta de avances del proceso (procesos de información y gestión del conocimiento)
- b) TIC para la presentación de escritos o notificación de actuaciones (procesos transaccionales),
- c) TIC para construcción de la verdad procesal (informática forense),
- d) TIC en apoyo de la ejecución de lo resuelto (Herramientas TICs de cumplimiento).

En cada una de las fases tendrá sus complejidades desde la óptica de los derechos fundamentales, por cuanto las tecnologías empleadas, podrían afectar otros derechos, tales como la privacidad o la honra de las personas (por ejemplo el caso de la vigilancia telemática de personas, durante el proceso o en la fase de ejecución de la sentencia, debe ser escrupulosamente diseñada e implementada, a los efectos de no afectar indebidamente la privacidad, la honra o incluso la salud de las personas).

En lo que nos interesa, en relación a la igualdad en el acceso a la justicia y al debido proceso legal, los principales principios que emanan de esta garantía son los siguientes:

- a) **Prohibición de toma de decisiones informatizadas:** en general se ha entendido que la facultad de juzgar debe ser ejercida por una persona y no una máquina. En este sentido, se ha cuestionado el desarrollo de los sistemas expertos de decisión judicial, no obstante existe un consenso en la legitimidad de su empleo en los procesos administrativos, relativos a infracciones en las cuales, frente a la constatación de la infracción, procede hacer una aplicación cuasi matemática de la norma correspondiente para determinar la sanción a aplicar.
- b) **Bilateralidad de la audiencia:** que en este ámbito se traduce en que las partes tengan las mismas posibilidades de intervenir en el proceso, con independencia de si actúan de manera presencial o a través de sistemas tecnológicos. Asimismo, que las partes tengan las posibilidades ciertas de opinar respecto de los antecedentes allegados por la contraria y/o por orden del Tribunal. A vía de ejemplo, cuando se dictó la ley de firma electrónica en Chile no se advirtió que su texto afectaba este derecho, al no considerar una oportunidad cierta para la percepción de los documentos electrónicos que pudieren ser presentados por las partes. Es por ello que la ley 20.217 debió modificar el Código de Procedimiento Civil, y establecer la audiencia de percepción documental, momento desde el cual empiezan a correr los plazos para impugnar los documentos. Por esta misma razón, el nuevo texto del artículo 348 de este cuerpo normativo establece que es de carga de la parte que presenta el documento el proveer los medios necesarios para la percepción del documento, y por tanto si no lo hace, se tendrá por no presentado el documento.
- c) **Equivalencia funcional:** Este principio, que vimos ya en el capítulo primero de esta obra, se manifiesta en este ámbito en el sentido que en el proceso se considerará el mérito probatorio de los antecedentes allegados a los autos, con independencia del soporte en el cual consten o en el que se hayan generado, en la medida que se resguarde la seguridad, fiabilidad y disponibilidad de esas pruebas, temas que se tratan más en profundidad en el área de informática forense.
- a) **No discriminación:** En lo que nos interesa, queremos destacar la imposibilidad de que los sistemas jurídicos impongan condiciones inequitativas para el acceso al medio

tecnológico, cuando este represente una mejora en las condiciones de la persona, de cara al circuito judicial. A vía de ejemplo, a nuestro juicio sería discriminatoria la norma que prescribire un cobro de dinero como condición para acceder a un sistema de vigilancia telemático en reemplazo de la prisión.

4.- El derecho a la educación y libertad de enseñanza

En la línea argumental que venimos sosteniendo, resulta esencial referirnos al derecho a la educación y libertad de enseñanza, derechos de segunda generación, cuyo origen es el Pacto de Derechos Civiles y Políticos (1969)

Este Derecho implica que cada niño y joven, con independencia de sus condiciones personales, sociales, económicas o geográficas, debe poder acceder, permanecer en el sistema educativo en los niveles que alcanza su cobertura (educación básica y media). Además, el niño y luego joven tiene derecho a un aprendizaje de calidad y a un trato no discriminatorio, acorde con su dignidad humana (respeto) (UNICEF-2000).

La educación cumple una función socio económica relevante en pos de la superación de la pobreza y el acortamiento de la brecha de desigualdad socioeconómica. De su parte, la libertad de enseñanza supone la posibilidad de que cualquier persona o grupo de personas pueda abrir y mantener establecimientos educacionales. En este modelo, el Estado tiene un rol fundamental como promotor y regulador de la actividad educativa.

Ahora bien, una sociedad conectada en Red requiere políticas de alfabetización digital que consideren de una parte las destrezas necesarias para el manejo de los sistemas de información y de otra, la formación de una “cultura digital” que permee en todas las capas sociales y les permita a las personas conocer e internalizar no sólo el funcionamiento técnico, sino las implicancias de su desenvolvimiento en la nueva sociedad. A vía de ejemplo, las personas no sólo deben saber cómo utilizar los sistemas y servicios asociados a las redes sociales, sino que además deben ser capaces de comprender las consecuencias de sus actos en dichas redes. Debieran ser capaces de diferenciar entre las actividades *off line* y *on line*. Así como a nuestros niños les enseñamos a interpretar las señales de advertencia en la vía pública, habrá de transmitirles las medidas de autocuidado que deben emplear en las redes digitales. Esto, es lo que se ha dado en llamar *Alfabetización digital*.

En segundo lugar, el Derecho a la Educación se ha visto potenciado, en su vis “informal” por las redes y servicios de comunicaciones electrónicas, que recogen, administran y ponen a disposición de los usuarios de Internet, una gran cantidad de contenidos relevantes tanto para apoyar los procesos educativos formales, como para crear esta cultura digital.

Es en este aspecto que nuevamente debemos enfatizar la importancia del acceso a las redes (la conectividad) como un factor esencial para que todos los niños, niñas y adolescentes tengan las posibilidades de acceder a los beneficios de la sociedad en Red en materia educativa.

Ahora, en lo que respecta a la libertad de enseñanza, así como toda persona puede fundar colegios, cualquier persona puede acceder a los nuevos servicios para crear y distribuir contenidos educativos, sobre todo sirviéndose de los beneficios de la convergencia tecnológica.

5.- La libertad de expresión, Derecho a la Información y Derecho de Petición

La libertad de expresión, se erigió en su momento como uno de los bastiones de las democracias modernas, en tanto que empodera a los ciudadanos frente al poder del Estado. Este Derecho, reconocido en el artículo 13 de la Declaración Americana de Derechos del Hombre, en el Artículo 19 de la Declaración Universal de Derechos Humanos y en el Artículo 8 de la Declaración Universal de la UNESCO sobre la Diversidad Cultural, entre otros instrumentos internacionales de Derechos Humanos hoy en día se encuentra en el ojo del huracán pues mientras la ciudadanía se abre espacios en Internet, los grandes conglomerados de las industrias de información hacen asimismo ingentes esfuerzos para copar este nuevo espacio, haciendo avanzar sus poderes hacia las redes digitales.

En todo caso, la evidencia demuestra que se han abierto nuevos canales para expresarse, con una cobertura y alcance mucho mayor, por la naturaleza del medio. Este poder social se ha visto reflejado en el interés creciente de los Estados y de las Grandes corporaciones en que se regule la Red.

Ahora bien, las facilidades para acceder a un medio de expresión en Internet, especialmente en su presentación actual (World Wide Web), que se muestra a los usuarios como una planicie en la que no es fácil diferenciar y categorizar a cada uno de los oferentes de información, pues aparecen como similares o al menos muy parecidos entre sí. En lo que nos concierne, esto conlleva dos situaciones conflictivas:

- a) De una parte basta navegar un poco en la red para que se advierta su fuerte orientación al consumo de bienes o servicios. Pues bien, las dificultades para diferenciar a los distintos oferentes de productos o servicios impide al consumidor categorizar adecuadamente sobre las confianzas que cada uno de los oferentes pueda proporcionarles.

Agrava esta situación el que hay personas que no han alcanzado un grado de “madurez digital”, muchas veces terminan aceptando ofertas de bienes o servicios que se le presentan, sin tomar conciencia real de las consecuencias jurídicas de su actuación. En efecto, la desmaterialización de las relaciones, hace que pierdan el cariz de reales y por tanto no siempre podremos hablar de un consentimiento perfecto de parte del aceptante.

- b) En un segundo punto, en la red encontramos un conjunto descentralizado e inorgánico de información, la que normalmente no está estructurada y menos aún “comentada”. Esto hace que el usuario no siempre esté en condiciones de discriminar en cuanto a la calidad de los contenidos que arroja una búsqueda temática. De esta forma, si bien una cara de la moneda nos lleva a alabar la red, como un modelo de democracia participativa, en que todo quien desee puede publicar información, la otra cara nos hace poner la voz de alarma en cuanto a que en ella encontramos mucha información “basura” y otra definitivamente errónea, inexacta, ilegítima o aún ilícita. Nuevamente llamamos la atención aquí en la necesidad de contribuir a generar una cultura digital en los usuarios, que les permita diferenciar la información de buena calidad de la información basura.

Agrava esta situación el entorno gráfico hipertextual de la red, en cuanto a que una información puede ser presentada ante el usuarios como un hipertexto, dotado de enlaces a distintas partes de la red, que añadirá a la sensación veracidad de la información la de ser información muy bien documentada, y a su vez difuminará la responsabilidad por dichas informaciones.

- c) Un tercer aspecto relevante dice relación con las facilidades para expresarse de manera “anónima” en la red. Esta posibilidad también tiene dos caras, de una parte las tecnologías facilitan que se difundan las ideas en sociedades en donde el temor a la represalia, el terrorismo de Estado o simplemente del más fuerte, ha sido una de las principales mordazas, en este contexto surgen las nuevas tecnologías como liberadoras. Sin embargo la otra cara nos muestra un laboratorio ideal para la difamación, teorías conspirativas y otros vicios de los procesos comunicacionales. Más aún, el hipertexto permite descontextualizar la información, mediante el enlace de distintos sectores de la red, con la consecuente tergiversación de la realidad.

En este aspecto, se habla de contenidos nocivos e ilícitos, que son difundidos a través de estos medios, entre los cuales se menciona: a) aquellos que **incitan al odio** “hate speech”, al desprecio a alguna raza, cultura o grupo determinado, por el sólo hecho de su pertenencia a dicho grupo; b) Los contenidos destinados a la **apología de ideologías extremas** o radicales, tanto en el plano político como religioso; c) en tercer lugar, los contenidos que **desprecian la dignidad humana**, tales como la pornografía, información difamante, imágenes distorsionadas o deformes, etc..

Estos contenidos en general representan un abuso de la libertad de expresión y quedan en consecuencia prohibidos.

En cuanto al derecho de petición, las tecnologías de la información y las comunicaciones han abierto nuevos canales y nuevos espacios para que los ciudadanos formulen sus requerimientos a los distintos poderes de un Estado y/o una sociedad. Este derecho, se relaciona en la sociedad en red al derecho de reunión, en el sentido que a veces cientos o incluso miles de personas, se hacen parte de redes sociales, para los efectos de organizarse frente a la autoridad, si ésta no cede frente a las demandas sociales.

Ahora bien, surge la duda sobre el alcance de estas libertades, en el sentido que en algunas oportunidades los manifestantes ya no se reúnen en una plaza pública, sino que se citan en una determinada dirección electrónica, a la cual atacarán de manera sistemática, como una forma de rechazo a su actuación o simplemente a una persona.

6.- la Protección a la Vida Privada y Honra de las personas: La inviolabilidad del hogar y de toda forma de comunicación privada, y la libertad de conciencia.

En la sociedad en red, el análisis de estos derechos es especialmente crítico, por cuanto las ingentes capacidades de los sistemas de información y las potencialidades de las redes de telecomunicaciones las amenazan de manera constante y uniforme.

Sin entrar en los conceptos de “vida privada”, “honra” o “comunicación privada”, conceptos que los constitucionalistas han tratado de manera extensa, y en el entendido que éstas no son garantías absolutas, sino que admiten limitaciones, derivadas del interés general o de los derechos de terceros de acceder a información específica respecto de una persona, pondremos el acento en tres tipos de tecnologías que pueden resultar atentatorias contra estos derechos fundamentales:

- a) **Sistemas de escucha tecnológica**, que tienden a recoger información desde las redes y sistemas de comunicaciones electrónicas, proveniente por ejemplo de las navegaciones web, de la participación de una persona en redes sociales, del empleo de sistemas de telecomunicaciones, entre otros.
- b) **Sistemas de videovigilancia**: consistente en la captura de imágenes o sonido o ambos, sumado normalmente al procesamiento y almacenamiento de estos materiales.
- c) **Sistemas de control telemático**: Que consisten en dispositivos y sistemas que tienen la capacidad de realizar vigilancia a distancia de personas y/o cosas. Se distingue entre dispositivos RIFD por sus siglas en Inglés, que son Dispositivos de identificación por radiofrecuencia, Mecanismos de control Biométrico, tales como lectores de iris, de huella digital o mecanismos de identificador por reconocimiento de voz; dispositivos GPS, que son capaces de posicionar a la persona o cosa en tiempo real, para conocer su ubicación y desplazamientos. Este último es el caso de los brazaletes telemáticos de videovigilancia
- d) **Sistemas de identificación tecnológica**: Tales como sistemas de recogida y análisis de evidencia, por ejemplo muestras biológicas para su análisis y comparación de huellas de ADN. Bases de datos de ADN para finalidades de interés criminal, como la identificación de víctimas o victimarios de delitos

Atendida la variedad de sistemas que pueden afectar estos derechos, en nuestro caso fijaremos los límites que se reconocen respecto del desarrollo e implementación de tecnologías en estos ámbitos, a saber:

- e) **Razonabilidad**: Reconociendo que puede existir un derecho o interés legítimo en la recogida de información respecto de una persona, el respeto a las garantías fundamentales en comento exige que exista fundamento razonable para la implementación de estas medidas, que las autoridades que las imponen hagan un tratamiento de las mismas dentro del marco de la finalidad para la que se establecieron y que se mantengan almacenadas sólo el tiempo que se necesario para esa finalidad.
- f) **Licitud**: El empleo de tecnologías intrusivas debe fundarse en normas jurídicas que regulen la oportunidad, forma y condiciones de las medidas. De su parte, las autoridades que las impongan y/o apliquen en cada caso concreto, deben estar investidas de las competencias necesarias para realizar estas actividades.
- g) **Calidad**: En el sentido que los procesos y sistemas de tratamiento de esta información deben cumplir exactamente con los imperativos anteriores y además garantizar la seguridad de que esta información no será afectada por ataques o por errores o fallas que pueda destruirla, inutilizarla o alterarla. Asimismo, afecta la calidad el que los sistemas no prevean mecanismos de seguridad asociadas a los procesos de comunicación de esta información, tales como sesionización, control de accesos, registros de la información requerida y aquella que efectivamente se entregó, etc.

Como podemos apreciar, los Derechos Fundamentales que hemos seleccionado, que vienen desde la primera generación de Derechos, que se re moldearon en la segunda o tercera generación, se han visto impactadas por las Tecnologías de la información y las comunicaciones, pero esto no es todo, como señalamos, hay entornos en los cuales se han

venido configurando nuevos derechos fundamentales. Este es el caso de la protección de Datos personales, como veremos en el acápite siguiente.

Nueva sociedad, nuevos Derechos Humanos?.

El desarrollo progresivo de los derechos humanos, se ha sistematizado por la doctrina en las “generaciones”, que no son sino diversos estadios de avance del bloque de derechos. En nuestro análisis anterior nos hemos referido a algunos derechos y las amenazas u oportunidades que les afectan y que se originan en las tecnologías de la información y las comunicaciones. Pues bien, hay casos concretos en los cuales existe la convicción de que un hecho tecnológico afecta la dignidad, la igualdad, o la libertad humana, pero no queda claro que alguna de las categorías tradicionales de derechos humanos se ajuste completamente a su descripción. Es el caso del tratamiento de datos personales, en que existe un consenso bastante amplio en que hay derechos (fundamentales y no fundamentales) que se ven afectados por el tratamiento de datos, pero no queda claro cuál es el derecho fundamental al que debe adscribirse.

Si bien en un principio se pensó que la intimidad era el derecho adecuado para radicar la protección de datos personales, hoy en día queda claro que esto no es efectivo.

Desde el año 1983, en que el tribunal constitucional Alemán se pronuncia respecto de la ley del Censo, y configura la “autodeterminación informativa” como un derecho autónomo, y más tarde el Tribunal Constitucional Español, en 1990, hiciera lo propio, bajo la denominación “libertad informática” se ha ido configurando las bases de este nuevo derecho, que en definitiva se sienta sobre tres bases concretas:

- a) El reconocimiento de que las personas a que se refieren o conciernen los datos personales son sus únicos “dueños” y por ende la imposibilidad de que los terceros que los recogen, almacenan, y en general, que realizan operaciones de tratamiento, adquieran el dominio de estos datos, sino que a lo más serán sus custodios. Del mayor o menor desarrollo de este eje dependerá el régimen de responsabilidad que se defina en un Estado Determinado.
- b) La convicción de que todo dato personal es relevante y por tanto ha de protegerse respecto de su tratamiento por terceros, distintos de su titular. Esto sin perjuicio de reconocerse que existen datos más sensibles que otros, como veremos más adelante. El desarrollo de este aspecto conlleva la configuración legal del derecho a tratar datos de terceros y el encasillamiento de cada tipo de dato personal en cada una de las categorías que se definan (datos de libre acceso al público, datos sensibles, etc.)
- c) La consecuencia necesaria de las dos anteriores: los titulares de los datos deben, en todo momento, poder controlar el uso que los terceros hacen de los datos personales que le conciernen. Esta es la base sobre la cual se desarrollan los distintos derechos que se reconocen al titular de datos personales, usualmente conocidos como derechos ARCO, esto es Acceso, Rectificación, Cancelación y Oposición, al tratamiento de datos personales.

Como señalamos antes, este nuevo derecho ha sido reconocido en las nuevas constituciones, en los aspectos antes señalados, haciendo especial énfasis en la necesidad de proteger a la

persona (titular de los datos) contra la actuación abusiva de los terceros que por distintas razones, acceden a sus datos personales.

Libertad Informática o autodeterminación informativa como un Derecho Humano emergente en la sociedad en Red. Situación Chilena

Si bien Chile no ha reconocido la libertad informática o la autodeterminación informativa como un Derecho Fundamental, luego de un largo proceso legislativo que se inició en 1984, el 28 de agosto de 1999 se publicó en el diario oficial la Ley 19.628, bajo el título “Ley sobre protección de la vida privada”, pero que respondería mejor al título “Regulación del Tratamiento de Datos Personales”.

Si bien en principio la ley vino a desarrollar el artículo 19 No. 4 de la Constitución, que garantiza **“El Derecho al Respeto o Protección de la Vida Privada y la Honra de las Personas y su Familia”**.

En cuanto a su estructura, la ley, se divide en un título preliminar, referido a su ámbito de aplicación y algunos conceptos básicos, 5 títulos en que regula la utilización de datos personales en general y la de aquellos relativos a obligaciones de carácter económico, financiero, bancario o comercial; asimismo dedica un título al tratamiento realizado por organismos públicos, otro a los derechos de los titulares de datos y uno a las infracciones y sanciones a esta ley; finalmente podemos apreciar un título final y tres artículos transitorios, referidos a la vigencia de la norma. En términos generales, la ley entró en vigor vencidos los 60 días desde su publicación en el Diario Oficial, salvo el artículo 22, que regula la obligación de registro de los bancos de datos que administra el Estado, que entró en vigor el día 28 de agosto del año 2000.

Desde su publicación hasta hoy, más de 50 proyectos de ley han tratado de modificarla, pero sólo han llegado a término un par iniciativas. La primera fue la ley 19812 (2002), y la ley 20463 (2010), ambas dictadas en periodo de crisis económica y para limitar el tratamiento de datos personales relativos a solvencia patrimonial y morosidades.

A.- Ámbito de aplicación de la ley 19628

El ámbito de aplicación de esta ley está regulado en su artículo 1º, en los términos siguientes **“El tratamiento de datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley”**. Como podemos apreciar, el ámbito de aplicación de la ley se fija a partir de tres conceptos fundamentales, a saber:

- a) **Tratamiento de datos:** conceptualizado en el artículo 2 letra o), como “cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizados o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal o utilizarlos de cualquier forma”.

Como podemos apreciar, esta norma no discrimina entre operaciones manuales o automatizadas de tratamiento de datos personales, acogiendo de esta forma el estándar europeo. Esto tiene por objeto ampliar la protección frente al reconocimiento

de que todas las fases de tratamiento entrañan riesgos para la persona que es titular de los datos personales.

El legislador, en todo caso, se ocupa de definir algunas de las operaciones de tratamiento de datos. Este es el caso de “almacenamiento de datos” (Art. 2 letra a)), definido como “la conservación o custodia de datos en un registro o banco de datos”; la comunicación o transmisión de datos (Art. 2 letra c), que consiste en dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas. Finalmente define el procedimiento de disociación de datos, en tanto tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable.

- b) En segundo lugar y en cuanto al objeto de dicho tratamiento, la norma señala que éste recae sobre los **datos personales** o **datos de carácter personal** que la Ley define como “los relativos a cualquier información concerniente a personas naturales identificadas o identificables” (Art. 2 letra f) Ley 19628).

Como podemos apreciar, la ley, en su texto vigente, acoge las tendencias generales en derecho comparado, que exigen que **los datos sean concernientes a personas naturales**, no así a personas jurídicas; esto si bien hoy existen proyectos de ley que se tramitan en el parlamento, que buscan ampliar la protección hacia las personas jurídicas.

Un segundo requisito es que las personas a que se refieren los datos sean identificadas o identificables. A partir del análisis de este requisito en derecho comparado podemos señalar que el que la persona sea identificable significa que sea posible determinar la identidad del titular de los datos a partir de los mismos y/o de otras operaciones de tratamiento de datos complementarias. En todo caso, uno de los aspectos más críticos en esta materia ha sido fijar los límites de las potencialidades de identificación de un dato, especialmente en aquellos ámbitos en que el desarrollo de la técnica es la condición para la identificabilidad.

Como contrapartida, los **datos estadísticos**, son aquellos que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable (Art. 2 letra e) Ley 19628).

- c) Continuando con nuestro análisis, el tratamiento de datos personales debe realizarse en un **Registro o Banco de Datos**. A este respecto la ley entiende por tal un “conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento” (Art. 2 letra m) de la ley).

Desde otra óptica, el ámbito de aplicación de la ley, en cuanto a los sujetos involucrados en el tratamiento de datos, la Ley se aplica tanto a los organismos públicos como a las entidades privadas que hacen tratamiento de datos personales. Sin perjuicio de ello, en la ley se atiende especialmente a los **Organismos Públicos**, entendiendo por tales “las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1° de la Ley 18.575, Orgánica Constitucional de bases Generales de la Administración del Estado”, esto es el conjunto de organismos que forman la administración del Estado, a saber: “los Ministerios, las

Intendencias, las Gobernaciones y los órganos y servicios públicos creados para el cumplimiento de la función administrativa, incluidos la Contraloría General de la República, el Banco Central, las Fuerzas Armadas y las Fuerzas de Orden y Seguridad Pública, las Municipalidades y las empresas públicas creadas por ley".

Ahora bien, también podemos mirar el ámbito de aplicación de la ley **desde la óptica de la finalidad** del tratamiento de datos personales. En este aspecto diremos que la ley se aplica a todo tratamiento de datos, salvo que se efectúe en ejercicio de las libertades de emitir opinión y de informar, reconocidas por el artículo 19 No. 12 de la Constitución Política de la República, el que se regulará por la Ley 19733, Sobre Libertades de opinión e Información y Ejercicio del Periodismo.

B.- Categorías de Datos Personales en la Legislación nacional

Como señalamos antes, en la legislación nacional, reconociendo la tendencia internacional, reconoce que existen al menos dos categorías de datos personales: a) Los **datos de libre acceso al público, y datos sensibles**. El encasillamiento de los datos personales en alguna de estas categorías va a depender de la consideración en cuanto si su tratamiento afecta negativamente o no a algún Derecho Fundamental. Analicemos los contenidos de cada una de estas categorías:

- a) **Datos de acceso público:** En general, en Chile son datos de libre acceso al público, aquellos que constan en fuentes de acceso público, entendiéndose por tales los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes (Artículo 2 letra i). Este es uno de los conceptos más controvertidos de la ley, por cuanto basta que el titular del banco de datos defina las condiciones de no restringido o reservado para que todos los datos almacenados queden exceptuados de muchos de los mecanismos de resguardo que establece la ley. De hecho, durante la tramitación de la ley se planteó la necesidad de que sólo fueran fuentes accesibles al público, aquellas que la ley expresamente calificara como tales, lo que no fue aceptado en definitiva.
- b) **Datos sensibles:** De su parte, la ley considera que son "sensibles" los datos personales que se refieren a las **características físicas o morales** de las personas o a **hechos o circunstancias de su vida privada o intimidad**, tales como los **hábitos personales**, el **origen racial**, las **ideologías y opiniones políticas**, las **creencias o convicciones religiosas**, los **estados de salud físicos o psíquicos** y la **vida sexual** (Art. 2 letra g) de la Ley).

La como "sensibles" de estos datos, se funda en que su uso indiscriminado puede traer aparejado que se tomen decisiones arbitrarias respecto de sus titulares, con el consecuente desmedro de la dignidad humana y las garantías personales que de ella derivan. Es por lo anterior que en cuanto a estos datos y atendido el peligro ínsito en su tratamiento, la Ley invierte la norma de base, estableciendo que en general no podrán ser objeto de tratamiento, sino en caso que **una ley lo autorice o que el titular consienta** en ello **o que el tratamiento sea necesario para la**

determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

Adicionalmente, frente a esta evidencia, el artículo 24 de la Ley introduce una importante modificación al artículo 127 del código Sanitario, en virtud de la cual otorga el carácter de reservado a las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios de salud. De esta forma, sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito, bajo apercibimiento de aplicarse al infractor las sanciones previstas en el título X de dicho cuerpo legal.

Como excepción a esta norma, se establece la posibilidad de que las farmacias puedan dar a conocer, para fines estadísticos, las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos, siempre y cuando no se consigne el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos.

- c) Aunque la ley no dice nada, de sus normas desprendemos que establece una categoría especial de datos personales, regulada latamente a lo largo de sus normas. Es el caso de los **“datos de carácter económico, financiero o de carácter comercial”**, que comprende tanto datos relevantes en procesos de mercadeo como aquellos datos necesarios para la determinación de la solvencia patrimonial de la persona.

C.- Principios que rigen el tratamiento de datos personales en Chile

Al igual que en Derecho Comparado, la ley 19628 se basa en principios, los cuales, en todo caso, no son sistematizados ni conceptualizados expresamente por la ley, como sí lo hace la ley 20.285, de transparencia y acceso a la información pública. En este acápite realizaremos el ejercicio conceptual y sistematizador, basándonos en la experiencia comparada. En todo caso, debemos tener presente que la forma de organizar estos principios puede variar de acuerdo al énfasis con el que cada jurista se acerca a este fenómeno. Siendo así, la nuestra es sólo una propuesta, que apunta a la mejor comprensión de esta problemática.

1.- Buena fe (lealtad en el Tratamiento de datos personales)

Este principio es una derivación del principio de buena fe que informa a nuestro sistema jurídico. Conforme a él, las personas naturales o jurídicas, privadas o públicas, que realicen tratamiento de datos personales, deben observar este principio en todas las etapas del procedimiento de tratamiento de datos. Las siguientes son las principales manifestaciones de este principio:

a) **Finalidad:** En general, los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, con la excepción de aquellos datos que provengan o se hayan recolectado de fuentes accesibles al público (Art. 9 ley 19628).

El principio informa todas las etapas del procedimiento de datos personales. A vía de ejemplo, en la operación de comunicación de datos, la ley establece que el responsable del banco de datos deber realizar una evaluación del requerimiento, y podrá establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes.

Consecuentemente con este principio, la Ley exige que ante a un requerimiento de datos personales mediante una red electrónica, deberá dejarse constancia de la **individualización del requirente; el motivo y el propósito del requerimiento, y el tipo de datos que se transmiten**. En todo caso la responsabilidad de la petición será del requirente, quien sólo puede utilizar los datos personales para los fines que motivaron la transmisión, salvo que se trate de datos personales accesibles al público en general o si se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes (Art. 5 Ley 19628).

b) Consentimiento /Autorización: Si bien la ley habla de autorización, es más adecuado hablar de consentimiento, por cuanto de su contenido se desprende que sólo será legítimo el tratamiento de datos cuando concurra la voluntad del titular de los datos personales, el cual debe ser adecuadamente informado acerca de las consecuencias jurídicas de su consentimiento u oposición al tratamiento de sus datos (Art. 4 Ley 19628).

Cualidades del consentimiento:

i.- Informado. al momento de requerir los datos deberá darse a conocer al titular de los mismos: a) el **propósito del almacenamiento** de sus datos, esto es la finalidad del tratamiento de sus datos personales; y b) su **posible comunicación** al público, o sea quienes serán en definitiva los destinatarios del fichero y de los datos que a él conciernen; y c) Asimismo, cuando los datos personales se recolecten a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, se deberá informar a las personas del carácter **obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información**.

ii.- Expreso y por escrito: El escrito correspondiente de deberá dar cuenta de sus alcances, en relación con los aspectos que deben ser objeto de información.

iii.- Revocable: El titular puede **revocar** en cualquier momento la autorización del tratamiento de datos que le conciernen. En todo caso y cuanto a las características de esta revocación, debe realizarse por escrito y no tendrá efecto retroactivo.

Excepciones al consentimiento:

Si bien la regla general es que se exija consentimiento del afectado por el tratamiento de datos, la Ley prevé algunas excepciones. En primer lugar y tal como señaláramos antes, la Ley permite que exista un tratamiento de datos personales aún sin el consentimiento del interesado en los siguientes casos:

i.- tratándose de **datos de carácter económicos, financieros o comerciales** extraídos de **fuentes accesibles al público** y que se contengan en listados relativos a una **categoría de personas** que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento o que sean **necesarios para comunicaciones comerciales de respuesta directa** o comercialización o venta directa de bienes o servicios. En consecuencia, esta excepción requiere la concurrencia de las siguientes condiciones:

- Que se trate de datos que se recolecten de **fuentes accesibles al público**. Como ya vimos, en este aspecto la ley ha sido muy controvertida.
- En segundo lugar se requiere que sean de carácter **económico, financiero, bancario o comercial**. La respuesta al alcance de este requisito la debemos buscar en la legislación general. Siendo así y atendiendo a la necesaria interpretación restrictiva de esta norma, debiera tratarse de datos personales referidos a aquellas actividades reguladas expresamente por la legislación económica, financiera o comercial.
- En cuanto a la **finalidad de la recogida**, la legislación exige que se cumpla al menos una de las condiciones siguientes:
 - Que los datos se contengan en listados relativos a una **categoría de personas** que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento. Con esta enumeración meramente ejemplar, el legislador impide que se incluyan datos sensibles en este tratamiento “no autorizado” por el titular de los datos, O
 - Que el tratamiento sea necesario para **comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios**. Se trata de ficheros destinados a actividades de marketing directo. En consecuencia y conforme al principio en estudio, ésta será la única actividad en que es posible utilizar estos datos; todo uso de estos ficheros fuera de ella constituirá una intrusión ilegítima, sancionada conforme a las normas que analizaremos en su oportunidad.

En todo caso, conforme al principio en estudio, debiera reconocerse el derecho de oposición al tratamiento de datos por parte de su titular, a través del establecimiento de mecanismos que le permitan oponerse al tratamiento de sus datos para estas finalidades. Un principio de regulación en este aspecto lo encontramos en la ley 19496, en su artículo 28 B inciso II, que dispone: *“Los proveedores que dirijan comunicaciones promocionales o publicitarias a los consumidores por medio de correo postal, fax, llamados o servicios de mensajería telefónicos, deberán indicar una forma expedita en que los destinatarios podrán*

solicitar la suspensión de las mismas. Solicitada ésta, el envío de nuevas comunicaciones quedará prohibido”.

ii.- En segundo lugar, no es necesario el consentimiento cuando se trate de un tratamiento de datos efectuado por **personas jurídicas privadas**; para el **uso exclusivo suyo, de sus asociados o de las entidades a que estén afiliadas** y que sea realizado con **finés estadísticos, de tarificación u otros de beneficio general de aquellos**.

Nos parece que esta norma es extremadamente peligrosa, por cuanto viene a legitimar prácticamente cualquier tratamiento de datos personales, bajo el pretexto de realizarse en el marco de una asociación y para cualquier beneficio de los asociados. En todo caso nos parece que la excepción no alcanza a aquellos tratamientos de datos que sean contrarios a la normativa general o que vulneren garantías personales de los afectados.

c) Publicidad: Conforme con el principio de lealtad y licitud, el tratamiento de datos personales no puede ser reservado y menos aún secreto. Así se ha reconocido en derecho comparado. A vía ejemplar, la Directiva Europea 46/95 prevé que los ordenamientos jurídicos internos deben considerar la obligación de dar publicidad a los bancos de datos, a través de registros de libre acceso al público. El fundamento de este requisito dice relación con la necesidad de que los titulares de datos puedan ejercer efectivamente los derechos que les reconoce la ley, para lo cual requieren al menos saber qué bancos de datos existen.

En Chile el reconocimiento de este principio es sólo parcial, pues sólo se prevé respecto de los organismos públicos, a cuyo respecto se prevé el **deber de notificación y registro** (Art. 22 inc 2 y 3 Ley 19628): Los organismos públicos que tratan datos, deberán notificar al Registro Civil, respecto de cada uno de los bancos de datos que administre, el **fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas** que comprende.

En cuanto a la oportunidad, la ley prevé que deberá notificarse las circunstancias anteriores al momento de dar inicio a la actividad de tratamiento de datos, en relación al respectivo banco de datos y luego, mientras el banco de datos esté en funcionamiento, si cambia alguno de estos elementos, deberá notificarlo dentro de los quince días siguientes.

En todo caso, esta obligación no ha sido del todo acogida por los organismos públicos, principalmente por desconocimiento y porque la ley no prevé mecanismos efectivos para exigir su cumplimiento. En efecto, la ley no establece, como infracción específica el no cumplimiento de la obligación de registro, sin perjuicio de lo establecido en materia de responsabilidad, como veremos más adelante.

2.- Legalidad (Licitud del tratamiento de datos personales)

En términos generales, si consideramos que la protección de la persona frente al tratamiento de datos personales, afecta derechos fundamentales o incluso puede llegar a constituirse en una garantía autónoma, estaremos contestes en que las actividades de tratamiento de datos personales se rigen por el principio de legalidad y por tanto deben cumplir una serie de condiciones en el tratamiento de datos personales, a saber:

a) Deber de calidad: Podríamos incluir esta obligación en cualquiera de las clasificaciones de principios, sin embargo hemos optado por tratarla a propósito de la legalidad por cuanto entendemos que el tratamiento de datos que no cumple con esta condición no sólo es ilegítimo sino derechamente es contrario a la ley. Siendo así, la calidad se refiere a tres ámbitos esenciales:

i.- Fundamento legal: Esto es, que exista autorización legal para realizar tratamiento de datos personales. Dicho en otros términos, para que el tratamiento de datos sea lícito debe existir una ley que autorice el tratamiento y señale las condiciones que deben cumplirse en esta actividad. En último término, esta ley será la propia ley 19.628, que dispone que podrá realizarse tratamiento de datos cuando una ley lo señale, o el titular consienta en ello o concurra alguna de las excepciones que esta misma norma señala.

En todo caso, entendemos que el fundamento legal, además de la autorización para tratar datos, modela esta actividad, al establecer las reglas de tratamiento para cada categoría de datos personales

ii.- Calidad de datos: Para que un tratamiento de datos personales cumpla con esta condición, es necesario que se cumplan los siguientes requisitos:

- Que se trate de **datos verídicos y vigentes en cada momento**, de forma tal que la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos. De esta forma, infringe la normativa el tratamiento de datos caducos, erróneos inexactos, equívocos o incompletos.

Consecuente con lo anterior, la ley prevé que si los datos personales objeto de tratamiento son erróneos, inexactos, equívocos o incompletos, procede su **modificación** (Arts. 6 y 12 inc. 2 Ley 19628). De su parte dispone **su eliminación** cuando hayan devenido en caducos o su tratamiento carezca de fundamento legal (Art. 6 inc. 1 y 12 Ley 19628). Finalmente la norma exige que **se bloqueen** los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación.

En caso que los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos deberá **comunicarles** a la brevedad posible la operación efectuada. Si no fuese posible determinar las personas a quienes se les hayan comunicado, deberá poner un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos (Art. 12 Ley 19628).

Para los efectos del cumplimiento del deber de calidad, en cuanto a los datos, deberemos considerar que la Ley entiende por **dato caduco** el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que

consigna (Art. 2 letra d ley 19.628). En cuanto a los datos erróneos la Ley no los define y por tanto deberemos atender al sentido natural y obvio de estos términos.

De manera consecuente, la ley prevé las obligaciones correspondientes, respecto del Titular del banco de datos: a) Deber de **eliminación o cancelación, que implica** la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello (Art. 2 letra h), ley 19628) cuando concurren las causales legales; b) Deber de **modificación**, entendida como todo cambio en el contenido de los datos almacenados en registros o bancos de datos (Art. 2 letra j) , ley 19628) cuando éstos sean erróneos, inexactos; c) Deber de **bloqueo**, que consiste en la suspensión temporal de cualquier operación de tratamiento de los datos almacenados (art. 2 letra b), Ley 19628) en caso que la exactitud de los datos no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación. Estas obligaciones adquieren vigencia por el solo hecho de que los datos pierdan estas condiciones de calidad, sin necesidad incluso de requerimiento del titular.

Tratándose de datos **relativos a obligaciones de carácter económico, financiero, bancario o comercial obtenidos de fuentes accesibles al público, procede el deber de modificación** si se extingue la obligación por el pago o por otro modo en que intervenga directamente el acreedor. En este caso el acreedor deberá avisar dentro de los siete días siguientes a la extinción de la obligación, al responsable del **registro o banco de datos accesible al público** que en su oportunidad comunicó el protesto o la morosidad, a fin que consigne el nuevo dato correspondiente. Asimismo el titular de los datos podrá requerir directamente la modificación y liberar del cumplimiento de esa obligación al acreedor que le entregue constancia suficiente del pago; decisiones que deberá expresar por escrito. En este caso, el legislador se ha alejado de las reglas generales y ha previsto que si la modificación de los datos involucra una tarifa, cobrada por el responsable del banco de datos accesible al público, ésta será de cargo del deudor.

Ahora bien, en caso de incumplimiento de su deber de consignar esta nueva información el afectado podrá exigir su cumplimiento por vía judicial (Art. 19 inc. 2, ley 19628).

En todo caso la doctrina estima que esta norma sólo puede aludir al boletín comercial como responsable del tratamiento de estos datos en la legislación vigente. Esta interpretación se funda en que la norma, a renglón seguido, establece que quienes efectúen el tratamiento de datos personales provenientes o recolectados de la aludida fuente accesible al público, deberán modificar los datos en el mismo sentido tan pronto aquélla comunique el pago o la extinción de la obligación, o dentro de los tres días siguientes. Si no les fuera posible, **bloquearán** los datos del respectivo titular hasta que esté actualizada la información (Art. 19 Inc. 3, Ley 19628).

Estimamos que estas obligaciones se aplican en este caso conforme a las reglas generales, esto es aún sin necesidad de requerimiento del titular y sin que sea lícita la exigencia de contraprestación pecuniaria alguna. En cuanto a la infracción de cualquiera de estas obligaciones se conocerá y sancionará de acuerdo a lo que veremos a propósito de la tutela efectiva del interesado.

- **Que sean adecuados, pertinentes y no excesivos:** Se trata de que las personas que realizan tratamiento de datos personales circunscriban sus actividades sólo a los datos estrictamente necesarios para satisfacer las necesidades de información asociadas a la finalidad del tratamiento de datos. Adicionalmente, que mantengan los datos personales en

sus registros sólo durante el tiempo que sea necesario para cumplir con esta finalidad, de ahí que se hable de que el tratamiento de datos es esencialmente temporal.

iii.- **Calidad de Procesos:** Se refiere a que las operaciones de tratamiento de datos personales se rijan, en su desarrollo, por estándares de calidad y adecuación. A vía ejemplar, el artículo 5 de la ley 19628, es una norma de calidad de procesos, en tanto los resguardos que deben tomarse por los responsables del tratamiento de datos personales, cuando establezcan sistemas de transferencia electrónica. Lo mismo sucede con las normas que vimos, que regulan la obligación de modificación, cancelación y bloqueo de datos personales. Adicionalmente, cuando hablamos de calidad de procesos, necesariamente debemos atender a los siguientes aspectos:

i.- Seguridad en el Tratamiento de los Datos Personales

Nuestro legislador a este respecto dispone que el responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños (Art.11, ley 19.628). Como ya analizáramos la responsabilidad alcanza tanto al daño patrimonial como al daño moral.

De su parte, las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo (Art. 7 Ley 19628).

ii.- Temporalidad del Tratamiento.

La normativa internacional en general es conteste en señalar que no puede existir un tratamiento de datos personales que contenga datos “históricos”. En efecto la sociedad en general ha establecido ciertas instituciones que involucran un olvido de ciertas circunstancias en pos del principio de seguridad jurídica y de la paz social. Los sistemas informáticos de tratamiento de datos personales no pueden quedar ajenos a estas instituciones, más aún si atendemos a que tradicionalmente el tiempo y la distancia ayudaban a pacificar las relaciones sociales al borrar ciertas huellas que podían traer discordia entre los integrantes de una comunidad. Hoy en día las redes informáticas y las posibilidades de almacenamiento de grandes cantidades de información hacen más difícil este olvido social, cuestión que los legisladores tratan de paliar a través de las instituciones del bloqueo y la cancelación de datos.

De esta forma, la Ley dispone que en ningún caso pueden comunicarse datos **relativos a obligaciones de carácter económico, financiero, bancario o comercial**, que se relacionen con una persona identificada o identificable, luego de transcurridos siete años desde que la respectiva obligación se hizo exigible o después de tres años del pago de dicha obligación o de su extinción por otro modo legal, salvo que el requirente sea un tribunal de justicia y la solicite con motivo de algún juicio pendiente (Art. 28, ley 19628).

Asimismo, tratándose de datos sobre sanciones administrativas o penales, los organismos públicos que mantengan los bancos de datos en que se contengan no podrán comunicarse una vez que haya prescrito la acción penal o administrativa, o que se haya cumplido o prescrito la sanción o la pena (Art. 21 inc. 1 Ley 19628), salvo cuando esos datos les sean solicitados por los tribunales de Justicia u otros organismos públicos dentro del ámbito de su competencia.

C.- Tutela Efectiva al Titular de los Datos.

Como contrapartida al deber de calidad, la ley considera a los derechos del titular de datos personales como herramientas que pone a su servicio para controlar la calidad de los datos y de los procesos de tratamiento y como contrapartida de las obligaciones de los titulares de bancos de datos. La ley destina su Título II al análisis de los **derechos del titular de los datos**: derecho de **acceso, modificación, cancelación o bloqueo** de sus datos personales, en los términos siguientes:

- Conforme al derecho de acceso, que la ley llama **derecho de información**, toda persona tiene derecho a exigir a quien sea responsable de un banco de datos, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente (Art. 12 inc. 1 Ley 19628). Este derecho podrá ejercerse de manera gratuita en la medida que medien al menos 6 meses entre cada oportunidad en que lo ejerza.
- De su parte, el derecho de **modificación** podrá exigirlo en caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite.
- El **derecho de cancelación**, podrá ejercerlo para que se eliminen los datos que le conciernen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos o cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.
- Adicionalmente, en todo caso, si así lo estima pertinente podrá solicitar el **bloqueo de los datos**.

Estos derechos podrán ser exigidos por el titular de los datos al responsable del fichero en forma absolutamente gratuita, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente. Asimismo, si con posterioridad se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, obtener sin costo copia del registro actualizado, siempre que haya transcurrido a lo menos seis meses desde la precedente oportunidad en que hizo uso de este derecho. En todo caso el derecho a obtener copia gratuita sólo podrá ejercerse personalmente (Art. 12 inc. 4, ley 19628).

Naturaleza Jurídica de los derechos del Titular de Datos Personales

En cuanto a la **naturaleza Jurídica** de los derechos del Titular de datos personales, entendemos estamos frente a derechos irrenunciables. No obstante no son derechos absolutos, la ley dispone que no podrán ser limitados por medio de ningún acto o convención (Art. 13, ley 19628).

Ahora bien, tratándose de bancos de datos de la administración pública, podrá denegárseles si con su ejercicio se impide o entorpece el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o se afecta la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional (Art. 15 inc. 1, Ley 19628). Asimismo, tampoco procede la modificación, cancelación o bloqueo de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva; en este caso sin embargo no puede restringirse el derecho de información (Art. 15 inc. 2 Ley 19628).

Sujeto pasivo de los derechos del Titular de datos personales:

El **sujeto pasivo** de estos derechos es el responsable del banco de datos (conforme a la nomenclatura adoptada por la Ley). Tratándose de la administración pública lo será el organismo respectivo y si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos (Art. 14, ley 19628).

Habeas Data como acción judicial prevista en la ley para la tutela de los derechos del Titular de Datos Personales

La acción de habeas data representa una adecuación del tradicional habeas corpus a la protección de datos personales. Se trata de proveer un medio coersitivo para que la persona pueda acceder al reporte de sus datos personales, que son objeto de tratamiento de datos terceros, cuando el requerido **no se pronuncia de manera oportuna frente a su requerimiento**, o responde con una **negativa injustificada**.

Causales:

i.- la primera causal es el **no pronunciamiento dentro del plazo legal**, que es de **dos días hábiles**.

ii.- La segunda causal es la **denegación injustificada**. Al respecto la ley distingue entre negativas fundadas en la necesidad de protección del interés nacional o la seguridad de la nación o negativas que no esgrimen este fundamento, lo cual tendrá importancia para los efectos de la determinación del Tribunal competente y del procedimiento aplicable, como veremos.

Tribunal competente:

Si el requerido derechamente no fundamenta o no funda la negativa en el interés de la nación o la seguridad nacional el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, que se encuentre de turno según las reglas correspondientes, solicitando amparo a los derechos de información, modificación, bloqueo o cancelación según sea el caso. En el caso contrario, deberá interponer la acción en la Corte Suprema (Art. 16, ley 19628).

Requisitos de interposición:

La ley exige que la acción sea fundada, esto es que se explicita claramente la infracción cometida y los hechos que la configuran. Además esta presentación deberá acompañarse de los medios de prueba que los acrediten, en su caso (Art. 16 inc. 1, Ley 19.628).

Procedimiento:

De la reclamación se notificará por cédula dejada en el domicilio del responsable del banco de datos correspondiente, quien deberá presentar sus descargos dentro de quinto día hábil y adjuntar los medios de prueba que acrediten los hechos en que los funda. De no disponer de ellos, expresará esta circunstancia y el tribunal fijará una audiencia, para dentro de quinto día hábil, a fin de recibir la prueba ofrecida y no acompañada.

La sentencia definitiva se dictará dentro de tercero día desde que la causa quede en estado de fallo, esto es desde que venció el plazo para presentar descargos háyanse presentado o no, o desde la fecha fijada para la audiencia de prueba.

La sentencia se notificará por cédula y respecto de ella procederá el recurso de apelación, el que deberá interponerse en el término fatal de cinco días, contado desde la notificación de la parte que lo entabla. La apelación en todo caso deberá ser fundada; deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan.

Interpuesta apelación, el recurso se concederá en ambos efectos y el tribunal elevará de inmediato los autos a la Corte de Apelaciones respectiva. Recibidos los autos en la Secretaría de la Corte, el Presidente ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes. En todo caso si la sala a quien toca conocer del

asunto lo estima conveniente o se le solicita con fundamento plausible, podrá ordenar que se traigan los autos en relación para oír a los abogados de las partes, caso en el cual la causa se agregará extraordinariamente a la tabla respectiva de la misma sala. El fallo que recaiga sobre este recurso no será susceptible del recurso de casación.

En todo caso, toda otra resolución distinta de la sentencia definitiva, que se dicte en el procedimiento será inapelable y se notificará por el estado diario.

Tratándose de la **denegación de la solicitud invocando como causal la seguridad de la Nación o el interés nacional**, la reclamación deberá deducirse **ante la Corte Suprema**. Una vez interpuesto la Corte Suprema solicitará informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual resolverá en cuenta la controversia; sin embargo si la sala que conoce del asunto lo estima pertinente o se le solicita con fundamento plausible podrá ordenar que se traigan los autos en relación para oír a los abogados de las partes, caso en el cual el asunto se agregará en forma extraordinaria a la tabla de esa misma sala; en todo caso y atendida la causal invocada, el presidente del tribunal ordenará que la audiencia no sea pública. En caso de recibirse prueba, se consignará en un cuaderno separado y reservado, que conservará ese carácter aun después de afinada la causa si por sentencia ejecutoriada se denegare la solicitud del requirente.

Tanto en uno como en otro caso si se acoge la reclamación, la misma sentencia fijará un plazo prudencial para dar cumplimiento a lo resuelto y podrá aplicar una multa de una a diez unidades tributarias mensuales. De su parte, tratándose de la falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decreta el Tribunal, serán castigados con multa de dos a cincuenta unidades tributarias mensuales y, si el responsable del banco de datos requerido fuere un organismo público, el tribunal podrá sancionar al jefe del Servicio con la suspensión de su cargo, por un lapso de cinco a quince días (Art. 16 inc. Final, ley 19628).

Acción indemnizatoria conjunta con el habeas data

La ley contempla la posibilidad que conjuntamente con la reclamación destinada a establecer la infracción el afectado impetere la acción destinada a obtener de la persona natural o jurídica privada o el organismo público responsable del banco de datos personales, una indemnización por los daños y perjuicios patrimoniales y morales sufridos por el titular de los datos, a raíz del uso indebido de los datos que le conciernen. La indemnización será fijada prudencialmente por el Tribunal atendiendo a las circunstancias del caso y a la gravedad de los hechos. Esta acción es sin perjuicio del deber de eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal y de lo establecido en el artículo 173 del Código de Procedimiento Civil. Esta acción se tramitará conforme al procedimiento sumario y las pruebas rendidas serán apreciadas en conciencia por el Tribunal (Art. 23 Ley 19628).

Otras vías judiciales para la tutela efectiva de los derechos

Asimismo se tramitarán conforme al procedimiento sumario, los procesos derivados de infracciones no contempladas en los artículos 16 (infracción al derecho de información,

modificación, bloqueo o cancelación) y 19 (cancelación o bloqueo datos personales referidos a obligaciones de carácter económico, financiero, bancario o comercial) (Art. 23 Ley 19628).

Finalmente es importante señalar que la ley dispone que el juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que establece.

Un tercer caso en este sentido está constituido por la infracción de los responsables de bancos de datos **relativos a obligaciones de carácter económico, financiero, bancario o comercial obtenidos de fuentes accesibles al público**. Una primera observación a este respecto está constituida por la clarificación acerca de qué debe entenderse por fuentes accesibles al público, a nuestro entender sólo podrá ser el Boletín de Informaciones Comerciales creado por el decreto supremo de Hacienda N° 950, de 1928, único organismo previsto por el ordenamiento jurídico nacional para los efectos de comunicar esta información al público. Respecto de las infracciones contempladas en este sentido, en primer lugar deberemos señalar la **comunicación de datos cuando las obligaciones a que se refieren no consten en alguno de los documentos expresamente señalados en la ley o en un Decreto Supremo (Art.17 Ley 19628)**. En segundo lugar, si se realizare alguna **comunicación fuera de las oportunidades señaladas por la Ley (Art.18 Ley 19628)**. Finalmente cuando se infringen los deberes de modificación, bloqueo o cancelación, conforme a las normas especialmente previstas a estos efectos.

D.- Control del Tratamiento de Datos Personales

Otro de los aspectos controvertidos de la ley 19628 dice relación con este principio, conforme al cual los Estados deben prever autoridades de control que supervigilen el tratamiento de datos personales, las cuales deben ser independientes y con atribuciones suficientes como para dotarlas de efectividad en su función de velar por un tratamiento adecuado, con pleno respeto a los titulares de datos personales. En Chile no se ha regulado adecuadamente esta materia y ello ha sido uno de los principales obstáculos para que la Comunidad Europea nos considere un país con niveles adecuados de protección. Entre las falencias del modelo nacional destacan las siguientes:

- a. La ley sólo prevé una especie de autoridad de control respecto de los organismos públicos. En efecto, de una parte la ley 19628 en su artículo 22 inc. 1 prevé el registro de los bancos de datos públicos, en el Registro que debe llevar el **Registro Civil, que es uno de los ejes del principio de control, no contempla sanciones a la infracción. Adicionalmente, el Registro Civil no cumple** con los requisitos de independencia y autonomía que se exigen en Derecho Comparado. En efecto, tratándose de un órgano público dependiente de la administración central y más aun siendo uno de los principales tenedores de datos personales, malamente podríamos estar ante un régimen garante de los derechos del interesado. En cuanto al alcance del control, éste se circunscribe a la mantención de un registro de los bancos de datos personales a cargo de organismos públicos.

De su parte, la ley 20.285 de transparencia y acceso a la información pública, en su artículo 33 letra m) dispone que: corresponderá al Consejo de la Transparencia

“Velar por el adecuado cumplimiento de la ley N° 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado”. Ahora bien, esta norma ha levantado sospechas, en cuanto que el consejo de la transparencia no cumple con los principios de independencia ni jerarquía necesarios para dar cabal cumplimiento a las tareas que típicamente corresponden a una autoridad de control. A lo anterior se suma que este órgano no tiene competencias para supervigilar el tratamiento de datos personales realizado por las instituciones y/o personas privadas, por lo que no es una solución general.

D.- Sujetos que Intervienen en el Tratamiento de Datos Personales

La Ley reconoce tres tipos de sujetos que intervienen en el tratamiento de datos personales. En primer lugar el legislador conceptúa a la persona del **titular de los datos personales** como la persona natural a la que se refieren los datos de carácter personal. Es así como el legislador nacional acoge la tendencia general que sostiene que sólo las personas naturales son titulares de la garantía denominada “intimidad informática”, lo cual aparece como comprensible si hacemos presente que esta garantía deriva directamente de la dignidad humana, constituyendo una nueva expresión de la tradicional garantía de la intimidad, inherente a todo ser humano.

En segundo término la ley 19628 señala que será **responsable del registro o banco de datos**, la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal. Estamos en consecuencia ante el responsable del tratamiento, conforme a la nomenclatura establecida en la normativa internacional. Cabe destacar a este respecto la escasa precisión técnica utilizada por el legislador en su definición, ya que hace sinónimas las expresiones “registro” y “banco de datos”, en tanto que entre ambas expresiones existe una relación contenido continente; además y recordando lo estudiado antes, porque confunde en definitiva al responsable del tratamiento con el responsable del fichero. Dentro de estos responsables la ley se ocupa especialmente de la administración pública como tenedora y administradora de bancos de datos personales. Tal y como ya señaláramos, la ley entiende por organismos públicos, las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1º de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado. A este último respecto baste con las reflexiones que vertiéramos en su oportunidad. Ahora deberemos analizar cuáles son las normas especiales previstas por el legislador, para los organismos públicos como responsables del tratamiento de datos personales a través de bancos de datos.

Esta materia está regulada en el título IV de la ley 19628 que en primer lugar establece que estos organismos sólo podrán efectuar tratamiento de datos personales respecto de las materias de su competencia y con sujeción a las normas de dicha ley (Art. 20 Ley 19628).

En cuanto a los principios que rigen su actuar, en primer lugar en cuanto al **principio del consentimiento del titular**, este principio no les afecta si el tratamiento se efectúa dentro de las materias de su competencia y con sujeción a las normas de la ley 19628. En segundo término y como ya se analizara en su momento, a su respecto rige el **principio de publicidad**, en virtud del cual el organismo público responsable del banco de datos debe comunicar al

Servicio de Registro Civil e Identificaciones, quien mantendrá un **registro público al efecto**, respecto de cada uno de los bancos de datos que mantenga, el fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende (Art. 22 inc. 2 Ley 19628). Esta comunicación deberá practicarse cuando se inicien las actividades del banco y comunicará cualquier cambio de los elementos indicados en el inciso anterior dentro de los quince días desde que se produzca.

En cuanto a la comunicación de los datos a terceros, tratándose de datos relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, les afecta el principio de la **temporalidad en el tratamiento**. De esta forma, no podrán comunicar los datos correspondientes una vez que haya prescrito la acción penal o administrativa, o que se haya cumplido o prescrito la sanción o la pena (Art. 21 inc. 1 Ley 19628), salvo cuando esos datos les sean solicitados por los tribunales de Justicia u otros organismos públicos dentro del ámbito de su competencia. En todo caso al organismo receptor le afectará el principio de seguridad en el tratamiento, debiendo en consecuencia el responsable del tratamiento garantizar la seguridad de los datos. Asimismo y, en todo caso, les será aplicable el deber de utilizar los datos únicamente para las finalidades que motivaron la transmisión, el deber de secreto que afecta a todos los sujetos que participen de alguna forma en el tratamiento y el principio de temporalidad del tratamiento, en el sentido que no podrán comunicarse los datos una vez vencidos siete años desde que la respectiva obligación se hizo exigible.

En cuanto al momento en que estos deberes rigen para la administración, deberemos señalar que todos ellos, salvo el deber de notificación, entraron en vigor a los sesenta días contados desde la fecha de publicación de la ley 19628 en el Diario Oficial. A su turno para el deber de notificación se ha previsto una vigencia diferida, estableciéndose que entrará en vigor un año después de esta fecha, debiendo en todo caso los organismos que a la fecha de entrada en vigor de la ley tengan bancos de datos personales, remitir esa información con anterioridad, en el plazo que fije el reglamento (esta norma aún no se ha dictado).

En este punto deberemos señalar que podrá realizarse un tratamiento de datos a nombre propio o en virtud de un mandato. En este último caso, se aplicarán las reglas generales, el mandato será otorgado por escrito, dejando especial constancia de las condiciones de utilización de los datos y en todo caso, el mandatario deberá respetar esas estipulaciones en el cumplimiento de su encargo (Art. 8 Ley 19628).

Finalmente deberemos hacer una referencia a los **terceros** y su participación dentro del tratamiento de datos personales. A su respecto deberemos señalar que la Ley les reconoce normalmente como destinatarios de la transferencia o comunicación de los datos personales y dentro de este marco, como ya analizáramos reconoce los principios de lealtad en el tratamiento, calidad de los datos, información al titular de los datos, tutela al titular, etc.