UNIVERSIDAD DE CHILE
FACULTAD DE DERECHO
DEPARTAMENTO DE DERECHO COMERCIAL

ANÁLISIS LEGAL COMPARATIVO DE LA PROTECCIÓN DE DATOS PERSONALES A NIVEL LATINOAMERICANO.

MEMORIA DE PRUEBA PARA OPTAR AL GRADO DE LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

ALUMNO:
WASHINGTON ALEJANDRO JAÑA TAPIA
PROFESOR GUÍA:ARTURO PRADO PUGA ASESORA METODOLÓGICA: PAULA JERVIS ORTIZ

SANTIAGO – CHILE. 2003

RESUMEN

Análisis Legal Comparativo de la Protección de Datos Personales a Nivel Latinoamericano

Washington Alejandro Jaña Tapia

En la presente investigación se realiza un análisis comparativo de la protección jurídica brindada en Latinoamérica a las personas ante el tratamiento automatizado o manual de sus datos. Asimismo, se muestra el estado actual de desarrollo de cada uno de los diecinueve ordenamientos jurídicos abarcados en este estudio en materia de protección de datos personales.

La investigación está organizada en cinco capítulos: el primero, está dedicado a la contextualización histórica de la protección de datos personales y a la revisión de los conceptos generales relativos a la materia en estudio. En el segundo, se analiza particularmente cada uno de los diecinueve ordenamientos jurídicos abarcados por el trabajo. El Capítulo III presenta la información obtenida en el apartado anterior en nueve tablas comparativas, las que a su vez sirven de base para el desarrollo del Capítulo IV, constituido por el análisis comparativo de los sistemas jurídicos estudiados. Finalmente, en el Capítulo V se exponen las conclusiones de la investigación realizada.

Los resultados obtenidos demuestran que en la actualidad existe un disímil grado de desarrollo normativo en los ordenamientos jurídicos latinoamericanos en materia de protección de datos personales, tanto a nivel constitucional como legal, lo que en definitiva se traduce en una desprotección de las personas frente al tratamiento de sus datos o información personal.

INTRODUCCIÓN

En este trabajo se efectúa un análisis comparativo de la normativa jurídica relativa a la protección a los datos personales existente en diecinueve ordenamientos jurídicos de Latinoamérica. Los sistemas jurídicos abarcados en este estudio son los siguientes: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela. No se han considerado para este efecto algunos sistemas jurídicos, en especial, aquéllos pertenecientes al Caribe. La razón de ello ha sido la falta de información jurídica relativa a esos sistemas. En el caso de Puerto Rico, su exclusión obedece a otras causas; la particularidad de este ordenamiento jurídico como consecuencia de su calidad de Estado Libre Asociado de los Estados Unidos de Norteamérica, lo cual implicaría detenerse tanto en el estudio de la legislación norteamericana -de carácter predominantemente sectorial y ajena al sistema europeo de protección de datos- como la puertorriqueña, tarea que estimamos sería propia de un estudio particular, dada su envergadura.

La presente investigación está estructurada en cinco capítulos. En el primero de ellos se revisan los conceptos más importantes que giran en torno al tema de estudio, se reseña la historia de la protección jurídica a los datos personales, se aclaran los términos comúnmente utilizados para referirse al derecho a la protección de datos, así como también se exponen las diversas opiniones doctrinarias en materia de bienes jurídicos tutelados por las normas de protección de datos. Por último, se explica el contenido y las variadas formas que se han adoptado comúnmente en el mundo para la protección a los datos personales. En el Capítulo II de este trabajo se realiza el análisis particular de cada

ordenamiento jurídico incluido en este estudio, desarrollándose diversas áreas temáticas que servirán de base para el posterior análisis comparativo. En éste se abordan los siguientes puntos de interés: niveles de protección jurídica a los datos personales, bienes jurídicos protegidos por las normas de protección a los datos personales, principios informativos de la legislación general de protección de datos personales, regulación diferenciada o indiferenciada del sector público y privado, modelos de tutela, mecanismos de control, transmisión internacional de datos personales y el régimen de responsabilidad. A continuación, en el Capítulo III se presenta la información obtenida de los respectivos análisis particulares de los países estudiados, en nueve tablas comparativas, las cuales han servido de base a su vez para el análisis comparativo propiamente tal que se realiza a continuación. En el Capítulo IV, se llevan a cabo los análisis comparativos de los diecinueve ordenamientos jurídicos estudiados, en base a las tablas de análisis particulares señalados anteriormente. Finalmente, en el Capítulo V se presentan las conclusiones generales del presente estudio.

Ha motivado la realización de este trabajo, la inquietud por explorar más allá de nuestras fronteras un ámbito jurídico que presenta gran interés en la actualidad, cual es, la protección de los derechos de las personas ante el tratamiento automatizado de su información personal. Lo anterior, en atención al vertiginoso desarrollo que presentan las tecnologías de la información en todo el mundo, lo que ha permitido entre otras cosas, que los datos o información personal pueda ser transmitida a cualquier lugar del planeta de manera casi instantánea, así como también, que puedan crearse determinados perfiles humanos cruzando datos que en principio pudieran parecer inocuos, etc.

Lo señalado, presenta ciertamente un escenario de riesgo para los derechos fundamentales de las personas, dentro de los cuales la intimidad ocupa sin duda un lugar de preocupación constante. Por otra parte, y para justificar ahora el estudio de los ordenamientos de Latinoamérica, debemos señalar que ello obedece, en general, a una tendencia de integración regional, la que incluye un interés por la armonización de las legislaciones. Para lograr este objetivo, es necesario previamente conocer el estado actual de las instituciones jurídicas extranjeras, en el caso de este trabajo, de la normativa relacionada a la protección a los datos personales.

Justificada la realización del presente estudio, debemos señalar que nuestra hipótesis de trabajo consiste en sostener que el análisis legal comparativo de la protección de datos personales a nivel latinoamericano dará cuenta del diverso grado de desarrollo que presentan los sistemas jurídicos estudiados en materia de protección de datos personales. Ahora bien, los objetivos específicos del presente trabajo son: identificar las normas jurídicas de protección de datos y su jerarquía en cada sistema jurídico, analizar asimismo si la regulación tiene el carácter de ley general o sectorial; determinar los bienes jurídicos protegidos; identificar los principios que informan cada legislación general; determinar la regulación sobre protección de datos que prevé cada legislación especial tanto para el sector público como para el sector privado; analizar los mecanismos de control que estatuye cada sistema jurídico; identificar los modelos de amparo jurídico a los derechos de los titulares de los datos personales; determinar la existencia de regulación a la transferencia internacional de datos y, describir el régimen de responsabilidad que contempla cada sistema jurídico latinoamericano en la materia de

estudio.

El estudio que se presenta constituye una investigación jurídica de tipo formalista dogmática, de carácter descriptivo comparativo. Tiene el carácter de comparativo, pues el análisis se llevó a cabo cotejando las diversas soluciones que los sistemas jurídicos latinoamericanos contemplan en materia de protección de datos personales. Por otra parte, tiene el carácter de descriptivo, pues se espera que los resultados de esta investigación puedan servir de base para la elaboración de futuros trabajos que abarquen ámbitos de estudio de tipo explicativo en la materia.

Para la elaboración de esta investigación hemos utilizado diversas fuentes: textos autoritativos, revistas jurídicas, otras publicaciones e información obtenida de la Internet. Ésta última, se ha constituido en la principal fuente de información para nuestro trabajo. Con todo, esa misma ventaja que ha presentado la utilización de la red, ha terminado limitando nuestra investigación, pues no toda la información requerida para este trabajo ha podido ser recolectada. Lo anterior, en atención al incipiente desarrollo que en algunos países presenta la utilización de la Internet para publicar la legislación vigente en aquéllos. Por lo tanto, hemos tenido que asumir las ventajas y desventajas de realizar una investigación como ésta, basada fundamentalmente en la utilización de la Web.

CAPÍTULO I. LA PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES

1. Generalidades

La protección de datos personales no es un tema nuevo o novedoso, sí actual. La información referente a las personas se ha utilizado desde antaño [1] , para diversos fines; algunos de éstos las han beneficiado, otros las han perjudicado. Por otra parte, el avance tecnológico ha permitido que el almacenamiento y tratamiento de datos haya evolucionado desde los métodos manuales o mecanizados a sistemas automatizados. Lo anterior, representa un potencial peligro para los derechos de las personas, pues mediante la utilización de la informática [2] y de la transmisión de datos entre ordenadores o computadores [3] a través de la telemática [4] , se puede ejercer un control social, sin que

[1] Se ha señalado por Puccinelli –citando la Sentencia de la Corte Constitucional colombiana T-443/94- que los archivos han sido parte esencial de la civilización. Ello se grafica en máximas atribuidas a personajes históricos, como Aristóteles, quien los habría considerado indispensables para un Estado moderno. Napoleón por su parte, habría acuñado la siguiente máxima: "un buen archivista es más necesario que un buen general de artillería". En Puccinelli, Óscar: *"El hábeas Data en Indoiberoamérica"*, Ed. Temis, Bogotá, 1999, pág. 11. Se repite la misma idea pero sin citar la fuente en Carranza Torres, Luis: *"Hábeas data. La protección jurídica de los datos personales"*, Averoni Ediciones, Córdoba, 2001, pág. 18.

el titular de los datos llegue a percatarse de ello, ni interfiera aparentemente en su vida. Dentro de los riesgos que este nuevo escenario tecnológico presenta, se cuenta la posibilidad de cruzar datos personales de manera muy rápida, casi instantánea, con lo cual se puede elaborar una información muy particular, incluso a partir de simples datos [5] que en principio pueden aparecer inocuos. Esa información creada a partir de simples datos, puede ser utilizada para diversos fines; uno de éstos es el estudio de aspectos de un perfil determinado de las personas. Con ello, se corren grandes riesgos para la dignidad y libertad de ellas, pues una vez perfiladas a través del uso de la informática, pueden ser objeto de discriminaciones –sea por el Estado o por los particulares-, sin ni siquiera tener el más mínimo contacto con quien toma una decisión de trascendencia jurídica respecto de ellas, sino por el contrario, en base al solo currículum creado a partir del procesamiento y tratamiento de sus datos personales. Junto con ello, también se corre el riesgo que esa información creada a partir del uso de la informática, pueda ser transmitida a terceros, sin que el titular de los datos llegue a enterarse de ese hecho, de la identidad de su receptor o receptores, ni menos de la finalidad para la cual será utilizada esa información.

Ante tales riesgos, tanto la doctrina, como la jurisprudencia y las legislaciones del mundo se han avocado de distinta forma e intensidad a buscar los mecanismos que tutelen los derechos de las personas acechadas por el inmenso poder que puede llegar a tener la informática unida a otros factores, entre éstos el gran desarrollo de las telecomunicaciones.

[2] Siguiendo a Davara, entendemos por informática, la ciencia del tratamiento automático de la información (Davara Rodríguez, Miguel A.: *"Manual de Derecho Informático"*, Ed. Aranzadi, Pamplona, 1997, pág. 22).

[3] El ordenador o computador ha sido definido como un dispositivo capaz de recibir, procesar y presentar datos, formado por un conjunto de máquinas intercomunicadas física y lógicamente entre sí. Las distintas unidades o elementos físicos que lo componen se conocen con el nombre de 'hardware'. A su vez, el 'hardware' por sí solo, no tiene aptitud para realizar ninguna de esas actividades, por lo que necesita de instrucciones y órdenes lógicas para funcionar como ordenador. Esa serie de instrucciones u órdenes forman los programas que guían o dirigen las actividades del sistema. Ahora bien, el soporte lógico de las instrucciones y órdenes que forman los programas que se introducen en un ordenador para que se realice un proceso, se denomina 'software'. *Ídem*, págs. 28 y 29.

[4] El término telemática surge de la unión de los vocablos telecomunicaciones e informática, el cual hace referencia al diálogo entre equipos informáticos. Se ha dicho que a consecuencia de la unión del mundo de las comunicaciones con la informática, el tratamiento de automático de la información ha podido realizarse a grandes velocidades y desde cualquier punto, desapareciendo las distancias en el tratamiento y transmisión de la información, con lo cual empieza a no contar el tiempo ni el espacio. *Ídem*, pág. 23.

[5] La palabra dato, ha sido entendida como el antecedente o noticia cierta que sirve de punto de partida para la investigación de la verdad. A su vez, al conjunto de datos se le ha denominado documentación. Caracterizan tanto al dato como a la documentación, el que no hayan sido sometidas a ningún tratamiento ni adecuación a un fin tendiente a obtener un resultado elaborado, pues si este fuera el caso, ya no estaríamos en presencia de un mero dato o documentación sino que frente a la información, entendida como el resultado orientado y adecuado a un fin determinado. *Ídem*, págs. 44 y 45.

2. Reseña Histórica sobre la Protección de los Datos Personales

El almacenamiento y recopilación de los datos personales no son actividades recientes creadas por la informática. Los riesgos de que un fichero [6] tuviera datos incompletos, falsos o utilizados para una finalidad distinta para la cual se hayan recogido ya estaban presentes en la época de los ficheros manuales [7] . Ejemplos del torcido uso de los datos personales podemos encontrarlos en la Alemania Nazi de la primera mitad del siglo XX [8] y, más cercano a nosotros, podemos visualizarlo en las acciones de los sucesivos regímenes dictatoriales en América Latina a partir de la década de los setenta del siglo pasado, que clasificaban a las personas por medio de sus datos personales, para fines de 'seguridad nacional' [9] .

Se ha señalado por Suñé Llinás, que al comienzo de la era informática -inmediatamente después de concluida la Segunda Guerra Mundial- el ser humano "se vuelve más y más de cristal, a partir del tratamiento masivo de los más diversos datos de las múltiples acciones de su vida cotidiana, que son susceptibles de quedar, y de hecho quedan, registrados en un ordenador" [10] . Se agrega por este autor, que ese 'hombre de cristal' es una realidad en los países más avanzados desde principios de la década de los setenta, cuya consecuencia ha sido el 'control difuso de la persona', mediante el cual no es necesario que se recojan datos de distinta procedencia para que se vulneren los

[6] Siguiendo a la Ley Orgánica de Protección de Datos Personales española 15/1999, entendemos por fichero: *"todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso"* (Art. 3 letra b). El texto de esta ley puede consultarse: [en línea] < http://www.ua.es/oia/es/legisla/datos.html > [consulta: 10 de Mayo 2003].

[7] Estadella Yuste, Olga: *"La Protección de la Intimidad Frente a la Transmisión Internacional de Datos Personales"*, Ed. Tecnos, Madrid, 1995, pág.21.

[8] Este oscuro período de la historia ha sido encuadrado dentro del final de la era preinformática, en donde el régimen nacionalsocialista alemán, "emprendió una minuciosa búsqueda sobre todo en los ficheros de los padrones municipales, de apellidos expresados en cualquier idioma, que tuviesen una presunta vinculación con la etnia judía, al efecto de localizar más fácilmente a las consiguientes víctimas de sus atrocidades" (Suñé Llinás, Emilio: *"Tratado de Derecho Informático*, *Vol. I, Introducción y Protección de Datos Personales"*, Universidad Complutense, Facultad de Derecho e Instituto Español de Informática y Derecho, Madrid, 2000, pág. 36).

[9] En el caso uruguayo, cuya dictadura militar se extendió desde 1973 hasta 1985, se ha señalado que "los militares clasificaron a toda la población en tres categorías de acuerdo al grado de riesgo que la persona presentara para el régimen", en Nino, Carlos S., *"Juicio al Mal Absoluto. Los Fundamentos y la Historia del Juicio a las Juntas del Proceso"*, tr. Böhmer, Martín F., Emecé Editores, Buenos Aires, 1997, pág. 63.

[10] Suñé Llinás, Emilio, *op. cit*., pág. 36.

derechos de las personas, sino que "la mera existencia de tales datos, sin limitaciones legislativas al *cruce* de los mismos, es suficiente para que el *perfil personal* de cualquier ciudadano aparezca diáfano ante los ojos de quien tenga el poder de reunir tales datos y relacionarlos entre sí" [11] .

Sólo fue hasta que los computadores demostraron el aumento de riesgos adicionales que resultaban del tratamiento automatizado de los datos personales, "que la sociedad, en general, empezó a demostrar preocupación sobre el tema y que los Gobiernos nacionales sintieron la necesidad de elaborar normas reguladoras que protegieran a los individuos" [12] . Esas normas reguladoras que aparecieron a principios de los años setenta no fueron contempladas por la doctrina internacional con el mismo entusiasmo, pues se señalaba que el poder de la nueva tecnología en el procesamiento de datos debía controlarse hasta cierto límite, de lo contrario se desembocaría en un abrumador poder de vigilancia sobre los individuos y las actividades de ciertas organizaciones [13] . Para otro sector doctrinal (en particular el norteamericano) y el empresariado, en ese entonces, las normas que aparecieron fueron consideradas como barreras comerciales cuyo fin era proteger la industria doméstica, bajo el pretexto de defender ciertos derechos fundamentales de las personas. La discusión máxima acerca de la protección de datos, tuvo por objeto dilucidar la posibilidad de incluir a las personas jurídicas en la *ratione materiae* de los instrumentos nacionales e internacionales sobre protección de datos [14] . Para poder aclarar lo anterior, entendemos que es preciso reconducir la discusión a los bienes jurídicos protegidos por las diversas legislaciones y, a partir de ello, buscar posibles respuestas a esa interrogante de manera particularizada. Al respecto, cabe consignar que mientras más cerca se esté de postular un bien jurídico vinculado a los tradicionales derechos de la personalidad, en especial la intimidad individual, más lejos se estará de poder fundamentar una tutela a las personas jurídicas basada en ese solo derecho.

Históricamente, Puccinelli ha señalado que el proceso de reconocimiento del derecho a controlar los datos personales se inicia tempranamente con la Constitución de Weimar de 1919, la cual en su artículo 119 establecía reglas mínimas al debido proceso en los procedimientos disciplinarios aplicados a los funcionarios públicos, dentro de los cuales se reconocían los derechos de acceso al expediente personal y a que no fueran anotados datos desfavorables en su legajo, sino hasta después de haber tenido oportunidad de formular su descargo [15] . Respecto de este antecedente, cabe señalar que no es mencionado por otros autores, salvo Puccinelli.

En el ámbito de las organizaciones internacionales, la preocupación por la protección

[11] *Ibídem*.

[12] Estadella Yuste, Olga, *op. cit*., pág.21.

[13] *Ibídem*.

[14] *Ídem*, págs. 22 y 23.

[15] Puccinelli, Oscar, *op. cit*. pág. 139.

de los datos personales habría comenzado a explicitarse con la Proclama de Teherán de 1968, la que será antecedente de la adopción en 1990, de una serie de principios rectores para la reglamentación de ficheros computarizados de datos personales por parte de la Asamblea General de la ONU [16] . Por otra parte, cabe destacar la labor de la OCDE (Organización para la Cooperación Económica y el Desarrollo), la cual en 1980 estableció las Directrices para la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales [17] .

En las legislaciones nacionales, las primeras leyes de protección de datos personales se comenzaron a dictar a partir de 1970. El mérito inicial le correspondió -según Suñé Llinás- a un Estado integrado en la antigua República Federal de Alemania: el Land de Hesse. Luego, en 1973 se dictan las Leyes de Protección de Datos en Suecia. Posteriormente, Estados Unidos dicta su propia ley en el año 1974 (*Privacy Act*). A éste le siguen Nueva Zelanda y Canadá en 1976, conjuntamente con la constitucionalización de la protección de datos personales en Portugal ese mismo año. En 1977, se promulga en la República Federal Alemana la Ley Federal de Protección de Datos (*Bundesdatenschutzgesetz*). Al año siguiente, se produce la mayor oleada legislativa en la materia, la cual se desarrolla en la Europa libre con la promulgación de leyes en Francia, Noruega, Dinamarca y Austria. Este mismo año (1978), España adopta una nueva Constitución que establece la protección a los datos personales [18] .

Dentro de la normativa de Derecho Internacional, especialmente en Europa, se han acordado importantes Convenios en materia de protección de datos personales. El primero de éstos es el Convenio 108 del Consejo de Europa del año 1981, denominado Convenio de la Protección de las Personas en Relación con el Tratamiento Automatizado de los Datos de Carácter Personal [19] . Este instrumento establece por primera vez un modelo que permitirá una relativa homogeneidad legislativa en Europa Occidental [20] . Por su parte, el Parlamento Europeo y el Consejo de la Unión Europea dictaron en 1995 la Directiva 95/46/CE relativa a la protección de datos personales, la cual está dirigida a los Estados miembros y cuyo objetivo expreso es precisar y ampliar los principios del Convenio 108 del Consejo de Europa [21] . Debemos hacer presente, que la Directiva europea de 1995, es uno de los referentes más importantes en la materia que ha trascendido las fronteras del viejo continente. En el caso de América Latina, Argentina ha

16 *Ídem*, págs. 140-145.

17 *Ídem*, págs. 45 y 46. También puede consultarse lo relativo de las líneas directrices de la OCDE en Estadella Yuste, *op. cit*., págs. 62-64.

18 Suñé LLinás, Emilio, *op. cit*., págs. 37 y 38.

19 Un análisis pormenorizado de este Convenio puede consultarse en Suñé Llinás, Emilio, *op. cit*., págs. 54-59.

20 *Ídem*, pág 38.

21 El texto de la Directiva 95/46/CE puede ser consultado [en línea] en < http://www.ua.es/oia/es/legisla/D9546CE.htm > [consulta: 2 de Mayo 2003].

sido el país que mayor influencia ha recibido de ésta, cuestión que ha sido confirmada por el denominado Grupo de Trabajo del artículo 29 de la Directiva (Article 29 Data Protection Working Party) [22] .

Finalmente, cabe hacer referencia a importantes hitos ocurridos a nivel doctrinario y jurisprudencial tanto en Estados Unidos como en Alemania, los cuales tendrán efecto directo en la protección de los datos personales en Occidente. El primer hito en la materia se ubica cronológicamente en la última década del siglo XIX, con la publicación de un artículo en 1890, en la *Harvard Law Review* por dos jóvenes abogados norteamericanos de Boston, Warren y Brandeis, titulado "*The Right to the privacy*" (traducido al español como "el derecho a la intimidad") [23] . En este artículo los autores sostuvieron la existencia de un derecho a la *privacy*, entendido como el "derecho a estar solo", o derecho a que a uno lo dejen en paz. La garantía de este derecho, se fundamentó en la Cuarta enmienda a la Constitución Norteamericana, dándose por sentado que ese derecho a la *privacy* coexiste y está siempre en tensión con el derecho a la libertad de expresión. [24] Asimismo, el concepto de *privacy* se entendió como un derecho autónomo, desgajado del derecho a la propiedad y de la protección del derecho al honor [25] . Este concepto fue desarrollado por la doctrina y jurisprudencia norteamericana; esta última, representada por el Tribunal Supremo norteamericano, aceptó entre los años 1956 y 1966 un nuevo concepto de *privacy.* Al respecto, se ha señalado por Zúñiga que en ese período la doctrina sentada por Warren y Brandeis era citada, a pesar de que la referencia al "derecho a la privacía"

[22] El artículo 29 de la Directiva, intitulado *"Grupo de protección de las personas en lo que respecta al tratamiento de datos personales"*, dispone entre otras cosas, que se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, en lo sucesivo denominado: "Grupo". Dicho Grupo tendrá carácter consultivo e independiente. Luego, el artículo 30 Nº 6 señala que el Grupo *"elaborará un informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Comunidad y en los países terceros, y lo transmitirá al Parlamento Europeo, al Consejo y a la Comisión. Dicho informe será publicado"*. En ejercicio de esas facultades, se enmarca la Opinión 4/2002 sobre el nivel de protección de los datos personales en Argentina, adoptada el 3 de octubre de 2002, en el cual se señala como conclusión que "en virtud de todo lo anterior, el Grupo de Trabajo asume que Argentina garantiza un nivel de protección adecuado con arreglo a lo dispuesto en el apartado 6 del artículo 25 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Sin embargo, el Grupo de Trabajo invita también a las autoridades argentinas a tomar las medidas necesarias para solucionar los puntos débiles de los actuales instrumentos legales identificados en el presente dictamen y solicita a la Comisión Europea continuar el diálogo con el Gobierno argentino con el citado objetivo. En particular, el Grupo de Trabajo insta a las autoridades argentinas a garantizar la aplicación efectiva de la legislación a nivel provincial mediante la creación de los necesarios órganos de control independientes en los casos en los que éstos no existan y, mientras tanto, a buscar soluciones temporales apropiadas que sean conformes con el orden constitucional argentino". [En línea]< http://www.protecciondedatos.com.ar/dic42002.htm > [consulta: 12 de Mayo 2003].

[23] Warren, Samuel D. y Brandeis, Louis D., *"El derecho a la intimidad"*, tr. Baselga, Pilar, Ed. Civitas S.A, Madrid, 1995.

[24] Zúñiga, Francisco: *"El Derecho a la Intimidad y sus Paradigmas"*, en Revista Ius et Praxis, Universidad de Talca, año 3, N° 1. Talca, 1997, pág. 289.

[25] Rebolledo Delgado, Lucrecio: *"El Derecho Fundamental a la Intimidad"*, Ed. Dykinson, Madrid, 2000, pág.63.

(sic) se hacía a la ley común norteamericana [26] . El segundo hito en la materia, está dado por el desarrollo en la jurisprudencia constitucional alemana de un "concepto subjetivo" de intimidad, el cual se identifica con el denominado 'derecho a la autodeterminación informativa' cuyo origen se encontraría en las argumentaciones de Warren y Brandeis [27] .

El concepto de autodeterminación informativa se plasma en la Sentencia del Tribunal Constitucional alemán de 1983 en la cual se declaran inconstitucionales algunos artículos de la Ley del Censo y de Población (Ley del 25 de Marzo de 1982). En esa sentencia se establece que del artículo 2 de la Ley Fundamental de Bonn surge "la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida" [28] .

De acuerdo a lo señalado por José Cuervo, esta sentencia constituye un hito en la defensa de los derechos de las personas a preservar su vida privada, pues el Tribunal Constitucional señala que la proliferación de centros de datos ha permitido, gracias a los avances tecnológicos, producir una imagen total y pormenorizada de la persona respectiva (un perfil de la personalidad), incluso en el ámbito de su intimidad, convirtiéndose así el ciudadano en 'hombre de cristal'. Cuervo agrega que lo importante de esta sentencia es que "el derecho a la intimidad ha pasado de ser un *status* negativo de la persona a convertirse en un *status* positivo, activo. De una actitud pasiva de simple defensa de nuestra intimidad, delimitadora de un ámbito de no interferencia, hemos pasado a una postura activa con la posibilidad de ejercer el control sobre el caudal de información que puede existir en los diferentes bancos de datos sobre nuestra persona" [29] . En este mismo sentido, Zúñiga señala que el derecho a la autodeterminación informativa ha sido concebido desde un punto de vista positivo de libertad, como poder de control sobre informaciones personales, a diferencia del concepto de *privacy* acuñado por Warren y Brandeis, entendido como libertad en sentido negativo, o sea, como facultad de tutelar la subjetividad de la injerencia ajena sea estatal o privada [30] .

[26] Zúñiga, Francisco, *op. cit*, pág.290.

[27] Rebolledo Delgado, Lucrecio, *op. cit*., pág.91

[28] *Ibídem*.

[29] Cuervo, José: *"Autodeterminación Informativa"*. [En línea] < http://www.informatica-juridica.com/trabajos/autodeterminacion_informativa.asp#4.%20CONCLUSIONES > [consulta: 10 de Diciembre de 2002]. De lo señalado por este autor cabe hacer la prevención relativa al bien jurídico protegido, pues no es claro en la actualidad que la autodeterminación informativa tutele o se refiera sólo al ámbito de la intimidad, sino que es expresiva de algo más que ésta, lo que para algunos llega a constituir un nuevo derecho con contenido propio e independiente (en este sentido Puccinelli, *op. cit*., pág. 70)

[30] Zúñiga, Francisco, *op. cit*, pág. 288. Cabe hacer presente que el paso de una consideración de la libertad desde un punto de vista negativo a uno de carácter positivo, tiene su base principalmente en los escritos de Benjamín Constant e Isaiah Berlin titulados respectivamente *"De la Libertad de los Antiguos Comparada con la de los Modernos*" y "*Dos ensayos sobre la Libertad"*. El desarrollo del pensamiento de estos autores aplicado a la materia de nuestro estudio, puede consultare en Murillo de la Cueva, Pablo, *op. cit*., págs. 45 y ss.

En suma, puede decirse que a partir de la evolución doctrinal, jurisprudencial y normativa en materia de datos personales se llega a fundamentar una protección y regulación jurídica de los registros de datos, tratando de lograr la convivencia de opuestos intereses, a saber; la intimidad de las personas y/o la autodeterminación informativa y el justificado interés del Estado y del mundo privado de contar con registros, archivos o bases de datos personales para el desarrollo de sus finalidades. Las bases de esta protección se encuentran planteadas -en general- sobre la consideración del derecho a la autodeterminación informativa como un derecho fundamental. No obstante, se discute por los autores la autonomía de este derecho [31] o su dependencia del derecho a la intimidad [32] , discusión que tiene importancia para determinar el nivel de protección que tendría el derecho a la autodeterminación informativa o libertad informática dentro de un Estado democrático de Derecho.

3. Derecho a la Protección de los Datos Personales, Derecho a la Autodeterminación Informativa, Libertad Informática y Hábeas Data

Aunque ya se ha adelantado la significación de algunos términos en materia de protección de datos personales, es menester dilucidar algunos de esos conceptos ampliamente utilizados por la doctrina y la jurisprudencia en la materia.

Qué se entiende por derecho de protección de los datos personales, derecho a la autodeterminación informativa, libertad informática y hábeas data es una cuestión que no se puede responder simplemente, pues no existe unanimidad en el parecer de la doctrina para referirse a estos términos. Con todo, cabe señalar que esas expresiones tienen en general como común denominador, el querer significar el reconocimiento de un nuevo derecho, cuyo núcleo esencial está dado por un poder de control de cada persona sobre la propia información y su calidad.

Para algunos autores, el término correcto a utilizar para significar este nuevo derecho sería *derecho a la protección de datos personales* (Puccinelli) [33] o *protección de datos* (Estadella Yuste). Otros autores utilizan términos más específicos como *libertad informática* (Moeykens) [34] , *autodeterminación informativa* (Pérez-Luño y Murillo de la Cueva) [35] e incluso el término *hábeas data* (Pomed Sanchéz) [36] .

Respecto de los términos derecho a la protección de datos personales o protección

[31] En este sentido Murillo de la Cueva, Pablo (*op. cit*., págs 123 y 124); Nogueira Alcalá, Humberto, (*op. cit*., págs. 266 y 275) y, Puccinelli (*op. cit*, págs. 69-71).

[32] Son exponentes de esta doctrina, Suñé Llinás (*op. cit*., pág. 29) y Estadella Yuste, Olga (*op. cit*., págs. 24-26).

[34] Moeykens, Federico Rafael: *"Derecho a la Libertad Informática: Consecuencia del Habeas Data"* Revista Electrónica Alfa-Redi Nº 48, [en línea] < http://www.alfa-redi.org/revista/data/48-6.asp > [consulta: 27 de Noviembre 2002].

de datos, se ha señalado que si bien el contenido o extensión de éstos es un punto discutido en la doctrina, existe al menos un grado de acuerdo, el cual consiste en afirmar que en estricto rigor, el derecho a la protección de datos, no dice relación o no está destinado a la protección del dato en sí mismo o el dato *per se*, sino que se relaciona con la protección de diversos bienes jurídicos. Cuáles sean éstos en definitiva, es otra cuestión controvertida dentro de la doctrina. Para la autora española Estadella Yuste, el derecho a la protección de datos protegería una parte del derecho a la intimidad personal, específicamente la referida a la información individual [37] . Hondius- citado por Estadella- señala por su parte que la protección de datos es "aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular el derecho individual a la intimidad respecto del procesamiento manual o automático de datos" [38] . Puccinelli en cambio, no limita el ámbito de bienes jurídicos protegidos, entendiendo por derecho a la protección de datos "la suma de principios, derechos y garantías establecidos a favor de las personas que pudieran verse perjudicados por el tratamiento de los datos nominativos a ella referidos" [39] .

Otro término utilizado por la doctrina para referirse a la materia es el de derecho a la libertad informática. En este sentido, Moeykens lo ha definido como "aquel derecho fundamental de naturaleza autónoma, que asegura la identidad de las personas ante el riesgo de que sea invadida o expropiada a través del uso ilícito de las nuevas tecnologías por parte del Estado o por parte de los particulares" [40] . Cabe hacer presente que para

[33] Desarrollando este tema, Puccinelli ha dicho que el fundamento del reconocimiento del derecho a la protección de los datos nominativos se encuentra en la "necesidad de tutelar una amplia gama de bienes jurídicos que pueden verse afectados por el tratamiento de datos nominativos mediante una regulación con pautas propias que exceden del marco de aquellos derechos a los que pretende proteger". Por este motivo -agrega este autor-, se trataría de un derecho de carácter instrumental y autónomo, con reglas de fondo propias y tutelable mediante ciertas garantías específicamente creadas para ello. Sería de carácter instrumental, "porque sirve de medio para la tutela de los derechos implicados, pero no pierde la categoría de derecho- y en ello está conteste la doctrina-, pues no alcanza a reunir las notas típicas de la moderna concepción de las garantías". Por otra parte, el carácter autónomo del derecho (cuestión discutida por la doctrina), estaría dado por el contenido esencial de éste, aunque se enriquezca en aspectos parciales con los otros derechos que coadyuvan a su integración. Con todo, cabe hacer presente que la visión que tiene Puccinelli del concepto 'derecho a la protección de datos personales', está mirada de un modo general u omnicomprensivo tanto del derecho a la autodeterminación informativa, como de su garantía específica (acción de hábeas data) por lo que la autodeterminación informativa sería una especie del derecho a la protección de datos personales (*op. cit*., págs. 69 y 70).

[35] Puccinelli, *op. cit*., págs. 66 y 67.

[36] *Ídem*, pág. 102.

[37] Estadella Yuste, Olga, *op. cit.*, pág. 24.

[38] Citado por Estadella Yuste, Olga: *Ibídem*.

[39] Puccinelli, *op. cit*., pág. 68.

[40] Moeykens, Federico R., *op. cit*., [en línea].

Puccinelli, la libertad informática debiera significar otra cosa: el derecho de los operadores de los sistemas informáticos de colectar, procesar y transmitir toda la información cuyo conocimiento, registro y difusión no esté legalmente restringido por motivos razonables, fundados en la protección de los derechos de las personas o en algún interés colectivo relevante que justifique tal limitación [41] .

Murillo de la Cueva, por su parte, para referirse a la materia de estudio, utiliza el término derecho a la autodeterminación informativa en vez de derecho a la protección de datos personales [42] . Así, señala que "el derecho a la autodeterminación informativa, en cuanto posición jurídica subjetiva correspondiente al *status* de *hábeas data*, pretende satisfacer la necesidad, sentida por las personas en las condiciones actuales de la vida social, de preservar su identidad controlando la revelación y el uso de los datos que les concierne y protegiéndose frente a la ilimitada capacidad de archivarlos, relacionarlos y transmitirlos propia de la informática y de los peligros que esto supone" [43] . Agrega este autor que ese objetivo se consigue por medio de la denominada técnica de protección de datos, la cual está integrada por un "conjunto de derechos subjetivos, deberes, procedimientos, instituciones y reglas objetivas" [44] . Se observa en este planteamiento, la preponderancia del bien jurídico "identidad", a diferencia del planteamiento de Estadella Yuste, para quien la base jurídica de la protección de los datos personales frente al tratamiento automatizado de éstos se encuentra en el derecho a la intimidad individual [45] .

En cuanto al alcance del término *hábeas data*, se ha señalado por Puccinelli que no existe consenso ni en la doctrina ni en la jurisprudencia en cuanto a la naturaleza jurídica que tendría el hábeas data [46] , pues mientras para la mayoría sería la garantía específica de otro derecho (libertad informática o autodeterminación informativa), para otros, como

41 En sentido similar Cifuentes. Todo lo anterior en Puccinelli, *op. cit*., pág. 67.

42 Estadella Yuste, Olga, *op. cit*., pág. 24

43 Murillo de la Cueva, Pablo, *op. cit*., págs. 173 y 174.

44 *Ídem*, pág. 174.

45 Estadella Yuste, Olga, *op. cit*., pág. 24.

46 Se ha señalado por José Cuervo que el habeas data constituye un cauce procesal para salvaguardar la libertad de la persona en la esfera informática, que cumple una función paralela, en materia de derechos humanos de la tercera generación, a la que en los de la primera generación correspondió al *hábeas corpus* respecto a la libertad física o de movimiento de la persona, pues éste surge como réplica frente a los abusos de privación de la libertad física de la persona, que habían conturbado la Antigüedad y el Medioevo proyectándose, a través del absolutismo, hasta las diversas manifestaciones del totalitarismo de nuestros días. Agrega además que en la actualidad la consagración de la libertad informática y el derecho a la autodeterminación informativa en el marco de los derechos de la tercera generación, han determinado que se postule el *status* de *hábeas data* (frase ya utilizada por Pérez-Luño en 1984 y por Murillo de la Cueva en 1990, *op. cit*., págs.119 y 174, entre otras) concretado en las garantías de acceso y control a las informaciones procesadas en bancos de datos por parte de las personas concernidas. La importancia que revisten las normas de procedimiento, y entre ellas el habeas data, se halla corroborada por la difusión creciente de instituciones de protección que tienden a completar la función de garantía de los tribunales. Cuervo, José, *op. cit*., [en línea].

Pomed Sanchéz y el Tribunal Constitucional colombiano sería un término sinónimo de libertad informática y del derecho a la autodeterminación informativa, es decir, tendría el carácter de derecho, cuya tutela estaría entregada a las vías judiciales tradicionales, como los serían la acción de amparo, tutela o protección [47] . Gozaíni, por su parte -haciendo referencia al caso argentino- señala que el hábeas data tiene una doble consideración; como derecho constitucional de las personas enraizado en el derecho a la intimidad y, como garantía o proceso constitucional [48] . Dentro de la doctrina chilena, Nogueira ha señalado que el hábeas data "es un subtipo de la acción de amparo o protección en cuanto ámbito del derecho procesal constitucional protector de derechos fundamentales o jurisdicción constitucional de la libertad, según la conocida expresión de Cappelletti y Fix Zamudio. Este es un derecho que asiste a toda persona a solicitar administrativamente y judicialmente la exhibición de registros o bases de datos -públicos o privados - en los cuales estén incluidos sus datos personales o de su familia, para tomar conocimiento de su exactitud solicitar su rectificación, superación, completarlos o solicitar su reserva" [49] . En síntesis y siguiendo a Puccinelli, puede decirse que la naturaleza jurídica del hábeas data depende de la forma en que se lo ha programado en cada ordenamiento jurídico. Si bien es más común encontrarlo diseñado como acción o proceso, y más precisamente como proceso constitucional (p.ej. Brasil, Paraguay, Perú, Argentina), también se lo ha concebido como un derecho constitucional, como en el caso de Colombia [50] .

En suma, puede afirmarse que no existe consenso terminológico entre los autores para referirse a la protección a los datos personales, por lo que debe entenderse que para algunos, el derecho a la protección de datos es sinónimo de derecho a la autodeterminación informativa. Para otros, el derecho a la protección de datos sería el término genérico que engloba tanto la autodeterminación informativa, como su garantía, es decir, el hábeas data. Otra doctrina utiliza el término derecho a la libertad informática para referirse a la materia, sin hacer mayores distingos entre éste término usado y los otros ya señalados. Finalmente, cabe señalar que para una parte muy minoritaria, el término hábeas data sería omnicomprensivo tanto de un derecho de hábeas data (como autodeterminación informativa) como de su garantía, la acción de hábeas data.

Por nuestra parte, adherimos al planteamiento de Puccinelli, y optamos por la

47 Puccinelli, *op. cit*., págs. 68 y 102. A este respecto, este autor ha señalarse que el Tribunal Constitucional colombiano ha dicho que el derecho de hábeas data es "el derecho fundamental y autónomo que permite a toda persona conocer, actualizar y rectificar las informaciones que sobre ella hayan sido consignadas en bancos de datos y en archivos de entidades públicas o privadas, en defensa de sus derechos fundamentales a la intimidad, a la honra y al buen nombre" (Corte Constitucional de Colombia, Sent. T-094/95).

48 Gozaíni, Osvaldo (coord.): *"La Defensa de la Intimidad y de los datos personales a través del Habeas Data".* EDIAR, Buenos Aires, 2001, pág. 7.

49 Nogueira, Humberto*: "Reflexiones sobre el Establecimiento Constitucional del Hábeas Data y del Proyecto de Ley en Tramitación Parlamentaria sobre la Materia".* En Revista Ius Et Praxis. Año 3, N° 1, Talca, 1997, pág. 266.

50 Puccinelli, *op. cit*., pág. 212.

utilización en este trabajo del término *derecho a la protección de datos*, dado que éste logra comprender a los diversos institutos relacionados con la materia, tanto desde un punto de vista de derecho sustantivo y procesal, como desde una óptica de principios generales. Con todo, cabe hacer presente que en razón de la diversa terminología utilizada por los autores y, para no confundir al lector, cuando corresponda se utilizará en forma disyuntiva tanto el término derecho a la protección de datos junto con alguno de los demás vocablos ya señalados (autodeterminación informativa, libertad informática o hábeas data).

4. Bienes Jurídicos Protegidos por el Derecho a la Protección de Datos Personales o la Autodeterminación Informativa

La determinación de los bienes jurídicos protegidos por el derecho a la protección de datos personales o la autodeterminación informativa es un tema también discutido a nivel doctrinal. Una primera concepción acerca del bien jurídico implicado, señala que los derechos humanos se nutren de valores o principios rectores, "que si bien fueron formulados como derechos durante la modernidad, en un contexto de separación y relativa autonomía entre el Estado y la sociedad civil, con el tiempo escalaron a la categoría de principios básicos" [51] . En este sentido, Pérez-Luño afirma que en la actualidad existe la tendencia prácticamente consolidada de reconducir el concepto de derechoshumanos a la realización de los valores dignidad humana, libertad e igualdad. Luego, el tratamiento de datos personales puede afectar a uno o a todos estos principios, por lo que la autodeterminación informativa protegería en última instancia los principios-valores dignidad, libertad e igualdad [52] .

Para Spiros el bien jurídico tutelado sería el derecho de propiedad sobre los datos. Esta teoría tiene dos vertientes; la primera se fundamenta en la existencia de una suerte de derecho de propiedad sobre los datos por parte de sus titulares, en razón de que el dato constituiría un elemento de la identidad de la persona, por lo tanto perteneciente a ésta. La segunda variante señala que el derecho de propiedad sobre los datos se adjudica a quien colectándolos o elaborándolos, los incorpora a su patrimonio. Esta teoría ha sido fuertemente criticada pues la concepción privatista-propietaria de los derechos niega la dimensión social y comunitaria de éstos [53] .

Otros autores han señalado el derecho a la identidad como objeto de tutela del derecho a la protección de datos personales o autodeterminación informativa. Ahora bien,

[51] *Ídem* pág. 72.

[52] Citado por Puccinelli. *Ibídem*.

[53] *Ídem* pág. 77.

la identidad puede ser mirada tanto desde un punto de vista estático como dinámico; el primero estaría referido a ciertos atributos que identifican a la persona (nombre, nacionalidad, estado civil, etc.). El punto de vista dinámico, a su vez, extiende el derecho a la identidad a la imagen pública de las personas y a los proyectos de vida de ellas, entendida en esta dimensión como: "el conjunto de atributos y características psicosomáticas que individualizan a la persona en sociedad; es todo aquello que hace que cada cual sea uno mismo y no otro; rasgos de la personalidad que se proyectan hacia afuera y permiten a los demás conocer a cierta persona en su "mismicidad", en lo que ella es en cuanto ser humano"(sic) [54] . El punto más interesante de esta concepción señala que "la identidad puede ser claramente atacada, pues el procesamiento de datos crea 'perfiles virtuales de las personas', que no siempre coinciden con lo que verdaderamente son" [55] . Si bien estimamos acertada en parte la afirmación reciente, tenemos dudas acerca de la eventual independencia del derecho a la identidad respecto de otros derechos que pudieren comprenderlo, como la intimidad. Por otra parte, creemos que se presentan serias dificultades al pretender determinar la identidad de una persona, pues lo que denominamos identidad es el resultado de un proceso complejo en el cual intervienen diversos factores tanto biológicos, psicológicos como sociales. Esta complejidad hace de cualquier intento por determinarla un asunto bastante más complicado de lo que se supone con aquellos planteamientos que de alguna manera pretenden determinar lo que 'verdaderamente *es* una persona'. En suma, pensamos que la identidad como objeto jurídicamente tutelable es demasiado amplio como para ser el fundamento de la protección a los datos personales, por lo que éste debería buscarse en otros bienes jurídicos.

Cabe mencionar por otra parte, aquella doctrina que ve en el derecho a la protección de datos o autodeterminación informativa, la protección de los bienes jurídicos intimidad o vida privada. Al respecto, se ha señalado que la mayoría de los autores coinciden tácitamente en que el derecho a la protección de datos personales (para nosotros) o autodeterminación informativa (para otros), es una suerte de mutación evolutiva del derecho a la privacidad "que hoy no se agota en ella, pues cumple una función tutelar de éste y muchos otros derechos son comprendidos en su concepto (…)" [56] . En un sentido más restringido -como ya se señaló más arriba-, para Estadella Yuste, la protección de datos personales no protege los datos *per se* "sino una parte del derecho a la intimidad personal, es decir, la que se refiere a la información individual", por lo que señala que en principio la base jurídica de la protección de datos personales frente al tratamiento automatizado de éstos "hay que encontrarla en el derecho a la intimidad individual" [57] .

Suñé Llinás por su parte, acepta la afirmación relativa a que el derecho a la autodeterminación informativa constituya la nueva dimensión que ha adquirido el derecho a la intimidad, condicionado al hecho de tener plena conciencia de que el "hablar de autodeterminación informativa, puede ser una forma práctica de referirse a las

[54] *Ídem*, pág. 78 y 79.

[55] *Ídem*, pág. 80.

[56] *Ibídem*.

particulares características que adquiere el derecho a la intimidad en la era informática: pero en el plano estrictamente conceptual, lo cierto es que la intimidad es un derecho reciente en términos históricos, sobre el que no se ha puesto suficientemente de relieve que su nacimiento mismo, como Derecho Fundamental diferenciado, está vinculado a la tecnología y, en el fondo, siempre fue autodeterminación informativa" [58] .

Por otra parte Herrán Ortiz plantea que debe superarse el enfrentamiento entre los términos privacidad e intimidad, los cuales han sido presentados como dos realidades irreconciliables e incompatibles. Al respecto postula que la intimidad y la privacidad constituyen dos aspectos complementarios e interdependientes de la existencia humana, por lo que una completa protección de la persona frente a las agresiones de las tecnologías de la información, únicamente se alcanzará a través de la tutela de ambas esferas de actuación de la persona, concluyendo que el punto no es decidir cuál de esas esferas se identifica con el bien jurídico tutelado mediante la protección de datos personales, "sino delimitar y establecer los mecanismos jurídicos apropiados para la protección de los bienes y derechos de la persona, que garanticen al individuo el pleno desenvolvimiento de su personalidad y un adecuado y libre desarrollo de las relaciones sociales e interpersonales" [59] .

Murillo de la Cueva a su vez- citado por Puccinelli-, propugna el abandono de la referencia a la intimidad y opta en definitiva por señalar un nuevo derecho, el derecho a la autodeterminación informativa. Con esto, se lograría diferenciarlo del derecho a la intimidad, pues éste sería un clásico derecho de defensa que no se aviene con la técnica de la protección de datos, porque los datos que se protegen no tienen por qué ser íntimos, siendo suficiente que se trate de datos personales, aunque sean inocuos [60] . Pérez-Luño por su parte -citado por Nogueira- ha señalado que el derecho a la autodeterminación informativa está constituido por "el conjunto de bienes o intereses que pueden ser afectados por la elaboración de informaciones referentes a personas identificadas o identificables". Es decir, es una facultad del titular de datos almacenados en un archivo público o privado, para "autorizar su recolección, conservación, uso y circulación, como asimismo para conocerla, actualizarla, rectificarla o cancelarla" [61] . De

[57] Estadella Yuste, Olga *op. cit*., pág. 24. Esta autora -citando a Hondius a propósito de la protección de datos de las personas jurídicas- matiza su afirmación señalando que si bien el interés jurídico protegible en última instancia en materia de protección de datos personales es la intimidad, "el interés de cada individuo en garantizar esta parcela de la vida privada puede ser diferente: mantener la reputación personal frente a la sociedad, cuestiones de honor, intereses económicos o un simple interés en conseguir la veracidad o el control de datos personales que están en manos de terceros"(Op cit., págs. 35 y 36).

[58] Suñé Llinás, Emilio, *op. cit*., pág. 29.

[59] Herrán Ortíz, Ana: *"El Derecho a la Intimidad en la Nueva Ley Orgánica de Protección de Datos Personales"*, Ed. Dykinson, Madrid, 2002, pág. 44.

[60] Puccinelli, *op. cit*., pág. 82. Con todo, cabe señalar que este autor, en otro texto, reconoce que el derecho a la autodeterminación informativa "se construye a partir de la noción de intimidad, *privacy, riservatezza o vie privée* y se encamina fundamentalmente a dotar a las personas de cobertura jurídica frente al peligro que supone la informatización de sus datos personales" (Murillo de la Cueva, Pablo, op cit, pág. 25).

lo señalado por este autor, puede desprenderse que la autodeterminación informativa a su vez tutelaría diversos intereses, los cuales no solamente son reconducibles en último término a la intimidad individual, como lo postula Estadella Yuste.

Finalmente, cabe agregar que para Puccinelli, el fundamento del reconocimiento del derecho a la protección de los datos nominativos se encuentra en la "necesidad de tutelar una amplia gama de bienes jurídicos que pueden verse afectados por el tratamiento de datos nominativos mediante una regulación con pautas propias que exceden del marco de aquellos derechos a los que pretende proteger". Por este motivo, se trataría de un derecho de carácter instrumental y autónomo, con reglas de fondo propias y tutelable mediante ciertas garantías específicamente creadas para ello. Sería de carácter instrumental, "porque sirve de medio para la tutela de los derechos implicados, pero no pierde la categoría de derecho- y en ello está conteste la doctrina-, pues no alcanza a reunir las notas típicas de la moderna concepción de las garantías". Por otra parte, el carácter autónomo del derecho (cuestión discutida por la doctrina), estaría dado por el contenido esencial de éste, aunque se enriquezca en aspectos parciales con los otros derechos que coadyuvan a su integración. Con todo, cabe recordar que la visión que tiene Puccinelli del concepto 'derecho a la protección de datos personales'- a la cual nos hemos sumado-, está mirada de un modo general u omnicomprensivo tanto del derecho a la autodeterminación informativa, como de su garantía específica (acción de hábeas data) por lo que la autodeterminación informativa sería una especie del derecho a la protección de datos personales [62] .

En suma, puede decirse que no existe consenso para señalar cuál sería él o los bienes jurídicos protegidos por el derecho a la protección de datos personales. Con todo, creemos que no existe un solo bien jurídico que sea omnicomprensivo de ese derecho de carácter instrumental, sino que confluyen varios derechos de los ya señalados, que sin duda en última instancia tutelan a las personas tanto en el ámbito de su dignidad como en el de la libertad e igualdad.

5. Contenido y Formas de Protección a los Datos Personales

Siguiendo la estructura explicativa propuesta por Puccinelli, se reseñará brevemente el contenido de la protección a los datos personales, esto es el objeto de protección, respecto de quién se protege y, de qué forma se tutelan los derechos de los titulares de los datos. Asimismo, se revisarán las diversas formas adoptadas por los ordenamientos jurídicos para la protección de los datos personales.

[61] Nogueira, Humberto, *op. cit*., pág. 265.

[62] Puccinelli, *op. cit*., págs. 69 y 70.

5.1 Objeto de Protección

Davara ha señalado que el objeto de tutela de la protección de datos es la persona en lo que concierne al tratamiento automatizado de datos. Es en el "carácter y la calidad de informatización- o posible informatización- y en las consecuencias del tratamiento informático de datos, donde nace esta necesidad de protección" [63] . Asimismo agrega que, si bien no cabe duda que se protege a la persona del titular de los datos, el término protección de datos es adecuado, universalmente conocido y claro [64] . En un sentido similar, Estadella Yuste ha dicho que el contenido de la protección de datos no es la tutela de los datos *per se*, sino una parte del derecho a la intimidad personal, es decir, la que se refiere a la libertad individual [65] . Por lo tanto, se deduce de lo señalado por esta autora, que el objeto de protección en definitiva es la persona.

En un sentido diverso al anterior se ha pronunciado Puccinelli, para quien si bien los datos no son el objeto de protección *per se*, se tutelan 'datos', entendidos como "elementos circunscriptos y aislados (v.gr. nombre o nacionalidad) aunque lo que en realidad se protege es la información que pudiera surgir de la relación entre datos (nombre y nacionalidad)" [66] . Estos datos a su vez deben ser 'personales', es decir, relativos a personas identificadas o identificables. Asimismo, deben corresponder a personas físicas o naturales, discutiéndose la procedencia de la protección de los datos de las personas morales o jurídicas [67] .

Finalmente, tampoco existe unanimidad de parecer en cuanto al tipo de dato a proteger, pues mientras para algunos (Ekmekdjan y Pizzollo) sólo deben ser protegidos aquéllos vinculados a un ámbito más cerrado a la publicidad, para otros -como Puccinellli-, no deben agotarse los datos protegibles a ciertas y limitadas categorías, sino que éstos deben ser evaluados en función de la cantidad y calidad que se pretenda tratar y de los medios técnicos que se utilicen para ese efecto, pues señala que "ciertos tipos de datos aparentemente irrelevantes, al ser interconectados y procesados con sistemas 'inteligentes' permiten descubrir aspectos de la persona que no debieran trascender sin su consentimiento" [68] .

[63] Davara R., Miguel Ángel, *op. cit*., pág.47.

[64] *Ídem*, pág. 50.

[65] Estadellla Yuste, Olga, *op. cit*., pág. 24.

[66] Puccinellli, *op. cit*., pág. 106.

[67] Para Puccinelli, si bien debe atenderse prioritariamente los datos de las personas, no deben excluirse las personas jurídicas, las personas extranjeras ni las residentes (*op. cit*., pág. 107.)

[68] *Ibídem*. En este mismo sentido se pronuncia Suñé Llinás, para quien no existen los datos inocuos. No obstante lo anterior, reconoce que no todos los datos requieren igual protección (*op. cit*, págs. 68 y 69).

5.2 Ámbito de Protección y Sujeto Pasivo

En lo relativo al ámbito de lo protegido por la normativa de protección de datos -siguiendo a Puccinelli-, puede afirmarse que las principales situaciones que se busca evitar a través del sistema de protección de datos personales son:

El acceso a información personal por terceros no autorizados;

El registro de ciertos datos;

El tratamiento ilegítimo de los datos registrados y,

La transferencia no autorizada de los datos.

Por otra parte, y respondiendo a la interrogante por los sujetos pasivos en materia de protección de datos personales, se señala de manera genérica que podrían ser sujetos pasivos todos aquellos que realizaran las actividades ya señaladas. Al respecto, se ha planteado una discusión en torno a la calidad que debiera tener el sujeto pasivo en relación con el ámbito objetivo de aplicación de la ley. La disputa se centra en si debe incluirse o no a los responsables de los ficheros manuales además de los responsables de los bancos y bases de datos informatizados [69] . En el plano normativo europeo, esta discusión ha sido resuelta jurídicamente por la Directiva 95/46/CE, la cual establece la aplicación de las normas de protección de datos tanto a los responsables de los ficheros manuales, como a los automatizados [70] .

5.3 Formas o Variantes Generalmente Adoptadas para la Protección de los Datos Personales

Como respuesta a la pregunta sobre el modo de protección de los datos personales, Puccinelli -siguiendo a Estadella Yuste-, ha dicho que el derecho a la protección de los datos personales puede ser tutelado de diversas formas, dentro de las cuales destacan:

Las normas generales o específicas, convencionales, constitucionales o legales que establezcan:

Ciertas garantías mínimas para el tratamiento de datos y para la habilitación de las bases y los bancos de datos, específicamente limitando sus actividades a las estrictamente necesarias para cumplir la finalidad a que obedeció la autorización de su funcionamiento;

Los derechos de los registrados o titulares de los datos (derechos de acceso, rectificación, supresión, bloqueo de datos, de oposición al tratamiento, etc…);

69 *Ídem*, pág. 108.

70 A este respecto cabe señalar que la Directiva 95/46/CE, dispone en el Artículo 3.1 que: *"Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".*

Las sanciones administrativas y penales para quienes infrinjan ciertas normas. Nosotros agregaríamos en este punto, una regulación de la responsabilidad civil, optando en lo posible por un sistema de responsabilidad estricta u objetiva o, a lo menos, por un sistema de responsabilidad por culpa, definiendo deberes de conducta a nivel legal o reglamentario (culpa infraccional);

Deberes institucionales de garantía (como una comisión de habilitación y seguimiento de los bancos de datos personales);

Recursos frente a los responsables de bancos de datos u otras vías administrativas;

Vías judiciales de amparo, específicamente diseñadas para la tutela de los derechos de los titulares de los datos (p.ej. la acción de hábeas data) y,

La remisión a mecanismos procesales generales de tutela de los derechos fundamentales (acción de amparo, de tutela o de protección).

Las normas sectoriales que tratan aspectos puntuales (p.ej. alcance del secreto fiscal o impositivo y del secreto estadístico);

Los contratos-acuerdo respecto del tratamiento de determinados datos;

Convenios internacionales (regionales o globales) que regulen ciertos aspectos comunes, en especial el tratamiento de la transmisión internacional de datos personales y,

Los códigos de conducta o códigos de buena práctica profesional [71] . Éstos, según Carranza, tendrían por objeto hacer efectiva la vigencia real de las leyes de protección de datos, buscando generar la responsabilidad de los destinatarios más individualizados de la misma, al asignarles una participación en la redacción de las normas más específicas destinadas a implementar lo que la norma legal requiere de ellos [72] . En suma, el objetivo de estos códigos es propender a la autorregulación de los actores que participan dentro del ámbito tutelado por las normas de protección de datos, con la finalidad "de la elaboración de normas de *soft law,* que sirvan de base a ulteriores disposiciones reglamentarias sectoriales" [73] .

Finalmente, y en relación a las formas en que las legislaciones mundiales se han ocupado de la protección de los datos personales, cabe señalar que no todos los Estados han asumido la protección de los datos de la misma manera; algunos han optado por constitucionalizar el derecho a la autodeterminación informativa o ciertos aspectos típicos de éste que permiten inferirlo. Otros Estados, en cambio, han optado sólo por la vía legislativa ordinaria [74] . En el caso de Europa, excepcionalmente se ha constitucionalizado algún aspecto específico del instituto (como en Portugal y España), cuestión que en materia legal ha sido objeto de desarrollo general complejo en donde incluso se establecen órganos de control [75] . Esta misma tendencia estaría presente en

[71] Puccinelli, *op. cit*., págs. 106-111.

[72] Carranza Torres, Luis, *op. cit*., pág. 135.

[74] *Ídem*, pág. 134.

Estados Unidos, país en el cual se ha optado por una regulación legal y jurisprudencial sin llegar a constitucionalizar el instituto. En el ámbito indoiberoamericano, la regla ha sido inversa, pues en algunos países se ha constitucionalizado la garantía procesal (acción de hábeas data) conjuntamente con el reconocimiento de derechos a los titulares de los datos, apreciándose en el ámbito legal, por el contrario, una ausencia de regulación específica [76] . Ahora bien, dentro de los ordenamientos jurídicos que han optado por una protección legal de datos, algunos de éstos han recurrido a leyes de carácter "ómnibus" (reguladoras de todos los sectores) y otros, han optado por regular la materia a través de leyes sectoriales, es decir, referida a temas específicos. Se ha señalado por Puccinelli que ambas fórmulas han sido criticadas por parte de la doctrina; la legislación sectorial, por su falta de integridad y la consecuencial ausencia de un órgano de control y la legislación ómnibus, por su falta de especificidad y la rigidez frente a las nuevas tecnologías, lo que en definitiva conllevaría a una desprotección [77] . Con todo, creemos que es preferible una legislación completa o general que incluya la mayor cantidad de ámbitos sectoriales, que entregue a un organismo independiente el control de la observancia de ésta, así como también que establezca un claro régimen de responsabilidad, tanto administrativa como civil, y eventualmente penal. Con una legislación que reuniera tales características, se ganaría en claridad frente a una materia de la cual ningún ser humano se escapa y que comienza a afectarlo desde su nacimiento, pudiendo incluso perpetuarse más allá de la muerte, pues siempre quedará algún registro de nuestro paso por esta vida.

[73] Heredero Higueras, Miguel: *"La Directiva Comunitaria de Protección de los Datos de Carácter Personal"*, Ed. Aranzadi, Pamplona, 1997, pág. 198. En esta materia la Directiva 95/46/CE recomienda a los Estados miembros y a la Comisión, alentar a los sectores profesionales para que elaboren códigos de conducta a fin de facilitar la aplicación de la Directiva, habida cuenta del carácter específico del tratamiento de datos efectuado en determinados sectores. Al efecto, se dispone por el artículo 27 que: *"1. Los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva. 2. Los Estados miembros establecerán que las asociaciones profesionales, y las demás organizaciones representantes de otras categorías de responsables de tratamientos, que hayan elaborado proyectos de códigos nacionales o que tengan la intención de modificar o prorrogar códigos nacionales existentes puedan someterlos a examen de las autoridades nacionales. Los Estados miembros establecerán que dicha autoridad vele, entre otras cosas, por la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, la autoridad recogerá las observaciones de los interesados o de sus representantes. 3. Los proyectos de códigos comunitarios, así como las modificaciones o prórrogas de códigos comunitarios existentes, podrán ser sometidos a examen del grupo contemplado en el artículo 29. Éste se pronunciará, entre otras cosas, sobre la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, el Grupo recogerá las observaciones de los interesados o de sus representantes. La Comisión podrá efectuar una publicidad adecuada de los códigos que hayan recibido un dictamen favorable del grupo".*

[75] Ejemplo de ello en España lo ha sido la derogada Ley Orgánica 5/92, de Regulación del Tratamiento Automatizado de Datos (LORTAD) y la actual Ley Orgánica 15/99, de Protección de Datos de Carácter Personal (LOPD).

[76] Puccinelli, *op.cit.*, pág. 134.

[77] *Ibídem*.

CAPITULO II. ANÁLISIS NORMATIVO DE LA PROTECCIÓN DE DATOS PERSONALES A NIVEL LATINOAMERICANO

Introducción

En este capítulo se efectuará un análisis particular de cada uno de los ordenamientos jurídicos latinoamericanos comprendidos en este estudio comparativo relativo a la protección de datos personales. El orden a seguir en la exposición de los análisis particulares será el siguiente: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela. Cada análisis en particular se desarrolla a través de diversos puntos, dentro de los cuales se abordan los siguientes temas:

Niveles de Protección Jurídica a los Datos Personales

El objetivo central de este punto, es analizar las normas jurídicas presentes en cada ordenamiento jurídico comprendido en nuestro estudio. En primer lugar, se examinarán las normas constitucionales, determinándose en cada caso la existencia o no de disposiciones especiales en materia de datos personales. Asimismo, existan o no normas constitucionales especiales en la materia, se señalarán en cada caso las disposiciones relacionadas con la protección de los derechos fundamentales y garantías constitucionales, poniendo especial énfasis en aquellas normas que tutelen los bienes jurídicos intimidad y vida privada, los cuales en general han sido señalados por la doctrina y jurisprudencia latinoamericana como fundamento último de las normas de protección de datos personales. En cada caso además, se hará referencia al derecho internacional de los derechos humanos aplicable a cada ordenamiento jurídico, centrándose específicamente en la Convención Americana de Derechos Humanos o Pacto de San José de costa Rica, por ser el instrumento más significativo a nivel latinoamericano en la materia. En segundo lugar, se analizará a nivel infraconstitucional la normativa en materia de protección de datos personales por cada país, abarcando cuando corresponda, tanto las leyes de protección de datos personales, como aquéllas de carácter sectorial que se ocupen de un específico ámbito de protección, las cuales dicho sea de paso, representan la regla general en Latinoamérica. Finalmente, nos detendremos en este punto-cuando sea procedente-, a analizar aquellas disposiciones legales que establezcan reglas de carácter procedimental administrativo o extrajudicial para hacer efectivos los diversos derechos reconocidos por el legislador a los titulares los datos personales, ante los responsables de los bancos de datos registros o archivos, tengan estos últimos carácter de públicos o privados.

Bienes Jurídicos Protegidos por la Legislación de Datos Personales

Dentro de este punto, se analizarán los bienes jurídicos tutelados a través de las normas de protección de datos personales en aquellos países que cuentan con disposiciones constitucionales y/o legales especiales en la materia. Para tal efecto, nos apoyaremos en lo señalado por la doctrina existente en cada ordenamiento jurídico a la cual hemos tenido acceso, así como también en la jurisprudencia disponible. Finalmente, expondremos nuestro punto de vista en relación a este tema.

Principios Informativos de la Legislación de Protección de Datos Personales

Al hablar de principios informativos, nos referiremos a aquellos principios generales relativos al tratamiento de datos personales que pueden visualizarse tanto en las legislaciones que cuentan con ley de protección de datos personales, como en aquéllas que sin tenerla, poseen al menos una legislación sectorial compleja influida por esos principios. En esta materia cabe señalar que se tendrán en consideración a modo de

guía, aquéllos señalados en la Directiva 95/46/CE de Protección de Datos Personales, así como también, los Principios Rectores para la Reglamentación de los Ficheros Computarizados de Datos Personales, señalados por al Asamblea General de la ONU en la Resolución 45/95, de 14 de Diciembre de 1990 [78] . Estos principios se señalarán y explicarán brevemente a continuación:

Principio de licitud y lealtad de los archivos de datos: los datos personales no se deberán recoger a través de procedimientos desleales o ilícitos, así como tampoco deberá elaborarse información de la misma forma [79] .

Principio de la calidad de los datos:los datos personales deberán ser tratados de manera leal y lícita, recogidos con fines determinados, explícitos y legítimos, y tratados posteriormente de manera compatible con dichos fines. Asimismo, deberán ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente. Finalmente, este principio señala que los datos deben ser exactos, actualizados y conservados de manera que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente [80] .

Principio del consentimiento informado del titular de los datos: para el tratamiento de datos personales los titulares deben prestar su consentimiento, debiendo informarse previamente a éstos en forma expresa y clara: 1) La identidad del responsable del tratamiento y, en su caso, de su representante; 2) Los fines del tratamiento de que van a ser objeto los datos; 3) Los destinatarios o las categorías de destinatarios de los datos; 4) El carácter obligatorio o no de la respuesta, así como también las consecuencias que tendría para la persona interesada una negativa a responder y, 5) La existencia de derechos de acceso y rectificación de los datos que la conciernen [81] .

Principio de la seguridad de los datos: los responsables del tratamiento de datos personales, deben aplicar las medidas técnicas y de organización adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales [82] .

Principio de la confidencialidad de los datos: las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento de datos personales, incluido

78 Esta Resolución puede ser consultada en: [en línea] < http://www.onu.org.gt/~oacdh/oacdh/Derechos%20Humanos/CDROM/Normativa/UN/Normas%20Orient/Der%20Economico,%20Soc%20y%20Cul/Princ > [consulta: 05-05-2003].

79 Resolución 45/95, Asamblea General ONU, A.1.

80 Directiva 95/46/CE, artículo 6.

81 *Ídem*, artículo 10.

82 *Ídem*, artículo 17.

este último, están obligados a guardar reserva respecto de los datos que hayan tenido conocimiento en razón de su oficio [83] .

Principio del consentimiento para la cesión de los datos: los datos personales objeto de tratamiento, sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo [84] .

Principio de la finalidad: la finalidad de un fichero y su utilización en función de esta finalidad deben especificarse y justificarse y, en el momento de su creación, ser objeto de una medida de publicidad o ponerse en conocimiento de la persona interesada a fin de que ulteriormente sea posible asegurarse de que: 1) Todos los datos personales reunidos y registrados siguen siendo pertinentes a la finalidad perseguida; 2) Ninguno de esos datos personales es utilizado o revelado sin el consentimiento de la persona interesada, con un propósito incompatible con el que se haya especificado; 3) El período de conservación de los datos personales no excede del necesario para alcanzar la finalidad con que se han registrado [85] .

Regulación Diferenciada o Indiferenciada del Sector Público y Privado

En este punto se analizarán las diferencias observadas en las leyes generales de protección de datos latinoamericanas, en cuanto a la forma de regular el sector público, representado por el Estado y sus organismos, y el sector privado en la materia de estudio. Al efecto, dividiremos los análisis por áreas temáticas, entre las cuales se incluye la regulación legal del consentimiento del titular tanto para el tratamiento de datos como para su cesión, los datos sensibles, la transferencia internacional de datos, los derechos de los titulares de los datos, entre otros.

Modelos de Tutela

Bajo este título se analizarán las acciones establecidas por cada ordenamiento jurídico para la protección de los datos personales, las cuales dividiremos en dos grupos: acciones especiales y acciones generales. En los casos en que el ordenamiento jurídico respectivo contemple acciones o alguna acción de carácter especial, en particular la acción de hábeas data, se analizará ésta señalándose al efecto sus aspectos más relevantes, como lo son: 1) La procedencia de la acción; 2) La legitimación activa; 3) La legitimación pasiva; 4) La competencia; 5) El procedimiento aplicable y, 6) La sentencia. En el caso de no contemplarse mecanismos de tutela especiales por un determinado ordenamiento jurídico, se analizarán las acciones constitucionales de amparo, tutela o

[83] *Ídem*, artículo 16

[84] *Ídem*, artículos 10 y 11 y, Ley 25. 326, República Argentina, artículo 11.

[85] Resolución 45/95, Asamblea General ONU, A.3.

protección (denominación que varía según el ordenamiento jurídico en estudio), las cuales tienen por finalidad general, tutelar o amparar a las personas en sus derechos y garantías constitucionales. Hemos contemplado el estudio de estas acciones, pues dada la naturaleza cautelar de ellas estimamos serían aptas para el amparo de los derechos constitucionales que sirven de fundamento a una protección a los datos personales, en especial, el derecho a la intimidad y el derecho a la vida privada. Por otra parte, en los casos en que no se haya contemplado por un ordenamiento jurídico determinado la acción constitucional de amparo o tutela, nos hemos remitido a las disposiciones de la Convención Americana de Derechos Humanos para salvar normativamente la falta de disposición al respecto.

Finalmente, cabe señalar que el estudio de las acciones de carácter administrativo en materia de protección de datos personales se desarrollará dentro del análisis particular de la legislación que la contemple, en el punto relativo a la protección legal de los datos personales, y no bajo el título modelos de tutela, el cual hemos reservado sólo para los procedimientos de carácter jurisdiccional.

Mecanismos de Control

La normativa internacional sobre protección de datos personales -en particular la europea-, señala que para la efectiva aplicación de la legislación dictada en la materia, los Estados deben designar autoridades públicas encargadas de vigilar la aplicación de las normas prescritas por éstos, así como también de controlar el respeto a los principios señalados en materia de protección de datos. Dichas autoridades deberán ofrecer garantías de imparcialidad e independencia respecto de las personas u organismos responsables del procesamiento de los datos o de su aplicación, y de su competencia técnica [86] . Por lo tanto, en este punto nos referiremos a esos mecanismos de control jurídico, los cuales deben ser ejercidos por autoridades administrativas independientes e imparciales –también denominadas órganos de control-, quienes tienen por misión principal velar por el cumplimiento de las normas legales dictadas en materia de protección de datos personales. Además del ámbito control ya señalado -al cual denominamos jurídico-, nos referiremos cuando sea pertinente a otro mecanismo o esfera de control, al cual llamaremos deontológico. Esta otra esfera está referida al control ejercido por las asociaciones profesionales y otras categorías de responsables del tratamiento de datos personales, a través de la aplicación de normas de buena práctica profesional desarrollados por éstos, las cuales se encuentran contenidas en los códigos de conducta o códigos deontológicos. Una autorregulación en esta materia creemos que sin duda aporta, pues incentiva a quienes participan del mercado de la información a comportarse según los estándares fijados por ellos mismos, dictados en base a los principios y normas generales en materia de protección de datos personales. Pensamos asimismo que para la efectiva implementación de lo anterior, debería tenderse a la creación de las denominadas jurisdicciones domésticas, a fin de garantizar la efectiva aplicación de las normas de buena práctica profesional contenidas en los códigos de buena conducta o deontológicos.

Transmisión Internacional de Datos Personales

Nos referiremos en este punto a una materia de gran importancia, cual es, la regulación del flujo transfronterizo de datos personales. Al efecto, abordaremos las normas aplicables en cada ordenamiento jurídico respecto de la transferencia o cesión de datos personales fuera del territorio del país transmisor. Cabe señalar en esta materia, que dentro del ámbito europeo de protección de datos personales, se ha entendido que la transmisión de estos datos a países terceros, sólo debe operar en los casos en que el país tercero de que se trate garantice un nivel de protección adecuado a los datos personales recibidos desde otra nación [87] .

[86] En este sentido, la Directiva 95/46/CE ha señalado en el artículo 28: "1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva. Estas autoridades ejercerán las funciones que les son atribuidas con total independencia. 2. Los Estados miembros dispondrán que se consulte a las autoridades de control en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal. 3. La autoridad de control dispondrá, en particular, de: - Poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control; - Poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales; - Capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial. Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional. 4. Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud. Toda autoridad de control entenderá, en particular, de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de la presente Directiva. Dicha persona será informada en todos los casos de que ha tenido lugar una verificación. 5. Toda autoridad de control presentará periódicamente un informe sobre sus actividades. Dicho informe será publicado. 6. Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro. Las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de información que estimen útil. 7. Los Estados miembros dispondrán que los miembros y agentes de las autoridades de control estarán sujetos, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre informaciones confidenciales a las que hayan tenido acceso".

[87] El artículo 25 de la Directiva 95/46/CE dispone al respecto que: *"(…) 2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".*

Régimen de Responsabilidad

Finalmente, bajo este título analizaremos las normas legales de responsabilidad aplicables a la protección de los datos personales. Para tal cometido, hemos optado por diferenciar tres ámbitos o clases de responsabilidad: administrativa, civil y penal. Dentro de la responsabilidad administrativa, se señalarán las normas especiales, sectoriales y comunes referidas a la protección de datos personales, cuyas sanciones deben ser aplicadas por órganos de la administración del Estado, tengan el carácter de autoridad u órgano de control o sean simplemente autoridades administrativas particulares. En cuanto a las normas de responsabilidad civil en la materia, se analizará tanto la legislación especial y sectorial como la de carácter común. Por último, nos referiremos a la responsabilidad penal. Respecto de esta última, haremos algunas prevenciones; en materia penal, la regla general en las legislaciones latinoamericanas es la inexistencia de tipos penales que tutelen directamente el bien jurídico autodeterminación informativa o libertad informática. Esta situación obedece a diversas circunstancias, la más importante a nuestro juicio, dice relación con la falta de un desarrollo doctrinario y legal en la materia que estudiamos. Lo anterior, milita en contra de quien pretenda sostener la eventual aplicación de los clásicos tipos penales que tutelan bienes jurídicos relacionados con la protección de datos, como lo son el derecho a la intimidad y el derecho a la vida privada, pues una afirmación en ese sentido, chocaría sin duda con el principio de legalidad, piedra angular del Derecho Penal. No obstante lo anterior, hemos creído necesario incluir dentro del análisis de la responsabilidad penal todos los tipos penales que se vinculen directa o indirectamente con la protección de la intimidad y la vida privada, pues éstos han sido señalados tanto por la doctrina como por la jurisprudencia, como los bienes jurídicos que fundamentarían la tutela a los datos personales (salvo para los que postulan la autonomía de la libertad informática). Por lo tanto, las menciones que se hagan en esta clase de responsabilidad, sólo tienen por finalidad explicitar el estado de la legislación penal en materia de intimidad y vida privada, pero en ningún caso, señalar que esos tipos penales serían aplicables sin más. Es por ello que cada vez que nos topemos con ciertas aproximaciones al bien jurídico autodeterminación informativa en algún tipo penal lo señalamos expresamente, pero sin desarrollar el tema, pues aquella tarea queda entregada a los especialistas de un área tan árida y compleja como lo es el derecho penal y que con todo, excede por mucho el ámbito de nuestra investigación.

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN ARGENTINA

1. Generalidades

El régimen de protección a los datos personales en Argentina tiene fundamentos

constitucionales. La reforma de la Carta Fundamental del año 1994 es de gran importancia, pues introduce dentro del artículo que contempla la acción de amparo, una acción constitucional que la doctrina ha denominado de hábeas data. El Constituyente, no le asigna ningún nombre en particular a esta acción, limitándose a señalar el contenido de ésta a renglón seguido de la acción de amparo [88] , antes del hábeas corpus. A partir de los artículos constitucionales N^{OS}. 18, 19, 43 y 75 Nº 22, se ha desarrollado una normativa general en materia de protección de datos personales, plasmada en la Ley Nº 25.326. Finalmente, cabe anotar que la Ley de protección de datos personales argentina se encuentra complementada por una regulación de carácter reglamentaria dictada por el Poder Ejecutivo por expreso mandato legal [89] .

2. Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional

En el orden constitucional, la protección a los datos personales en la Argentina tiene su base en la reforma a la Constitución de 1994 [90] , la cual incluyó un Capitulo Segundo en la Primera Parte, denominado *"Nuevos derechos y garantías"*. Dentro de éste, se inserta el artículo 43 el cual dispone en el inciso tercero -a renglón seguido de la acción de amparo constitucional-, que: *"Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística".*

Es precisamente dentro del tercer inciso ya señalado, donde se ubica el fundamento de la protección dispensada por el Constituyente argentino a los datos personales, a través de la acción de hábeas data. A partir de esa configuración constitucional se desarrolla a nivel legal una regulación más específica, a través de la Ley Nº 25.326 sobre

88 En el derecho chileno, la acción de amparo del derecho argentino equivaldría a la acción de protección del artículo 20 de la Constitución Política de 1980.

89 Para comprender el sistema jurídico argentino de protección a los datos personales es necesario tener presente aspectos de la organización política del Estado, en particular la forma de gobierno adoptada por el Constituyente trasandino, cual es, un sistema representativo republicano federal. Así, el territorio argentino se divide en Provincias, las cuales a su vez han dictado textos constitucionales propios que deben enmarcarse a los *"principios, declaraciones y garantías de la Constitución Nacional"* (Artículo 5º y 123º Constitución de la Nación Argentina), por lo que cada provincia tiene la facultad de regular constitucional y legalmente a nivel provincial la protección de los datos personales, en armonía con la Constitución de la Nación y con la legislación dictada por el Poder Legislativo nacional. Lo anterior, dado que las provincias no ejercen el poder delegado de la nación (Art.126 C.Política.) Finalmente cabe anotar que la ciudad de Buenos Aires tiene un régimen de gobierno autónomo con facultades propias de legislación y jurisdicción, cuyo jefe de gobierno es elegido directamente por el pueblo de la ciudad (Art.129, C.Política.).

90 [En línea] < http://www.georgetown.edu/pdba/Constitutions/Argentina/argen94.html > [consulta: 27 de Diciembre 2002].

Protección de Datos Personales, publicada en el Boletín Oficial el 2 de Noviembre de 2000. La Ley a su vez, se encuentra reglamentada parcialmente por el Poder Ejecutivo Federal en virtud del expreso mandato del legislador.

La historia de la modificación constitucional que incluyó dentro del artículo 43 la acción del hábeas data ha sido objeto de varios estudios en la Argentina. En síntesis, puede señalarse que el proceso de reforma se inicia con la dictación de la Ley Nº 24.309, la cual declaró la necesidad de reforma a la Constitución y habilitó -a través de su artículo 3º- para un debate a la Convención Constituyente, a fin de consagrar expresamente los procesos de amparo y hábeas corpus, sin mencionar el hábeas data. Luego, al advertirse por los convencionales el hecho de no existir autorización expresa para legislar acerca del hábeas data, se optó por introducirlo como un subtipo de amparo, para lo cual sí estaba autorizada la Convención. Al respecto, Padilla -citando a Puccinelli- señala que ésa fue la razón del por qué se ubicó en el párrafo tercero del artículo 43 la acción de hábeas data sin mencionarla por su nombre [91] . De lo anterior, se desprende que originalmente nunca estuvo en mente del Constituyente trasandino el establecer la garantía del hábeas data, sino que la necesidad de plasmarla en el texto reformado de 1994, surgió con posterioridad a la dictación de la ley que declaró la necesidad de una reforma constitucional.

Los antecedentes más importantes tenidos a la vista por el Constituyente argentino en materia de hábeas data, fueron la legislación española y la francesa de 1978 [92] . Se ha señalado al respecto, que la importancia del artículo 18 inciso 4º de la Constitución Española tuvo sus frutos incluso antes de la propia reforma de 1994 en la Argentina, ya que aquélla sirvió de fuente directa a las reformas de las Constituciones provinciales argentinas, las cuales comenzaron a desarrollarse a partir del año 1985 [93] .

Otras disposiciones constitucionales relacionadas con los bienes jurídicos tutelados por las normas de protección de los datos personales son las siguientes:

Artículo 18.- *"(…) El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación (…)".*

Artículo 19.- "*Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ello no prohíbe*".

El artículo 18 ya señalado, ha sido mencionado por alguna doctrina como aquella disposición constitucional de la que es posible deducir una protección al derecho a la

91 En Padilla, Miguel P.: *"Bancos de datos y acción de hábeas data",* Abeledo Perrot, Bs. As., 2001, pág. 57.

92 Padilla, Miguel, *op. cit*., pág. 39.

93 En este sentido se da la paradoja de haberse introducido en Argentina modificaciones a las Constituciones Provinciales antes de una reforma a la Constitución Nacional, la cual finalmente fija el umbral mínimo de protección, sea a la intimidad, sea a otro derecho distinto más específico que aquélla (Art.43 inciso. 3º).

intimidad. Así lo ha planteado Padilla, para quien "antes de la reforma era el Artículo 18 de la Constitución el bastión de la intimidad- el cual no sufrió modificación-" [94] . En opinión de otros, el derecho a la intimidad estaría consagrado tradicionalmente en el ratificado del texto histórico del artículo 19 de la Constitución Argentina, por lo que el artículo 43 sólo sería una variante de este último [95] . Toda esta discusión tiene su base en la consideración del bien jurídico protegido respecto de los datos personales cuestión que se abordara más adelante.

Finalmente en materia constitucional, cabe hacer mención al artículo 75 Nº 22, el cual establece la incorporación al ordenamiento jurídico argentino de los más significativos tratados internacionales sobre Derechos Humanos. Al efecto, se dispone que: *"Corresponde al Congreso: (…) 22. Aprobar o desechar tratados concluidos con las demás naciones y con las organizaciones internacionales y los concordatos con la Santa Sede. Los tratados y concordatos tienen jerarquía superior a las leyes".* A renglón seguido, se agrega que los tratados internacionales sobre Derechos Humanos que enumera,tienen jerarquía constitucional, pero *"no derogan artículo alguno de la primera parte de la Constitución y deben entenderse complementarios de los derechos y garantías por ella reconocidos"*. Asimismo, señala que sólo podrán ser denunciados, en su caso, por el Poder Ejecutivo nacional previa aprobación de las dos terceras partes de la totalidad de los miembros de cada Cámara [96] . Se desprende de lo anterior, que si bien se incorporarían al derecho argentino las disposiciones de los tratados sobre Derechos Humanos, éstos no tendrían rango supraconstitucional, ni tampoco derogarían la primera parte de la Constitución, la cual establece los derechos y garantías constitucionales. Con ello, estimamos se limita el sentido propio que caracteriza a esta clase de pactos, cual es, servir de estándar mínimo en la protección de los derechos humanos. Una disposición como la mencionada, no permite que la jurisprudencia constitucional -en los casos difíciles- pueda echar mano a esos tratados. Así, la larga enumeración de instrumentos internacionales de Derechos Humanos que hace el Constituyente en el Nº 22 del artículo

94 En Padilla, Miguel M., *op. cit*., pág.35.

95 Quiroga Lavié, Humberto*, "Hábeas Data"*, Zavalia, Bs. As., 2001, pág. 30.

96 El artículo 75 señala textualmente que: corresponde al Congreso: (…) 22. *"Aprobar o desechar tratados concluidos con las demás naciones y con las organizaciones internacionales y los concordatos con la Santa Sede. Los tratados y concordatos tienen jerarquía superior a las leyes. La Declaración Americana de los Derechos y Deberes del Hombre; la Declaración Universal de Derechos Humanos; la Convención Americana sobre Derechos Humanos; el Pacto Internacional de Derechos Económicos, Sociales y Culturales; el Pacto Internacional de Derechos Civiles y Políticos y su Protocolo Facultativo; la Convención sobre la Prevención y la Sanción del Delito de Genocidio; la Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial; la Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer; la Convención contra la Tortura y otros Tratos o Penas Crueles, Inhumanos o Degradantes; la Convención sobre los Derechos del Niño: en las condiciones de su vigencia, tienen jerarquía constitucional, no derogan artículo alguno de la primera parte de esta Constitución y deben entenderse complementarios de los derechos y garantías por ella reconocidos. Solo podrán ser denunciados, en su caso, por el Poder Ejecutivo nacional, previa aprobación de las dos terceras partes de la totalidad de los miembros de cada Cámara. Los demás tratados y convenciones sobre derechos humanos, luego de ser aprobados por el Congreso, requerirán del voto de las dos terceras partes de la totalidad de los miembros de cada Cámara para gozar de la jerarquía constitucional".*

75, se vuelve más bien inepta y carente de sentido.

En suma, puede afirmarse que a nivel constitucional, Argentina contempla una normativa favorable a la protección de los datos personales, plasmada expresamente en la acción de hábeas data del artículo 43. Sin embargo, resulta criticable del denominado hábeas data argentino, la limitación establecida en relación a los archivos, registros o bancos de datos de carácter privado, ya que sólo hace procedente la acción de hábeas data respecto de aquéllos de carácter *"privados destinados a proveer informes"*. Lo anterior, si bien refuerza la garantía de la inviolabilidad de los papeles privados, debilita por otra parte el derecho de cada persona a velar por el control de cierta información que revela aspectos de su intimidad, como lo son los datos sensibles. Asimismo, prevé el Constituyente trasandino otras normas que si bien no se refieren directamente al derecho a la intimidad o a la vida privada, se ha entendido que las incluiría por alguna doctrina. Con todo, entendemos que las deficiencias que presenta la Constitución de 1994 en materia de intimidad y vida privada, pueden ser suplidas por las disposiciones de los pactos internacionales sobre Derechos Humanos ratificados por el legislador argentino.

2.2 Protección Legal de los Datos Personales

El ordenamiento jurídico argentino además de contar con una disposición constitucional de hábeas data, establece a nivel legal la protección de los datos personales. Al efecto, la Argentina dispone de una reciente legislación de carácter federal en la materia cuyas disposiciones esenciales tienen el carácter de normas de orden público, razón por la cual son de aplicación general en todo el territorio de la República. En los ámbitos en que esa ley no fuere de aplicación nacional, el legislador dispone que: *"se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional"* [97] . Por lo tanto, en las materias que no son consideradas de orden público, las Provincias recuperan su plena autonomía normativa para regular aquéllas, debiendo tener siempre a la vista sus respectivas Constituciones, las cuales a su vez deben respetar la Constitución nacional de 1994.

En cuanto a los antecedentes de la Ley 25.326, Pablo Palazzi señala que a partir de la reforma constitucional del año 1994, numerosos proyectos legislativos fueron presentados para reglamentar la figura del hábeas data y establecer principios de protección de datos personales. La propuesta definitiva, tuvo como base el proyecto del Senador Eduardo Menem junto con otros pares, aprobándose en 1998 un Proyecto de Ley de hábeas data y protección de datos personales. Luego de la media sanción senatorial, se remitió a la Cámara de Diputados en Noviembre de 1998. Dos años más tarde, el 14 de Septiembre de 2000, la Cámara de Diputados aprueba su versión de Ley de Protección de Datos Personales, siendo promulgada como Ley de la República en Noviembre de 2000 y publicada en el Boletín Oficial el segundo día de ese mismo mes [98] . A su vez, la Ley 25.326 dejó entregada la reglamentación de sus disposiciones al Poder

[97] Artículo 44º. Ámbito de aplicación. *"Las normas de la presente ley contenidas en los Capítulos I, II, III y IV, y el artículo 32 son de orden público y de aplicación en lo pertinente en todo el territorio nacional.* Se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional. *La jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes del alcance interjurisdiccional, nacional o internacional".*

Ejecutivo, el cual dictó el Reglamento respectivo a través del Decreto Nº 1.558/01.

Comentando la regulación legal argentina, Palazzi señala que ésta sigue en varios artículos a la ley española de 1992 [99] , por lo que sus interpretaciones doctrinarias y jurisprudenciales serán de gran utilidad para la aplicación de la ley Argentina.

Finalmente, podemos señalar en este punto que junto con la Ley 25.326, se contempla por el ordenamiento jurídico argentino una serie de normas sectoriales que se relacionan con la protección a los datos personales, las cuales en general establecen deberes de confidencialidad sobre ciertas informaciones vinculadas al ámbito de las operaciones financieras y declaraciones impositivas, entre otras. Estas disposiciones legales las señalaremos y revisaremos en el punto siguiente.

2.2.1) Otras Normas Legales de Protección de los Datos Personales

Como ya se ha señalado, dentro del ordenamiento jurídico argentino además de la Ley 25.326, existen diversas normas jurídicas que se ocupan de la protección a los datos personales en los más variados ámbitos. A modo de enumeración no exhaustiva, podemos mencionar las siguientes normas.

2.2.2) Artículo 1071 bis del Código Civil Argentino

Se suele señalar por la doctrina trasandina que la protección a los datos personales en la Argentina antes de la reforma constitucional del año 1994, estaba resguardada en cierta forma por el artículo 1071 bis del Código Civil, pues éste consagra la protección del derecho a la intimidad de las personas desde el punto de vista civil. Por lo tanto, la protección a los datos de las personas antes de la reforma constitucional había que buscarla en el concepto de intimidad personal. Sin embargo, la afirmación anterior es discutida dado que esa disposición, sólo estaría referida a ámbitos hogareños de violación de la intimidad [100] . Este artículo dispone a la letra lo siguiente: *"El que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otros en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado, y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias; además, podrá éste, a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación"*.

En nuestro concepto la disposición anterior es bastante estrecha como para poder construir un derecho a la autodeterminación informativa. No obstante lo anterior, es

98 Palazzi, Pablo: *"La transmisión internacional de datos personales y la protección de la privacidad",* Ed. Ad-Hoc, Bs. As., 2002, págs.139-140.

99 Esa ley, era la Ley Orgánica 5/92, sobre Regulación del Tratamiento Automatizado de Datos (LORTAD), actualmente derogada por la Ley Orgánica 15/99 de Protección de Datos de Carácter Personal (LOPD).

100 En este último sentido se pronuncia, por ejemplo Padilla, *op. cit*., pág. 35.

plenamente aplicable como regla especial de responsabilidad extracontractual para reparar las consecuencias que se derivan de la vulneración del derecho a la intimidad. Con todo, el pretender fundar una acción de hábeas data en el precepto del artículo 1.071 del C. Civil, creemos que es pedirle demasiado al intérprete.

2.2.3) Ley 21.526 Sobre Entidades Financieras

La Ley 21.526 sobre entidades financieras contempla en el Título V el epígrafe denominado*"Secreto"*. Dentro de éste, se insertan dos disposiciones que consagran el secreto bancario; artículos 39 y 40. El primero de ellos, señala que las entidades comprendidas en la Ley (bancos en general y otros organismos de crédito) *"no podrán revelar las operaciones pasivas que realicen"* [101] Por su parte, el artículo 40 de la Ley preceptúa que: *"las informaciones que el Banco Central de la República Argentina reciba o recoja en ejercicio de sus funciones, vinculadas a operaciones pasivas, tendrán carácter estrictamente confidencial. El personal del Banco Central de la República Argentina o de auditorías externas que éste contrate para cumplir sus funciones, deberá guardar absoluta reserva sobre las informaciones que lleguen a su conocimiento"* [102] . En estos casos se protege un especial tipo de dato, cual es el relativo a las operaciones bancarias pasivas. Desde ese punto de vista, se estarían tutelando de manera sectorial los derechos de las personas a través de la prohibición de divulgación de esos datos personales.

2.2.4) Ley Nº 11.683 Sobre Procedimientos Fiscales

El Decreto Nº 821/98 aprobó el texto ordenado de la Ley Nº 11.683 sobre Procedimientos Fiscales, el cual en su artículo 101 establece que: *"Las declaraciones juradas, manifestaciones e informes que los responsables o terceros presentan a la Administración Federal de Ingresos Públicos, y los juicios de demanda contenciosa en*

[101] Luego el precepto señala las excepciones al deber de secreto, disponiendo que: *"Sólo se exceptúan de tal deber los informes que requieran: a) Los jueces en causas judiciales, con los recaudos establecidos por las leyes respectivas; b) El Banco Central de la República Argentina en ejercicio de sus funciones; c) Los organismos recaudadores de impuestos nacionales, provinciales o municipales. sobre la base de las siguientes condiciones: - Debe referirse a un responsable determinado; - Debe encontrarse en curso una verificación impositiva con respecto a ese responsable, y - Debe haber sido requerido formal y previamente. Respecto de los requerimientos de información que formule la Dirección General Impositiva, no serán de aplicación las dos primeras condiciones de este inciso. d) Las propias entidades para casos especiales, previa autorización expresa del Banco Central de la República Argentina. El personal de las entidades deberá guardar absoluta reserva de las informaciones que lleguen a su conocimiento"*. [En línea] < http://infoleg.mecon.gov.ar/txtnorma/texactley21526.htm **>** [consulta: 27 de Diciembre 2002].

[102] Continúa el artículo 40 señalando que: *"Los profesionales intervinientes en dichas auditorías externas quedarán sujetos a las disposiciones de los artículos 41 y 42 de la presente ley. Las informaciones que publique o exija hacer públicas el Banco Central de la República Argentina, sobre las entidades comprendidas en esta ley, mostrarán los diferentes rubros que, para las operaciones pasivas, como máximo podrán contener la discriminación del Balance General y cuenta de resultados mencionados en el artículo 36".* La legislación especial que regula el funcionamiento de las instituciones financieras en la argentina, en especial los artículos recién señalados establecen la regla general para las operaciones pasivas (deudas), pero como no es un derecho absoluto, la propia ley se encarga de establecer la excepciones ya expuestas en la norma (*Ídem*).

cuanto consignen aquellas informaciones, son secretos" [103] . En razón de lo preceptuado por la ley, puede afirmarse que también existe una especial protección a los datos personales relacionados con los ingresos rentas o gastos, que servirán para determinar la base impositiva de los contribuyentes. 2.2.5) Ley Nº 25.065 que Establece Normas que Regulan Diversos Aspectos Vinculados con el Sistema de Tarjetas de Crédito, Compra y Débito [104]

El artículo 53 de la ley que regula el sistema de las tarjetas de crédito establece que las entidades emisoras de Tarjetas de Crédito, bancarias o crediticias tienen prohibido *"informar a las bases de datos de antecedentes financieros personales sobre los titulares y beneficiarios de extensiones de Tarjetas de Crédito u opciones cuando el titular no haya cancelado sus obligaciones, se encuentre en mora o en etapa de refinanciación. Sin perjuicio de la obligación de informar lo que correspondiere al Banco Central de la República Argentina".* Se agrega en esta materia, que las entidades informantes serán solidaria e ilimitadamente responsables por los daños y perjuicios ocasionados a los beneficiarios de las extensiones u opciones de Tarjetas de Crédito por las consecuencias de la información provista.

En lo que a nuestro estudio interesa, la disposición anterior se refiere directamente a la protección de los datos personales en un ámbito más específico que el secreto

[103] El texto del artículo 101 señala a continuación que: *"Los magistrados, funcionarios, empleados judiciales o dependientes de la Administración Federal de Ingresos Públicos, están obligados a mantener el más absoluto secreto de todo lo que llegue a su conocimiento en el desempeño de sus funciones sin poder comunicarlo a persona alguna, ni aun a solicitud del interesado, salvo a sus superiores jerárquicos. Las informaciones expresadas no serán admitidas como pruebas en causas judiciales, debiendo los jueces rechazarlas de oficio, salvo en las cuestiones de familia, o en los procesos criminales por delitos comunes cuando aquéllas se hallen directamente relacionadas con los hechos que se investiguen, o cuando lo solicite el interesado en los juicios en que sea parte contraria el Fisco Nacional, provincial o municipal y en cuanto la información no revele datos referentes a terceros. Los terceros que divulguen o reproduzcan dichas informaciones incurrirán en la pena prevista por el artículo 157 del Código Penal para quienes divulgaren actuaciones o procedimientos que por la ley deben quedar secretos. No están alcanzados por el secreto fiscal los datos referidos a la falta de presentación de declaraciones juradas, a la falta de pago de obligaciones exigibles, a los montos resultantes de las determinaciones de oficio firmes y de los ajustes conformados, a las sanciones firmes por infracciones formales o materiales y al nombre del contribuyente o responsable y al delito que se le impute en las denuncias penales. La Administración Federal de Ingresos Públicos, dependiente del Ministerio de Economía y Obras y Servicios Públicos, queda facultada para dar a publicidad esos datos, en la oportunidad y condiciones que ella establezca. Excepciones al secreto: El secreto establecido en el presente artículo no regirá: a) Para el supuesto que, por desconocerse el domicilio del responsable, sea necesario recurrir a la notificación por edictos. b) Para los Organismos recaudadores nacionales, provinciales o municipales siempre que las informaciones respectivas estén directamente vinculadas con la aplicación, percepción y fiscalización de los gravámenes de sus respectivas jurisdicciones. c) Para personas o empresas o entidades a quienes la Administración Federal de Ingresos Públicos encomiende la realización de tareas administrativas, relevamientos de estadísticas, computación, procesamiento de información, confección de padrones y otras para el cumplimiento de sus fines. En estos casos regirán las disposiciones de los TRES (3) primeros párrafos del presente artículo, y en el supuesto que las personas o entes referidos precedentemente o terceros divulguen, reproduzcan o utilicen la información suministrada u obtenida con motivo o en ocasión de la tarea encomendada por el organismo, serán pasibles de la pena prevista por el artículo 157 del Código Penal.*

[104] Esta ley puede consultarse [en línea] < http://infoleg.mecon.gov.ar/txtnorma/texactley25065.htm > [consulta: 27 de Diciembre 2002].

bancario, referido sólo al mercado de las tarjetas de crédito.

Respecto de las sanciones establecidas a las empresas informantes, la regla tiene importancia, pues establecería a modo de sanción la solidaridad entre los involucrados en la divulgación de antecedentes personales, mediando un contrato.

2.2.6) Ley Nº 23.798 sobre Prevención y Lucha contra el Síndrome de Inmunodeficiencia Adquirida (SIDA) [105]

En materia de salud, la legislación argentina se ocupó en el año 1990 de dictar una ley que tiene por finalidad la lucha contra el síndrome de inmunodeficiencia adquirida. En el artículo 2º de esta ley se establecen reglas de interpretación disponiéndose al efecto que: *"las disposiciones de la presente ley y de las normas complementarias que se establezcan, se interpretarán teniendo presente que en ningún caso pueda: (…) c) Exceder el marco de las excepciones legales taxativas al secreto médico que siempre se interpretarán en forma restrictiva;* **(…) e) Individualizar a las personas a través de fichas, registros o almacenamiento de datos, los cuales, a tales efectos, deberán llevarse en forma codificada" . Sin duda que las letras c) y e) se relacionan fuertemente con el ámbito de los datos personales; el primero dado su carácter de dato sensible y, el segundo como una manifestación de aquél.**

Por otra parte, se prescribe que las autoridades sanitarias " *establecerán y mantendrán actualizada, con fines estadísticos y epidemiológicos, la información de sus áreas de influencia correspondiente a la prevalencia e incidencia de portadores, infectados y enfermos con el virus de la IDA, así como también los casos de fallecimiento y las causas de su muerte. Sin perjuicio de la notificación obligatoria de los prestadores"* (Art. 11).

Esta ley a su vez está complementada por el **Decreto Nacional 1.244/91** [106] **, Reglamentario de la Ley 23.798** . De éste destaca el artículo 2 el cual señala que: *"(…) c) Los profesionales médicos, así como toda persona que por su ocupación tome conocimiento de que una persona se encuentra infectada por el virus HIV, o se halla enferma de SIDA, tienen prohibido revelar dicha información y no pueden ser obligados a suministrarla (…)* [107] .

2.2.7) Ley Nº 712 de la Ciudad Autónoma de Buenos Aires sobre Garantías del Patrimonio Genético Humano [108]

Hemos dejado para el último esta ley que ha sido dictada para su vigencia sólo dentro del territorio que comprende la Ciudad Autónoma de Buenos Aires. Esta normativa tiene por finalidad evitar la discriminación de personas o miembros de sus familias sobre la base de información genética y, resguardar el derecho a la dignidad, identidad e integridad de

[105] **[En línea] < http://www.iijusticia.edu.ar/privacidad/ley23798.htm > [consulta: 27 de Diciembre 2002].**

[106] *Ídem*.

[108] **[En línea] < http://www.msn.com.ar/cbsas/contenidonumero.asp?idfdlcba=7422 > [consulta: 27 de Diciembre 2002].**

todas las personas con relación a su patrimonio genético.

Al respecto el artículo 5º señala que: *"Prohíbese difundir o hacer pública por cualquier medio la información genética de las personas, con excepción de los casos autorizados por el propio interesado o judicialmente"* [109] .

Para sostener que esta ley está referida en algún ámbito a la protección de datos personales, tendríamos que asumir que la información genética es un tipo especial de dato personal y, que en consecuencia, esa información es susceptible de ser protegida por la ley. Nosotros pensamos que es posible fundamentar el carácter de dato personal, especialmente sensible, en razón de la propia definición legal, la cual señala que se entiende por datos sensibles, los *"datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical o política e información referente a la salud o a la vida sexual"* (Art. 2º). En el caso de la información genética, ésta podría caber en la referencia hecha a la salud, pues es sabido que a través de los genes, es posible determinar ciertas condiciones de salud de las personas, sean pasadas, presentes, e incluso futuras, sea de la propia persona, sea de la potencial descendencia de ella misma.

[107] La salvedades a la regla general son las siguientes: 1) A la persona infectada o enferma, o a su representante, si se trata de un incapaz; 2) A otro profesional médico, cuando sea necesario para el cuidado o tratamiento de una persona infectada o enferma; 3) A los entes del Sistema Nacional de Sangre , así como a los organismos comprendidos en el artículo 7 de la Ley N. 21.541;4) Al Director de la Institución Hospitalaria o, en su caso, al Director de su servicio de Hemoterapia, con relación a personas infectadas o enfermas que sean asistidas en ellos, cuando resulte necesario para dicha asistencia; 5) A los Jueces en virtud de auto judicial dictado por el Juez en causas criminales o en las que se ventilen asuntos de familia; 6) A los establecimientos mencionados en el artículo 11, inciso b) de la Ley de Adopción, N. 19.134. Esta información sólo podrá ser transmitida a los padres sustitutos, guardadores o futuros adoptante y, 7) Bajo la responsabilidad del médico a quien o quienes deban tener esa información para evitar un mal mayor (Artículo 2º). Se agrega en el inciso e) que: *"Se utilizará, exclusivamente, un sistema que combine las iniciales del nombre y del apellido, día y año de nacimiento. Los días y meses de un sólo dígito serán antepuestos del número CERO (0)".*De la disposición anterior destaca la voluntad de dar la mayor protección a los datos personales sensibles relacionados con el estado de salud de las personas. Haciendo un parangón con la protección dispensada a los datos relativos a la salud por la Ley 25.326 (Art.8º), cabe señalar que la reglamentación especial que estudiamos presenta un plus respecto de la ley general, pues dispone de un mecanismo de disociación de datos que impida identificar a los pacientes infectados por el VIH. El mecanismo de codificación obviamente dificulta la identificación directa o indirecta del paciente.

[109] Asimismo la ley dispone en el artículo 8º que *" Prohíbese a las compañías de seguro, obras sociales, empresas de medicina prepaga o aseguradoras de riesgos de trabajo: a) Solicitar análisis genéticos previos a la cobertura de seguros o servicios de salud; b) Requerir, recopilar, canjear o comprar información genética; c) Entregar bajo ningún concepto o condición, información genética a otras compañías de seguros, obras sociales, empresas de medicina prepaga o aseguradoras de riesgos de trabajo, ni a persona o empresa que recopile, compile, publique o difunda información sobre seguros, ni a un empleador respecto de sus empleados.* Luego el artículo 11 señala que: *"es obligatoria la confidencialidad en el manejo de la información genética que formare parte de los informes médicos de un empleado. Su violación hará responsable al empleador por daños y perjuicios*". La excepciones al deber anterior se señalan en al artículo 12. Finalmente el artículo 13 agrega que: *"Los organismos públicos están autorizados a utilizar la información genética con fines exclusivamente estadísticos y garantía de anonimato, destinada a la aplicación de políticas públicas, quedando en lo restante incluidos en las disposiciones de la presente ley".*

3. Bienes Jurídicos Protegidos por la Legislación de Datos Personales

Determinar el bien jurídico protegido por las normas de protección de datos personales en la Argentina no es tarea fácil, pues existen las más diversas opiniones sobre el tema. A continuación se señalarán los pareceres tanto de miembros de la Convención Nacional Constituyente encargados de la reforma de la Constitución (convencionales, según la terminología argentina), como de autores trasandinos al respecto.

Como señala Puccinelli, algunos convencionales estimaron que el bien jurídico protegido por la disposición contenida en el artículo 43 de la Constitución sería el derecho a la intimidad [110] . Para la convencional Roque, si bien el bien jurídico es la intimidad, la disposición del artículo 43 "tiene la elasticidad y la amplitud conceptual que aconsejan las nuevas corrientes doctrinarias, permitiendo una legislación más ajustada a la hora de reglamentar, revalorizando al Congreso como factor de mediación social y política" [111] . En un sentido más amplio se pronunciaron los convencionales Ancarani, Cullen y Delich. El primero sostuvo que los bienes jurídicos protegidos por la norma constitucional eran "la intimidad, la privacidad, la honra, la integridad psicofísica, la integridad e intimidad familiar, los propios datos de las personas (derecho a la identidad) y las reservas del hombre en sus aspectos más íntimos" [112] . Delich por su parte, señaló que el más importante o uno de los más importantes derechos privados era el derecho a la privacidad, el derecho a disponer de la información que hace a su propia identidad [113] . Finalmente, Cullen se inclinó por el derecho a la reputación y a la honra como bien jurídico protegido por la acción de hábeas data [114] .

En la doctrina, la discusión acerca del bien jurídico protegido tampoco presenta unidad de pareceres. Para Palazzi, Pizzolo y Ekmekdjan, el bien jurídico protegido sería la intimidad, adhiriendo a una tesis restrictiva de aquélla. [115] . Padilla se inclina por el derecho a la intimidad, pero al definir éste lo hace como si se refiriera al derecho a la autodeterminación informativa [116] . Para Basterra, se tutelaría tanto el derecho la libertad informática como el derecho la propia imagen o perfil [117] . Finalmente, Puccinelli señala

[110] En este sentido los convencionales, Cavagna, Hernández, Menem, Natale y Quiroga Lavié. En Puccinelli, Oscar: *"El hábeas data en Indoiberoamérica"*, Temis, Bogotá, 1999, pág.241.

[111] *Ídem*. pág. 242.

[112] *Ibídem*.

[113] *Ibídem*.

[114] *Ibídem*.

[115] En Puccinelli, Oscar, *op. cit*., pág. 243.

[116] Padilla, *op. cit*., pág. 31.

que dada la amplitud del texto constitucional, éste es capaz de proteger no sólo a la intimidad sino que también abarcaría teleológicamente el honor, la imagen, la autodeterminación informativa, incluso otros derechos que pueden ser inferidos en cada caso concreto [118] .

En el plano del derecho positivo, la Ley 25.326 señala en el inciso primero de su artículo 1º, que el objeto de ésta es la protección integral de los datos personales para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información [119] .

En suma, la determinación del bien jurídico protegido por las normas de protección de datos personales en la Argentina es algo debatido. Desde el punto de vista del legislador, diversos serían los bienes jurídicos a proteger, por lo que se estaría lejos de poder postular una teoría monista al respecto.

En nuestra opinión, la configuración constitucional y legal del ordenamiento jurídico argentino en materia de protección de datos personales, no permitiría fundamentar sin dificultades que el bien jurídico protegido sea la autodeterminación informativa, pues el propio texto constitucional del artículo 43 restringe doblemente la procedencia de la acción de hábeas data; primero, respecto de los bancos de datos o registros privados, sólo a aquéllos *"destinados a proveer informes"*,y segundo, al exigir para la supresión, rectificación, confidencialidad o actualización de datos personales, que éstos sean falsos o discriminatorios. Por otra parte, la propia Ley de protección de datos personales no es lo suficientemente explícita al respecto, más bien parece un tenue asomo de la libertad informática cuando señala que el objeto es garantizar el honor y la intimidad de las personas *"así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional"*. Las restricciones ya señaladas, nos hacen pensar en definitiva que existiría más de un bien jurídico protegido, destacando principalmente el derecho a la intimidad, la vida privada y el derecho al honor, este último en virtud de exigirse "*falsedad*" de los datos para la procedencia del hábeas data y por contemplarse expresamente en la Ley 25.326.

4. Principios Informativos de la Legislación de Protección de Datos

[117] Basterra, Marcela: *"Los Derechos Tutelados por el hábeas data: doctrina y jurisprudencia, en La defensa de la intimidad y de los datos personales a través del hábeas data"*, Gozaíni, Alfredo, Coord., Ediar, Bs. As., 2001, pág. 243.

[118] Puccinelli, *op. cit*., págs. 245-246.

[119] Artículo 1º Objeto. *"La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de trata miento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.* Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal. *En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas".*

Personales

Apoyada en la legislación comparada, especialmente en la española [120] , la Ley argentina 25.326 establece ciertos principios informativos en materia de tratamiento de datos personales, pudiendo señalarse los siguientes:

1º) Principio de la licitud y lealtad de los archivos de datos

Para que pueda afirmarse que un ordenamiento jurídico contempla este principio, la ley respectiva debe encargarse de establecer ciertas reglas mínimas a respetarse por todo sujeto que pretenda tratar mecánica o automatizadamente datos personales. En el caso de Argentina este principio se traduce en la exigencia previa al tratamiento de datos personales, de una inscripción de los archivos de datos, respetando los demás principios de la Ley 25.326 y del Reglamento. Asimismo, los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública. Al efecto, se dispone en el artículo 3º que: *"La formación de archivos de datos será lícita cuando se encuentren debidamente inscritos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia. Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública"*.

2º) Principio de la calidad de los datos

Este principio, el legislador lo consagra de manera directa en el artículo 4º, el cual señala:

Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.

Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

Los datos deben ser exactos y actualizarse en el caso que ello fuere necesario.

Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados por el responsable del archivo o base de datos, cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.

Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

También encontramos plasmado este principio, en el artículo 23 inciso 3º, el cual

[120] Quiroga Lavié, *op. cit.*, pág. 69.

dispone que los datos personales registrados con fines policiales se cancelaran cuando *"no sean necesarios para las averiguaciones que motivaron su almacenamiento".*

A nivel reglamentario, se desarrolla el principio de la calidad de los datos en el artículo 4º, el cual prescribe que para determinar la lealtad y buena fe en la obtención de los datos personales, así como el destino que a ellos se asigne, *"se deberá analizar el procedimiento efectuado para la recolección y, en particular, la información que se haya proporcionado al titular de los datos de acuerdo con el artículo 6º de la Ley Nº 25.326"* [121] .

3º) Principio del consentimiento informado del titular de los datos

Este principio está desarrollado en el artículo 5º de la Ley el cual preceptúa que: *"El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento expreso, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, juntamente con las advertencias previstas en el artículo 6º de la presente ley"* [122] .

A su vez, el artículo 6º preceptúa que cuando se recaben datos personales se deberá *"informar previamente a sus titulares en forma expresa y clara"*: 1) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; 2) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; 3) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente; 4) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos y, 5) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

No obstante el carácter de principio que tiene el consentimiento previo e informado

[121] . Se agrega por esta disposición que: *"Cuando la obtención o recolección de los datos personales fuese lograda por interconexión o tratamiento de archivos, registros, bases o bancos de datos, se deberá analizar la fuente de información y el destino previsto por el responsable o usuario para los datos personales obtenidos. El dato que hubiera perdido vigencia respecto de los fines para los que se hubiese obtenido o recolectado debe ser suprimido por el responsable o usuario sin necesidad de que lo requiera el titular de los datos. La Dirección Nacional de Protección de Datos Personales efectuará controles de oficio sobre el cumplimiento de este principio legal, y aplicará las sanciones pertinentes al responsable o usuario en los casos que correspondiere. La Dirección Nacional de Protección de Datos Personales procederá, ante el pedido de un interesado o de oficio ante la sospecha de una ilegalidad, a verificar el cumplimiento de las disposiciones legales y reglamentarias en orden a cada una de las siguientes etapas del uso y aprovechamiento de datos personales: a)Legalidad de la recolección o toma de información personal; b)Legalidad en el intercambio de datos y en la transmisión a terceros o en la interrelación entre ellos; c) Legalidad en la cesión propiamente dicha; d) Legalidad de los mecanismos de control interno y externo del archivo, registro, bases o bancos de datos"* (Artículo 4º Reglamento).

[122] Agrega el artículo 5º del Reglamento que: *"(…) La Dirección Nacional de Protección de Datos Personales establecerá los requisitos para que el consentimiento pueda ser prestado por un medio distinto a la forma escrita, el cual deberá asegurar la autoría e integridad de la declaración. El consentimiento dado para el tratamiento de datos personales puede ser revocado en cualquier tiempo. La revocación no tiene efectos retroactivos (…)".*

del titular de los datos personales, existen excepciones a éste. El artículo 5º inciso 3º de la Ley, señala que no será necesario el consentimiento cuando: 1) La obtención de los datos provenga de fuentes de acceso público irrestricto; 2) Cuando se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de obligación legal; 3) Cuando se trate de listados de datos limitados al nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; 4) En caso que deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios su cumplimiento y, 5) Las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes afectas al secreto bancario.

Además de las excepciones recién señaladas, el inciso 2º del artículo 23º de la Ley establece otros casos vinculados con la excepción señalada en el Nº 2) del párrafo anterior. Este artículo dispone que:*"(…) el tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad".*

Por lo tanto, en el caso de los datos personales recabados y tratados por los organismos de seguridad o inteligencia y fuerzas armadas para fines de defensa nacional o seguridad de la nación, no se requiere el consentimiento del titular de los datos, y en esos casos el tratamiento debe limitarse estrictamente al cumplimiento de las misiones legalmente asignadas a esos organismos.

Finalmente, podemos señalar otros casos de excepción contemplados a propósito de la prestación de servicios de información crediticia. A este respecto, el artículo 26º dispone en el Nº 2 que: *"pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés"*. Más adelante, se añade que: *"la prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios"* (Art. 26 Nº 5).

4º) Principio de seguridad de los datos

El artículo 9º de la Ley consagra este principio explícitamente señalando al respecto que:

1. *"El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado".*

2. *"Queda prohibido registrar datos personales en archivos, registros o bancos que*

no reúnan condiciones técnicas de integridad y seguridad".

Por su parte, el artículo 9º del Reglamento dispone que la Dirección Nacional de Protección de Datos Personales *"promoverá la cooperación entre sectores públicos y privados para la elaboración e implantación de medidas, prácticas y procedimientos que susciten la confianza en los sistemas de información, así como en sus modalidades de provisión y utilización"* [123] .

En suma, puede afirmarse que este principio además de consagrarse directamente por el legislador, se reafirma a través de la importante labor a que está llamada la Dirección Nacional de Protección de Datos Personales en uno de sus diversos roles; promover la cooperación entre el sector público y privado en materia de seguridad en el tratamiento de datos.

5º) Principio de la confidencialidad de los datos

El principio de la confidencialidad de los datos en la Ley argentina apunta a que: *"el responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos"* (Art. 10º inciso 1º).

Las excepciones a este principio son las siguientes: 1) Resolución judicial y, 2) Cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública (Art. 10º inciso 2º).

6º) Principio del consentimiento para la cesión de los datos

El artículo 11º de la Ley señala en esta materia que los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y *"con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo"* [124] . El consentimiento para la cesión es revocable.

En materia de excepciones, la Ley señala en el artículo 11º inciso 3º, que el consentimiento no será exigible en caso de: 1) Disposición legal; 2)Cesión de datos realizada entre dependencias de los órganos del Estado en forma directa, en la medida

[123] Más adelante, el artículo 11º del Reglamento señala a propósito del principio del consentimiento para la cesión de datos personales que la Dirección Nacional de Protección de Datos Personales fijará los estándares de seguridad aplicables a los mecanismos de disociación de datos. A su vez, la disociación de datos está definida en el artículo 2º de la Ley como *"todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable".* Hasta el momento, no tenemos conocimiento del cumplimiento de la obligación señalada por parte de la Dirección.

[124] El artículo 11 del Reglamento dispone por su parte que: *"Al consentimiento para la cesión de los datos le son aplicables las disposiciones previstas en el artículo 5º de la Ley Nº 25.326 y el artículo 5º de esta reglamentación (…) La cesión masiva de datos personales de registros públicos a registros privados sólo puede ser autorizada por ley o por decisión del funcionario responsable, si los datos son de acceso público y se ha garantizado el respeto a los principios de protección establecidos en la Ley Nº 25.326".*

del cumplimiento de sus respectivas competencias; 3) Cesión de datos personales relativos a la salud por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, preservándose la identidad de los titulares de los datos mediante mecanismos de disociación adecuados y, 4) Cesión de datos personales en que se haya aplicado un procedimiento de disociación de la información que garantice la no identificación del titular.

7º) Principio de la finalidad

Este principio se contiene en diversas disposiciones de la Ley 25.326. En este sentido, el artículo 3º prescribe que los archivos de datos *"no pueden tener finalidades contrarias a las leyes o a la moral pública*". El artículo 4º Nº 1 a su vez prescribe que los datos personales que se recojan a los efectos de su tratamiento deben ser *"ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido"*. En el Nº 3 del mismo artículo se agrega que los datos objeto de tratamiento no pueden ser utilizados para *"finalidades distintas o incompatibles con aquellas que motivaron su obtención".* Asimismo, el artículo 6º letra a), señala que cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara entre otras cosas *"la finalidad para la que serán tratados (…)"*. Por otra parte, el ya visto artículo 11º dispone en el Nº 1 que sólo pueden ser cedidos los datos para el cumplimiento de los *"fines directamente relacionados con el interés legítimo del cedente y del cesionario"* y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la *"finalidad de la cesión"* e identificar al cesionario o los elementos que permitan hacerlo. Finalmente, el artículo 22 al establecer el deber de inscripción de los registros de archivos de datos señala en el Nº 2 que el registro de archivos de datos debe comprender como mínimo la siguiente información: *"(…) b) Características y finalidad del archivo"*.

En suma, el principio de la finalidad se encuentra consagrado en diversas normas de la Ley argentina, de manera específica y clara, acorde a las disposiciones internacionales de protección de datos, en especial la europea de 1995.

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

En el ámbito de la Ley 25.326 y su respectivo Decreto reglamentario, es posible encontrar diversos aspectos en los cuales se encuentran regulados de forma diferenciada el sector público y el sector privado. Cabe precisar que la ley argentina, al hablar sobre su objeto (Art. 1º), se encarga de hacer suya lo preceptuado por la Constitución, en el sentido que la protección integral de los datos personales se extiende a todos aquellos datos asentados en archivos o bancos de datos *"públicos o privados destinados a dar informes"* [125] .

[125] La disposición del artículo 43 de la Constitución habla por su parte de archivos o banco de datos *"públicos, o los privados destinados a proveer informes"*.

A continuación se analizarán temáticamente los puntos de divergencia normativa o tratamiento diferenciado que la Ley 25.326 y el respectivo Reglamento contemplan respecto del sector público y el privado.

5.1 Consentimiento para el Tratamiento de los Datos

En lo relativo a este requisito, como se dijo, la regla general es el consentimiento expreso del titular de los datos. Ahora bien, dentro de las excepciones a ese requisito-principio encontramos diferencias de tratamiento entre el sector público y privado.

En cuanto al sector público, no se necesita el consentimiento del titular de los datos personales cuando es el Estado quien recaba datos personales para el ejercicio de las funciones que le son propias, o cuando la recolección se hace en virtud de una disposición legal (Art. 5º N º2 letra b).

Muy relacionada con la disposición anterior es aquella contemplada en el artículo 23º de la Ley, denominado por ésta como *"casos especiales"*, la cual también establece una excepción al principio del consentimiento del titular, al señalar que el tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, *"sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos"* (Art. 23º Nº 2). Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad.

Dentro de las excepciones legales a la regla general del consentimiento, en el ámbito de los privados o particulares, cabe mencionar que no se requiere del consentimiento del titular cuando:1) Los datos son recabados de fuentes accesibles al público; 2) Se trate de listados limitados al nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación , fecha de nacimiento y domicilio; 3) Deriven de una relación contractual, científica o profesional del titular de los datos y sean ellos necesarios para el cumplimiento de esa relación y, 4) Tratándose de las operaciones realizadas por las entidades financieras y aquellas recibidas de los clientes de éstas, no afectas al secreto bancario (Art. 5º Nº 2) [126] .

Dentro del ámbito privado, también se contemplan otras excepciones a propósito de la prestación de servicios de información crediticia; quienes realizan estas actividades, pueden tratar datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés, por lo que no se requiere el consentimiento del deudor o titular de los datos (Art. 26 Nº 2).

[126] En relación con el secreto bancario, el artículo 5º del Reglamento viene a aclarar la última excepción señalada, disponiendo que: *"(…) En ningún caso se afectará el secreto bancario, quedando prohibida la divulgación de datos relativos a operaciones pasivas que realicen las entidades financieras con sus clientes, de conformidad con lo dispuesto en los artículos 39 y 40 de la Ley Nº 21.526".*

5.2 Consentimiento para la Cesión de Datos Personales

Como ya señalamos, la regla general en materia de tratamiento de datos es el previo consentimiento del titular de los datos. Este mismo requisito es necesario para la licitud de la cesión de datos personales. Al respecto, el artículo 11º de la Ley, dispone que los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario [127] y con *"el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo".* Ahora bien, dentro de las excepciones al principio del consentimiento para la cesión de datos, podemos encontrar diferencias de tratamiento entre el sector público y privado. De aquellas excepciones, al menos una es de aplicación exclusiva para el sector público, representado por el Estado y sus organismos; sólo éstos pueden obviar la prohibición de la cesión de los datos personales sin el consentimiento del titular cuando: 1) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal y, 2) Cuando se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus propias funciones (Art.11).

Cabe agregar que el Reglamento en el artículo 11, dispone que para la cesión masiva de datos personales de registros públicos a registros privados *"se requerirá autorización legal o autorización del funcionario responsable, si los datos son de acceso público y se ha garantizado el respeto a los principios de protección establecidos en la Ley Nº 25.326".* Luego agrega este mismo artículo que: *"no es necesario acto administrativo alguno en los casos en que la ley disponga el acceso a la base de datos pública en forma irrestricta. Se entiende por cesión masiva de datos personales la que comprende a un grupo colectivo de personas* (Art.11 del Reglamento).

En el caso de las excepciones que tocan al sector privado o a los particulares, el artículo 26º Nº 5 de la ley prescribe que: *"La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios".*

En suma, las diferencias de tratamiento entre el sector público y privado en materia de consentimiento para la cesión de datos personales, sólo operan el al ámbito de las excepciones.

5.3 Tratamiento de los Datos Sensibles

Antes de entrar a analizar si existen puntos de tratamiento diferenciado entre el sector público y privado en esta materia, señalaremos el marco general normativo aplicable a

[127] El artículo 11 del Reglamento, establece el ámbito de aplicación del requisito *"interés legítimo"*del cesionario en relación a las cesiones de datos realizadas por organismos públicos autorizados para tratar datos de ese mismo carácter, señalando que: *"en el caso de archivos o bases de datos públicas dependientes de un organismo oficial que por razón de sus funciones específicas estén destinadas a la difusión al público en general, el requisito relativo al interés legítimo del cesionario se considera implícito en las razones de interés general que motivaron el acceso público irrestricto".*

los datos sensibles contemplado por el sistema legal argentino.

El artículo 2º de la Ley 25.326, define los datos sensibles como aquellos *"datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical o política e información referente a la salud o a la vida sexual"* [128] .

Luego, en el artículo 7º se establece la regla general respecto de este tipo de datos, preceptuándose que:

"1. Ninguna persona puede ser obligada a proporcionar datos sensibles.

2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.

4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas".

Volviendo a la definición legal de datos sensibles, como se recordará, ésta incluye las informaciones relativas a la salud de las personas. A esa especial clase de dato se refiere el artículo 8º de la Ley, señalando que: *"Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional".*

Aclarado el concepto y la forma en que el legislador trasandino se ocupa de reglamentar los datos sensibles, entraremos al análisis de las diferencias que pueden apreciarse en cuanto a la regulación del sector público y privado en materia de datos sensibles. Cabe adelantar al respecto, que éstas sólo se aprecian en el ámbito de las excepciones a la regla general de prohibición de recolección y tratamiento de datos sensibles.

Respecto del sector público, puede señalarse que existe tratamiento diferenciado en relación a los particulares, en la medida que la Ley 25.326 reserva exclusivamente al Estado la facultad de recolectar y tratar datos relativos a antecedentes penales o contravencionales, a través de sus autoridades públicas competentes (Art.7 Nº 4).

Al sector privado, por su parte, sólo se lo faculta excepcionalmente para recolectar algunos tipos de datos sensibles. Este es el caso de las instituciones religiosas, los

[128] Esta definición es muy similar a la del artículo 8 1. de la Directiva europea de protección de datos personales Nº 95/46, la cual señala que *"los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad".*

partidos políticos y, las organizaciones sindicales, las cuales pueden llevar registros de sus miembros (Art.7 Nº 3).

Finalmente, entendemos que la excepción a la prohibición de tratamiento de las informaciones relativas a la salud de las personas, sería aplicable tanto a los establecimientos sanitarios públicos como privados, y a los profesionales de las ciencias de la salud, quienes son los únicos autorizados para recolectar y tratar esa clase de datos personales, debiendo respetar en todo caso los principios señalados por la Ley, así como también el secreto profesional.

5.4 Derechos de los Titulares de los Datos Personales

Esta materia se relaciona directamente con la acción de hábeas data establecida en la Constitución y regulada en la Ley 25.326. Como ya se ha dicho, la Constitución argentina refiriéndose al hábeas data, dispone en el párrafo 3º del artículo 43 que toda persona podrá interponer esa acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que *"consten en registros o bancos de datos públicos, o los privados destinados a proveer informes*, *y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos"*.

En el ámbito legal, se reconocen diversos derechos a los titulares de los datos, los cuales pueden ser ejercidos en dos instancias distintas; directamente ante los responsables de los archivos, registros o bancos de datos a través de un procedimiento extrajudicial o administrativo (según sea el carácter del archivo en contra del cual se procede) y, a través del ejercicio de la acción de hábeas data o de protección de datos que se ejerce ante los Tribunales de justicia, una vez agotada la vía previa informal o administrativa.

Dentro de los derechos reconocidos a los titulares de los datos, podemos mencionar al derecho de información, el cual se concibe en los siguientes términos: *"Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita"* (Art.13º). En este caso la información debe ser requerida de la Dirección Nacional de Protección de Datos, nombre que se le dio en Argentina al órgano de control previsto por la Ley 25.326. La razón de ello, radica en que todos los archivos, registros o bancos de datos sean éstos públicos, o privados destinados a proporcionar informes, deben inscribirse en el registro que al efecto deba llevar la Dirección (Art. 21).

Otro de los derechos constitucionales desarrollados por el legislador es el derecho de acceso, el cual se regula en el artículo 14 y dispone lo que sigue:

1. *"El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes".*

2. *"El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará*

expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley" (Art. 14 Nº 2) [129] .

En lo relativo al contenido de la información que debe ser entregada por el responsable del archivo, registro o banco de datos, el artículo 15º dispone que: 1) La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen; 2) La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado; 3) La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen u otro idóneo a tal fin.

Ahora bien, en cuanto a los derechos de rectificación, actualización o supresión de datos y bloqueo de éstos, el artículo 16º prescribe lo que sigue:

"1. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.

2. El responsable o usuario de un banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de haber recibido el reclamo del titular de los datos o advertido el error o falsedad.

3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley.

4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.

5. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.

6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.

7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos".

Finalmente, el artículo 33 de la Ley 25.326 señala que la acción de protección de los datos personales o de hábeas data procederá: *"a) para tomar conocimiento de los datos*

[129] Agrega la disposición que*: "3.-El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto. (…)4.- El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales"* (Art. 14 Nº 3 y 4).

personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos; b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización".

De lo señalado por las disposiciones anteriores, se aprecia la existencia de un tratamiento diferenciado en relación a la procedencia de la acción de hábeas data. En el caso que ésta se ejerza en contra de los responsables de archivos, registros o bancos de datos de carácter privado, sólo es procedente respecto de aquéllos *"destinados a proporcionar informes"*. En cambio, la acción de hábeas data en contra de archivos, registros o bancos de datos públicos procede en principio sin restricciones, salvas las excepciones legales.

5.5 Excepciones al Ejercicio de los Derechos de los Titulares de Datos

Tanto el Constituyente como la ley de protección de datos personales argentina, reconocen los derechos de acceso, rectificación, actualización o supresión y el bloqueo de datos, los cuales deben ejercerse ante los responsables o usuarios de bancos de datos públicos y de los privados destinados a proveer informes. No obstante lo anterior, la ley ha señalado casos en los cuales no podrá ejercerse uno o más de esos derechos.

Dentro del campo de las excepciones contempladas por la Ley a los derechos ya mencionados (Art. 17), cabe anotar diferencias de tratamiento entre el sector público y el sector privado o particulares [130] .

En el caso de los organismos del Estado que sean responsables o usuarios de bancos de datos públicos, éstos pueden por decisión fundada *"denegar el acceso, rectificación o supresión"* de los datos personales, en función: 1) De la protección de la defensa de la nación; 2) Del orden público; 3) De la seguridad pública y, 4) De la protección de los derechos e intereses de terceros. Asimismo, pueden denegarse estos derechos cuando pudiere obstaculizarse actuaciones judiciales o administrativas en curso que se vinculen a: i) La investigación sobre cumplimiento de obligaciones tributarias o previsionales; ii) El desarrollo de funciones de control de la salud y del medio ambiente; iii) La investigación de delitos penales y, iv) La verificación de infracciones administrativas. Con todo, se permite el acceso a los registros en el momento en que se ejerza el derecho a defensa por el titular de los datos (Art.17).

[130] El artículo 17 de la Ley 25.326 señala textualmente que: 1.*"Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión, fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros".* 2. *"La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado".* 3. *"Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa".*

En el ámbito de los particulares o sector privado, los derechos de acceso, rectificación y actualización de datos personales operan sin excepción. Sin embargo, no pueden afectarse en ningún caso las fuentes de información periodísticas (Art. 43 C. Pol.).

En cuanto al ejercicio del derecho de supresión de datos personales, el artículo 16 Nº 5 ha restringido nuevamente el ámbito de aplicación de manera general (antes lo hizo en el art. 17), disponiendo que: *"La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos"*. Entendemos que esta excepción se aplica tanto al sector público como al privado en virtud del tenor de la disposición. Serán los jueces los que en definitiva determinarán en cada caso cuando opera dicha regla.

5.6 Creación y Registro de los Archivos, o Bancos de Datos Personales

El legislador argentino, con el objeto de hacer pública la información relativa a la identificación de los archivos, registros o bancos de datos personales, los responsables de éstos, el carácter y su finalidad, entre otros aspectos, ha dispuesto en el artículo 21 que todo archivo, registro o base de datos pública o privada destinada a proporcionar informes *"debe inscribirse"* en el Registro que para ese efecto lleva el organismo de control denominado Dirección Nacional de Protección de Datos. La información que debe contener el Registro es la misma, sea que se trate de archivos o bases de datos del sector público o del sector privado [131] .

En materia de creación y registro de los archivos y bancos de datos personales, se aprecian ciertas diferencias en el tratamiento que la ley dispone para los órganos públicos y los particulares o sector privado. Para el sector público, representado por el Estado y

[131] El artículo 21 de la ley argentina dispone que: *"1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control. 2. El registro de archivos de datos debe comprender como mínimo la siguiente información: a) Nombre y domicilio del responsable; b) Características y finalidad del archivo; c) Naturaleza de los datos personales contenidos en cada archivo; d) Forma de recolección y actualización de datos; e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos; f) Modo de interrelacionar la información registrada; g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información; h) Tiempo de conservación de los datos; i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.* 3. Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro. *El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en el capítulo VI de la presente ley".* Por otra parte, el Reglamento dispone a su turno en el artículo 21 que: *"El registro e inscripción de archivos, registros, bases o bancos de datos públicos, y privados destinados a dar información, se habilitará una vez publicada esta reglamentación en el Boletín Oficial. Cuando el archivo, registro, base o banco de datos privado se constituya con el fin de proporcionar información de datos personales dentro de un mismo grupo económico de empresas controladas y controlantes, en los términos de la Ley Nº 19.550, no será obligatoria la inscripción, sin perjuicio de ser alcanzados por las sanciones previstas en el Capítulo VI de la Ley Nº 25.326 cuando se verifique la cesión o transferencia de los datos a personas no vinculadas. Esta disposición no alcanzará a las Uniones Transitorias de Empresas. Deben inscribirse los archivos, registros, bases o bancos de datos públicos y los privados a que se refiere el artículo 1º de esta reglamentación. A los fines de la inscripción de los archivos, registros y bases de datos con fines de publicidad, los responsables deben proceder de acuerdo con lo establecido en el artículo 27, cuarto párrafo, de esta reglamentación".*

sus organismos, el artículo 22 la Ley dispone que: *"las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos, deben hacerse por medio de disposición general publicada en el Boletín oficial de la Nación o diario oficial"*. Luego, la misma disposición señala una serie de indicaciones que deben contener las normas legales de creación, modificación o supresión de los archivos o bancos de datos de éstos organismos [132] . En el caso de los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal, éstos deberán inscribirse en el Registro que para tal efecto lleva la Dirección Nacional de Protección Datos (Art.24). Por lo tanto, aquellos bancos de datos, registros o archivos de uso exclusivamente personal, no están sujetos a la obligación general de inscripción.

5.7 Archivos, Registros o Bancos de Datos Relativos a Encuestas

La Ley 25.326 dispone en el artículo 28, que ésta no será aplicable *"a las encuestas de opinión, mediciones y estadísticas relevadas conforme a la ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable"*. En esta materia, podríamos señalar que al sector público, en lo relativo a las mediciones y estadísticas realizadas a través del censo nacional, tampoco se le aplicaría la ley 25.326, pues esa actividad se rige por ley especial Nº 17.622. En los demás casos, la regla operaría ampliamente tanto respecto del sector público como el privado, y por ende, no existirían diferencias de regulación legal. Debemos agregar que para todos los casos ya señalados se prescribe la utilización de técnicas de disociación de la información en caso de no ser posible mantener el anonimato (Art. 28 inciso 2º). Por otra parte, el artículo 28 del Reglamento prescribe que estos archivos, bancos de datos o registros (sin distinguir) son responsables y pasibles de las multas establecidas en la ley cuando se infrinjan sus disposiciones.

5.8 Tratamiento Manual o Automatizado de Datos

La ley argentina, a lo menos en dos disposiciones hace referencia al tipo de tratamiento de datos que será objeto de regulación legal. Así, el artículo 1º de la Ley señala que el objeto de ésta es la protección integral de los datos personales *"asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes"*. Luego, en el artículo 2º, al definir legalmente el término archivo, registro, base o banco de datos señala que éstos

[132] Al efecto, el artículo 22 de la Ley señala que: *"(…) Las disposiciones respectivas, deben indicar: características y finalidad del archivo; personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas; procedimiento de obtención y actualización de los datos; estructura básica del archivo, informatizado o no , y la descripción de la naturaleza de los datos personales que contendrán; las cesiones, transferencias o interconexiones previstas; órganos responsables del archivo, precisando dependencia jerárquica en su caso; las oficinas ante las que se pudiesen efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación o supresión"*(Artículo 22inciso 2º). Agrega en el inciso 3º que*"En las disposiciones que se dicten para la supresión de los registros informatizados se establecerá el destino de los mismos o las medidas que se adopten para su destrucción".*

indistintamente, designan al conjunto organizado de datos personales que sean *"objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso"*. Por otra parte, la misma disposición anterior define el tratamiento de datos como las *"operaciones y procedimientos sistemáticos, electrónicos o no"*, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

De las normas recién señaladas se desprende que el legislador argentino ha incluido dentro del ámbito objetivo de regulación legal, tanto al tratamiento de datos personales de carácter automatizado como manual, lo cual se refleja además en el carácter de los archivos, registros, o bancos o bases de datos personales.

En cuanto al trato dado por el legislador tanto al sector público como el privado en la materia, no se aprecian diferencias. Por lo tanto, puede afirmarse que tanto el tratamiento manual como el automatizado de datos personales que realicen el Estado, o los particulares con el fin de proporcionar informes, están sujetos de igual manera a la normativa legal del año 2000.

5.9 Personas Jurídicas como Titulares de Datos

En lo relativo a los sujetos de los derechos reconocidos por la ley argentina de protección de datos persales, debemos señalar que la titularidad de éstos es reconocida tanto a las personas físicas como a las personas de existencia ideal. Es decir, la Ley 25.326 reconoce expresamente como titulares de los derechos consagrados por ella no sólo a las personas naturales, sino que también a las personas jurídicas sin distinción. Al efecto, el artículo 2º, define los datos personales como la *"información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables".*

En esta materia, el legislador no ha hecho distinción alguna en razón del ámbito público o privado de tales personas, por lo que entendemos que la regla es aplicable tanto a las personas naturales o físicas, como a las personas jurídicas o ideales, sean éstas de derecho público o de derecho privado.

5.10 Transmisión Internacional de Datos Personales

Esta materia se abordará *in extenso* en el punto Nº 8 de este análisis. Por ahora, sólo adelantaremos que la regla general es la prohibición de la transmisión internacional de datos personales. En efecto, el artículo 12º de la Ley dispone que: *"Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados".* Con todo, aunque no se cumpla el requisito exigido por la ley, podrá realizarse la transmisión internacional de datos personales en determinados casos. De ésos casos excepcionales, es posible advertir diferencias entre la regulación prevista para el sector público y para el sector privado.

Las situaciones en que al Estado y a los organismos de éste se les faculta para

transmitir datos personales fuera de su territorio (sin necesidad de consentimiento del titular y, aunque el país receptor no contemple niveles de protección adecuados a esos datos) son los siguientes: 1) En caso de colaboración judicial internacional; 2) Cuando la transferencia se hubiere acordado en el marco de tratados internacionales en que el Estado argentino fuere parte; y 3) Cuando la transferencia tenga por objetivo la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, terrorismo o narcotráfico (Art.12).

Cabe agregar en este ámbito, que el Reglamento otorga a la Dirección Nacional de Protección de Datos la facultad de evaluar de oficio o a petición de parte, el nivel de protección existente en un Estado determinado u Organismo Internacional. De esta forma opera como un ente consultivo, que en caso de llegar a determinar que un determinado país no reúne las características de ser puerto seguro para la transmisión de datos, debe comunicarlo al Poder Ejecutivo y emitir un proyecto de decreto para emitir tal declaración (Art.12 del Reglamento).

5.11 Otras Diferencias

El artículo 18 de la Ley 25.326, establece ciertas prerrogativas para determinadas Comisiones Legislativas relacionas con la Defensa Nacional, con el fin de acceder sin el consentimiento de los titulares, a los archivos o bancos de datos personales que posean las Fuerzas Armadas, Fuerzas de Seguridad, policía y organismos de inteligencia, destinados al tratamiento de esos datos, con fines de defensa nacional o seguridad pública [133] .

6. Modelos de Tutela

La legislación argentina establece un mecanismo directo para la protección de los datos personales. En lo inmediato, contempla la denominada acción de protección de datos personales o hábeas data, la cual tiene consagración constitucional (Art. 43 inciso 3º), y se encuentra desarrolla en la Ley 25.326. Además de esta acción, y como norma especial de tutela, se examinará brevemente la acción de nominada “hábeas data financiero”que guarda semejanza con la acción del hábeas data.

A continuación analizaremos brevemente cada modelo de tutela de protección de

[133] El artículo 18 de la Ley dispone que: *“Las comisiones de Defensa Nacional y la Comisión Bicameral de Fiscalización de los Órganos y Actividades de Seguridad Interior e Inteligencia del Congreso de la Nación y la Comisión de Seguridad Interior de la Cámara de Diputados de la Nación, o las que las sustituyan, tendrán acceso a los archivos o bancos de datos referidos en el artículo 23, inciso 2, por razones fundadas y en aquellos aspectos que constituyan materia de competencia de tales Comisiones”.* Por otra parte, el artículo 23 Nº 2 prescribe que : *“El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad”.*

datos personales.

6.1. La Acción de Hábeas Data

Este mecanismo procesal contemplado primeramente en la reforma constitucional de 1994 y luego desarrollado por la Ley 25.326, es propiamente una acción en sentido procesal y no un recurso, pues su finalidad no es desconocer o atacar una resolución judicial previa enmarcada dentro de un proceso, sino poner en movimiento la actividad jurisdiccional para que tome las medidas que en derecho correspondan para el resguardo de una garantía constitucional.

6.1.1) Procedencia de la Acción

El artículo 33 de la Ley dispone que la acción de protección de los datos personales o de hábeas data procederá:

"a) Para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;

En los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización".

Cabe hacer presente que la Ley exige para la admisibilidad de la demanda de protección de datos personales o hábeas data, que se haya agotado previamente la vía prejudicial o administrativa. Es decir, el legislador señala que antes de que pueda demandarse judicialmente al responsable del archivo, registro o banco de datos, debe haberse ejercido con anterioridad por el titular de los datos personales el derecho de acceso rectificación, actualización o supresión de éstos de manera informal, ante el responsable del archivo, registro o banco de datos, y sólo en caso de no haberse satisfecho por esta vía el requerimiento, queda expedita la acción de hábeas data (Arts.14 y 16).

6.1.2) Legitimación Activa

De lo señalado por el artículo 34 [134] de la Ley, se desprende que para determinar quién puede ejercer válidamente la acción de hábeas data, es preciso efectuar previamente una distinción:

i) Si el afectado es una persona natural: el hábeas data podrá ejercerse por el propio afectado, por sus tutores o curadores y por los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado.

[134] Artículo 34: *"La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado. Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto. En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo".*

ii) Si el afectado es una persona jurídica: la acción será ejercida por sus representantes legales, o apoderados que éstas designen al efecto.

En el proceso podrá intervenir como tercero coadyuvante, el defensor del pueblo.

Destaca de la normativa anterior el que la Ley atribuya titularidad activa para ejercer la acción de hábeas data a las personas jurídicas o ideales, cuestión discutida en doctrina y excepcional en el derecho comparado.

6.1.3) Legitimación Pasiva

En virtud del artículo 43 inciso 3º de la Constitución y 35 de la Ley, la acción de hábeas data procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes [135].

En base al texto constitucional, se ha concluido por Néstor Sagüés que en principio estarían excluidos de la acción de hábeas data los archivos o registros "de y para uso exclusivo de su propietario", pues éstos estarían cubiertos por la regla constitucional que ampara el derecho a la privacidad (Art. 19) [136] y, porla que asegura la inviolabilidad de los papeles privados [137] . En nuestra opinión, la existencia de los derechos anteriores no obsta al ejercicio de la acción de hábeas data cuando se trate de datos sensibles, pues entran a jugar los derechos del titular de los datos en lo que respecta su intimidad o vida privada. En este sentido, creemos que el legislador habría desarrollado acertadamente el tenor del texto constitucional al tratar los datos sensibles, pues señala en el artículo 7º Nº 2 que: *"queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros".* De lo anterior, concluimos que la Ley 25.326 en cuanto a la regulación de los datos sensibles, fundado en el derecho a la intimidad o en la vida privada relativizaría el texto del artículo 19 de la Carta Fundamental, pues para determinar si alguien está tratando datos personales sensibles, debe previamente ejercitarse la acción de hábeas data. Así, en el caso que una persona recolecte y efectúe

135 Palazzi critica la estrechez del término utilizado por el Constituyente, señala que el término *"destinado a proveer informes"* es lo suficientemente impreciso para generar un marco de duda. Concluye que no le parece adecuada la limitación, pues en los hechos, pueden existir ficheros privados que no tengan la finalidad de proveer informes, pero que recolecten información sensible que pueda resultar discriminatoria para las personas o adolezcan de falsedad (Palazzi, Pablo: *"El Hábeas Data en el Derecho Constitucional Argentino".* En *"La defensa de la intimidad y de los datos personales a través del hábeas data"*, Gozaíni, Osvaldo (Coord.), Ed. Ediar, Bs.As., 2001, pág.47). Cabe agregar por nuestra parte, que la Ley 25.326 ha señalado expresamente la prohibición de formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles, por lo que la posibilidad de creación de esos registros ha sido limitada en sede legislativa (Art.7, inciso 3º).

136 El artículo 19º de la Constitución argentina dispone*: "Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ello no prohíbe".*

137 Sagüés, Néstor: "*Elementos de derecho constitucional"*, Ed. Astrea, Bs. As., 1997, pág. 256 (citado por Puccinelli, *op. cit*., pág. 252). Los respectivos artículos ya los hemos señalado más arriba, punto Nº 2.1.

tratamiento de datos sensibles de terceros, es claro que se está contraviniendo una prohibición legal y un derecho fundamental, con lo cual se abre la posibilidad de ejercicio de una acción de hábeas data que tenga como finalidad la supresión (destrucción) del archivo, registro o banco de datos sensibles tratados por un particular. Por otra parte, creemos que existe una razón adicional para sostener que sería procedente el hábeas data respecto de un particular que recolecta datos sensibles de terceros; el solo hecho de detentar información de ese carácter presenta un riesgo para cada uno de los terceros titulares de esos datos, por lo que aunque se adujera por el particular detentador del archivo, registro o banco de datos, que la información es para su sólo uso personal, ello no altera la probabilidad que por cualquier circunstancia, incluso un caso fortuito (robo de la información, incautación del soporte por causa distinta a una acción de hábeas data, entre otros), esa delicada información llegue a manos de terceros que puedan hacerla pública. Por lo tanto, cada titular de datos sensibles tendría el derecho de solicitar la eliminación de sus datos. Aún más, estimamos que podría incluso solicitar la destrucción de todo el archivo que contenga datos sensibles no exceptuados de tratamiento por la ley.

6.1.4) Competencia

El artículo 36 de la Ley dispone que: "*será competente para entender en esta acción, el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor".* Agrega esta norma queprocederá la competencia federal: *"a) Cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y b) Cuando los archivos de datos se encuentren interconectados en redes interjurisdicciones, nacionales o internacionales"* (sic).

6.1.5) Procedimiento Aplicable

El procedimiento aplicable para la tramitación de la acción de hábeas data está señalado en el artículo 37 de la Ley 25.326, el cual dispone que: *"la acción de hábeas data tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo común y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo"* (sic).

El procedimiento puede esquematizarse de la siguiente forma:

1) *Demanda*: la demanda deberá interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del archivo, registro o banco de datos y, en su caso, el nombre del responsable o usuario del mismo. En el caso de los archivos, registros o bancos públicos, se procurará establecer el organismo estatal del cual dependen (Art. 38 Nº 1). El accionante deberá alegar las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley (Art. 38 Nº 2).

2)*Medidas cautelares*: el afectado podrá solicitar que mientras dure el procedimiento,

el registro o banco de datos asiente que la información cuestionada está sometida a un proceso judicial (Art. 38 Nº 3). Asimismo, el Juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate (Art. 38 Nº 4).

3)*Informe*: admitida la acción el juez requerirá al archivo, registro o banco de datos la remisión de la información concerniente al accionante. Podrá asimismo solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente en la resolución de la causa que estime procedente (Art. 39 Nº 1). El plazo para contestar el informe no podrá ser mayor de cinco días hábiles, el que podrá ser ampliado prudencialmente por el juez (Art. 39 Nº 2). Los registros, archivos o bancos de datos privados no podrán alegar la confidencialidad de la información que se les requiera salvo el caso en que se afecten las fuentes de información periodísticas (Art. 40 Nº 1). Cuando un archivo, registro o banco de datos público se oponga a la remisión del informe solicitado con invocación de las excepciones al derecho de acceso, rectificación o supresión, autorizadas por la presente ley o por una ley específica; deberá acreditar los extremos que hacen aplicable la excepción legal. En tales casos, el juez podrá tomar conocimiento personal y directo de los datos solicitados asegurando el mantenimiento de su confidencialidad (Art. 40 Nº 2). Al contestar el informe, el archivo, registro o banco de datos deberá expresar las razones por las cuales incluyó la información cuestionada y aquéllas por las que no evacuó el pedido efectuado por el interesado, de conformidad a lo establecido en los artículos 13 a 15 de la Ley (Art. 41).

4)*Ampliación de la demanda*: contestado el informe, el actor podrá, en el término de tres días, ampliar el objeto de la demanda solicitando la supresión, rectificación, confidencialidad o actualización de sus datos personales, en los casos que resulte procedente a tenor de la presente ley, ofreciendo en el mismo acto la prueba pertinente. De esta presentación se dará traslado al demandado por el término de tres días (Art. 42).

6.1.6) La Sentencia

En lo medular, la sentencia que acoja la acción debe especificar si la información debe ser suprimida, rectificada, actualizada o declarada confidencial, estableciendo un plazo para su cumplimiento. Se acoja o se deniegue la acción ésta deberá ser comunicada a la Dirección Nacional de Protección de Datos la que lleva un registro al efecto [138] .

6.2 El Hábeas Data Financiero

El sistema jurídico argentino establece normas que contemplan el derecho de acceso a la

[138] El artículo 43 dispone en esta materia lo siguiente: 1. *"Vencido el plazo para la contestación del informe o contestado el mismo, y en el supuesto del artículo 42, luego de contestada la ampliación, y habiendo sido producida en su caso la prueba, el juez dictará sentencia.* 2. *En el caso de estimarse procedente la acción, se especificará si la información debe ser suprimida, rectificada, actualizada o declarada confidencial, estableciendo un plazo para su cumplimiento. 3. El rechazo de la acción no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir el demandante*. 4. *En cualquier caso, la sentencia deberá ser comunicada al organismo de control, que deberá llevar un registro al efecto".*

información del cliente financiero. Estas disposiciones son dictadas por el Banco Central de la República Argentina (en adelante BCRA) y están contenidas en el artículo 8.1 del Texto Ordenado y Actualizado de Normas sobre Clasificación de Deudores (última comunicación incorporada: "A" 3.630 del 10 de Junio de 2002 [139]).

El tema que ahora tratamos ha sido denominado por la doctrina como el "hábeas data financiero", y dice relación con el derecho de todo cliente de una institución financiera para solicitar de ésta la calificación de su comportamiento crediticio, conjuntamente con los fundamentos que la justifican conforme a las pautas fijadas por la autoridad de control. Esa autoridad es la Central de Deudores del Sistema Financiero (en adelante CDSF) dependiente del BCRA. La CDSF establece entre otras normas, parámetros específicos para la calificación de los deudores del sistema financiero. Asimismo crea un procedimiento de revisión de las calificaciones y fija una autoridad de control que en este caso es el BCRA. A su vez, éste queda sujeto a la revisión judicial de sus actos. Se ha señalado que todo este sistema jurídico que regula el hábeas data financiero tiene su base en el artículo 43 de la Constitución [140] .

El texto del artículo 8.1 contenido en la Comunicación "A" 3.630 del 10 de Junio de 2002 señala en su epígrafe "Informaciones a suministrar" que a solicitud de cada cliente, dentro de los 10 días corridos del pedido, la entidad financiera deberá comunicarle la última clasificación que le ha asignado, junto con los fundamentos que la justifican según la evaluación realizada por la entidad, el importe total de deudas con el sistema financiero y las clasificaciones asignadas que surjan de la última información disponible en la Central de deudores del sistema financiero [141] .

Según Sagüés -citado por Dubié- el hábeas data financiero tendría seis objetos:1) Conocer de la entidad financiera la última calificación asignada al comportamiento crediticio del cliente peticionante, más las deudas informadas a la CDSF; 2) Conocer de la entidad financiera las razones del encuadre calificativo por las que calificó al cliente peticionante de acuerdo a los parámetros establecidos por el BCRA; 3) Conocer de las demás calificaciones asignadas por otras casas bancarias que estén disponibles en el CDSF; 4) Solicitar a la entidad financiera la actualización de la calificación o monto asignado en la CDSF; 5) Solicitar a la entidad financiera la rectificación de la calificación o monto asignado y, 6) Solicitar la exclusión de una calificación y/o del monto asignado [142] .

Señala Dubié que el plazo para que la entidad financiera informe al cliente es de 10 días corridos, pues la norma no habla de días bancarios como en otras disposiciones del BCRA, por lo que en su ausencia entiende que son días corridos conforme el Código Civil [143] .

[139] [En línea] < http://www.bcra.gov.ar/folio/t-cladeu.pdf > [consulta: 24 de Enero 2003].

[140] **Todo lo anterior en Dubié, Pedro: *"El hábeas data financiero"*, en Revista electrónica Alfa-Redi Nº 39 [En línea] < http://www.alfa-redi.org/revista/data/39-7.asp > [consulta: 27 de Noviembre 2002].**

[141] *Ibídem*.

[142] *Ibídem*.

En suma, el instituto reseñado se relaciona con la acción de hábeas data en la medida que permite a los clientes de las instituciones financieras conocer no sólo la calificación financiera que se le ha asignado, sino que los fundamentos de esa calificación, el importe total de la deuda que sirve de base a la clasificación financiera, así como también actualización, rectificación o exclusión de una calificación o monto asignado. La importancia de esta acción, radica en poder ejercer el derecho a controlar periódicamente la historia crediticia de cada persona, la cual se basa en datos personales de carácter financiero, pues si los datos relativos al importe total de deuda o información del pasivo del titular son erróneos, conllevará consecuencialmente a una calificación equívoca, que podrá tener adversas consecuencias a efecto de solicitar, por ejemplo, un nuevo crédito en el sistema financiero.

7. Mecanismos de Control

La legislación argentina, con la finalidad de asegurar la efectiva aplicación de los derechos establecidos por la Ley 25.326, dispone la creación de un órgano administrativo de control que goza de autonomía funcional y actúa como órgano descentralizado en el ámbito del Ministerio de Justicia. Este órgano es la Dirección Nacional de Protección de Datos.

El artículo 29 de la Ley, le encomienda al órgano de control realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la ley de protección de datos. Para tales efectos, la Dirección Nacional de Protección de Datos deberá:

a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la Ley de Protección de Datos Personales, y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza;

b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por la Ley;

c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos;

d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos;

e)Sancionar administrativamente a quienes violen la Ley 25.326 y su Reglamento;

f) Hacerse parte en las acciones penales que se promuevan por violaciones a la ley de protección de datos personales;

g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la Ley y,

h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes para obtener la correspondiente inscripción en el Registro (Art. 29).

[143] *Ibídem*.

Por su parte, el Reglamento también se ocupa del órgano de control en el artículo 29, señalando en el numeral 5º que serán funciones de la Dirección Nacional de Protección de Datos además de las que surgen de la Ley Nº 25.326 y de las que establezca su reglamento: a) Dictar normas administrativas y de procedimiento relativas a los trámites registrales y demás funciones a su cargo, y las normas y procedimientos técnicos relativos al tratamiento y condiciones de seguridad de los archivos, registros y bases o bancos de datos públicos y privados; b) Atender las denuncias y reclamaciones interpuestas en relación al tratamiento de datos personales en los términos de la Ley Nº 25.326; c) Percibir las tasas que se fijen por los servicios de inscripción y otros que preste; d) Organizar y proveer lo necesario para el adecuado funcionamiento del Registro de archivos, registros y bases o bancos de datos públicos y privados previsto en el artículo 21 de la Ley Nº 25.326; e) Diseñar los instrumentos adecuados para la mejor protección de los datos personales de los ciudadanos y el mejor cumplimiento de la legislación de aplicación y, f) Homologar los códigos de conducta que se presenten de acuerdo a lo establecido por el artículo 30 de la Ley 25.326, previo dictamen del Consejo Consultivo, teniendo en cuenta su adecuación a los principios reguladores del tratamiento de datos personales, la representatividad que ejerza la asociación y organismo que elabora el código y su eficacia ejecutiva con relación a los operadores del sector mediante la previsión de sanciones o mecanismos adecuados.

8. Transmisión Internacional de Datos

En lo que respecta a la transmisión internacional o transfronteriza de datos personales, la ley argentina establece en el artículo 12 que: *"Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados"* [144] .En virtud de lo anterior, estimamos que la regla general es la prohibición de la transferencia internacional de datos personales.

Ahora bien, para que pueda operar la excepción a la regla general, es preciso tener una idea de lo que entiende la ley por *"niveles de protección adecuados"*. La tarea de darle contenido a esa frase legal, fue llevada a cabo por el Poder Ejecutivo Federal, el cual a través del artículo 12º del Decreto Reglamentario respectivo [145] señala que: *"Se entiende que un Estado u organismo internacional proporciona un nivel adecuado de protección cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente, o de sistemas de autorregulación, o del amparo que establezcan las cláusulas*

[144] La Ley señala en el artículo 12º que: *"1.Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados". "2. La prohibición no regirá en los siguientes supuestos: a) Colaboración judicial internacional; b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior; c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicables; d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte; e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico".*

contractuales que prevean la protección de datos personales" [146] .

Según el mismo Reglamento, el carácter adecuado o no del nivel de protección que ofrece un país u organismo internacional se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, tomándose en consideración: 1) La naturaleza de los datos; 2) La finalidad y la duración del tratamiento o de los tratamientos previstos; 3) El lugar de destino final; 4) Las normas de derecho, generales o sectoriales, vigentes en el país de que se trate; 5) Las normas profesionales, códigos de conducta y las medidas de seguridad en vigor en dichos lugares, o que resulten aplicables a los organismos internacionales o supranacionales (Art. 12 del Reglamento) [147] .

Con todo, de lo señalado por artículo 12 la Ley, complementado por su homónimo del Reglamento, se puede concluir que la prohibición de transmisión internacional de datos personales tampoco regirá en los siguientes casos: 1) Colaboración judicial internacional; 2) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto no pueda

[145] El artículo 12 del Decreto Reglamentario dispone a su turno que: *"la prohibición de transferir datos personales hacia países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados, no rige cuando el titular de los datos hubiera consentido expresamente la cesión. No es necesario el consentimiento en caso de transferencia de datos desde un registro público que esté legalmente constituido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones legales y reglamentarias para la consulta. Facúltase a la Dirección Nacional de Protección de Datos Personales a evaluar, de oficio o a pedido de parte interesada, el nivel de protección proporcionado por las normas de un Estado u organismo internacional. Si llegara a la conclusión de que un Estado u organismo no protege adecuadamente a los datos personales, elevará al Poder Ejecutivo Nacional un proyecto de decreto para emitir tal declaración. El proyecto deberá ser refrendado por los Ministros de Justicia y Derechos Humanos y de Relaciones Exteriores, Comercio Internacional y Culto. El carácter adecuado del nivel de protección que ofrece un país u organismo internacional se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el lugar de destino final, las normas de derecho, generales o sectoriales, vigentes en el país de que se trate, así como las normas profesionales, códigos de conducta y las medidas de seguridad en vigor en dichos lugares, o que resulten aplicables a los organismos internacionales o supranacionales. Se entiende que un Estado u organismo internacional proporciona un nivel adecuado de protección cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente, o de sistemas de autorregulación, o del amparo que establezcan las cláusulas contractuales que prevean la protección de datos personales*".

[146] El Reglamento a su vez, otorga facultades a la Dirección Nacional de Protección de Datos Personales para evaluar de oficio o a pedido de parte interesada, el nivel de protección proporcionado por las normas de un Estado u organismo internacional.

[147] Palazzi señala que este artículo viene a aclarar lo que la Ley 25.326 no explicaba, esto es la posibilidad de evaluar cuándo un país posee niveles adecuados de protección al efecto de transferir datos personales más allá de las fronteras, pues la ley prohíbe la transferencia internacional pero no explica qué se entiende por un *"nivel de protección adecuado"*. A ese efecto, el Decreto Reglamentario sigue las pautas de la Directiva Europea (Arts. 25 y 26), no obstante, la normativa argentina innova respecto de aquellas, pues "permite concluir que un país es adecuado si la protección deriva de los sistemas de autorregulación o del amparo que establezcan las cláusulas contractuales que prevean la protección de los datos personales" (Palazzi, *op. cit*., 2002, pág.166 y 167).

identificarse a las personas cuyos datos se transfieran; 3) Transferencias bancarias o bursátiles, respecto de las transacciones y conforme la legislación que les resulte aplicables; 4) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte; 5) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico y, 6) Cuando el titular de los datos hubiera consentido expresamente la cesión [148] (Art. 12 del Reglamento).

Cabe agregar finalmente, que a nivel de legislación sectorial, la Ley 25.392 que crea el Registro Nacional de Donantes de Células Progenitoras Hematopoyéticas, contempla una disposición relativa a la transmisión internacional de datos personales relativos a la salud, en la que establece que la autoridad de aplicación de la Ley está facultada para intercambiar información con todos aquellos países que tengan registros similares a los creados por esa ley, a efectos de dar una mejor, más amplia y rápida cobertura a aquellos pacientes que la requieran [149] . Pareciera que lo anterior guarda concordancia con la excepción establecida en el artículo 12 Nº 2 letra b de la Ley 25.326, en tanto se cumpla con el requisito de tratarse de un *"intercambio de datos de carácter médico, cuado así lo exija el tratamiento del afectado, o una investigación epidemiológica"* y se realice preservando la identidad de los titulares de los datos mediante procesos de disociación adecuados (Art.11 Nº 3 letra e).

9. Régimen de Responsabilidad

El marco regulatorio de protección a los datos personales argentino dispone de reglas de responsabilidad tanto en el ámbito del Derecho Civil, Administrativo y Penal. En la protección a nivel administrativo, se prevén por la Ley 25.326 sanciones cuya aplicación está entregada a la Dirección Nacional de Protección de Datos, el órgano de control previsto por la Ley 25.326. En materia civil, sólo se establece una regla especial de solidaridad, por lo que en definitiva la responsabilidad por daño se rige por las reglas generales. Finalmente, para las situaciones más graves, la Ley ha introducido en el Código Penal dos artículos que tipifican delitos por conductas que violan gravemente los derechos de los titulares de los datos.

Junto con las disposiciones específicas contenidas en la Ley 25.326, existen otras

[148] El artículo 12 del Reglamento agrega que el consentimiento para la transferencia internacional de datos no será necesario en caso de transferencia de datos desde un registro público que esté legalmente constituido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones legales y reglamentarias para la consulta.

[149] La legislación argentina reglamenta la utilización de células humanas para fines terapéuticos. En este sentido, la donación de las células progenitoras hematopoyéticas tiene como finalidad el realizar un transplante de médula ósea, la cual tiene por objeto a su vez, el tratamiento de un sinnúmero enfermedades, como por ejemplo: anemia aplástica, leucemia, mieloma múltiple, algunos tipos de cáncer, entre otros. Para mayor información se recomienda visitar [en línea] < http://www.myeloma.org/myeloma/article.jsp?articleId=39 > [consulta: 25 de Enero 2003].

normas sectoriales y de derecho común que a su vez establecen sanciones en los ámbitos arriba señalados, con lo cual se completa la protección de los bienes jurídicos que fundamentan la tutela a los datos personales, como lo son principalmente el derecho a la vida privada e intimidad.

9.1 Responsabilidad Administrativa

En este punto revisaremos las distintas disposiciones legales que establecen sanciones de carácter administrativas, partiendo por la ley de protección de datos personales argentina, que prescribe normas de aplicación general en la materia. En lo que respecta a las demás normas legales referidas a la protección de ciertos datos personales, debe estarse a la regulación sectorial y a la legislación común pertinente al efecto, la cual no trataremos. En el caso de Argentina, sólo nos referiremos a la Ley 21.526 y a la Ley 25.065, por ser aquellos estatutos que contemplan reglas específicas.

9.1.1) Ley 25.326

En materia de responsabilidad administrativa, el artículo 31 de esta Ley dispone que:

1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control (Dirección Nacional de Protección de Datos) podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000) a cien mil pesos ($ 100.000), clausura o cancelación del archivo, registro o banco de datos.

2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.

Según el artículo 31 del Reglamento, la cuantía de las sanciones se graduará en atención a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceros, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora. Es decir, se opta por un sistema de responsabilidad subjetivo o no estricto, de marcado carácter punitivo.

Por lo tanto, en los casos de violación a las normas sobre protección datos, se contemplan mecanismos para hacer valer la responsabilidad administrativa del responsable del archivo, registro o banco de datos personales.

9.1.2) Ley sobre Entidades Financieras (Ley Nº 21.526)

Esta normativa establece en el artículo 41 sanciones para quienes violen las disposiciones de la Ley, entre la cuales se incluyen las relativas al secreto bancario de los

artículos 39 y 40. Las sanciones establecidas son de carácter general y se aplican por el Banco Central de la República Argentina. Aquéllas que parecieran pertinentes de aplicación en caso de violación del secreto bancario serían las siguientes: 1) Llamado de atención; 2) Apercibimiento, y 3) Multas.

9.1.3) Ley sobre sistema de Tarjetas de Crédito, Compra y Débito (Ley Nº 25.065)

El artículo 48 de esta Ley establece sanciones genéricas para el evento de violación a sus disposiciones. Al efecto, señala que la autoridad de aplicación, según la gravedad de las faltas y la reincidencia en las mismas, o por irregularidades reiteradas, podrá aplicar a las emisoras las siguientes sanciones de apercibimiento: multas hasta veinte veces el importe de la operación en cuestión y cancelación de la autorización para operar. Según el artículo 50, la autoridad de aplicación de ley será: a) El Banco Central de la República Argentina en todas las cuestiones que versen sobre aspectos financieros y, b) La Secretaría de Industria, Comercio y Minería de la Nación, en todas aquellas cuestiones que se refieran a aspectos comerciales. Con todo, estimamos que las sanciones genéricas no cuadran con la naturaleza de la infracción al deber de no informar señalado en el artículo 53, pues éstas no se relacionan con el importe de una operación determinada.

9.2 Responsabilidad Civil

En el ámbito de la responsabilidad civil, la legislación argentina sólo establece reglas especiales para los eventos de cesión de datos (Art. 11 Nº 4). Por lo tanto, a falta de disposiciones especiales en materia civil estimamos que deben aplicarse las reglas generales de la responsabilidad por daño para el caso de no mediar una relación contractual entre el autor del daño y la víctima, o las reglas generales de la responsabilidad civil contractual, para el evento de existir una relación contractual previa. En este sentido, y dentro del ámbito de la responsabilidad civil extracontractual, será aplicable el artículo 1.109 del Código Civil argentino para todos los casos en que a consecuencia de una acción u omisión culpable por parte del responsable o usuario de archivos, registros, o bancos de datos, se cause daño al titular de los datos personales. Por otra parte, el artículo 1.112 hace aplicables las reglas de la responsabilidad civil extracontractual, a los hechos y las omisiones de los funcionarios públicos en el ejercicio de sus funciones, que cumplan de manera irregular las obligaciones legales que les están impuestas. Todo lo anterior, sin perjuicio de la responsabilidad del Estado. En cuanto a la responsabilidad civil contractual, sería aplicable el artículo 1.204 del Código Civil argentino [150] .

Las reglas especiales en materia responsabilidad civil, circunscritas a las cesiones o transferencias de datos personales, están contenidas en el artículo 11 Nº 4 de la Ley 25.326, el cual prescribe que: *"El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate".* Luego, el artículo 11 del Reglamento complementa esta norma señalando que el

cesionario *"podrá ser eximido total o parcialmente de responsabilidad si demuestra que no se le puede imputar el hecho que ha producido el daño"*. Estas disposiciones, plantean dificultades a la hora de interpretarlas. La norma legal pareciera establecer una especie de responsabilidad estricta u objetiva, en cambio, la norma reglamentaria se pronuncia directamente por un sistema de responsabilidad por culpa [151] . Tampoco queda claro si en definitiva lo que la ley establece es la contribución tanto del cedente como del cesionario a la deuda (la ley habla de solidaria y conjuntamente) o si la solidaridad sólo se establece para facilitar el ejercicio de la acción por daño [152] .

Finalmente, debemos señalar que en materia de responsabilidad civil la ley sectorial que regula algunos aspectos del Sistema de Tarjetas de Crédito, Compra y Débito (Ley Nº 25.065), dispone en el art. 53 que serán solidaria e ilimitadamente responsables por los daños y perjuicios ocasionados, las entidades emisoras de Tarjetas de Crédito, bancarias o crediticias que violen la prohibición de informar a las bases de datos de antecedentes financieros personales, sobre los titulares y beneficiarios de extensiones de

[150] Artículo 1.204.- "*En los contratos con prestaciones recíprocas se entiende implícita la facultad de resolver las obligaciones emergentes de ellos en caso de que uno de los contratantes no cumpliera su compromiso. Mas en los contratos en que se hubiese cumplido parte de las prestaciones, las que se hayan cumplido quedarán firmes y producirán, en cuanto a ellas, los efectos correspondientes". "No ejecutada la prestación, el acreedor podrá requerir al incumplidor el cumplimiento de su obligación en un plazo no inferior a quince días, salvo que los usos o un pacto expreso establecieran uno menor, con los daños y perjuicios derivados de la demora; transcurrido el plazo sin que la prestación haya sido cumplida, quedarán resueltas, sin más, las obligaciones emergentes del contrato con derecho para el acreedor al resarcimiento de los daños y perjuicios". "Las partes podrán pactar expresamente que la resolución se produzca en caso de que alguna obligación no sea cumplida con las modalidades convenidas; en este supuesto la resolución se producirá de pleno derecho y surtirá efectos desde que la parte interesada comunique a la incumplidora, en forma fehaciente, su voluntad de resolver". "La parte que haya cumplido podrá optar por exigir a la incumplidora la ejecución de sus obligaciones con daños y perjuicios. La resolución podrá pedirse aunque se hubiese demandado el cumplimiento del contrato; pero no podrá solicitarse el cumplimiento cuando se hubiese demandado por resolución".*

[151] El párrafo final del artículo 11 del Reglamento dispone textualmente que: *"(…) El cesionario a que se refiere el artículo 11, inciso 4, de la Ley Nº 25.326, podrá ser eximido total o parcialmente de responsabilidad si demuestra que no se le puede imputar el hecho que ha producido el daño".*

[152] Para complicar más el análisis anterior, Palazzi agrega que el apartado final del artículo 11 del Reglamento (inciso final) adolecería de inconstitucionalidad, pues el cesionario puede ser eximido total o parcialmente de responsabilidad si demuestra que no se le puede imputar el hecho que ha producido el daño, señalando que un decreto no puede modificar la responsabilidad solidaria establecida por la Ley (Palazzi, 2002, *op. cit*., pág. 166). Concordamos con este autor en su apreciación, y es a propósito del régimen de responsabilidad establecido por la Ley que estimamos sería muy interesante explorar la factibilidad de modificarlo especialmente en el caso de la cesión masiva de datos. Pareciera que regular esta materia en base a un sistema de responsabilidad por culpa, entraba en demasía la operatividad de la misma, pues además de la dificultad probatoria de la falta de diligencia (culpa), quien está en la mejor posición para prever los riesgos es el propio cedente y no los potenciales afectados. Concretamente creemos que en atención a la actividad de cesión masiva de datos personales entraña un innegable riesgo, por lo que sería preferible que el régimen de responsabilidad aplicable fuese el de responsabilidad estricta u objetiva. En este mismo sentido a propósito de la ley chilena Nº 19.628, se ha pronunciado González Hoch, Francisco: *"Modelos comparados de protección de la información digital y la ley chilena de datos de carácter personal, en tratamiento de datos personales y protección de la vida privada"*, Universidad de los Andes, Facultad de Derecho, Cuadernos de Extensión Jurídica Nº 5, 2001, pág. 178.

Tarjetas de Crédito u opciones cuando el titular no haya cancelado sus obligaciones, se encuentre en mora o en etapa de refinanciación.

9.3 Responsabilidad Penal

La Ley 25.326 ha introducido dos artículos en el Código Penal argentino que han pasado a engrosar los delitos de la Parte Especial de dicho cuerpo legal. El primer grupo de ellos se ubica dentro del Libro Segundo, Título II, bajo el epígrafe "Delitos contra el honor" en el artículo 117 bis, el cual prescribe lo siguiente:

"*1º Será reprimido con la pena de prisión de un mes a dos años el que insertare o hiciere insertar a sabiendas datos falsos en un archivo de datos personales".*

"2º La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales".

"3º La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona".

"4º Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena".

Desde ya, cabe hacer presente que determinar el bien jurídico protegido en estos tipos penales resulta una labor algo compleja; pareciera ser que su inclusión dentro del epígrafe "De los Delitos Contra el Honor" tiende a confundir y no deja de llamar la atención, pues podría pensarse que el legislador ha renunciado a basar la tutela a los derechos de las personas en el derecho a la autodeterminación informativa, conformándose con remitir parte de la justificación de la protección a los datos personales al derecho al honor, lo cual no nos parece adecuado, pues no es congruente desde un punto de vista político criminal con la tutela que en sede no penal se le asigna a la protección de datos. Con todo, la labor interpretativa en esta materia, es una tarea que les corresponde analizar a los estudiosos del derecho penal.

El segundo grupo de delitos contemplados por la Ley 25.326, ha sido incorporado al Código Penal en el Libro Segundo, Capítulo Tercero, bajo el epígrafe "Violación de Secretos". La disposición correspondiente es la siguiente:

Artículo 157 bis.- *"Será reprimido con la pena de prisión de un mes a dos años el que: 1º. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2º. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.*

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años".

En relación con lo anterior, debe tenerse presente además lo dispuesto por el artículo 10 de la Ley, el cual faculta a los jueces a relevar de la obligación de secreto profesional que pesa sobre algunas personas, por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

Llama la atención de lo preceptuado por el legislador argentino, que al menos las conductas descritas en el numeral 1º del artículo 157 bis, no guardan relación con la violación de un deber de secreto propiamente tal, sino que corresponde más bien a un acceso no autorizado a un banco de datos personales. En este caso, se estaría en presencia de un delito de peligro abstracto, pues no se requeriría efectivamente que se vulnere o viole el derecho a la intimidad de las personas -suponiendo que éste sea el bien jurídico protegido por la norma-, sino que basta con poner en peligro la intimidad, que en este caso tampoco resulta fácil determinarlo. Nuevamente debemos endosarle la tarea a los estudiosos de las ciencias penales la labor de esclarecer todas las cuestiones que suscita la interpretación de estos tipos penales.

Además de los delitos especialmente establecidos por la ley de protección de datos personales, el Código Penal argentino contempla los clásicos tipos vinculados a la protección de la intimidad y la vida privada como son los siguientes:

a) Violación de domicilio:

Artículo 150.-"*Será reprimido con prisión de seis meses a dos años, si no resultare otro delito más severamente penado, el que entrare en morada o casa de negocio ajena, en sus dependencias o en el recinto habitado por otro, contra la voluntad expresa o presunta de quien tenga derecho de excluirlo".*

Artículo 151.-*"Se impondrá la misma pena e inhabilitación especial de seis meses a dos años, al funcionario público o agente de la autoridad que allanare un domicilio sin las formalidades prescritas por la ley o fuera de los casos que ella determina".*

Artículo 152.-*"Las disposiciones de los artículos anteriores no se aplicarán al que entrare en lo sitios expresados, para evitar un mal grave a sí mismo, a los moradores o un tercero, ni al que lo hiciere para cumplir un deber de humanidad o prestar auxilio a la justicia".*

b) Violación de correspondencia:

Artículo 153.-*"Será reprimido con prisión de quince días a seis meses, el que abriere indebidamente una carta, un pliego cerrado o un despacho telegráfico, telefónico o de otra naturaleza que no le esté dirigido; o se apoderare indebidamente de una carta, de un pliego, de un despacho o de otro papel privado, aunque no esté cerrado; o suprimiere o desviare de su destino una correspondencia que no le esté dirigida".*

"Se le aplicará prisión de un mes a un año, si el culpable comunicare a otro o publicare el contenido de la carta, escrito o despacho".

Artículo 154.-*"Será reprimido con prisión de uno a cuatro años, el empleado de correos o telégrafos que, abusando de su empleo, se apoderare de una carta, de un pliego, de un telegrama o de otra pieza de correspondencia, se impusiere de su contenido, la entregare o comunicare a otro que no sea el destinatario, la suprimiere, la ocultare o cambiare su texto".*

Artículo 155.-*"El que, hallándose en posesión de una correspondencia no destinada a la publicidad, la hiciere publicar indebidamente, aunque haya sido dirigida a él, será*

reprimido con multa de pesos mil quinientos a pesos noventa mil, si el hecho causare o pudiere causar perjuicios a terceros".

c) Violación de secretos:

Artículo 156.-"*Será reprimido con multa de pesos mil quinientos a pesos noventa mil e inhabilitación especial, en su caso, por seis meses a tres años, el que teniendo noticia, por razón de su estado, oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa".*

Artículo 157.-*"Será reprimido con prisión de un mes a dos años e inhabilitación especial por uno a cuatro años el funcionario público que revelare hechos, actuaciones o documentos que por la ley deben quedar secretos"* [153]

Finalmente, debemos aclarar que dada la tipificación específica de conductas que atentan contra los bienes jurídicos protegidos por la ley de protección de datos personales ya analizados, estimamos que los clásicos delitos recién señalados quedarían sin aplicación en virtud del principio en materia penal de la especialidad.

10. Códigos de Conducta

La normativa trasandina establece en el artículo 30 de la Ley 25.326, la posibilidad de la elaboración de códigos de conducta de práctica profesional por parte de las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada, que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en esa ley. Estos códigos deberán ser inscritos en el registro que al efecto lleve la Dirección Nacional de Protección de Datos, la cual puede negar inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia (Art.30 inciso 2º).

Por su parte, el artículo 30 del Reglamento también faculta a las asociaciones de profesionales y demás organizaciones representantes de otras categorías de responsables o usuarios de archivos, registros, bases o bancos de datos públicos o privados (que hayan elaborado proyectos de códigos éticos, o que tengan la intención de modificar o prorrogar códigos existentes), para que puedan someter códigos de conducta a consideración de la Dirección, la cual tiene dos opciones; aprobar el ordenamiento, o sugerir las correcciones q ue se estimen necesarias para su aprobación [154] .

11. Conclusiones

La protección de los datos personales en el ordenamiento jurídico argentino aparece garantizada tanto por vía constitucional, como legal. La reforma a la Constitución del año 1994 que consagra la denominada acción de hábeas data, ha sido fundamental para el

[153] Cabe hacer presente, que la disposición anterior resulta aplicable a la violación del secreto tributario o fiscal en virtud de la remisión expresa hecha por el artículo 101 de la Ley Nº 11.683 sobre procedimientos fiscales al texto del artículo 157 del Código Penal.

desarrollo de una consistente legislación federal de protección de datos personales, plasmada en la Ley 25.326, la cual tiene como fuente directa a las legislaciones extranjeras de protección de datos, en especial, la española de 1992 (LORTAD), hoy derogada por la Ley Orgánica 15/99 de Protección de Datos Personales. En general, puede decirse que la legislación argentina se adecua a los estándares internacionales de protección de datos personales, en particular a la Directiva 95/46 CE, pues no sólo se establecen reglas sustantivas y procedimentales para la protección de los titulares de los datos personales, sino que se contempla la creación de un organismo de control que vele por el respeto y aplicación de la Ley, así como también que oriente a los ciudadanos para el ejercicio de sus derechos. Por otra parte, estimula la autorregulación sectorial a través de los códigos de conducta. Finalmente, destaca el amplio régimen de responsabilidad establecido, el que va desde las sanciones administrativas hasta las sanciones penales.

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN BOLIVIA

1. Generalidades

En el ordenamiento jurídico boliviano no se contempla un estatuto específico que se ocupe de la protección a los datos personales. Sólo existen algunas normas dispersas en leyes sectoriales que protegen algunos ámbitos del derecho a la intimidad y a la vida privada. Este vacío legal podría ser suplido en parte por la Constitución, la cual reconoce garantías que protegen la vida privada e intimidad de las personas. Así, el reconocimiento de esas garantías constitucionales y el establecimiento de una acción de amparo que las tutele, permitiría fundamentar una protección a los datos personales a través de ésa vía.

2 Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional

El sistema jurídico boliviano, a nivel constitucional, no establece una protección directa respecto de los datos personales, por lo que ésta podría fundamentarse en garantías que

154 El artículo 30º del Reglamento dispone que: *"la Dirección Nacional de Protección de Datos Personales alentará la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por la Ley Nº 25.326 y esta reglamentación. Las asociaciones de profesionales y las demás organizaciones representantes de otras categorías de responsables o usuarios de archivos, registros, bases o bancos de datos públicos o privados, que hayan elaborado proyectos de códigos éticos, o que tengan la intención de modificar o prorrogar códigos nacionales existentes, pueden someterlos a consideración de la Dirección Nacional de Protección de Datos Personales, la cual aprobará el ordenamiento o sugerirá las correcciones que se estimen necesarias para su aprobación".*

puedan cubrir los ámbitos más próximos que en general se han aducido para basar una tutela a los datos personales. En este sentido, el derecho a la intimidad pareciera ser lo más cercano, en el entendido que el derecho a la autodeterminación informativa se construye a partir de aquélla [155] . Esta falta de protección constitucional directa ha sido constatada por parte de la doctrina boliviana, la cual reconociendo esa carencia, señala sin embargo, que ella puede ser suplida por la acción de amparo, en particular para abrir un espacio a la acción de hábeas data no contemplada tampoco por el legislador boliviano [156] .

A continuación se señalarán las normas constitucionales que a nuestro juicio, podrían fundamentar una protección a los datos personales en el ordenamiento jurídico boliviano.

El artículo 6º II [157] dispone que: *"La dignidad y la libertad de las personas son inviolables. Respetarlas y protegerlas es deber primordial del Estado"*. A partir del reconocimiento de la dignidad humana, valor supremo constitucional, sería posible fundamentar una protección a los datos personales, dado el carácter de parámetro valorativo que posee aquélla para interpretar los derechos fundamentales, lo que tendrá consecuencias en la tutela requerida a través de la acción de amparo [158] . A mayor abundamiento y, recurriendo a la jurisprudencia comparada, se ha señalado por el Tribunal Constitucional español que el derecho a la intimidad personal aparece estrictamente vinculado a la propia personalidad, derivado sin duda de la "dignidad humana" reconocida en el artículo 10.1 de la Constitución española de 1978 [159] .

Desde el ámbito de la libertad, también podría fundamentarse el derecho a la intimidad, y a partir de ésta basar una protección a los datos personales considerando a la libertad como componente del derecho a la intimidad, como garantía institucional de la libertad vital del individuo [160] . En palabras de Rebolledo, "podría decirse que la elaboración de la libertad comienza normalmente por los ámbitos de la vida privada", por lo que el derecho a la intimidad se configura como expresión de la libertad, como una manifestación de la misma [161] .

155 Lo anterior es sostenido por el autor español Murillo de la Cueva, Pablo Lucas, *op. cit*., pág. 45.

156 Esta es la opinión de Miguel Harb, Benjamín: *"Acción de amparo relacionada con la protección de datos personales en el orden jurídico Boliviano".* En *Revista Ius Et Praxis,* Universidad de Talca, año 3 Nº 1, Talca, 1997, pág. 163.

157 [En línea] < http://www.georgetown.edu/pdba/Constitutions/Bolivia/consboliv1615.html > [consulta: 17 de Octubre 2002].

158 Lo anterior como corolario de lo planteado por Benda y Vogel en la doctrina alemana, citados por Zúñiga Francisco, *op. cit*., págs. 293 y 294.

159 Citado por Ruiz Miguel, *op. cit*., pág. 80.

160 Sentencia del Tribunal Constitucional español 89/87, fundamento jurídico 2º. Citado por Rebolledo Delgado, Lucrecio, *op. cit*., pág. 78.

161 *Ídem*, págs. 78 y 81.

Por otra parte, el artículo 19 constitucional reconoce la acción de amparo la cual procede *"contra los actos ilegales o las omisiones indebidas de los funcionarios o particulares que restrinjan, supriman o amenacen restringir o suprimir los derechos y garantías de la persona reconocidos por esta Constitución y las leyes"*. Esta acción se encuentra regulada a su vez por la Ley del Tribunal Constitucional (Ley Nº 1.836-1998) [162] , la cual establece en su Título Cuarto, Capítulo IX, el recurso de Amparo Constitucional, señalando los requisitos de procedencia y trámites de éste en los artículos 94 y siguientes. Como ya se anotó, esta acción ha sido señalada por alguna doctrina como pertinente para resguardar la protección a los datos personales en tanto no exista normativa especial que se ocupe de ello [163] . En esta materia, el artículo 120 de la Carta Fundamental boliviana, le otorga competencia al Tribunal Constitucional para conocer la revisión de los recursos de amparo constitucional, y el artículo 127 de la misma, faculta al Defensor del Pueblo para interponer entre otros, el recurso de amparo sin necesidad de mandato.

Siguiendo el análisis de preceptos constitucionales, el artículo 20 reconoce la inviolabilidad de la correspondencia y de los papeles privados en los siguientes términos: *"Son inviolables la correspondencia y los papeles privados, los cuales no podrán ser incautados sino en los casos determinados por las leyes y en virtud de orden escrita y motivada de autoridad competente. No producen efecto legal los documentos privados que fueren violados o sustraídos".* El inciso 2º de esta disposición señala a su vez que: *"Ni la autoridad pública, ni persona u organismo alguno podrán interceptar conversaciones y comunicaciones privadas mediante instalación que los controle o centralice*".

El artículo 21 por su parte garantiza la inviolabilidad del domicilio, señalando al efecto: *"Toda casa es un asilo inviolable, de noche no se podrá entrar en ella sin consentimiento del que la habita, y de día sólo se franqueará la entrada a requisición escrita y motivada de autoridad competente, salvo el caso de delito in fraganti"*.

De las disposiciones anteriores, se desprende que no existe una remisión directa al derecho a la intimidad por parte del Constituyente boliviano, sino más bien al derecho a la vida privada a pesar de contener aspectos comprendidos en el derecho a la intimidad [164] . Con todo, y no obstante la falta de reglas explícitas, el Estado boliviano es parte en tratados de Derechos Humanos, como la Convención Americana o Pacto de San José de Costa Rica [165] , con lo cual es posible asir, si no el derecho a la autodeterminación informativa, el derecho a la vida privada e intimidad y el principio-valor dignidad, en virtud

[162] [En línea] < http://www.cajpe.org.pe/RIJ/bases/ddhh/bo_13.htm > [consulta: 6 de Febrero 2003].

[163] En este sentido Miguel Harb, Benjamín, ver *supra* punto Nº 2.1.

[164] El determinar el contenido del derecho a la intimidad no es cuestión pacífica en la doctrina comparada. Para algunos, la inviolabilidad del domicilio sería una manifestación de la seguridad individual. Otros señalan que existiría una vinculación con el derecho a la intimidad. Finalmente, la postura intermedia señala que la inviolabilidad del domicilio se fundamenta tanto en la seguridad personal como en la intimidad. Lo anterior, en Ruiz Miguel, Carlos, *op. cit*., págs. 85-87, quien se inclina por la segunda doctrina, al igual que el Tribunal Constitucional español.

del artículo 11 de dicha Convención.

Finalmente, debemos mencionar que en la actualidad existe un Proyecto de Ley de Necesidad de Reforma a la Constitución Política del Estado que incluye la figura del hábeas data, el cual ha sido aprobado por la Cámara de Diputados el año 2002 [166] . Este Proyecto contempla en su artículo 23 lo siguiente:

"I. Toda persona que creyere estar indebidamente o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos de datos públicos o privados que afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución, podrá imponer interponer el recurso de Hábeas Data ante la Corte Superior de Distrito o ante cualquier Juez de Partido a elección suya".

"II. Si el tribunal o el juez competente declara procedente el recurso, ordenará la revelación, eliminación o rectificación de los datos personales cuyo registro fue impugnado".

"III. La decisión que se pronuncie se elevará en revisión, de oficio, ante el Tribunal Constitucional, en el plazo de 24 horas, sin que por ello se suspenda la ejecución del fallo".

"IV. El recurso de Habeas Data no procederá para levantar el secreto en materia de prensa".

En relación al Proyecto de Ley de necesidad de reforma a la Constitución, cabe comentar que el numeral IV del artículo 23 fue objeto de polémica nacional, pues en un principio, la redacción de dicho artículo no consagraba la improcedencia del hábeas data respecto de los datos provenientes de las fuentes de información periodística, lo que inquietó al gremio respectivo. Para éstos, constituía una amenaza al ejercicio libre de la profesión periodística el que no se excluyera a sus archivos o bases de datos del objeto del hábeas data. Luego de arduas discusiones entre parlamentarios y representantes de los medios de prensa bolivianos se zanjó la disputa, quedando el artículo con la redacción ya señalada [167] .

En suma, en el ordenamiento jurídico constitucional boliviano, no es posible encontrar normas que directamente digan relación con la protección de los datos personales, por lo que para fundamentar una protección de éstos, debe realizarse un ejercicio interpretativo no exento de dificultades, en donde es menester tener presente lo señalado en los instrumentos internacionales sobre Derechos Humanos dado que

[165] Esta Convención fue ratificada después de 24 años por la Ley 1.430 el 27 de Julio de 1993, la que además reconoce competencia a la Corte Interamericana de DD.HH. [En línea] < http://www.oas.org/juridico/spanish/firmas/b-32.html > [consulta: 20 de Marzo 2003].

[166] [En línea] < http://www.portal-pfc.org/legislacion/2002/038.html#1 > [consulta: 6 de Febrero 2003].

[167] Para conocer el tenor de la diputa señalada, puede consultarse [en línea] < http://www.portal-pfc.org/legislacion/2002/038.html > [consulta: 6 de Febrero 2003].

representan el estándar mínimo normativo para todos aquellos Estados que han optado por hacerlos parte de su legislación. Por lo tanto, y mientras no se modifique la Constitución boliviana, la tutela a nivel constitucional está entregada al Tribunal Constitucional, el cual resolverá en definitiva las acciones de amparo tendientes a resguardar los derechos de los titulares de los datos personales.

2.2 Protección Legal de los Datos Personales

En lo relativo a la protección legal de los datos personales, cabe señalar que Bolivia no dispone de ley especial que se ocupe del tema. Tampoco tenemos conocimiento de algún Proyecto de Ley que trate la materia en estudio. No obstante esta carencia, sí es posible constatar algunas regulaciones sectoriales y otras de carácter general que tocan los ámbitos del resguardo de la vida privada e intimidad. Ejemplos de lo anterior, podemos constatarlo en diversas disposiciones legales relacionadas con los bienes jurídicos ya mencionados, las que pasamos a analizar.

2.2.1) Código Civil [168]

El artículo 18 de la ley civil común boliviana dispone que: "*Nadie puede perturbar ni divulgar la vida íntima de una persona. Se tendrá en cuenta la condición de ella. Se salva los casos previstos por la ley".* A continuación, el artículo 19 prescribe lo siguiente: *"I. Las comunicaciones, la correspondencia epistolar y otros papeles privados son inviolables y no pueden ser ocupados sino en los casos previstos por las leyes y con orden escrita de la autoridad competente".*

Más adelante, el artículo 21 del mismo cuerpo legal señala que: "los derechos de la personalidad son inherentes al ser humano y se hallan fuera del comercio. Cualquier limitación a su libre ejercicio es nula cuando afecta al orden público o a las buenas costumbres".

De las disposiciones anteriores podemos deducir que, a nivel legal, tanto la intimidad como la vida privada tienen el carácter de derechos de la personalidad [169], sancionándose con la nulidad cualquier limitación al libre ejercicio de esos derechos cuando se afecta el orden público o las buenas costumbres. En esta sede, no vemos inconvenientes para poder fundamentar un deber de protección general respecto de ciertos datos personales cuyo tratamiento y difusión pueda ser considerado atentatorio contra las buenas costumbres o el orden público. Este sería, a lo menos el caso de los

[168] El Código Civil boliviano puede ser consultado [en línea] < http://www.cajpe.org.pe/rij/bases/legisla/bolivia/ley11.HTM > [consulta: 3 de Febrero 2003].

[169] El Código Civil boliviano no define qué son los derechos de la personalidad, no obstante, ello, puede señalarse que el propio texto legal, en el Libro I, Capítulo III, contiene un epígrafe homónimo dentro del cual se incluye una serie de derechos como la capacidad, el derecho a la integridad física, la libertad personal, el derecho al nombre, protección del nombre, derecho a la imagen, derecho al honor, e inviolabilidad de las comunicaciones privadas. De lo anterior, podemos deducir que todos los derechos mencionados se consideran de la personalidad por el legislador boliviano, es decir, aquellos derechos inherentes a la condición de persona que pertenecen por el solo hecho de ser tal, a cada ser humano.

datos sensibles.

Finalmente, el Código Civil boliviano dispone en su artículo 23 que: "*Los derechos de la personalidad son inviolables y cualquier hecho contra ellos confiere al damnificado la facultad de demandar el cese de ese hecho, aparte del resarcimiento por el daño material o moral*". Lo anterior, reafirma la importancia que para el legislador boliviano tienen los derechos de la personalidad, y constituye sin dudas una herramienta directa para la protección de las personas afectadas por el tratamiento de sus datos personales, las cuales pueden solicitar al juez que ordene el cese de la acción u omisión atentatoria contra los derechos de la personalidad, a más de dejar a salvo las acciones correspondientes para la reparación del daño patrimonial y la compensación de los daños morales. Por otro lado, no vemos obstáculo legal para que los jueces bolivianos decreten medidas cautelares precautorias que puedan prevenir, aminorar o hacer cesar los daños que pudiesen provenir de un tratamiento inadecuado de los datos personales, como por ejemplo, que el tribunal ordene al responsable de la base de datos, archivo o registro, que se de noticia o se asiente en el registro, del hecho de existir *litis pendencia* en la materia o, que directamente se ordene la supresión o rectificación temporal del dato en discusión, cumpliéndose los requisitos generales del *fumus bonis iuris* y *periculum in mora.*

2.2.2) Código del Niño, Niña y Adolescente (Ley Nº 2.026-1999) [170]

Este estatuto jurídico contempla en su artículo 10 el deber de reserva y resguardo de la identidad de los niños o adolescentes que se vean involucrados en todo tipo de procesos, sean éstos administrativos o judiciales. Este deber, pesa sobre las respectivas autoridades. Asimismo, se contempla en el inciso 2º del mencionado artículo una restricción al derecho a la información que afecta a los medios de comunicación de la siguiente forma: "*Los medios de comunicación cuando publiquen o transmitan noticias que involucren a niños, niñas o adolescentes, no pueden identificarlos nominal ni gráficamente, ni brindar información que permita su identificación, salvo determinación fundamentada del Juez de la Niñez y Adolescencia, velando en todo caso, por el interés superior de los mismos".* De lo anterior resulta claro que la finalidad de la norma es la protección del menor en cuanto a su intimidad, lo que concuerda con lo preceptuado por el artículo 16 de la Convención Internacional sobre los Derechos del Niño de 1989, en vigencia desde el mes de Mayo de 1984 para Bolivia. Cabe hacer presente que la restricción anterior sólo es aplicable a los medios de comunicación social y no a otras entidades.

Finalmente, el artículo 229 de este estatuto legal establece la prohibición de registrar en los archivos policiales los datos personales de los adolescentes que incurran en una infracción, estableciéndose al efecto que: *"Los organismos policiales no podrán registrar en sus archivos datos personales del adolescente que incurra en una infracción. El registro judicial de infracciones será reservado y sólo podrá certificar antecedentes mediante auto motivado".* Este precepto también concuerda con la Convención Internacional ya señalada.

[170] **[En línea] < http://www.cajpe.org.pe/RIJ/bases/legisla/bolivia/2026.HTM > [consulta: 3 de Febrero 2003].**

En suma, el Código del Niño establece normas que resguardan la identidad y otros datos personales de los menores, circunscrito principalmente al ámbito infraccional, es decir, en los casos que niños o menores se vean involucrados en situaciones que lleguen a conocimiento de la justicia a fin de determinar responsabilidades y tomar eventuales medidas de protección o rehabilitación.

2.2.3) Ley de Bancos e Instituciones Financieras (Ley Nº 1.488-1993) [171]

El artículo 86 de esta Ley establece la regla general para las operaciones bancarias, cual es, el secreto de ellas. Al efecto se dispone: *"Las operaciones bancarias en general estarán sujetas al secreto bancario. No podrán proporcionarse antecedentes relativos a dichos operaciones sino a su titular, o a la persona que lo represente legalmente"*. De lo dicho, se desprende que la Ley no distingue entre clases de operaciones bancarias, por lo que entendemos se aplicaría respecto de toda clase de ellas, sean éstas activas o pasivas [172] . Las excepciones a la regla anterior las señala el artículo 87, el cual prescribe que el secreto bancario será levantado únicamente:

"1. Mediante orden judicial motivada, expedida por un juez competente dentro de un proceso formal y de manera expresa, por intermedio de la Superintendencia.

2. Para emitir los informes ordenados por los jueces a la Superintendencia en proceso judicial y en cumplimiento de las funciones que le asigna la Ley.

3. Para emitir los informes solicitados por la administración tributaria sobre un responsable determinado, que se encuentre en curso de una verificación impositiva y siempre que el mismo haya sido requerido formal y previamente. Dichos informes serán tramitados por intermedio de la Superintendencia.

4. Dentro de las informaciones que intercambian las entidades bancarias y financieras entre sí, de acuerdo a reciprocidad y prácticas bancarias.

5. Para emitir los informes de carácter general que sean requeridos por el Banco Central de Bolivia".

Del examen anterior llaman la atención los números 3 y 4. El primero, debido a que es el propio Estado quien está facultado para solicitar a los bancos la información de las operaciones bancarias sin intervención de un juez, y el segundo, en razón de dejar a la

[171] El texto de la ley puede consultarse [en línea] < http://www.solobolivia.com/politica/leyes/ley1488.shtml > [consulta: 2 de Marzo 2003].

[172] Se agrega en el artículos 88, que están obligados a guardar secreto de los asuntos y operaciones del sistema financiero y sus clientes, que lleguen a su conocimiento en el ejercicio de sus funciones, los directores, síndicos, gerentes y suplentes de: 1). Entidades de intermediación financiera; 2) Banco Central de Bolivia; 3) Empresas de auditoria externa; 4) Empresas valuadoras de riesgo; 5) Empresas vinculadas de entidades financieras. Por otra parte, el artículo 89 agrega*: "el Superintendente y los empleados de la Superintendencia, aún después de cesar en sus funciones, están prohibidos de dar a conocer información relacionada con los documentos, informes u operaciones de las instituciones financieras o de personas relacionadas con el sistema financiero. El funcionario o empleado que infrinja esta prohibición, será destituido de su cargo, sin perjuicio de las responsabilidades civil o penal que correspondan".*

sola práctica bancaria la determinación de cuál información, cuándo y de qué forma se levantará el secreto bancario, lo que nos parece vulneraría, al menos, un ámbito específico de la vida privada pues no se justificaría entregar la facultad de decisión en la materia a quien precisamente se le impone el deber de secreto en base a la 'reciprocidad' y a las 'practicas bancarias'. Por lo demás, estimamos que de ninguna práctica sectorial *per se* podría predicarse su licitud sin más. Más grave aún, se entrega una poderosa herramienta a uno de los sectores económicos más importantes la sociedad como son los bancos.

2.2.4) Ley del Estatuto del Funcionario Público (Ley Nº 2.027-1999) [173]

Esta normativa en su artículo 9º prescribe que: *"Los servidores públicos están sujetos a las siguientes prohibiciones: "(…) h) Disponer o utilizar información previamente establecida como confidencial y reservada en fines distintos a los de su función administrativa"*. Por lo tanto, para que se esté en presencia de una información con tal carácter, debe previamente establecerse su confidencialidad y reserva por la autoridad respectiva. Esta disposición, pasaría a convertirse en la legislación común de carácter administrativa aplicable a todo funcionario público.

2.2.5) Ley de la Abogacía (DL Nº 16.793-1979) [174]

Este estatuto jurídico dispone en el artículo 10 que es inviolable el consultorio jurídico de los abogados, así como también *"los documentos y objetos que le hayan confiado sus clientes para asumir su defensa, salvo previa y expresa resolución motivada de juez competente"*. En este caso, la ley se ocupa de garantizar instrumentalmente el secreto profesional del abogado, cuestión de máxima importancia para el ejercicio libre de la profesión. Cabe hacer presente que en la práctica, los estudios jurídicos y/o abogados realizan generalmente actividades de registro de datos personales, poseen archivos, ordenan y sistematizan la gran cantidad información que pueden llegar a utilizar para la defensa de los intereses de sus clientes. Lo anterior se confirma con lo dispuesto en el artículo 20 de esta misma ley, el cual dispone que: *"El Abogado exigirá de su cliente una relación escrita de los hechos que motivan la defensa o patrocinio, debidamente suscrito. Si el cliente fuere analfabeto, dos testigos idóneos, que sepan leer y escribir, harán la relación del caso, firmando, el cliente analfabeto imprimirá sus digitales. La omisión de este deber, se considerará presunción de derecho, en caso de acusarse al abogado por defensa culpable o demandarse el resarcimiento de daños y perjuicios".*

Por lo tanto, el deber de información escrita que pesa sobre el cliente y la custodia de la misma, no solo beneficia al cliente sino que directamente al propio abogado. Demás está decir que mucha de esta información será de carácter sensible, por lo que puede afirmarse que los abogados poseen bases de datos de carácter muy especial; para su uso exclusivo, dentro de los fines para los cuales se les ha entregado esa información y,

[173] **[En línea] < http://www.solobolivia.com/politica/leyes/ley2027.shtm > [consulta: 6 de Febrero 2003].**

[174] **[En línea] < http://www.ferjus.bizland.com/abogado.htm > [consulta: 6 de Febrero 2003].**

con estricto deber de reserva. En razón de lo anterior, es obvio que las normas de secreto profesional ceden en beneficio directo del cliente, pues está protegiendo tanto la vida privada como la intimidad de aquél. Creemos que en todas las situaciones de manejo de información tan delicada, se hace necesario establecer estrictos mecanismos de custodia y resguardo por parte del estudio de abogados o del abogado particular que posee esta clase de información, pues en caso de pérdida o mal uso de ésta, podría perjudicar al propio abogado.

2.2.6) Código Tributario (Ley Nº 1.340-1992) [175]

El artículo 132 de este Código prescribe que: *"Las informaciones que la Administración obtenga de los contribuyentes responsables y terceros por cualquier medio, tendrán carácter reservado. Sólo podrán ser comunicadas a la autoridad jurisdiccional cuando mediare orden de ésta".* Las sanciones para el caso de que se viole ese deber por los funcionarios públicos se señalan en los artículos 124 a 126 [176] .

3. Bienes Jurídicos Protegidos por la Legislación de Datos Personales

Dada la inexistencia de legislación especial que se ocupe en particular de la protección a los datos personales en Bolivia, no es posible señalar cuáles serían esos bienes jurídicos tutelados. Sin embargo, estimamos que en base a la Constitución sería factible desarrollar una protección a los datos personales, fundada en el derecho a la intimidad, pues está presente en sus diversas facetas que determinan su contenido. Lo anterior, en razón a que puede sostenerse que el derecho a la intimidad sería un derecho complejo o derecho de derechos, uno en su concepción y múltiple en cuanto a sus contenidos [177] .

4. Principios Informativos de la Legislación de Protección de Datos Personales

[175] Establecido por la Ley. Nº 1.340 de 1992. [En línea] < http://www.ferjus.bizland.com/ct.htm > [consulta: 6 de Febrero 2003].

[176] Los artículos respectivos del Código Tributario señalan: Artículo 124.- *"El funcionario o empleado de la Administración tributaria que divulgue dolosamente hechos o documentos que conozca en razón de su cargo y que por naturaleza o por disposición de la ley fueren reservados, será sancionado atendiendo a la gravedad de su falta con suspensión de su cargo por un tiempo de tres meses a un año o con la exoneración del mismo".* Artículo 125.- *"Si las infracciones establecidas en los artículos anteriores fueran culposas, la multa o el tiempo de suspensión serán reducidos a la mitad." y,* Artículo 126.- *"Las sanciones previstas en esta sección no se aplicarán si los hechos constituyen un delito o una contravención más grave, sancionados por otras disposiciones legales. En este caso, los actuados pertinentes serán enviados a la justicia ordinaria para el respectivo juzgamiento y sanción de los infractores".*

[177] Esta es la opinión de Ruiz Miguel, Carlos, *op.cit*., pág.76.

En lo que respecta a principios informativos de la legislación de protección de datos, no es posible constatarlos debido a la falta de regulación legal especial en la materia. Queda entonces la tarea previa entregada al legislador boliviano.

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

En este punto no nos detendremos, dada la ausencia de legislación especial de protección de datos personales en el ordenamiento jurídico boliviano.

6. Modelos de Tutela

Si bien ha podido comprobarse la inexistencia de una ley de protección de datos personales en el ordenamiento jurídico boliviano, estimamos que a pesar de ello es posible canalizar una tutela a los derechos de las personas a través de diversas vías; la constitucional, a falta de otro remedio o recurso para la protección inmediata de los derechos o garantías (Art. 94, Ley del Tribunal Constitucional), la vía administrativa y, la civil basada en la protección a los derechos de la personalidad.

6.1 La Acción de Amparo

La vía del amparo está consagrada constitucionalmente en el artículo 19, el cual señala que: *"(…) I.- Fuera del recurso de hábeas corpus a que se refiere el artículo anterior, se establece el recurso de amparo contra los actos ilegales o las omisiones indebidas de los funcionarios o particulares que restrinjan, supriman o amenacen restringir o suprimir los derechos y garantías de la persona reconocidos por esta Constitución y las leyes".*

6.1.1) Procedencia de la Acción

La procedencia de la acción de amparo está señalada en el artículo 94 de la Ley del Tribunal Constitucional, el cual dispone que: *"Procederá el recurso de Amparo Constitucional contra toda resolución, acto u omisión indebida de autoridad o funcionario, siempre que no hubiere otro medio o recurso para la protección inmediata de los derechos y garantías; así como contra todo acto u omisión indebida de persona o grupos de personas particulares que restrinjan, supriman o amenacen restringir o suprimir los derechos o garantías reconocidos por la Constitución Política del Estado y las leyes".*

6.1.2) Legitimación Activa

En cuanto el sujeto activo de la acción, se señala por la Constitución en el artículo 19 que: *"II. El recurso de amparo se interpondrá por la persona que se creyere agraviada o por otra en su nombre con poder suficiente -salvo lo dispuesto en el artículo 129 de esta Constitución-, ante las Cortes Superiores en las capitales de Departamento o ante los jueces de Partido en las provincias, tramitándoselo en forma sumarísima. El Ministerio Público podrá también interponer de oficio este recurso cuando no lo hiciere o no pudiere*

hacerlo la persona afectada". La excepción del artículo 129 significa que no será necesario cumplir con el requisito general del poder suficiente en el caso que sea el Defensor del Pueblo quien entable la acción, pues está facultado para interponer esta acción, sin necesidad de mandato.

6.1.3) Legitimación Pasiva

El sujeto pasivo de la acción de amparo es toda autoridad, funcionario público, persona o grupo de personas particulares que restrinjan, supriman o amenacen restringir o suprimir los derechos o garantías reconocidos por la Constitución y las leyes (Art. 94, Ley del Tribunal Constitucional).

6.1.4) Competencia

Son competentes para conocer de la acción de amparo: 1) Las Cortes Superiores de Distrito, en las Capitales de Departamento en sus salas, por turno y, 2) En las provincias los jueces de partido (Art. 19 II C. Pol.).

6.1.5) Procedimiento Aplicable

La Constitución señala que tendrá tramitación sumarísima (Art. 19 II). Por su parte, la Ley del Tribunal Constitucional (Arts. 98-101) se encarga de reglamentar el procedimiento que en síntesis es el siguiente:

1) *Demanda*: presentada la acción, se examina su procedencia por el juez dentro de las 24 horas de haberse entablado. En caso de existir defectos de forma de la presentación, se otorga un plazo de 48 horas para subsanarlos.

2) *Medidas cautelares*: pueden decretarse medidas cautelares de oficio o a petición de parte.

3) *Audiencia pública*: al admitirse el recurso se fija día y hora para la audiencia pública la cual debe realizarse a más tardar dentro de las 48 horas a partir de la providencia de admisión. La audiencia debe realizarse indefectiblemente y no es susceptible de suspensión por la no comparecencia del recurrido o el Ministerio Público.

4) *Ampliación de la demanda y presentación de informe*: en la misma audiencia el recurrente podrá ratificar, ampliar, o modificar los términos de su demanda, acto seguido el recurrido debe prestar su informe.

5) *Sentencia*: examinado lo alegado por las partes, se pronuncia la resolución final en la misma audiencia, sin que obste para ello la ausencia del recurrido o la falta de informe de éste

6.1.6) La Sentencia

En cuanto a la sentencia de amparo y sus alcances, el artículo102 de la Ley del Tribunal Constitucional señala que:

1) Si concede o deniega el amparo, ésta será ejecutada, sin perjuicio de la revisión,

inmediatamente y sin observaciones;

2) Si concede el amparo, determinará también la existencia o no de responsabilidad civil y penal, estimando en el primer caso, el monto indemnizable por daños y perjuicio y, en el segundo, disponiendo la remisión de antecedentes al Ministerio Público;

3) Si se deniega el amparo demandado, impondrá y fijará costas y multa al recurrente;

4) La ejecución de los efectos dispuestos en los números 2 y 3, se hará efectiva, una vez absuelta la revisión por el Tribunal o juez de instancia;

5) La resolución será elevada en revisión de oficio ante el Tribunal Constitucional en el plazo de 24 horas;

6) Sin perjuicio de la ejecución del fallo, si el Tribunal que declare procedente la acción no contara con los elementos necesarios que permitan la calificación de los daños y perjuicios, abrirá término de ocho días para que se acrediten los mismos y pronunciará resolución en el plazo de tres días, ordenando la retención de haberes, y el embargo de los bienes de la autoridad recurrida a los efectos de dicha reparación.

6.2 Otras Acciones

No tenemos conocimiento de otras acciones de carácter cautelar idóneas para resguardar los derechos de los titulares de datos personales.

7. Mecanismos de Control

Dentro de la legislación boliviana no se prevé un organismo de control, máxime si tampoco existe la normativa que justifique su existencia. Con todo, podría eventualmente recurrirse al Defensor del Pueblo, órgano independiente que vela por la vigilancia y el cumplimiento de los derechos y garantías de las personas en relación con la actividad administrativa de todo el sector público. Dicho defensor, tiene facultades constitucionales para interponer las acciones de amparo sin necesidad de mandato (Art. 129 I Constitución Política).

8. Transmisión Internacional de Datos

A este respecto tampoco existe legislación especial en la materia. Relacionado con este tema pero en materia bancaria, tenemos dudas acerca del alcance de la disposición del artículo 87 Nº 4 de la Ley de Bancos en cuanto a las excepciones contempladas al secreto bancario. La amplitud de su formulación podría ser interpretada como una autorización para la transmisión de información entre bancos extranjeros que operen en Bolivia y sus respectivas matrices extranjeras, o incluso con otros bancos no relacionados, pues la norma sólo señala que no regirá el secreto bancario *"dentro de las informaciones que intercambian las entidades bancarias y financieras entre sí, de acuerdo a reciprocidad y prácticas bancarias"*, por lo que en virtud de las prácticas bancarias y acuerdos de reciprocidad, eventualmente podría argumentarse que no regiría

la prohibición del secreto bancario. Al respecto creemos que esta excepción está pensada para ser aplicada sólo dentro de las fronteras bolivianas, como tal debería interpretarse restrictivamente.

9. Régimen de Responsabilidad

Dada da la inexistencia de una ley de protección de datos personales en Bolivia, el régimen de responsabilidad aplicable a algunos ámbitos de la protección de los derechos fundamentales de la intimidad y vida privada, debe buscarse en otras normas de carácter general y sectorial.

9.1 Responsabilidad Administrativa

En el ámbito de la responsabilidad administrativa estimamos que debe estarse a los estatutos particulares de cada repartición pública, o en su defecto, a la normativa general aplicable. Es el Derecho Administrativo el que entra en juego en el caso de existir una violación a los deberes de confidencialidad respecto de ciertas informaciones, como la tributaria, judicial de menores o la establecida en el Estatuto del Funcionario Público, el cual prohíbe la utilización para fines distintos a los de la función administrativa de información previamente establecida como confidencial y reservada (Art. 9º, Ley Nº 2.027). A continuación se señalarán las reglas específicas en la materia.

a) Ley de Bancos e Instituciones Financieras

El artículo 89 de esta Ley disponeque el Superintendente y los empleados de la Superintendencia, aún después de cesar en sus funciones, tienen prohibido de dar a conocer información relacionada con los documentos, informes u operaciones de las instituciones financieras o de personas relacionadas con el sistema financiero. Agregando luego que: *"El funcionario o empleado que infrinja esta prohibición, será destituido de su cargo, sin perjuicio de las responsabilidades civil o penal que correspondan".*

b) Código Tributario

Este Código por su parte, dispone en el artículo 124 que: *"El funcionario o empleado de la Administración tributaria que divulgue dolosamente hechos o documentos que conozca en razón de su cargo y que por naturaleza o por disposición de la ley fueren reservados, será sancionado atendiendo a la gravedad de su falta con suspensión de su cargo por un tiempo de tres meses a un año o con la exoneración del mismo"*.

A continuación, el artículo 125 añade que: *"Si las infracciones establecidas en los artículos anteriores fueran culposas, la multa o el tiempo de suspensión serán reducidos a la mitad.".* Finalmente, prescribe el artículo 126 que: *"Las sanciones previstas en esta sección no se aplicarán si los hechos constituyen un delito o una contravención más grave, sancionados por otras disposiciones legales. En este caso, los actuados pertinentes serán enviados a la justicia ordinaria para el respectivo juzgamiento y sanción de los infractores".*

9.2 Responsabilidad Civil

En el ámbito civil, estimamos que cabría la aplicación de las reglas generales de responsabilidad civil extracontractual (Art. 984 C. Civil), en el evento que no medie una relación contractual entre el titular de los datos y el responsable del archivo, registro o banco de datos personales. La propia ley civil boliviana señala que es procedente la indemnización no sólo del daño material para el caso de vulnerarse la intimidad, sino que también es procedente la compensación del daño moral (Art. 23 Código Civil) [178] .

9.3 Responsabilidad Penal

En materia penal, no existen tipos que explícitamente se encarguen de sancionar conductas que atenten contra un bien jurídico como el derecho la autodeterminación informativa. Sólo es posible encontrar dentro del Código Penal [179] normas que castigan conductas que atentan de distinta forma en contra de la vida privada y el derecho a la intimidad, cuya eventual aplicación en materia de protección de datos es una cuestión que queda planteada como interrogante. A continuación se señalarán tales disposiciones.

a) Allanamiento de domicilio por particulares*:*

Artículo 298.- *"El que arbitrariamente entrare en domicilio ajeno o sus dependencias, o en un recinto habitado por otro, o en un lugar de trabajo, o permaneciere de igual manera en ellos, incurrirá en la pena de privación de libertad de tres meses a dos años y multa de treinta a cien días, se agravará la sanción en un tercio, si el delito se cometiere de noche, o con fuerza en las cosas o violencia en las personas, o con armas, o por varias personas reunidas".*

b) Allanamiento de domicilio por funcionario público:

Artículo 299.-*"El funcionario público o agente de la autoridad, que con abuso de sus funciones o sin las formalidades previstas por ley cometiere los hechos descritos en el artículo anterior, será sancionado con privación de libertad de uno a cuatro años".*

c) Violación de correspondencia:

Artículo 300.-*"El que indebidamente abriere una carta, un pliego cerrado o una comunicación telegráfica, radiotelegráfica o telefónica, dirigidos a otra persona, o el que, sin abrir la correspondencia, por medios técnicos se impusiere de un contenido, será sancionado con reclusión de tres meses a un año o multa de sesenta a doscientos cuarenta días.*

Con la misma pena será sancionado el que de igual modo se apoderare, ocultare o destruyere una carta, un pliego, un despacho u otro papel privado, aunque estén abiertos, o el que arbitrariamente desviare de su destino la correspondencia que no le pertenece.

[178] El artículo 23 del Código Civil señala que*: "Los derechos de la personalidad son inviolables y cualquier hecho contra ellos confiere al damnificado la facultad de demandar el cese de ese hecho, aparte del resarcimiento por el daño material o moral".*

[179] [En línea] < http://www.unifr.ch/derechopenal/legislacion/bo/cp_bolivia5.pdf > [consulta: 2 de Marzo 2003].

Se elevará el máximo de la sanción a dos años, cuando el autor de tales hechos divulgare el contenido de la correspondencia y despachos indicados".

d) Violación de comunicaciones:

Artículo 301.-*"El que grabare las palabras de otro no destinadas al público, sin su consentimiento, o el que mediante procedimientos técnicos escuchare manifestaciones privadas que no le estén dirigidas, o el que hiciere lo mismo con papeles privados o con una correspondencia epistolar o telegráfica aunque le hubieren sido dirigidos, siempre que el hecho pueda ocasionar algún perjuicio, será sancionado con privación de libertad de tres meses a un año"*

e) Revelación de secreto profesional:

Artículo 302.-*"El que teniendo conocimiento de secretos en virtud de su estado, ministerio, profesión, empleo, oficio, arte o comisión, los revelare sin justa causa, o los usare en beneficio propio o ajeno, si de ello se siguiere algún perjuicio, será sancionado con privación de libertad de tres meses a un año y multa de treinta a cien días".*

10. Conclusiones

Del análisis anterior es posible concluir que el ordenamiento jurídico boliviano no cuenta con una legislación que se encargue de proteger los datos personales. Sólo posee algunas normas dispersas que tratan de manera especial ámbitos relativos a la protección de algunos aspectos de la vida privada e intimidad. Sin duda que al legislador boliviano le queda aún una ardua tarea para lograr una protección a los datos personales. Por lo pronto, es necesario esperar el desarrollo del proceso de reforma constitucional que pretende incluir un artículo que contemple la acción de hábeas data, el cual sería un buen comienzo para erigir un mecanismo de tutela directo a los derechos de las personas afectados por el tratamiento de sus datos personales.

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN BRASIL

1. Generalidades

El ordenamiento jurídico brasileño cuenta con una Constitución que reconoce los derechos fundamentales de la intimidad, vida privada e imagen. Asimismo, protege los datos personales a través de la consagración de una acción de tutela denominada expresamente hábeas data, la cual puede ser ejercida para acceder a los registros, archivos o bancos de datos a cargo del Estado o de carácter público.

En el ámbito legal, Brasil no dispone de ley de protección de datos personales. Sólo existe en la actualidad una legislación de carácter Federal que viene a reglamentar

procesalmente la acción constitucional del hábeas data del artículo 5º.

En atención a la restricción al ámbito de aplicación del hábeas data constitucional, la doctrina y, la Ley de Protección al Consumidor, han ampliado la acción de hábeas data, la cual también puede interponerse en contra de los registros o bancos de datos a cargo de personas que presten servicios de carácter público o para el público.

Cabe agregar, que existen diversas normas jurídicas de variado carácter relacionadas con la tutela a los datos personales, las cuales se encuentran dispersas dentro del ordenamiento jurídico brasileño.

2 Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional

A nivel constitucional, el ordenamiento jurídico brasileño, se ha ocupado de establecer en el artículo 5º- en palabras de José Alfonso da Silva- el derecho al conocimiento de datos personales y de rectificarlos, el cual es otorgado en el mismo dispositivo que instituye el remedio de su tutela [180] . Es decir, el Constituyente brasileño consagra el derecho al acceso y rectificación de los datos a través del establecimiento de su garantía específica. El señalado artículo establece lo siguiente:

Artículo 5.- *"Todos son iguales ante la ley, sin distinción de cualquier naturaleza garantizando a los brasileños y a los extranjeros residentes en el país la inviolabilidad del derecho a la vida, a la libertad, a la igualdad, a la seguridad y a la propiedad en los términos siguientes: (…) LXXII.- Se concederá el "Habeas-Data": a) Para asegurar el conocimiento de informaciones relativas a las personas solicitantes, constantes en registros o bancos de datos de entidades gubernamentales o de carácter público; b) Para la rectificación de datos, cuando no se prefiera hacerlos por proceso secreto, judicial o administrativo"*.

Luego, se agrega más adelante en el mismo artículo 5º LXXVII que: *"Son gratuitas las acciones "Habeas-Corpus" y "Habeas-Data", y, en la forma de la ley los actos necesarios al ejercicio de la ciudadanía;*

1) Las normas definidoras de los derechos y garantías fundamentales tienen aplicación inmediata.

2) Los derechos y garantías expresos en esta Constitución no excluyen otros resultantes del régimen y de los principios por ella adoptados, o de los tratados internacionales en que la República Federal del Brasil sea parte" [181] .

Cabe hacer presente, en otro ámbito, que además de estas previsiones se establece en el Nº XXXIII del artículo 5º el denominado hábeas data impropio, acción ejercitable por

[180] Citado por Puccinelli, *op. cit*., pág. 301.

[181] El texto constitucional del Brasil en español se encuentra disponible [en línea] < http://www.congreso.gob.hn/sil/WEBCONS/c/CBRASIL.htm > [consulta: 7 de Febrero de 2003].

cualquier persona con la finalidad solicitar informaciones a los órganos públicos en materias de interés general o colectivo o información relativa a actos de la administración pública, a excepción de informaciones de carácter secreto imprescindibles para la seguridad de la sociedad o del Estado.

Lo señalado por el Constituyente en el artículo 5º, en materia de hábeas data, tiene sus orígenes en el viejo continente, precisamente en la Constitución portuguesa de 1976 -fuertemente influenciada por los pactos sobre de Derechos Humanos- la que sirvió de modelo para la actual Constitución brasileña de 1988 [182] .

Hasta el año 1997, la acción constitucional de hábeas data no contó con una reglamentación que la regulara. Ante éste vacío, se aplicaba lo preceptuado en el parágrafo 1 del artículo 5º, el cual señala que las normas definidoras de los derechos y garantías fundamentales tienen aplicación inmediata, por lo que no dependen de reglamentación. La solución práctica para el ejercicio procesal de esta acción fue la aplicación por analogía del procedimiento de hábeas corpus [183] .

Además de las disposiciones recién señaladas, el propio artículo 5º ha reconocido -como la mayoría de los países- la *"inviolabilidad de la intimidad, la vida privada, el honor y la imagen de las personas, asegurándose el derecho a indemnización por el daño material o moral derivado de su violación"* (Art. 5º; X). Lo anterior, es clave para la interpretación que pueda hacerse de la acción de hábeas data constitucional dado el rol atribuido por la doctrina comparada al derecho a la intimidad, que lo sitúa como base para la fundamentación del derecho a la libertad informática.

Por su parte, el artículo 5º XI constitucional establece la inviolabilidad del hogar, no pudiendo penetrar nadie en ella sin el consentimiento del morador, salvo en caso de flagrante delito o desastre, o para prestar socorro, o, durante el día, por determinación judicial. Asimismo señala que es inviolable el secreto de la correspondencia, de las comunicaciones telegráficas, de las informaciones y de las comunicaciones telefónicas, salvo, en el último caso, por orden judicial, en las hipótesis y en la forma que la ley establezca para fines de investigación criminal o instrucción penal (Art.5º XII). Al respecto, cabe preguntarse por la opción del Constituyente de tratar en números separados la inviolabilidad del hogar y la inviolabilidad de las comunicaciones, pues podría pensarse que éstos derechos tendrían una conexión más cercana con la seguridad individual que con la intimidad. Con todo, dentro de la doctrina española Ruiz Miguel ha señalado que "los grandes documentos internacionales sobre derechos fundamentales conectan el secreto de las comunicaciones con la intimidad, por lo que aquélla sería una manifestación de ésta" [184] . En cuanto a la inviolabilidad del domicilio

[182] Explicando los antecedentes de la Constitución brasileña De Abreu señala que en Portugal se llegó al hábeas data con el objetivo de obtener acceso a las informaciones que poseía "la policía política tradicional, violenta, arbitraria, creada por Salazar". Luego agrega "Y nosotros teníamos en Brasil también una policía política, arbitraria, violenta, que hacía registros de los que eran considerados enemigos del gobierno. El órgano del Brasil se llamaba Servicio Nacional de Informaciones. Entonces, así como los portugueses quisieron saber qué cosas estaban en los registros de la policía política, los brasileños igualmente" (De Abreu, Dalmo: *"El Hábeas Data en Brasil"*, en Revista Ius et Praxis, Universidad de Talca, año 3 Nº 1, Talca 1997, pág. 72).

[183] De Abreu, Dalmo, *op. cit*., pág. 75.

-como lo hemos señalado a propósito del análisis en Bolivia-, este mismo autor español señala que también guardaría estrecha relación con el derecho la intimidad.

En otro ámbito de materias, la Constitución brasileña señala que es de competencia del Tribunal Superior de Justicia, procesar y juzgar, originariamente, entre otros, los hábeas data en contra de los Ministros de Estado, Comandantes de la Marina, del Ejército y de la Aviación, así como del propio Tribunal Superior de Justicia (Art. 105; 1.b). Luego, en el artículo 108 señala que son competencia de los Tribunales Regionales Federales, entre otros los hábeas data contra los actos del propio Tribunal o de los jueces federales (Art.108; I c).

De lo dicho hasta ahora podemos concluir que, el ordenamiento jurídico brasileño posee una normativa constitucional que contempla una protección a los datos personales de manera directa, estableciendo la acción del hábeas data como tutela a éstos. Asimismo, reconoce las garantías a los derechos de la intimidad y vida privada de las personas, a partir de las cuales podría intentarse una construcción doctrinaria y jurisprudencial del derecho a la autodeterminación informativa.

2.2 Protección Legal de los Datos Personales

El sistema legal brasileño no cuenta con una ley de protección de datos personales. En esta materia sólo existe en la actualidad una ley especial de carácter federal que viene a reglamentar procesalmente la acción constitucional del hábeas data del artículo 5º. No obstante lo anterior, existe en la actualidad un Proyecto de Ley del año 1999 sobre estructuración y uso de los bancos de datos personales y regulación de la acción de hábeas data, que pretende suplir la falta de normativa sustantiva al respecto [185] .

A pesar de la falta de legislación de carácter general en la materia, el ordenamiento jurídico brasileño sí dispone de legislación sectorial que reglamenta algunos aspectos de la protección de datos. En esta línea se enmarca la Ley de Protección al Consumidor, la cual establece normas para el funcionamiento de las bases de datos de consumidores, señalando asimismo los derechos que a éstos competen en el evento que las informaciones tratadas por las bases de datos no se adecuen a la realidad. Finalmente, esta Ley consagra el derecho al olvido en materia de obligaciones entre consumidores y proveedores.

En otros ámbitos legales existe regulación sectorial que incide de manera directa en la protección de la intimidad de las personas, con lo cual se tutela de manera

[184] Ruiz Miguel, Carlos, op.cit., pág. 90.

[185] El Proyecto de Ley aludido es el Nº 268 del año 1999, presentado por el Senador Lucio Alcántara, el cual se encuentra en actual tramitación en la Cámara de Diputados. El estado de su tramitación puede consultarse [en línea] < http://www.senado.gov.br/lucioalcantara/1999/projetos/indproje.htm# > [consulta: 7 de Febrero 2003]. Cabe hacer presente que hasta Enero del año 2003, se tramitaba otro Proyecto de Ley que trataba sobre la privacidad de los datos personales de los usuarios de redes electrónicas, el cual fue presentado por el Diputado Proença el año 2000. Actualmente está archivado desde el 31 de Enero de 2003. Para mayor información [en línea] < http://www.camara.gov.br/Internet/sileg/Prop_Detalhe.asp?id=19533 > [consulta: 7 de Febrero 2003].

consecuencial a los datos personales. A continuación pasaremos a examinar las disposiciones encontradas en la materia [186] .

2.2.1) Ley de Protección al Consumidor (Ley Nº 8.078) [187]

Desde el año 1990, Brasil cuenta con una legislación especial que vela por los derechos de los consumidores. En ella, se contempla una Sección VI intitulada "De los Bancos de Datos" y, entre esas disposiciones, se encuentran algunas que dicen relación con la protección de los datos personales de los consumidores. De éstas destaca el artículo 43 [188] , el cual dispone que los consumidores tendrán acceso a las informaciones existentes en los catastros, fichas y registros de los proveedores respecto de los datos personales y de consumo que sobre aquéllos tengan, asimismo tienen ese derecho de acceso a las respectivas fuentes. Por lo tanto, en esta materia se reconoce el derecho de acceso a los consumidores titulares de datos personales.

El parágrafo 1º del artículo 43 señala por su parte que los catastros de datos personales y datos de los consumidores deben ser *"objetivos, claros, verdaderos"* y deben ser redactados en un *"lenguaje de fácil comprensión"* no pudiendo contener informaciones negativas referentes a un periodo superior a 5 años (la cursiva es nuestra). Lo anterior, claramente es un reconocimiento explícito del principio de la calidad de los datos por parte del legislador brasileño, el cual sin duda podría extrapolarse a los ámbitos no regulados por la ley en materia de protección de datos.

A su turno, el parágrafo 2º del artículo 43 prescribe que la apertura del catastro, ficha, registro de datos personales y de consumo debe ser comunicada por escrito al consumidor cuando no sea solicitado por él. Acá vislumbramos implícitamente el principio de la finalidad.

A renglón seguido, el parágrafo 3º reconoce el derecho del consumidor a la corrección inmediata de sus datos inexactos (derecho de rectificación). En este caso el

186 Traducción libre (WJT).

187 **LEI Nº 8.078 *" Dispõe sobre a proteção do consumidor, e dá outras providências".* [En línea] < http://www.crea-mg.com.br/infor/legislacao/l8078.htm > [consulta: 3 de Enero 2003].**

188 El artículo 43 de la Ley 8.078 dispone que*: "o consumidor, sem prejuízo do disposto no artigo 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1º - Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a 5 (cinco) años.* § 2º - A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3º - O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de 5 (cinco) dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. *§ 4º - Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.* § 5º - Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores".

encargado del archivo tiene un plazo de 5 días hábiles para comunicar la modificación a los eventuales destinatarios de las informaciones incorrectas.

Lo señalado hasta ahora por la Ley, guarda concordancia con algunos de los principios generales aplicables al tratamiento de datos personales, por lo que su inclusión en esta materia especial, en nuestra opinión, reviste singular importancia pues podrían extenderse a otras sedes legales en materia de protección de datos personales, a falta de ley general aplicable.

Por su parte, el parágrafo 4º del artículo 43 señala que se considerarán entidades de carácter público los bancos de datos y catastros relativos a los consumidores, los servicios de protección al crédito y los congéneres. Esta norma es de singular importancia pues amplía el ámbito objetivo de tutela a los datos reconocido en el artículo 5º LXXII letra a) de la Constitución, el cual dispone que la acción de hábeas data se concederá para asegurar el conocimiento de informaciones relativas a las personas solicitantes, constantes en *"registros o bancos de datos de entidades gubernamentales o de carácter publico"*. De no existir la disposición especial señalada, se habría dificultado el ejercicio del hábeas data respecto de los bancos de datos de consumidores, que en general escapan al carácter de 'público'.

Luego, el parágrafo 5º de esta Ley preceptúa que una vez prescritas las acciones de los proveedores para la cobranza de los créditos en contra de los consumidores, no podrán los sistemas de protección de crédito seguir manteniendo información que pueda impedir o dificultar un nuevo acceso a créditos respecto de los proveedores. Lo anterior, claramente es un reconocimiento del denominado 'derecho al olvido' en materia de obligaciones de carácter económico, comercial o financiero que beneficia al deudor moroso y sanciona indirectamente al acreedor negligente.

Finalmente, la Ley de Protección al Consumidor dispone en el artículo 44 [189] que los órganos públicos de defensa de los consumidores mantendrán registros actualizados de las reclamaciones fundadas que se hayan realizado en contra los proveedores de productos o servicios, debiendo divulgar anual y públicamente si la reclamación fue o no acogida por el proveedor [190] .

En suma, la Ley de Protección al Consumidor brasileña establece reglas especiales de protección a los datos personales, aplicables a las relaciones jurídicas entre proveedores de productos o servicios finales y los consumidores. No obstante lo anterior, estimamos que las disposiciones que reconocen ciertos principios generales en materia de de tratamiento de datos personales, como la calidad de los datos y la finalidad, pueden servir de base para una protección más general aplicable por analogía a otras situaciones no previstas por el legislador.

[189] El artículo 44 señala*: "Os órgãos públicos de defesa do consumidor manterão cadastros atualizados de reclamações fundamentadas contra fornecedores de produtos e serviços, devendo divulgá-lo pública e anualmente. A divulgação indicará se a reclamação foi atendida ou não pelo fornecedor.* § 1º - É facultado o acesso às informações lá constantes para orientação e consulta por qualquer interessado. § 2º - Aplicam-se a este artigo, no que couber, as mesmas regras enunciadas no artigo anterior e as do parágrafo único do artigo 22 deste Código".

2.2.2) Estatuto del Niño y Adolescente (Ley Nº 8.069) [191]

Esta normativa del año 1990 establece normas de protección para los niños y adolescentes. Dentro de éstas, destacan para nuestro estudio aquéllas que tienen por finalidad velar por el respeto de la intimidad de los menores. Regla común en este tipo de estatutos, es la que establece la prohibición de identificar a los menores a quienes se les atribuye participación en actos infraccionales o delitos. En este sentido, el artículo 247 [192] -ubicado dentro del capítulo de las Infracciones Administrativas- señala la prohibición de divulgación total o parcial, sin la autorización debida, por cualquier medio de comunicación, del nombre, documento de procedimiento policial, administrativo o judicial relativo a un niño o adolescente a quien se le atribuya un acto infraccional. En estos casos el resguardo de la intimidad de los menores tiene como consecuencia la protección de sus datos personales, los que no podrán divulgarse por regla general.

2.2.3) Ley Complementaria Nº 105 de 2001 [193]

190 Para aclarar el sistema brasileño de protección al consumidor nos valdremos de lo dicho por un autor argentino el cual señala que, "en Brasil tradicionalmente los comerciantes se agrupan en centros de Directores 'Lojistas' (los que tienen tiendas), que mantienen, en carácter privado el Sistema de Protección al Crédito (SPC), que a lo sumo es una central de catastro de deudores en retraso o en falta con los abonos que les corresponde. Este sistema quedó reconocido bajo el Código del Consumidor, reglamentada la protección de los consumidores contra el uso abusivo de las informaciones. La contrapartida a favor del consumidor, fue la creación de un Catastro de Proveedores, en el cual los órganos públicos de defensa del consumidor anotan las empresas que sean objeto de reclamación, publicando anualmente un listado donde consta si las reclamaciones fueran o no atendidas, transformándose pues en una especie de servicio de protección al consumidor. Por supuesto esto se torna un importante instrumento de coerción legítima sobre las empresas que violan los derechos de los consumidores, porque nadie querrá que su establecimiento tenga una publicidad negativa de esta especie". En Paván, Luis Carlos, *"La protección del consumidor en el MERCOSUR Análisis comparativo de los sistemas de Argentina, Brasil y Chile"*. [En línea] < http://www.acmp.org.br/docs/proteccion.doc > [consulta: 7 de Febrero 2003]. En nuestra opinión este registro de proveedores vendría cumplir una especie de rol de órgano de control informal respecto de los proveedores que participan del Sistema de Protección al Crédito.

191 Este estatuto jurídico puede ser visitado [en línea] < http://www.pge.sp.gov.br/centrodeestudos/bibliotecavirtual/dh/volume%20i/crian%C3%A7alei8069.htm > [consulta: 3 de Enero 2003].

192 El artículo 247 dispone que*: "Divulgar, total ou parcialmente, sem autorização devida, por qualquer meio de comunicação, nome, ato ou documento de procedimento policial, administrativo ou judicial relativo a criança ou adolescente a que se atribua ato infracional:* Pena - multa de três a vinte salários de referência, aplicando-se o dobro em caso de reincidência. § 1º - Incorre na mesma pena quem exibe, total ou parcialmente, fotografia de criança ou adolescente envolvido em ato infracional, ou qualquer ilustração que lhe diga respeito ou se refira a atos que lhe sejam atribuídos, de forma a permitir sua identificação, direta ou indiretamente. *§ 2º - Se o fato for praticado por órgão de imprensa ou emissora de rádio ou televisão, além da pena prevista neste artigo, a autoridade judiciária poderá determinar a apreensão da publicação ou a suspensão da programação da emissora até por dois dias, bem como da publicação do periódico até por dois números.*

193 [En línea] < http://www.planalto.gov.br > [consulta: 7 de Febrero 2003].

Esta ley se ocupa de reglamentar todo el instituto del denominado secreto bancario. Entre otras cosas, deroga el artículo 38 de la Ley Nº 4.595 de 1964 sobre Política de las Instituciones Financieras, bancarias y crediticias. Este artículo trataba el secreto bancario y sus excepciones de manera breve [194] . La nueva ley, más extensa que el derogado artículo, desarrolla el concepto de secreto financiero y sus excepciones. Llama la atención el hecho de definir aquella información susceptible de secreto a través de una enumeración negativa, es decir, de aquellas acciones que no constituyen violación de secreto. El artículo 1º parágrafo 3 [195] de esta ley señala que no constituirá violación del deber de sigilo: 1) El intercambio de información entre instituciones financieras, para fines estadísticos, inclusive por centrales de riesgo, observando las normas dictadas por el Consejo Monetario Nacional y por el Banco Central de Brasil; 2) Las informaciones que constan en el registro de giradores de cheques sin provisión de fondos o deudores incumplidores, observando las normas señaladas por el Consejo Monetario Nacional y por el Banco Central de Brasil; 3) Las informaciones entregadas a las autoridades competentes que den cuenta de ilícitos penales o administrativos incluyendo la información sobre las operaciones en que la fuente de los recursos procedan de cualquier práctica criminal; 4) La revelación de informaciones confidenciales con el consentimiento de expreso de los interesados; 5) Cuando sea necesario para la verificación de la ocurrencia de cualquier ilícito en cualquier fase de la investigación, y especialmente en los crímenes siguientes: terrorismo, tráfico ilícito de sustancias narcóticas o de drogas similares, contrabando o tráfico de armas, secuestro, delitos contra el sistema financiero nacional, contra la administración pública, entre otros [196] . En esta materia se ha señalado que, pese a la reforma legal del año 2001, el secreto bancario aún cubre las operaciones activas, pasivas y servicios prestados por las instituciones bancarias, no obstante lo anterior, establece diversas excepciones bajo las cuales se puede transmitir la información sin violar el secreto [197]

Por lo tanto, en materia de datos personales referidos a las operaciones financieras,

[194] El artículo 38, sucintamente disponía el secreto de las operaciones activas y pasivas prestadas por las instituciones bancarias. A continuación de la regla general se contemplaban las excepciones e ese secreto, estas eran: 1) Orden judicial de información o esclarecimiento; 2) Informes legislativos solicitados a las instituciones financieras públicas existiendo motivos relevantes para ello; 3) Investigaciones realizadas por las Comisiones Parlamentarias de investigación en ejercicio de su competencia constitucional; 4) Examen por los fiscales tributarios de documentos, libros, y registros de cuentas de depósitos sólo en caso de existir un procedimiento incoado y, que ese registro sea considerado indispensable por la autoridad competente [En línea] < http://www.oficinadodireito.com.br/leifederal/4595.htm > [consulta: 3 de Enero 2003].

[195] El artículo 1º parágrafo 3º, dispone que *" Não constitui violação do dever de sigilo:* I – a troca de informações entre instituições financeiras, para fins cadastrais, inclusive por intermédio de centrais de risco, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil; II - o fornecimento de informações constantes de cadastro de emitentes de cheques sem provisão de fundos e de devedores inadimplentes, a entidades de proteção ao crédito, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil; III – o fornecimento das informações de que trata o § 2o do art. 11 da Lei no 9.311, de 24 de outubro de 1996; IV – a comunicação, às autoridades competentes, da prática de ilícitos penais ou administrativos, abrangendo o fornecimento de informações sobre operações que envolvam recursos provenientes de qualquer prática criminosa; V – a revelação de informações sigilosas com o consentimento expresso dos interessados; VI – a prestação de informações nos termos e condições estabelecidos nos artigos 2o, 3o, 4o, 5o, 6o, 7o e 9 desta Lei Complementar".

las excepciones al deber de secreto -que por regla general cubre tanto las operaciones activas como pasivas-, se han ampliado considerablemente, restringiéndose por otro lado el margen de protección a la confidencialidad de este tipo de información.

2.2.4) Resolución Nº 2.724/00 del Banco Central de Brasil [198]

El Banco Central del Brasil en ejercicio de sus facultades normativas, ha dictado resoluciones con carácter vinculante para los operadores del mercado financiero en general. Dentro de esas resoluciones destaca la Nº 2.724 del año 2000, la cual ordena a todos los bancos en general, sociedades de crédito inmobiliario, sociedades de crédito, financiamiento e inversión, compañías hipotecarias, entre otras, la presentación de informes acerca de los montos pasivos y responsabilidades por garantías de los clientes de las instituciones ya señaladas. Por lo tanto, para este particular sector económico se establece un deber de información de determinados datos personales, la cual obviamente no viola el secreto financiero.

2.2.5) Ley sobre el Sistema Tributario Nacional (Ley Federal Nº 5.172-1966) [199]

El artículo 198 del Código Tributario brasileño [200] , señala que está prohibida la divulgación, para cualquier fin, por parte de la Hacienda Pública o de sus funcionarios, de cualquier información obtenida en razón de su oficio, sobre la situación económica o financiera de los sujetos pasivos o de terceros y sobre la naturaleza y estado de sus negocios o actividades. Las excepciones a esta prohibición son dos: i) requisición judicial en interés de la justicia y, ii) la cooperación mutua para fiscalizar los respectivos tributos

196 El artículo 2 º de esta ley, agrega que el deber de confidencialidad se extiende al Banco Central brasileño en lo referente a las operaciones de éste, y a la información que disponga en el ejercicio de sus atribuciones. Luego, el Parágrafo N º1 señala que el secreto no puede ser opuesto al Banco Central de Brasil en cuanto a: las cuentas de depósitos, de usos y de inversiones mantenidas en las instituciones financieras, en el ejercicio de su función de fiscalización en cualquier momento por los ilícitos cometidos por los administradores, miembros del consejo estatutario, ejecutivos y de los presidentes de instituciones financieras, entre otros.

197 Del Villar, Rafael "'et al'": *"Regulación de Protección de Datos y de Sociedades de Información: una Comparación de Países seleccionados de América Latina, los Estados Unidos, Canadá y la Unión Europea"*. Documento de Investigación N° 2001-07, 2001. [En línea] < http://www.banxico.org.mx/gPublicaciones/DocumentosInvestigacion/docinves/doc2001-7/doc2001-7.pdf > [consulta: 18 de Noviembre 2002].

198 [En línea] < http://www.leasingabel.com.br/novosite/juridico/resolucao/res2724.htm > [consulta: 3 de Enero 2003].

199 [En línea] < http://www.sefp.df.gov.br/Legislacao/LeiordinariaFed/lei5172.htm > [consulta: 3 de Enero 2003].

200 El artículo 198 dispone que: *"Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, para qualquer fim, por parte da Fazenda Pública ou de seus funcionários, de qualquer informação, obtida em razão do ofício, sobre a situação econômica ou financeira dos sujeitos passivos ou de terceiros e sobre a natureza e o estado dos seus negócios ou atividades.* Parágrafo único. Excetuam-se do disposto neste artigo, unicamente, os casos previstos no artigo seguinte e os de requisição regular da autoridade judiciária no interesse da justiça".

entre la hacienda pública de la Unión de los Estados, el Distrito federal y los Municipios. En cuanto a la permuta de información para ese fin, ésta debe hacerse en la forma establecida por ley general o especial, o por convenio.

Finalmente, el artículo 199 contempla la posibilidad de intercambiar información entre los Estados de la federación brasileña en el interés la recaudación y de la fiscalización de los tributos, en la forma establecida en tratados o acuerdos [201] .

3. Bienes Jurídicos Protegidos por la Legislación de Datos Personales

Dada la inexistencia de una ley que se ocupe de la protección a los datos personales, sólo nos referiremos a la normativa existente en materia de protección de derechos del consumidor y a la normativa constitucional, dado que en ellas es posible visualizar bienes jurídicos generalmente reconocidos por el derecho a la protección de datos.

Si bien la Ley de Protección al Consumidor establece ciertas normas de tutela a los derechos de los titulares de datos, ellas aparecen del todo insuficientes, pues sólo regulan algunos aspectos mínimos en materia de tratamiento de datos y derechos de los titulares, aunque es preciso reconocer que en materia de hábeas data ha suplido la estrechez del texto constitucional que limita los sujetos pasivos de esta acción. En suma, creemos que tras esta Ley estaría presente tanto el derecho a la intimidad como a la vida privada de las personas, vislumbrándose eventualmente el derecho a la autodeterminación informativa sólo en alguno de sus ámbitos.

En cuanto a la Constitución, es posible constatar que existe un reconocimiento a la garantía del derecho a la intimidad, a la vida privada, honor e imagen de las personas (Art .5º, X). También consagra la acción de hábeas data en sus vertientes de acceso y rectificación de la información, por lo que cabría plantearse la posibilidad que el Constituyente brasileño haya reconocido un derecho a la autodeterminación informativa [202] . En este sentido, debemos hacer presente que, en general, la doctrina brasileña no habla de libertad informática, sino que más bien vincula la acción de hábeas data con la protección de la intimidad [203] . En otro sentido se ha pronunciado Cretella Junior, para quien el bien tutelado es el derecho de conocimiento de los datos personales y de rectificarlos [204] . En nuestra opinión, además de los derechos señalados expresamente por el Constituyente en el artículo 5º, eventualmente podría sostenerse que se estaría

[201] El artículo 199, por su parte dispone: *"A Fazenda Pública da União e as dos Estados, do Distrito Federal e dos Municípios prestar-se-ão mutuamente assistência para a fiscalização dos tributos respectivos e permuta de informações, na forma estabelecida, em caráter geral ou específico, por lei ou convênio".*

[202] En este sentido se pronuncia Morales Prats -citado por Da Silva- para quien el conjunto de facultades que otorga la acción de hábeas data constituye la denominada libertad informática o derecho al control de datos relativos al propio individuo, o sea, del derecho a la autodeterminación informativa. Todo lo anterior en Puccinelli, *op. cit*., pág. 304.

[203] En este sentido se pronuncia el constitucionalista Da Silva, José Alfonso, para quien la acción de hábeas data constitucional tiene por objeto proteger la esfera íntima de los individuos, citado por Puccinelli, *op. cit*., pág. 315.

reconociendo el derecho a la autodeterminación informativa. Sin embargo, no estimamos que lo consagre en plenitud, pues dada la configuración del artículo 5º LXXII, éste deja en principio fuera de la acción de hábeas data a los bancos de datos y registros de carácter privado o que no sean considerados de carácter público, lo cual limita *ab initio* al derecho.

4. Principios Informativos de la Legislación de Protección de Datos Personales

En materia de principios informativos, no es mucho lo que puede predicarse del ordenamiento jurídico brasileño dado el silencio del legislador al respecto. A pesar de ello y, a partir de Ley de Protección al Consumidor, pueden vislumbrarse a lo menos dos principios generales para el tratamiento de los datos personales. Éstos se señalan a continuación:

1º) Principio de la calidad de los datos

Este principio se patentiza en el parágrafo 1º del artículo 43 de la Ley de Protección al Consumidor al señalar que los catastros o registros de datos personales y datos de los consumidores deben ser objetivos, claros, verdaderos, redactados en un lenguaje de fácil comprensión, no pudiendo contener informaciones negativas referentes a un período superior a 5 años.

2º) Principio de la finalidad

Ley de Protección al Consumidor no reconoce explícitamente el principio de la finalidad, sino más bien éste podría deducirse de lo señalado en el parágrafo 2º del artículo 43º, el cual dispone que la apertura del catastro, ficha, registro de datos personales y de consumo debe ser comunicada por escrito al consumidor cuando no sea solicitado por él. Entendemos que dicha comunicación debería contener al menos el objeto y finalidad del tratamiento de los datos del consumidor, de lo contrario carecería de sentido tal deber, pues la sola comunicación del hecho de registrar datos por parte del proveedor, sería al menos una acción esperable, cuestión que no lo es tanto si se trata del objeto y finalidad de la utilización de los datos del consumidor. Con todo, aún así no puede hablarse con propiedad que se reconozca este principio de una forma adecuada.

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

En atención a la falta de ley general de protección de datos personales en el ordenamiento jurídico brasileño, no nos detendremos a analizar este punto.

6. Modelos de Tutela

[204] Citado por Puccinelli, *op. cit.*, pág. 315.

Como ya se ha adelantado, la Constitución del Brasil contempla expresamente la acción del hábeas data, la cual ha sido regulada procesalmente por la Ley Nº 9.507 [205] . Conjuntamente con ésta, consagra el derecho de acceso a las informaciones de interés particular, colectivo o general que posean los órganos públicos, denominado por la doctrina como hábeas data impropio.

6.1 La Acción de Hábeas Data

La norma constitucional del artículo 5º LXXII, o sea la del hábeas data propio, no fue objeto de regulación legal sino hasta el año 1997 con la Ley Nº 9.507 (en adelante la Ley). Antes de ella, la tramitación había quedado entregada al procedimiento de hábeas corpus, haciéndose aplicación por analogía de sus reglas al hábeas data. La Ley, de carácter eminentemente procesal, regula el derecho de acceso a las informaciones disciplinando la acción del hábeas data, consta de 23 artículos y entró en vigencia en el mes de noviembre de 1997.

6.1.1) Procedencia de la Acción

La acción de hábeas data procede para:

1)Asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público (Art. 5º LXXII C. Pol. y 7º Ley);

2) La rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo (Art. 5º LXXII, C. Pol. y 7º Ley) y

3)La anotación en los registros o bancos de datos de las explicaciones que sobre datos verdaderos pero justificables, solicite el titular de los datos aduciendo juicio pendiente o arbitraje (Art. 7 Ley).

6.1.2) Legitimación Activa

Los legitimados activos de esta acción son los titulares de los datos registrados, sean ellos nacionales o extranjeros residentes en el país. Para algunos, este sería un derecho personalísimo (Da Silva). En contra de lo anterior, en especial por los efectos negativos de considerarlo un derecho personalísimo se pronuncia De Abreu, quien sostiene que en ciertos casos, y en consideración al derecho de protección de la imagen, es menester ampliar la acción no solo al titular sino también a sus sucesores [206] .

6.1.3) Legitimación Pasiva

En cuanto al sujeto pasivo de la acción de hábeas data, la Ley señala que procederá respecto de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público (Art. 7º I). Lo

[205] Esta ley puede consultarse [en línea] < http://www.planalto.gov.br/ccivil_03/Leis/L9507.htm > [consulta: 26 de Noviembre 2002].

[206] Todo lo anterior en: De Abreu, *op. cit*., págs. 76 y 77.

anterior concuerda con lo preceptuado por el Constituyente en el artículo 5º LXXII; en ambas normas, el sujeto pasivo aparecería en principio restringido al Estado y a sus organismos. El punto ha sido discutido por la doctrina brasileña, la que ha llegado en general a interpretar de manera uniforme el texto, de tal modo que el término *"entidades de carácter público"* no pueda ser entendido sólo como organismo público, sino que incluya a las instituciones, entidades y personas jurídicas privadas que presten servicios para el público o de interés público, "envolviéndose allí no sólo a concesionarios, permisionarios o ejercitadores de actividades autorizadas y agentes de control y protección de situaciones sociales o colectivas, como las instituciones de catastro de datos personales para control o protección del crédito o divulgadoras profesionales de datos personales, como las firmas de asesoría y ventas directas" [207] . Con todo, cabe recordar que la propia Ley de Protección al Consumidor en su artículo 43 parágrafo 4º preceptúa que: *"los bancos de datos y catastros relativos a consumidores, los servicios de protección al crédito y los congéneres se consideran entidades de carácter público"*. Con ello se demuestra la intención del legislador, al menos en esta sede, de optar por una interpretación extensiva del texto constitucional.

En suma, a pesar de la restricción literal del texto constitucional respecto del sujeto pasivo de la acción de hábeas data, tanto la doctrina brasileña como el legislador, han entendido que también son sujetos pasivos de ésta acción aquellas entidades y personas jurídicas privadas que prestan servicios de interés público o servicios para el público [208] . En cuanto a jurisprudencia que haya aplicado el criterio doctrinario dominante en casos que no caigan bajo la Ley de Protección al Consumidor, no tenemos noticia de ésta.

6.1.4) Competencia

Según el artículo 20º I de la Ley, son competentes para conocer de las acciones de hábeas data, originariamente (en única instancia): 1) La Corte Federal Suprema, contra los actos del Presidente de la República, de las Mesas de la Cámara de Diputados y del Senado Federal, del Tribunal de Cuentas de la Unión, del Procurador General de la República y de los actos de la propia Corte Federal Suprema; 2) El Tribunal de Justicia Superior, contra actos de los ministros de Estado o de la propia Corte; 3) Las Cortes Regionales Federales contra actos de la propia Corte o de los jueces federales; 4) El juez federal, contra actos de la autoridad federal, excepto los casos de competencia de las cortes federales; 5) Las Cortes del Estado, según lo dispuesto en la Constitución del Estado y, 6) El juez del Estado, en los demás casos.

En virtud del artículo 20º II, también son competentes para conocer de la acción de hábeas data, en grado de recurso: 1) La Corte Federal Suprema, cuando la decisión denegatoria fuera dictada en única instancia por los Tribunales Superiores; 2) El Tribunal

[207] Esta es la interpretación de Da Silva, citado por Puccinelli, *op. cit*., pág. 311. Otros, como Pinto Ferreira y Zúñiga Urbina estiman que la frase "*de carácter público"* alcanzaría a los bancos de datos privados. Según Zúñiga, en razón a que ese concepto se refiere tanto a entes públicos como a entidades privadas que prestan un servicio público (*Ibídem*).

[208] En esta forma lo resume Pizzolo, Calógero: *"El Hábeas Data en el Derecho Constitucional Latinoamericano*". En *"La Defensa de la Intimidad y de los Datos Personales a través del Hábeas Data"*. Gozaini, Osvaldo (coord.), Ediar, Bs. As., 2001, pág. 86.

Superior de Justicia cuando la decisión haya sido pronunciada en única instancia por las Cortes Regionales Federales; 3) Las Cortes Regionales Federales, cuando la decisión haya sido pronunciada por un juez federal y, 4) Las Cortes del Estado, los de Distrito Federal y Territorios, de conformidad a lo dispuesto en la Constitución y en la respectiva ley de Organización de la Justicia de Distrito Federal.

Finalmente, es competente para conocer la acción de hábeas data a través de recurso extraordinario el Supremo Tribunal Federal, en los casos previstos en la Constitución (Art. 20º III Ley).

6.1.5) Procedimiento Aplicable

La acción de hábeas data se rige por un procedimiento especial, el cual requiere previamente agotar la vía administrativa respecto de los responsables de los archivos, registros o bancos de datos para que pueda accionarse judicialmente. Cabe destacar de este procedimiento que la prueba debe ser acompañada en la demanda. Notificada ésta, el demandado tiene un plazo de 10 días para presentar las informaciones que estime necesarias. Vencido este plazo y oído el Ministerio Público dentro de los 5 días siguientes, los autos pasan a manos del juez para que dicte sentencia dentro de los cinco días siguientes (Arts. 9º-13º Ley).

6.1.6) La Sentencia

En lo relativo a la sentencia, se dispone que en el caso de acogerse la acción ésta deberá señalar el día y hora en que el demandado: 1) Presente las informaciones que consten en el registro o banco de datos o, 2) Presente en juicio la prueba de la rectificación o de la anotación hecha en los registros del demandante (Art. 13º Ley). Tanto la sentencia que acoge como la que rechaza la demanda de hábeas data son apelables. En el caso de acogerse la acción, la apelación se otorgará en el solo efecto devolutivo (Art. 15º Ley). Cabe destacar que en el caso de haberse rechazado la acción, ésta podrá renovarse en el evento de no haberse apreciado el mérito de ella. Nosotros interpretamos esta disposición como el hecho de ser rechazada la acción por aspectos formales y no por haberse pronunciado sobre el fondo del asunto.

Finalmente, la Ley señala que los procesos de hábeas data tendrán preferencia sobre los otros actos judiciales, a excepción de los mandados de seguridad y del hábeas corpus. Con todo, el plazo para fallar el recurso no podrá exceder de 24 horas desde la distribución realizada por el tribunal *ad quem* (Art. 19º Ley).

6.2 Otras Acciones

Dentro de la legislación brasileña no se contemplan otras acciones que tengan por finalidad la protección de los datos personales, salvo las disposiciones de la Ley de Protección al Consumidor (Art. 43) que reconocen a los consumidores los derechos de acceso y rectificación de sus datos personales que son tratados por los proveedores de bienes y servicios. El procedimiento de carácter informal ya fue reseñado en el punto Nº 2.2.1 de este análisis, al cual nos remitiremos.

7. Mecanismos de Control

El ordenamiento jurídico brasileño no dispone de un órgano de control que vele por la aplicación y respeto de normas protectoras de datos personales, máxime si no existe tal clase de legislación en la materia. Cabe señalar no obstante, que la Ley de Protección al Consumidor otorga una facultad muy particular a los organismos públicos de defensa de los consumidores respecto de los proveedores que no respetan las normas referidas a los datos personales tratados por el Sistema de Protección al Crédito. Esta facultad consiste en mantener registros actualizados de las reclamaciones fundadas que se hayan interpuesto en contra de los proveedores, debiendo divulgar anual y públicamente si la reclamación fue o no acogida por éste. Lo anterior aparece como una especie de control informal a las disposiciones de protección de datos de los consumidores (Art. 44 Ley Consumidor).

8. Transmisión Internacional de Datos

La legislación del Brasil no contempla reglas que regulen el sistema de transmisión internacional de datos personales.

9. Régimen de Responsabilidad

En materia de responsabilidad, el sistema jurídico brasileño no dispone de una legislación especial que sancione conductas que vulneren los derechos de las personas en materia de datos personales. Sólo se establecen sanciones en estatutos sectoriales que, en general, están referidos a infracciones a deberes de secreto o confidencialidad de cierta información.

9.1 Responsabilidad Administrativa

En el ámbito del derecho administrativo estimamos que a falta de normas especiales deberá estarse a cada estatuto particular que rige la administración pública. En lo que respecta a las sanciones de carácter administrativo establecidas por algunos de los estatutos sectoriales ya señalados, destacan las siguientes:

9.1.1) Ley de Protección al Consumidor

En lo que a nosotros interesa, esta Ley establece sanciones administrativas para aquellos proveedores que violen las disposiciones relativas a los deberes de informar a los consumidores sobre los datos contenidos en los catastros de datos, corregirlos en los plazos señalados, etc. Estas sanciones pueden ser multas, suspensión temporal de actividades, término de la autorización para el funcionamiento de la actividad, intervención administrativa, obligación de contra propaganda, entre otras que no son atingentes a la protección de los datos personales de los consumidores (Art. 56).

9.1.2) Ley de Protección del Niño y del Adolescente

Está Ley también establece sanciones administrativas para quienes cometan infracciones a sus disposiciones, en especial aquellos funcionarios públicos que violan el deber de secreto respecto de la identidad de los niños a quienes se les imputa participación en actos infraccionales. Las sanciones en este caso son multas en relación al sueldo del infractor (Art. 247, Ley 8.069).

9.2 Responsabilidad Civil

En materia civil, dada la inexistencia de normas especiales, entendemos que es preciso remitirse a las reglas generales en la materia, las que por el momento desconocemos. Con todo, la propia Constitución brasileña asegura el derecho a la indemnización por el daño material o moral derivado de la violación al derecho a la intimidad, vida privada, el honor y la propia imagen (Art. 5º, X C. Pol.).

Por otra parte, y dentro de los estatutos sectoriales vistos, la Ley Complementaria 105 de 2001 -que establece el secreto bancario-, dispone en el artículo 11 que el servidor público que utilice cualquier información con infracción al deber de secreto impuesto por esta ley responderá personal y directamente por los daños ocasionados, sin perjuicio de la responsabilidad objetiva de la entidad pública, cuando se compruebe que el servidor actuó siguiendo órdenes oficiales. Por lo tanto, se establece claramente la responsabilidad civil del funcionario que cause daño a consecuencia de infringir las disposiciones de la Ley y, en caso que éste haya obedecido órdenes u orientaciones oficiales, responde el propio organismo de manera estricta u objetiva [209] .

9.3 Responsabilidad Penal

En cuanto a las sanciones penales, debemos señalar no se contemplan normas especiales que castiguen como delitos acciones u omisiones que digan directa relación con la protección a los datos personales, salva la norma sectorial que castiga la violación del secreto bancario establecido en la Ley 105. Las demás disposiciones que establecen delitos penales relacionados con la protección de la vida privada e intimidad se contemplan en el Código Penal del Brasil.

9.3.1) Ley Complementaria 105 de 2001

El artículo 10 de este estatuto dispone que la quiebra del sigilo o violación del secreto, fuera de las hipótesis autorizadas por la misma Ley Complementaria, constituye crimen y está sujeta a la pena de reclusión de uno a cuatro años y multa, aplicándose en lo no cubierto el Código Penal, sin perjuicio de otras sanciones civiles [210] .

[209] Art. 11. *"O servidor público que utilizar ou viabilizar a utilização de qualquer informação obtida em decorrência da quebra de sigilo de que trata esta Lei Complementar responde pessoal e diretamente pelos danos decorrentes, sem prejuízo da responsabilidade objetiva da entidade pública, quando comprovado que o servidor agiu de acordo com orientação oficial".*

9.3.2) Código Penal

Dentro de este Código sólo se contemplan tipos penales que castigan los siguientes delitos: a) Violación de domicilio (Art.150); b) Violación de la correspondencia y divulgación de su contenido (Arts. 151 y 153) y, c) Violación de secretos (Art. 154) [211] .

10. Conclusiones

El ordenamiento jurídico brasileño cuenta con una Constitución que reconoce los derechos fundamentales de la intimidad, vida privada e imagen. Asimismo, tutela un ámbito del derecho a la protección de datos mediante la consagración de la acción denominada expresamente hábeas data, la cual puede ser ejercida para acceder a los registros, archivos o bancos de datos de entidades gubernamentales o de carácter

[210] Art. 10 *"A quebra de sigilo, fora das hipóteses autorizadas nesta Lei Complementar, constitui crime e sujeita os responsáveis à pena de reclusão, de um a quatro anos, e multa, aplicando-se, no que couber, o Código Penal, sem prejuízo de outras sanções cabíveis".* "Parágrafo único. Incorre nas mesmas penas quem omitir, retardar injustificadamente ou prestar falsamente as informações requeridas nos termos desta Lei Complementar".

[211] Estos artículos señalan: "Art. 150 - *Entrar ou permanecer, clandestina ou astuciosamente, ou contra a vontade expressa ou tácita de quem de direito, em casa alheia ou em suas dependências:* Pena - detenção, de 1 (um) a 3 (três) meses, ou multa. § 1 - Se o crime é cometido durante a noite, ou em lugar ermo, ou com o emprego de violência ou de arma, ou por duas ou mais pessoas: Pena - detenção, de 6 (seis) meses a 2 (dois) anos, além da pena correspondente à violência. § 2 - Aumenta-se a pena de um terço, se o fato é cometido por funcionário público, fora dos casos legais, ou com inobservância das formalidades estabelecidas em lei, ou com abuso do poder. § 3 - Não constitui crime a entrada ou permanência em casa alheia ou em suas dependências: *I - durante o dia, com observância das formalidades legais, para efetuar prisão ou outra diligência; II - a qualquer hora do dia ou da noite, quando algum crime está sendo ali praticado ou na iminência de o ser. § 4 - A expressão "casa" compreende: I - qualquer compartimento habitado; II - aposento ocupado de habitação coletiva; III - compartimento não aberto ao público, onde alguém exerce profissão ou atividade.* § 5 - Não se compreendem na expressão "casa": I - hospedaria, estalagem ou qualquer outra habitação coletiva, enquanto aberta, salvo a restrição do número II do parágrafo anterior; II - taverna, casa de jogo e outras do mesmo gênero. Art. 151 - *Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem:* Pena - detenção, de 1 (um) a 6 (seis) meses, ou multa. Sonegação ou destruição de correspondência *§ 1 - Na mesma pena incorre: I - quem se apossa indevidamente de correspondência alheia, embora não fechada e, no todo ou em parte, a sonega ou destrói;Violação de comunicação telegráfica, radioelétrica ou telefônica II - quem indevidamente divulga, transmite a outrem ou utiliza abusivamente comunicação telegráfica ou radioelétrica dirigida a terceiro, ou conversação telefônica entre outras pessoas; III - quem impede a comunicação ou a conversação referidas no número anterior; IV - quem instala ou utiliza estação ou aparelho radioelétrico, sem observância de disposição legal.* § 2 - As penas aumentam-se de metade, se há dano para outrem. *§ 3 - Se o agente comete o crime, com abuso de função em serviço postal, telegráfico, radioelétrico ou telefônico: Pena - detenção, de 1 (um) a 3 (três) anos.* § 4 - Somente se procede mediante representação, salvo nos casos do § 1, número IV, e do § 3. Art. 153 - *Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem: Pena - detenção, de 1 (um) a 6 (seis) meses, ou multa.* Parágrafo único. Somente se procede mediante representação. Art. 154 - *Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa. Parágrafo único. Somente se procede mediante representação".* El Código Penal, puede ser consultado [en línea] < http://www.unifr.ch/derechopenal/legislacion/br/ljbre5.html > [consulta: 8 de Febrero 2003.

público. En atención a esta restricción al ámbito de aplicación del hábeas data, se ha señalado por la doctrina y, a nivel legal por expreso mandato del legislador en materia de protección de consumidores, que la acción de hábeas data también puede interponerse en contra de los registros o bancos de datos a cargo de privados que presten servicios de carácter público o para el público.

A nivel legal, Brasil no dispone de una ley que se ocupe de proteger los datos personales. Sí cuenta en este nivel jerárquico con una ley que regula procesalmente el ejercicio de la acción del hábeas data [212] . Finalmente, debemos señalar que en la actualidad se tramita un Proyecto de Ley desde el año 1999 sobre estructuración y uso de los bancos de datos personales y regulación de la acción de hábeas data, el cual que pretende suplir la falta de legislación al respecto.

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN CHILE

1. Generalidades

El ordenamiento jurídico chileno no cuenta con disposiciones constitucionales que se refieran directamente a la protección de los datos personales. En consecuencia, no se reconoce en este nivel normativo la acción hábeas data u otra garantía específicamente diseñada que proteja los derechos de los titulares de los datos personales [213] . No obstante lo anterior, el Constituyente chileno sí contempla disposiciones referidas a la protección de los bienes jurídicos vida privada e intimidad, en los cuales poder fundamentar una tutela a los derechos de las personas en la materia de estudio.

Dentro del ámbito legal, Chile dispone desde 1999 de una Ley de Protección de Datos Personales (Ley Nº 19.628), fundamentada en las disposiciones constitucionales que reconocen el derecho a la vida privada e intimidad. Esta Ley, fue objeto de una modificación parcial el año 2002, la que entre otras finalidades pretendía beneficiar a las personas naturales que figuraban en bases de datos con antecedentes comerciales negativos, con el objeto de reactivar el empleo, dado que no se contrataba a las personas que figuraban en bases de datos como deudoras de obligaciones de carácter comercial. La reforma a la Ley, también estableció una prohibición a los responsables de las bases de datos que tratan datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial, de transmitir información relacionada con deudas impagas exigibles a una fecha determinada y hasta un cierto monto de dinero.

Si bien Chile posee una Ley de Protección de Datos Personales, a su vez también

[212] Como ya se ha señalado la Ley Nº 9.507.

[213] Esta carencia es reseñada por Puccinelli, *op. cit*., pág. 333.

existen diversas disposiciones sectoriales dispersas en el ordenamiento jurídico que dicen relación con la protección de la vida privada e intimidad. Estas normas, generalmente establecen deberes de secreto respecto de informaciones reservadas o confidenciales.

A nivel reglamentario, la Ley 19.628 se encuentra parcialmente regulada por el Poder Ejecutivo, en lo relativo al Registro de bancos de datos personales a cargo de organismos públicos, pues en esta materia el legislador endosó al Ejecutivo dicha tarea. Finalmente, cabe destacar la existencia de un Decreto Supremo del año 1928 que establece la obligación de informar a la Cámara de Comercio de Santiago, ciertos datos de carácter económicos, financieros y comerciales por parte de algunas entidades públicas y privadas. Este Decreto tan añoso permanece aún vigente en todo lo que no se oponga a lo dispuesto en la Ley 19.628 por expreso mandato de ésta.

2. Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional

El ordenamiento jurídico chileno, con anterioridad a la actual Constitución de 1980, no contemplaba dentro de las garantías constitucionales el derecho a la vida privada, o al honor. En esta misma línea se enmarcaba la Constitución anterior de 1925 que reconocía como garantías, entre otras, la inviolabilidad del hogar y la inviolabilidad de la correspondencia epistolar y telegráfica (Arts. 12 y 13 respectivamente). Por lo tanto, sólo en la Carta de 1980 se reconoce por el Constituyente chileno la garantía del respeto y protección a la vida privada de las personas así como al honor de ésta y de su familia.

La Constitución chilena, a diferencia de otras latinoamericanas, no contempla ninguna disposición relativa a la protección de los datos personales ni tampoco alguna que reconozca la acción de hábeas data [214] . A pesar de esta carencia, la Carta Fundamental chilena establece dentro del Capítulo III "De los Derechos y Deberes Constitucionales", en el artículo 19 que: *"La Constitución asegura a todas las personas: (…) 4º El respeto y protección de la vida privada y pública y a la honra de la persona y su familia*".

A partir de la disposición anterior se ha entendido que se garantiza no sólo el

[214] Se ha planteado una discusión en la doctrina chilena en torno a la conveniencia o no de modificar el texto constitucional para adicionar el hábeas data. En contra de una eventual modificación se manifiesta Pfeffer, para quien basta con una ley receptora de los principios elementales del tratamiento de los datos personales, como los establecidos en la derogada LORTAD española, e instrumentar su tutela a través del recurso de protección. En este mismo sentido se pronuncia Benítez. Para Verdugo, tampoco es imprescindible una regulación constitucional. A favor de una consagración constitucional del hábeas data, se ha pronunciado Humberto Nogueira, quien señala que resulta imperioso reformar la Constitución con el fin de establecer el núcleo esencial del derecho a la autodeterminación informativa, pues si bien éste es posible deducirlo en la actualidad a través de otros derechos reconocidos por ésta, no estaría tutelado por el recurso de protección (Art. 20 C.P.R.) y más aún, sería del todo inconveniente que se tutelara por esta vía, pues el ejercicio del hábeas data no debe estar sujeto a caducidad, ni tener los mismos efectos que una sentencia de protección. Todo lo anterior en Puccinelli, *op. cit.*, págs. 338 y 339.

derecho a la vida privada y al honor, sino que también el derecho a la intimidad de las personas [215] . A renglón seguido, el numeral 5º del artículo 19 asegura a todas las personas "*la inviolabilidad del hogar y de toda forma de comunicación privada*". En estos dos numerales, especialmente en el Nº 4, se ha fundamentado la protección de los datos personales en Chile, en el entendido que "la intimidad y la privacidad son valores esenciales del ordenamiento jurídico, forman parte de los derechos humanos, y son una premisa de libertad (…)" [216] .

Luego en el artículo 20, el Constituyente consagra el mecanismo procesal (acción) para hacer efectivos los derechos y garantías constitucionales denominado inexactamente como 'recurso de protección', el cual tiene por finalidad *"restablecer el imperio del derecho y asegurar la debida protección del afectado"* para los casos en que cualquier persona sufra privación, perturbación o amenaza en el legítimo ejercicio de los derechos y garantías que la Constitución enumera exhaustivamente. Entre éstos, se encuentra el derecho a la vida privada y pública y, a la honra de la persona y su familia, así como también la inviolabilidad del hogar y de toda forma de comunicación privada [217] .

Siguiendo con el análisis constitucional, cabe hacer presente que el texto chileno en el artículo 5º inciso 2º, establece como límites al ejercicio de la soberanía "*el respecto a los derechos esenciales que emanan de la naturaleza humana*", agregando luego que: "*Es deber de los órganos del Estado respetar y promover tales derechos, garantizados en esta Constitución, así como por los tratados internacionales ratificados por Chile y que se encuentren vigentes*". Este precepto es de crucial importancia, pues incorpora al ordenamiento jurídico chileno la normativa de Derecho Internacional, especialmente en lo relativo a los Tratados sobre Derechos Humanos. Explicando la consecuencias de tal normativa, el profesor Nogueira señala que "(…) la Constitución establece en el artículo 5º inciso 2º, en forma expresa, dos modalidades de institucionalización de derechos

[215] En este sentido Nogueira Alcalá, quien señala que: "La vida privada en un círculo o ámbito más profundo lleva al concepto de intimidad (…) El derecho a la privacidad comprende el derecho a la intimidad que tiene un carácter más estricto y dimensión individual que abarca como aspectos básicos la concepción religiosa e ideológica, la vida sexual, el estado de la salud, la intimidad corporal o pudor, entre otros". En *"El Derecho a la Privacidad y a la Intimidad en el Ordenamiento Jurídico Chileno"*. Revista Ius et Praxis, Universidad de Talca, año 4 Nº 2, Talca, 1998, pág.68.

[216] Esto es lo que sostiene Viera-Gallo, uno de los Diputados redactores del texto de la Ley de Protección de Datos Personales, encomendado por la Comisión de Constitución, Legislación y Justicia de la Cámara de Diputados. En Viera-Gallo, José: *"Fundamentos y Características del Hábeas Data en Chile"* Revista Ius et Praxis, Universidad de Talca, año 3 Nº 1, Talca, 1997, pág. 197.

[217] En cuanto a la procedencia de la acción de protección para salvaguardar la protección de los datos personales, en nuestra opinión, su aplicación habría quedado restringida a los casos no contemplados por la Ley 19.628 o en su defecto, en los casos en que el procedimiento de reclamación ante el juez civil no sea el más rápido y efectivo remedio para proteger las garantías de la vida privada e intimidad, que ciertamente subyacen en la ley chilena de protección de datos personales. Para fundamentar esto último, nos basamos en el artículo 25 de la Convención Americana de Derechos Humanos el cual señala que: "*Toda persona tiene derecho a un recurso sencillo y rápido o a cualquier otro recurso efectivo ante los jueces o tribunales competentes, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la Constitución, la ley o la presente Convención, aun cuando tal violación sea cometida por personas que actúen en ejercicio de sus funciones oficiales".*

esenciales o humanos, la propia norma constitucional y el tratado internacional; siendo esta última la modalidad que permite incorporar a la constitución material los derechos esenciales o humanos que no están expresamente contenidos en el texto constitucional, o no se hayan incorporado formalmente a ella a través del procedimiento de reforma de la Constitución.(…)" [218] .

Finalmente, en materia constitucional el artículo 19 Nº 26 señala que se asegura a todas las personas que los preceptos legales que por mandato constitucional regulen o complementen las garantías que ésta establece, o aquéllos que las limiten en los casos autorizados por el constituyente, *"no podrán afectar los derechos en su esencia, ni imponer condiciones, tributos o requisitos que impidan su libre ejercicio*". Por lo tanto, se establece un límite al legislador, quien no podrá afectar la esencia de los derechos, ni impedir el libre ejercicio de éstos a través de condiciones, tributos o requisitos sin caer en inconstitucionalidad.

En suma, Chile no cuenta con un precepto constitucional que consagre el derecho a la protección de datos personales o autodeterminación informativa, ni su tutela a través de la acción de hábeas data. No obstante, a partir de la configuración del derecho a la vida privada y consecuencialmente al derecho a la intimidad, se ha fundamentado la protección de los datos personales, lo cual se plasma en la ley respectiva que luego se analizará.

2.2 Protección Legal de los Datos Personales

La protección legal de los datos personales en Chile, se concreta sólo a partir del 28 de agosto de 1999, fecha en la cual se publica en el Diario Oficial la Ley Nº 19.628 de Protección de Datos de Carácter Personal, la cual estuvo tramitándose desde el año 1993. Esta ley vino a llenar un gran vacío en el ordenamiento jurídico chileno, el cual ya se había hecho notar a mediados de la década de los ochenta.

La ley chilena si bien no responde plenamente a los estándares europeos en materia de protección de datos, en particular a la Directiva de 1995 -pues hace suya sólo parte de esa normativa-, al menos es un avance en la materia. Con todo, el hecho de seguir el legislador en parte un modelo y en otras apartarse de éste dando soluciones de carácter local, hace que la regulación adolezca de una falta de sistemática y, de todo ello resulte una normativa poco consistente, sobre todo en materia de principios, lo que se podrá apreciar con claridad más adelante. La configuración original ya ha tenido su primer acomodo en virtud de la modificación legal del 13 de Junio de 2002 (Ley Nº 19.812).

Por otra parte, y siguiendo dentro del ámbito legal, debemos señalar que también existen normas sectoriales relacionadas con la protección de datos personales. De éstas destacan la Ley General de Bancos, la cual establece el secreto bancario; el Código

[218] Nogueira Alcalá, Humberto: *"Las Constituciones y los Tratados en Materia de Derechos Humanos: América Latina y Chile"*. En Revista Ius et Praxis, Universidad de Talca, año 6 N º2, Talca, 2000, págs. 238 y 239. Cabe hacer presente que dentro de los tratados internacionales sobre Derechos Humanos ratificados por Chile se encuentran, entre otros la Convención Americana sobre Derechos Humanos (Diario Oficial 5 Enero 1991) y el Pacto Internacional de Derechos Civiles y Políticos de 1966 (Diario Oficial 29 de Abril 1989).

Tributario, que consagra el secreto fiscal o tributario, el Código Sanitario, que instituye el carácter de confidencial de las recetas médicas y exámenes de laboratorio y, el Código del Trabajo, el cual establece dos reglas; una de no discriminación de los trabajadores en base a sus antecedentes comerciales y, otra que obliga al empleador a mantener en reserva los datos privados del trabajador a que tenga acceso con ocasión de la relación laboral.

2.2.1) La Ley 19.628 sobre Protección de Datos Personales y sus antecedentes

En lo relativo a los antecedentes de la ley chilena, y siguiendo la exposición del profesor Suárez, podemos señalar que es posible constatar a lo menos cuatro etapas de intentos por regular la protección de datos personales [219] . A continuación se señalan tales momentos.

Una primera etapa la configuran los proyectos presentados durante el gobierno militar a partir de la segunda mitad de la década de los ’80. Entre éstos, destaca un anteproyecto de ley informática elaborado por una Comisión del Ministerio de Justicia presidida el señor Eduardo Hajna. Este anteproyecto luego se remitió para su análisis a diversas organizaciones relacionadas con la materia. Sobre la base de las respuestas recibidas “se elaboró en septiembre de 1986, el primer proyecto de ley informático realizado en Chile. Sin embargo, el proyecto fue sometido a sucesivas revisiones, que dieron lugar a nuevas versiones del mismo en abril de 1986, febrero de 1987, mayo de 1987 y junio de 1988. (…) Estos proyectos que contenían ya gran parte de los aspectos definitorios de las leyes de protección de datos, no derivaron nunca, pese a ello, en textos legales positivos” [220] .

La segunda etapa estaría conformada por el proyecto elaborado por la Comisión nombrada por el Ministro de Justicia -Francisco Cumplido-, bajo el mandato del Presidente Aylwin, a comienzos de la década de los ’90. Este proyecto- según cuenta el propio Cumplido- se denominó “Regulación Legal de la Informática”, y su objeto fue “regular la utilización de sistemas informáticos, de técnicas y medios de tratamiento automatizado y manuales, para la recolección, procesamiento, custodia, transmisión y

[219] En cuanto a estas etapas es preciso tener presente que la exposición del autor citado se realizó en el año 1997, dentro del seminario organizado por la Universidad de Talca denominado *“Derecho a la autodeterminación informativa y acción de Hábeas data en Iberoamérica”.*

[220] Lo anterior en Suárez Crothers, Christian: *“Informática, Vida Privada y los Proyectos Chilenos sobre Protección de Datos”*, en Revista Ius et Praxis, Universidad de Talca, Año 3 Nº 1, Talca, 1997, págs. 349-350. Agrega este autor que entre las dificultades que tuvo la materialización de estos proyectos, “se encuentra, probablemente, el intento por parte de las comisiones constituidas durante el régimen militar de resolver, en un solo cuerpo legal, todos los aspectos relativos a la informática; esto es, la regulación de aspectos tan variados como el delito informático, la regulación del software y el hardware, la modificación del sistema chileno de pruebas y la protección de la libertad informática. (…) La principal crítica que puede formularse a este proyecto se debe a la ausencia de disposiciones destinadas a establecer una autoridad de control de las bases de datos constituidas por el sector público o los particulares, situación que habría ocasionado un menoscabo en el ejercicio de los derechos por parte de las personas afectadas” (*Ídem*, págs. 350 y 351).

difusión de los datos personales" [221] . Éste seguía de cerca a la derogada Ley Orgánica sobre Regulación del Tratamiento Automatizado de Datos española (LORTAD), no obstante, presentaba el inconveniente de excluir del ámbito de aplicación de la ley a las bases de datos de las Fuerzas Armadas y a los registros policiales y de inteligencia, los cuales se regirían por sus estatutos propios [222] .

La tercera etapa, según Suárez, estaría dada por la moción original planteada por el Senador Cantuarias junto con las modificaciones que sufrió esa iniciativa de ley. Esta etapa se inicia el día 5 de enero de 1993, en el cual se presenta la moción de dicho Senador [223] con la que se inicia un proyecto de ley sobre protección de la vida privada. El proyecto buscaba crear un Código o estatuto jurídico de la privacidad. Los antecedentes de éste, según la misma moción, se encontraban fundamentalmente en: 1) La Ley Orgánica Nº 1 española, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen; 2) En la ley francesa de informática, ficheros y libertades de 1978 y, 3) En las leyes de protección de datos de Noruega (1978), Gran Bretaña (de 1984), entre otros textos. De éstos se citan el Código Civil argentino y el Código Civil francés [224] .

221 Cumplido Cereceda, Francisco: *"Análisis del Anteproyecto de Ley sobre Protección de datos Personales elaborado por el Ministerio de Justicia (1990-1994)"* en Revista Ius et Praxis, Universidad de Talca, 1997, pág. 202. Agrega el ex Ministro de Justicia chileno que: "Nosotros estudiamos el tema y preparamos un proyecto que enviamos al Ministerio Secretaría General de la Presidencia, eso sí que en noviembre del año 1993, de manera que no alcanzó a ser procesado. Además, contenía gastos, porque, después de mucho analizar los sistemas comparados, tanto euroatlánticos como el sistema latinoamericano y también el norteamericano, llegamos a la conclusión de que, para que pudiera ser efectiva y real la protección de los datos personales, era indispensable establecer un servicio del Estado que contribuyera a la protección de esos datos personales. Naturalmente, el servicio de protección de datos que se proponía en el proyecto y el Registro Conservador o Registro de Datos, implicaba un gasto que llegaba en ese momento alrededor de 300 millones de pesos y, en consecuencia, requería la aprobación de Hacienda. Y ustedes saben que en Chile una de las grandes limitaciones a la creatividad legislativa, tanto del gobierno como de los parlamentarios, es el Ministerio de Hacienda" (*Ídem*, págs. 201 y 202)

222 Suárez Crothers, Christian, *op. cit.,* pág. 351. Relacionado con esta situación, y comentando el fallido Proyecto de Ley que patrocinó el gobierno del Ex Presidente Aylwin, Francisco Cumplido ha señalado que: "uno se pregunta por qué el gobierno militar preparó dos proyectos sobre la materia y ninguno llegó a concretarse, con la velocidad con que era posible concretar los proyectos de decretos leyes o leyes posteriores (decretos leyes llamados leyes), y por qué tuvimos, en verdad, tremendas dificultades para redactar este proyecto. Para hacerlo tuvimos que pedirle opinión a todos los servicios públicos, que tenían de alguna manera relación con la recolección de datos, y entre otros, por supuesto, a las Fuerzas Armadas y de Orden. Ocurrió algo muy curioso: una especie de tendencia a no informar sobre lo que se tenía, no sólo, y a lo mejor lo que es propio de Fuerzas Armadas, Carabineros, Policía de Investigaciones, Gendarmería y Dirección de Seguridad Pública, sino que también de las instituciones públicas civiles como por ejemplo el Servicio de Impuestos Internos. No los dependientes de Justicia porque dependían del Ministro, de manera que en ese caso la información llegó rápidamente. Entonces yo me explico que hay una resistencia por parte de los servicios públicos, civiles y militares, y también por supuesto, intereses de las empresas en relación con la materia. Y esta presión hace que estos proyectos sean de difícil aprobación" (*op. cit*, pág. 203).

223 Boletín Nº 896-07.

224 *Ídem*, pág. 352.

La moción constaba de 26 artículos los cuales en su mayoría estaban dirigidos a regular la protección de los datos personales. Según Suárez, eran pocas las disposiciones que se encaminaban al establecimiento del estatuto de la vida privada, "no obstante que avanzaba en algunos sentidos al concebir la vida privada como comprensiva de, a lo menos, cuatro bienes jurídicos a los que se estima dignos de protección. Esto es (artículo 2º): a) el derecho a la propia imagen; b) el derecho a la intimidad personal y familiar; c) el anonimato y reserva; d) el derecho a una vida tranquila, sin hostigamientos ni perturbaciones y d) el derecho a la inviolabilidad del hogar y de toda forma de comunicaciones privadas (sic)" [225] .

En suma, si bien el proyecto tuvo la virtud de iniciar la discusión sobre el tema de la protección de datos, era muy imperfecto y sujeto a toda clase de correcciones [226] .

En cuanto a las modificaciones sustanciales que sufre el Proyecto Cantuarias en la Cámara de Diputados, éstas son fruto de la elaboración de un nuevo texto encomendado a los Diputados Ferrada y Viera-Gallo por la Comisión de Constitución, Legislación y Justicia de la Cámara baja. La tarea de los parlamentarios era redactar un texto que se abocara directamente a regular la protección de las personas frente al tratamiento automatizado de sus datos personales. Ese texto fue el que sirvió de base directa a la actual ley de protección de datos personales.

La cuarta etapa estaría relacionada con el giro que toma la Moción Cantuarias durante su discusión en la Comisión respectiva de la Cámara de Diputados, el análisis de ésta y su posterior remisión al Senado [227] . En relación con el texto legal aprobado, puede señalarse que éste consta de un Título Preliminar de "Disposiciones Generales",cinco títulos [228] y un Título Final de Disposiciones transitorias.

Desde la aprobación de la ley chilena por el Congreso Nacional y su posterior

[225] *Ídem*, págs. 352-353. Una de las críticas que hace Suárez al proyecto que se remitió por el Senado a la cámara de Diputados dice relación con "cierta falta de comprensión respecto a que el bien jurídico protegido a través de las técnicas de protección de datos no se reduce exclusivamente al derecho a la vida privada. Queda claro de la sentencia del Tribunal Constitucional alemán, recaída sobre la Ley del Censo de 1983, que basta con la presencia de datos absolutamente aislados, que no digan relación alguna con la intimidad, para que la lesión al derecho de autodeterminación informativa pueda producirse a consecuencia de la vinculación de estos datos y de la construcción de un perfil del individuo que no corresponde a su personalidad. Ha sido ampliamente demostrado que la tendencia seguida por algunas legislaciones, como la norteamericana y la italiana, consistente en subsumir bajo la figura de la *privacy* o de la *riservatezza*, el conjunto cada vez más amplio de atentados posibles en contra del derecho a la intimidad, conduce inevitablemente a un desperfilamiento cuantitativo y cualitativo de las figuras jurídicas que sirven de marco a este procedimiento". Esta apreciación tiene el valor de ser no sólo aplicable al aludido proyecto, sino que también en parte al texto definitivo de la Ley 19.628 de 1999 (*op. cit*., págs. 354 y 355).

[226] *Ídem*, pág. 356.

[227] *Ídem*, pág. 350.

[228] Estos títulos respectivamente la ley los denomina: *"De la utilización de datos personales"; "De los derechos de los titulares de datos"; "De la utilización de los datos personales relativos a las obligaciones de carácter económico , financiero, bancario o comercial";"Del tratamiento de datos por los organismos públicos"; y, "De la responsabilidad por las infracciones a esta ley".*

entrada en vigencia, ésta ha sido objeto de diversas críticas. Algunas de ellas lograron movilizar al Congreso Nacional, el cual aprobó una modificación legal el año 2002. Esta reforma se plasmó en la Ley Nº 19.812, la que junto con beneficiar a un gran número de deudores morosos que figuraban en las bases de datos de las instituciones de información comercial (a través de la caducidad de los datos comerciales negativos a la entrada en vigencia de la modificación legal), redujo los plazos durante los cuales podía informarse de los incumplimientos comerciales por parte de los responsables de los registros o de los bancos de datos. La modificación acortó de 7 a 5 años el plazo para informar obligaciones impagas, contados desde que éstas se hayan hecho exigibles (Art. 18 inciso primero). En el caso que la obligación fuere pagada o extinguida por otro modo legal, no se podrá continuar comunicando la situación de morosidad en que se incurrió (Art. 18 inciso 2º). La modificación legal también elevó las multas por infracción a ciertas disposiciones de la ley. Como ya se adelantó, además de modificarse la propia Ley de Protección de Datos de Carácter Personal, se introdujo una nueva norma en el Código del Trabajo que busca evitar la discriminación de quienes busquen trabajo y tengan antecedentes comerciales negativos.

Finalmente, cabe señalar que en la actualidad existen varios Proyectos de Ley en la materia. Uno de éstos pretende modificar la Ley 19.628; ampliando la aplicación de ésta en lo relativo a los informes comerciales, a las personas jurídicas del artículo 545 del Código Civil (Moción Tuma y Elgueta, Boletín Nº 2474-07, de 15 de Marzo de 2000). Otro, busca introducir el concepto de uso indebido o abusivo de datos (Moción del Diputado Navarro, Boletín Nº 3095-07, de 15 de Octubre de 2002). Por otro lado, existe un Proyecto que pretende establecer normas sobre comercialización y publicidad por medio de redes de telecomunicaciones e Internet (Moción del Diputado Navarro, Boletín Nº 3094-19, de 15 de Octubre de 2002). También existe un Proyecto de Ley sobre privacidad de los datos recolectados a través de Internet (Boletín Nº 3003-19, de Julio de 2002) [229] .

2.2.2) Otras normas Legales Relacionadas con la Protección de Datos Personales

En el ordenamiento jurídico chileno pueden encontrarse diversas normas jurídicas que dicen relación con la protección de datos personales. A continuación analizaremos algunas de éstas.

2.2.2.1) Código Sanitario

El artículo 127 de este cuerpo legal dispone que: *"Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados"* y sólo puede revelarse el contenido o darse copia de ellos *"con el consentimiento expreso del paciente, otorgado por escrito".* Luego agrega que: *"en ningún caso la información*

[229] Estos Proyectos de Ley son los que consideramos directamente relacionados con la protección de datos personales. Puede agregarse a éstos una moción parlamentaria que pretende constituirse en ley, y que establece la comunicación al boletín comercial de los incumplimientos graves de deudas alimenticias, Boletín Nº 2600-18, 12 de Octubre de 2000.

que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expendieron, ni datos que sirvan para identificarlos". También prescribe esta norma que la reserva no obsta para 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 [230] . La violación de lo prescrito por este artículo, será castigado en la forma y con las sanciones establecidas en el Libro Décimo de ese Código [231] .

En nuestra opinión, es claro que el carácter reservado de las recetas y exámenes médicos o de laboratorios, es consecuencia del mandato legal que incluye dentro de la categoría de datos sensibles a toda aquella información relacionada con "los estados de salud físicos o síquicos" (Art. 1º, letra g, Ley 19.628). Lo anterior, se basa en el hecho que tanto las recetas médicas, como los resultados de exámenes o análisis de laboratorio proporcionan información de la cual se puede deducir con mayor o menor facilidad, el estado físico o psíquico de las personas. Por lo tanto, esta disposición reafirma la normativa legal de protección de datos y tiende impedir la recolección y el tratamiento de los datos sensibles, lo que por regla general está prohibido (Art. 10 Ley 19.628).

2.2.2.2) Código Tributario

El artículo 30 inciso 4º del Código Tributario prescribe que: *"las personas que, a cualquier título, reciban o procesen las declaraciones o giros quedan sujetas a obligación de reserva absoluta de todos aquellos antecedentes individuales de que conozcan en virtud del trabajo que realizan. La infracción a esta obligación será sancionada con reclusión menor en su grado medio y multa de 5 a 100 UTM"*. Esta disposición establece el denominado secreto tributario o fiscal, el cual resguarda las informaciones relativas a los ingresos de los contribuyentes. En suma, toda persona que reciba o procese declaraciones relativas a impuestos o procese los giros efectuados por el Servicio de Impuestos Internos, está afecto a la obligación de reserva absoluta de toda la información conocida en virtud del trabajo realizado. En este caso, la norma no sólo es aplicable a los funcionarios del señalado Servicio sino que a también a los particulares que toman conocimiento de tales informaciones al recibir y procesar tales declaraciones tributarias, como lo son por ejemplo, los funcionarios bancarios que reciben tales documentos.

2.2.2.3 Ley General de Bancos

El inciso primero del artículo 154 de la Ley General de Bancos [232] , dispone que: *"Los depósitos y captaciones de cualquiera naturaleza que reciban los bancos están sujetos a secreto bancario y no podrán proporcionarse antecedentes relativos a dichas operaciones sino a su titular o a quien haya sido expresamente autorizado por él o a la persona que lo*

[230] Estas disposiciones fueron introducidas por el artículo 24 de la Ley 19.628.

[231] Las sanciones establecidas por el Código se indicarán más adelante en el punto Nº 9 de este análisis.

[232] El texto de esta ley se encuentra en el DFL Nº 3 del Ministerio de Hacienda, año 1997, que fija el texto refundido, sistematizado y concordado de la Ley General de Bancos y otros cuerpos legales, Diario Oficial, 19 de Diciembre 1997.

represente legalmente. El que infringiere la norma anterior será sancionado con la pena de reclusión menor en sus grados mínimo a medio". Por lo tanto, la infracción a este deber de secreto es constitutiva de delito penal.

Luego el inciso 2º de esa disposición señala que: *"Las demás operaciones quedan sujetas a reserva y los bancos solamente podrán darlas a conocer a quien demuestre un interés legítimo y siempre que no sea previsible que el conocimiento de los antecedentes pueda ocasionar daño patrimonial al cliente"*. Agrega el legislador en este mismo inciso que, no obstante lo anterior, y a objeto de evaluar la situación del banco, *"éste podrá dar acceso al conocimiento detallado de estas operaciones y sus antecedentes a firmas especializadas, las que quedarán sometidas a la reserva establecida en la ley y, siempre que la Superintendencia las apruebe e inscriba en el registro que abrirá para estos efectos".*

El inciso tercero del artículo 154, dispone por otra parte que: *"en todo caso, los bancos pueden dar a conocer las operaciones señaladas en los incisos anteriores, en términos globales, no personalizados ni parcializados, sólo para fines estadísticos o de información cuando exista un interés público o general comprometido, calificado por la Superintendencia".* Al respecto, debemos hacer presente que la Superintendencia de Bancos e Instituciones Financieras, en la Circular para Bancos Nº 2.544 de 8 de junio de 1990, ha señalado en relación a las informaciones que soliciten las instituciones del sector público a los bancos, que si bien aquellas instituciones se encuentran en la situación excepcional recién señalada cuando se requiera tal información para fines relacionados con la actividad que desarrollen, todas las peticiones de información que se hagan a los bancos e instituciones financieras deben ser canalizadas a través de la Superintendencia, a efecto de la calificación de la relación entre el antecedente solicitado y la función de la institución pública que pide la información [233] .

Siguiendo con las excepciones al secreto bancario, el inciso 4º del artículo 154, dispone que: *"la justicia ordinaria y la militar, en las causas que estuvieren conociendo, podrán ordenar la remisión de aquellos antecedentes relativos a operaciones específicas que tengan relación directa con el proceso, sobre los depósitos, captaciones u otras operaciones de cualquier naturaleza que hayan efectuado quienes tengan carácter de parte o inculpado o reo en esas causas u ordenar su examen, si fuere necesario"*.

Finalmente, cabe anotar que mediante la Ley Nº 19.806 de 31 de Mayo de 2002, se agregó un nuevo inciso final al artículo 154, el cual se aplica sólo en aquellas regiones en donde se encuentra vigente la reforma procesal penal. Este nuevo inciso señala que: *"los fiscales del Ministerio Público, previa autorización del juez de garantía, podrán asimismo examinar o pedir que se les remitan los antecedentes indicados en el inciso anterior, que se relacionen directamente con las investigaciones a su cargo".*

Llama la atención que el legislador haya dejado la puerta abierta en el inciso segundo del artículo 154 de la Ley de Bancos, para que un tercero pueda imponerse de aquellas operaciones bancarias que no correspondan a depósitos y captaciones de cualquiera naturaleza (*a contrario sensu* de lo preceptuado por el inciso primero), cuando

[233] La Circular anterior puede ser consultada [en línea] < http://www.sbif.cl/NormasSBIF/Bancos/C2544B.pdf > [consulta: 9 de Mayo 2003]

la entidad bancaria estime que se ha demostrado un interés legítimo por el tercero y no sea previsible que el conocimiento de los antecedentes pueda ocasionar daño patrimonial al cliente. Es decir, por esta vía, es posible que puedan conocerse datos personales relacionados con las operaciones bancarias, quedando al sólo criterio del banco determinar cuando se reúnen los requisitos legales. Estimamos que en esta materia la ley debiera ser más clara y no dejar entregado a juicio de quien tiene el deber de secreto el decidir cuando opera la excepción y cuando no. Con todo, creemos que al señalar la ley como directiva calificadora para la operatividad de la excepción, el que no sea previsible el "daño patrimonial del cliente", estaría indirectamente desconociendo un interés cuyo daño puede ser aún más grave que el solo daño patrimonial, este es el daño moral que previsiblemente puede causarse al cliente, al revelar datos diversos a los depósitos o captaciones. Ejemplo de ello podría ser una comisión de confianza a un banco para que éste ejerza la curaduría de ciertos bienes de un incapaz, cuya identidad, y negocios no se quiere sea conocida por terceros (Art. 86 Ley de Bancos).

2.2.2.4 Código del Trabajo

El Código del Trabajo chileno fue objeto de modificaciones legales el año 2001 (Ley 19.579) y el año 2002 (Ley Nº 19.812) en materia de protección de los derechos de los trabajadores, los cuales se relacionan a su vez con la protección a los datos personales de éstos.

Las modificaciones legales introducidas por la Ley 19.579 de fecha 5 de Octubre de 2001, tuvieron por finalidad introducir normas relativas a las nuevas modalidades de contratación, al derecho de sindicación y, a los derechos fundamentales de los trabajadores. Dentro de este último ámbito, agregó el artículo 154 bis el cual dispone que: *"El empleador deberá mantener reserva de toda la información y datos privados del trabajador a que tenga acceso con ocasión de la relación laboral"*. Dicha norma, establece un deber de conducta por parte del empleador, el cual está obligado a mantener en reserva toda información y datos privados del empleador a los cuales ha tenido acceso con ocasión de la relación de trabajo. En este sentido, la norma exigiría la existencia previa de relación laboral para los efectos de que exista la obligación de reserva por parte del empleador. La disposición anterior claramente viene a reforzar la normativa de protección de datos personales, regida por la Ley 19.628.

Por su parte, la Ley 19.812 que modificó el Código del Trabajo, tuvo por finalidad de evitar todo acto de discriminación en contra de los trabajadores, a causa de sus antecedentes comerciales negativos. Al respecto, el legislador chileno señala que: *"ningún empleador puede condicionar la contratación de trabajadores a la ausencia de obligaciones de carácter económico, financiero, bancario o comercial que, conforme a la ley, puedan ser comunicadas por los responsables de registros o bancos de datos personales; ni exigir para dicho fin declaración ni certificado alguno. Exceptúanse solamente los trabajadores que tengan poder para representar al empleador, tales como gerentes, subgerentes, agentes o apoderados, siempre que, en todos estos casos, estén dotados, a lo menos, de facultades generales de administración; y los trabajadores que tengan a su cargo la recaudación, administración o custodia de fondos o valores de cualquier naturaleza"* (Art. 2º inciso 6º C. del Trabajo).

Si bien estimamos acertada la inclusión de la norma recién señalada dentro del Código del Trabajo, no compartimos que las sanciones administrativas aplicables a esos casos se rijan por al régimen general establecido en el artículo 477 del Código del ramo, el cual dispone que: *"Las infracciones a este Código y a sus leyes complementarias, que no tengan señalada una sanción especial, serán sancionadas con multa de una a veinte unidades tributarias mensuales, según la gravedad de la infracción".* El *quantum* de estas multas se eleva dependiendo de la cantidad de trabajadores que laboren en la empresa infractora, pudiendo llegar hasta las sesenta U.T.M, cuando ésta tenga más de 200 trabajadores. Creemos que debió el legislador establecer sanciones específicas que realmente signifiquen un disuasivo para aquellos empleadores que discriminen a los postulantes a un cargo de trabajo, pues a nuestro modo de ver resulta una torpeza calificar la idoneidad laboral de las personas en base a sus antecedentes comerciales, sin tener en cuenta las razones de esos incumplimientos. Aún más, si se cierran las puertas de trabajo a las personas que lo necesitan con urgencia para así salir de una situación económica agobiante, no nos cabe duda que estamos además frente a una acción reprochable desde el punto de vista moral, que perpetúa el círculo de la pobreza, menoscaba la dignidad de las personas y conlleva a que el trabajo deje de ser un derecho, y pase a ser un premio entregado a quien cumple sus obligaciones o a quien no obstante haber incumplido, dispone de dinero suficiente para 'aclarar' ante la Cámara de Comercio la morosidad una vez que ha pagado la deuda [234] .

3. Bienes Jurídicos Protegidos por la Legislación de Datos Personales

Dilucidar el o los bienes jurídicos protegidos por la legislación sobre protección de datos personales no es tarea fácil en el sistema jurídico chileno, pues cobra relevancia toda la discusión doctrinal en la materia, que en último término tiene su base en la Constitución Política de 1980.

El rango dentro del cual se mueven la doctrina y parlamentarios que discutieron la ley, va desde considerar como bien jurídico protegido a la vida privada, la intimidad, el honor, e incluso un derecho a la identidad, hasta postular directamente que se estaría frente a un derecho implícito, el denominado derecho a la autodeterminación informativa.

A este respecto y como ya lo señalamos más arriba, para Viera-Gallo la intimidad y la privacidad serían los valores esenciales del ordenamiento jurídico, que resguardan la autonomía y la libertad. Dentro de la doctrina, Vial Claro señala que el honor, la imagen y la intimidad serían el objeto de protección de la Ley 19.628 [235] . Por su parte, Vásquez ha

[234] Sería interesante estudiar la naturaleza jurídica de la tarifa o precio que deben pagar los deudores que acuden ante las oficinas de la Cámara de Comercio para que sus datos de incumplimiento sean borrados de las bases de datos respectivas. Lo anterior no es por simple curiosidad, pues atendido el carácter progresivo que tiene el precio de 'quedar limpio', podría eventualmente sostenerse que ese precio actuaría como una especie de sanción encubierta.

[235] Vial Claro, Felipe: *"La Ley Nº 19.628 sobre Protección de Datos de Carácter Personal una Visión general"*. En Cuadernos de Extensión Jurídica, Universidad de Los Andes, Nº 5, Santiago, 2001, pág. 28.

dicho que la ley de protección de datos ampara "el derecho a la intimidad o a la privacidad en lo relativo a la información o a los datos sobre las personas" [236] . Mendoza, indica que es claro que la fuente constitucional de la ley de protección de datos chilena es "la vida privada", cuestión que además se desprende de la propia denominación de la ley [237] . Para Corral Talciani, si bien en parte los derechos de la Ley 19.628 son formas de aplicación del derecho general al respeto a la vida privada, por otro lado también se resguarda con esas normas el "derecho a la identidad", que no está contemplado como tal en el artículo 19 Nº 4 de la Constitución, pero que puede tener cabida en la alusión al respeto de la "vida pública" [238] .

Para el profesor de la Universidad de Chile, Francisco González, al consagrar la Constitución la garantía de la protección de la vida privada de las personas, "se está refiriendo precisamente a la intimidad, en el sentido en que emplea actualmente este término el derecho continental, esto es, incluyendo las facultades de exclusión y control" [239] . En un sentido similar, el profesor Carlos Carmona indica que "el derecho a la vida privada que consagra nuestra Constitución comprende lo que la doctrina denomina el derecho a la autodeterminación informativa" [240] .

Finalmente, citaremos al profesor de la Universidad de Talca, Humberto Nogueira, quien ya señalaba en 1997 que "el proyecto de ley en tramitación parlamentaria en la Cámara de Diputados busca asegurar un derecho fundamental no contemplado explícitamente en el texto de nuestra Constitución, el que sólo puede deducirse de otros derechos asegurados y de los derechos reconocidos por los tratados internacionales ratificados por el Estado de Chile y vigentes" [241] . El derecho al cual se refiere este autor

[236] Vásquez Márquez, José Ignacio: *"Análisis Crítico Sobre la Naturaleza Jurídica de la Ley de Protección de la Vida Privada"*, en Revista de Derecho Universidad Finis Terrae, año III, Nº 3, 1999, pág. 47.

[237] Mendoza Zúñiga, Ramiro Alfonso: *"Régimen de los Bancos de datos de organismos Públicos. Una Aproximación del Derecho Administrativo a la Ley Sobre Protección de la Vida Privada"*. En Cuadernos de Extensión Jurídica, Universidad de los Andes, Nº 5, Santiago, 2001, pág. 136.

[238] Corral Talciani, Hernán, en *"Cuadernos de Extensión Jurídica"* Universidad de los Andes, Nº 5, Santiago, 2001, págs. 58 y 59.

[239] González Hoch, Francisco, *op cit*. pág. 156. Agrega González que en la doctrina comparada, aún subsiste el debate en torno a determinar si ha surgido un nuevo derecho fundamental o de la personalidad (derecho a la autodeterminación informativa o libertad informática), o simplemente constatar si en la protección de la intimidad informática, no habría sino la tutela de derechos de la personalidad ya formulados, tales como la intimidad, el honor, o vida privada. Luego señala que independiente de la aceptación o no acerca de la teoría de la autodeterminación informativa, lo que importa es que de toda la discusión, el concepto de intimidad, integrado por las dos facetas; exclusión (libertad negativa) y control (libertad positiva), ha salido fortalecido y rejuvenecido. En *op. cit.*, págs. 154 y 156.

[240] El fundamento de tal afirmación es nuevamente el concebir al derecho a la vida privada integrado por las dos facetas ya señaladas; la idea de exclusión y la idea de control. Luego reafirma lo ya señalado -citando a Nogueira- diciendo que habría surgido un derecho implícito derivado de las libertades negativas, denominado autodeterminación informativa. En Carmona Santander, Carlos, *"Protección de datos personales-Ley 19.628"*. [En línea] < http://www.derechoenlinea.cl/index1.html > [consulta: 28 de Noviembre 2002].

es precisamente el derecho a la autodeterminación informativa [242] . Cabe recordar además que Nogueira, es partidario de consagrar constitucionalmente en Chile el derecho a la autodeterminación informativa así como también su garantía jurisdiccional, la razón de ello: "la necesidad de delimitar el núcleo esencial del derecho protegido, garantizándolo ante cualquier desnaturalización o limitación que los órganos instituidos puedan realizar de él bajo pretexto de regularlo (…)" [243] .

En nuestra opinión, creemos que resulta difícil afirmar la existencia de un derecho a la autodeterminación informativa en Chile, pues la historia de la Ley 19.628 nos muestra que el propio legislador, si bien lo tuvo presente en un momento del íter legislativo, finalmente lo desestimó, evitando su expreso reconocimiento como derecho en esta sede [244] . En razón de lo anterior, estimamos que de *lege data* los bienes jurídicos tutelados en nuestro ordenamiento jurídico serían el derecho a la vida privada e intimidad, así como también el honor de las personas, todo ello en razón de lo preceptuado por la ley chilena en base al texto constitucional de 1980. De *lege ferenda,* estimamos que debería renovarse una discusión seria en torno a la autodeterminación informativa como el principal bien jurídico tutelado por la Ley 19.628 y explicitarlo en una reforma a ésta, lo cual previamente debería traducirse en una modificación a la Constitución que reconociera a este derecho y a su garantía específica, de manera distinta a la modalidad de la acción de protección, la cual en la práctica limita la vida de los derechos a sólo 15 días (Numeral 1º, Auto acordado de la Corte Suprema sobre Tramitación del Recurso de Protección de Garantías Constitucionales).

En resumen, no existe unanimidad de parecer en la doctrina chilena para determinar cuál o cuáles serían los bienes jurídicos protegidos por la Ley de Protección de Datos de Carácter Personal. Sí puede constatarse que todos los autores parten de un punto en común: la protección de la vida privada, consagrada en el artículo 19 Nº 4 de la Constitución chilena. Luego, a partir de este punto de convergencia cada autor argumenta a favor de la protección de los datos personales. El extremo del desarrollo argumentativo señala que el bien jurídico protegido sería el derecho a la

241 Nogueira Alcalá, Humberto,1997 *op. cit*, pág. 265.

242 Luego, en otro artículo publicado en la Revista Ius et Praxis, Nogueira señala que "el derecho a la vida privada o a la privacidad comprende en su acepción genérica diferentes manifestaciones clásicas como son la inviolabilidad de hogar y de las comunicaciones privadas aseguradas en el artículo 19 Nº 5 de la Carta Fundamental como el derecho a la honra de la persona y de su familia, contenidas en el artículo 19Nº 4; pero, a su vez, contempla también nuevas dimensiones o manifestaciones del derecho a la privacidad o a la intimidad, que son recogidas en algunas constituciones más recientes de la segunda mitad del siglo XX, como son el derecho a la autodeterminación informativa y la acción de Hábeas Data, el derecho a la propia imagen, para señalar sólo las más significativas". Más adelante, al explicar cómo la autodeterminación informativa forma parte del derecho al respeto de la vida privada dice: "el respeto de la vida privada o intimidad se proyecta en el ámbito de los registros de informaciones manuales e informáticos, que permiten socializar esa información develando ámbitos de la privacidad de las personas. En tal perspectiva, el respeto a la vida privada e intimidad adopta un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona, un derecho a la autodeterminación informativa (…)". En *"El Derecho a la Privacidad y a la Intimidad en el Ordenamiento Jurídico Chileno"*, Revista Ius et Praxis, Universidad de Talca, Año 4 Nº 2, Talca, 1998, págs. 66-67 y 73.

243 Nogueira Alcalá, Humberto, 1997, *op. cit*., págs. 274 y 275.

autodeterminación informativa, el cual se encontraría implícitamente en la Constitución, complementada con los tratados sobre Derechos Humanos ratificados por Chile que se encuentren vigentes. Sin embargo, es necesario tener presente que el propio legislador chileno desechó la posibilidad de reconocer expresamente este derecho durante la tramitación de la Ley 19.628.

4. Principios Informativos de la Legislación de Protección de Datos Personales

El legislador chileno no señaló explícitamente los principios sobre los cuales se ordenará la ley de protección de datos personales. No obstante lo anterior, es posible constatar la presencia de ellos dentro de la normativa chilena con diversa intensidad.

1º. Principio de la licitud y lealtad de los archivos de datos

La Ley 19.628 señala en su artículo 1º que el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares, debe sujetarse a las disposiciones de dicha ley, salvo el tratamiento que se efectúe en ejercicio de las libertades de emitir opinión y de información Se agrega por el inciso 2º del artículo

[244] En efecto, en el segundo trámite constitucional del Proyecto de Ley chileno, la Cámara de Diputados optó por modificar el original artículo 1º aprobado por el Senado en el primer trámite constitucional, en el cual se definía el ámbito de aplicación de la iniciativa. El nuevo artículo 1º, estableció como objetivo de la ley "asegurar el derecho a la autodeterminación informativa de las personas respecto de los datos personales tratados en bancos de datos o registrados en otros soportes, con el fin de garantizar el pleno respeto y ejercicio de los derechos fundamentales". Ante esta nueva redacción, el Poder Ejecutivo hizo ver que si bien el derecho a la autodeterminación informativa es un derecho que ha sido seguido de cerca por los italianos y españoles, incluso por parte de nuestra doctrina (Nogueira y Zúñiga), el tema no era pacífico en la propia Alemania, país en el cual tuvo su consolidación doctrinal este derecho a raíz de la Sentencia del Tribunal Constitucional alemán de 1983 sobre la Ley del Censo. También se adujo por el Ejecutivo, que parte de la doctrina señala que existiría el riesgo de incurrirse en una concepción patrimonialista del nuevo derecho en caso de seguirse esta corriente, porque induciría a pensar que las personas ostentan un derecho de propiedad sobre sus datos. Luego, para relativizar aún más la concepción del derecho a la autodeterminación informativa e instar en definitiva a que se suprimiera del Proyecto –según se desprende de la historia de la ley-, el Gobierno señaló que el modelo anterior no era el único que existía, pues en Estados Unidos la jurisprudencia ha diseñado la *privacy,* homologándolo al derecho a la vida privada chileno, entendido de manera más amplia, explicando que la variante *informational privacy* era aquella aplicable al tema que se legislaba, pues con este término se intenta señalar el atentado a la persona perpetrado por la simple recogida y catalogación de la información. En razón de estos planteamientos, la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, en el informe recaído en el Proyecto de Ley en tercer trámite sobre protección de la vida privada, resolvió fijar directamente el ámbito de aplicación de la ley, circunscrita al tratamiento de datos de carácter personal en registros o bancos de datos, que efectúen organismos públicos o particulares, conjuntamente con reconocer a la persona natural la titularidad de los datos y no a quien realice su tratamiento. En suma, la Comisión borró del Proyecto el reconocimiento del derecho a la autodeterminación informativa, en nuestro concepto, en base a un poco logrado estudio del tema y en razón del temor del Estado de hacer suyo todo el planteamiento doctrinal sentado tras la sentencia del Tribunal Constitucional alemán, el cual sin duda limita el poder del Estado para obligar a los ciudadanos a entregar datos personales para fines estadísticos. Todo lo anterior, en *"Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado recaído en el Proyecto de Ley en tercer Trámite, sobre Protección de la Vida Privada"*, Sesión 18º ordinaria del 5 de Agosto de 1998, Diario de Sesiones del Senado, págs. 2086-2091.

1º que: *"Toda persona puede efectuar el tratamiento de datos personales siempre que lo haga de manera concordante con la Ley 19.628 y para finalidades permitidas por el ordenamiento jurídico"*. Por último, dispone el artículo 1º que en todo caso deberá respetarse el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que ésta ley les reconoce a aquéllos. Refuerza lo ya señalado la disposición del artículo 4º, la cual prescribe que: *"El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello"*.

2º. Principio de la calidad de los datos

Este principio, se encuentra contenido en diversas disposiciones de la Ley, tanto de manera directa como indirecta. De manera directa, está previsto en artículo 6º, el que prescribe lo siguiente: *"Los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado. Han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos. (…) Se bloquearán los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación. El responsable del banco de datos personales procederá a la eliminación, modificación o bloqueo de los datos, en su caso, sin necesidad de requerimiento del titular".*

Más adelante, el artículo 9º luego de establecer como regla general que los datos personales sólo pueden ser utilizados para la finalidad de su recolección, salvo que provengan o hayan sido recolectados de fuentes accesibles al público, señala que: *"en todo caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos"* (Art. 9º inc. 2º).

Cabe agregar que también respondería a este principio el denominado 'derecho al olvido'. En este sentido, el artículo 18 dispone que en ningún caso pueden comunicarse datos que versen, en general, sobre obligaciones de carácter económico, financiero, bancario o comercial que consten en ciertos títulos de crédito luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible. Tampoco se pueden comunicar los datos relativos a dicha obligación después de haber sido pagada o haberse extinguido por otro modo legal. No obstante lo anterior, se podrá comunicar a los Tribunales de Justicia la información que requieran con motivo de juicios pendientes.

Por otra parte, el artículo 21º dispone que: *"Los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena".* Esta regla tiene su excepción en los casos en que la información sea solicitada por los Tribunales de Justicia u otros organismos públicos dentro del ámbito de su competencia. Respecto de estos últimos, la Ley no precisa cuáles son.

Finalmente, estimamos que de manera indirecta se reconocería el principio de la calidad de los datos al definir la Ley que entiende por dato caduco. Al respecto, señala que para los efectos de esta ley se entenderá 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. 2º letra d).

De todo lo anterior, se deduce que los datos personales objeto de tratamiento manual o automatizado deben ser exactos, actualizados y veraces.

3º. Principio del consentimiento informado del titular de los datos

Este principio se encuentra consagrado en el artículo 4º inciso 1º de la Ley 19.628 en los siguientes términos: *"El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello".* Agregan los incisos 2º y 3º respectivamente que: *"la persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público"* y, que *"la autorización debe constar por escrito".* Además de esta norma, el artículo 3º inciso 1º dispone que en toda recolección de datos personales que se realice a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, sin perjuicio de los demás derechos y obligaciones que esta ley regula, 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".* De todo lo anterior, se desprende que el legislador chileno exige un mínimo deber información por parte de quien recolecta datos personales respecto del titular de éstos [245] . Asimismo se agrega que la autorización debe constar por escrito y puede ser revocada de la misma forma, aunque sin efecto retroactivo.

Si bien lo recién señalado es la regla general dentro del ordenamiento jurídico chileno, la Ley se ha encargado por otra parte de establecer diversas excepciones a este principio, dejándolo en definitiva casi vacío de contenido [246] . A este respecto, Herrera ha dicho que el principio del consentimiento ha sido desarrollado de forma dubitativa, convirtiéndose, en una débil declaración romántica que no ampara efectivamente al titular, pues aunque la Ley disponga que el tratamiento de datos sólo podrá realizarse con el consentimiento expreso, e incluso por escrito, no exige que sea específico, por lo que nada obsta a que en la práctica se utilice deslealmente un modelo de cláusula de consentimiento que pueda esconder un alcance mayor al que, en un comienzo, motivaba

[245] A este respecto, y en caso que a la recolección de la información le anteceda un contrato, estimamos que es indispensable tener presente la importante regla contenida en el artículo 1.546 de nuestro Código Civil el cual prescribe*: "Los contratos deben ejecutarse de buena fe, y por consiguiente obligan no solo a lo que en ellos se expresa, sino a todas las cosas que emanan precisamente de la naturaleza de la obligación, o que por la ley o la costumbre pertenecen a ella".* La importancia de esta norma radica en que no obstante existir una regla explícita que ordena un mínimo deber de información (Arts. 3º y 4º Ley 19.628), éste deber puede ampliarse, requerir mayores exigencias de información en atención a la naturaleza de la obligación o de la costumbre, por lo que en definitiva lo que prescribiría la ley de protección de datos sería un estándar mínimo de conducta exigible respecto de quien recolecta datos. Lo anterior, sin duda será de mucha importancia en un eventual juicio de indemnización de perjuicios por incumplimiento de contrato. Además de lo ya señalado, obviamente deberá tenerse presente la regla del artículo siguiente al citado, el artículo 1.547, que a falta de pacto expreso de las partes, señalará el deber de diligencia que debe emplearse por éstas en la ejecución de los contratos.

[246] Las excepciones al principio del consentimiento serán analizadas más abajo en el punto Nº 5.2.1 de este análisis.

al titular [247] . En este mismo sentido se pronuncia Jijena, para quien si bien el artículo 4º sienta el principio general en materia de procesamiento de datos personales, atendidas las excepciones que consagra, "no es sino una mera declaración de principios" [248] .

En suma, de lo anteriormente señalado se desprende que si bien la regla general en el ordenamiento jurídico chileno es el principio del consentimiento expreso del titular de los datos personales para que sea lícito el tratamiento de éstos, dadas las diversas excepciones que la Ley establece en la materia, éste se traduce en un principio meramente formal carente de contenido.

4º. Principio de seguridad de los datos

Este principio, que se traduce en la adopción de medidas técnicas y organizativas que garanticen la seguridad y confidencialidad de los datos personales por parte de los responsables o usuario del archivo de datos, se plasma en la legislación chilena en los siguientes términos: *"el responsable del registro o banco de datos personales 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"* (Art. 5º). Luego, el artículo 11 y final del Título I señala 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"*. De lo anterior, se desprende que en todo momento el responsable de los registros está obligado a prestar la debida diligencia en el cuidado y conservación de los datos personales que obren en sus archivos, registros o bases de datos, sean manuales o automatizados [249] . Asimismo, son aplicables estas normas de seguridad a los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias (Art. 21

247 Herrera Bravo, Rodolfo*: "Análisis de la Ley Chilena Nº 19.628, sobre Protección de la Vida Privada, de 28 de agosto de 1999"*. [En línea] < http://www.adi.cl/pdf/19628.pdf > [consulta: 30 de Octubre 2002], págs. 23 y 24. Agrega este autor que la Ley chilena además, "apoya este principio en una insuficiente información previa. No basta con señalar que la persona que autoriza debe ser debidamente informada del propósito del almacenamiento y de su posible comunicación al público, si se desconocen los derechos que se pueden hacer valer y el nombre y domicilio del responsable del registro. Más aún, si la información acerca de eventuales comunicaciones a terceros luego no se refleja en la obligación de requerir nuevamente el consentimiento específico e inequívoco del titular, para poder realizarlas, se transforma en una simple 'información de cortesía' ".

248 Jijena Leiva, Renato: *"La Ley Chilena de Protección de Datos Personales. Una visión crítica desde el punto de vista de los intereses protegidos"*, Cuadernos de Extensión Jurídica, Universidad de Los Andes, Nº 5, 2001, pág. 100.

249 En cuanto a la diligencia que debe emplear el responsable de los registros o bancos de datos, creemos que el estándar de conducta debido para el tratamiento de datos sensibles debería ser más exigente que el de la culpa leve. No obstante lo anterior, y como forma de otorgar una mayor protección a los datos sensibles, estimamos que el juez, al construir en abstracto el deber de cuidado debido por el responsable de los registros, podría determinar un deber de cuidado más estricto sin salirse del estándar de la culpa leve (Art. 44 C. Civil). Ejemplo de lo anterior en materia contractual podemos apreciarlo a propósito de la responsabilidad del mandatario, el cual responde por regla general de culpa leve, pero si es remunerado responde *"más estrictamente"* y, en caso que éste haya manifestado repugnancia al encargo y se haya visto en cierto modo forzado a aceptarlo, responderá de culpa leve *"menos estricta"* (Art. 2.129 C. Civil).

inciso 2º). Creemos que hace falta en la Ley chilena una disposición que haga extensivo el deber de cuidado a todos quienes participan en el proceso del tratamiento de datos, es decir, que alcanzara incluso a quien los recolecta manualmente, pues el riesgo de utilización indebida está generalmente presente.

5º. Principio de la confidencialidad de los datos

Este principio se traduce en un deber de secreto que pesa sobre toda persona que intervenga como trabajador en el tratamiento de datos personales respecto de la información que tome conocimiento en razón de ese oficio. Al respecto, la Ley Nº 19.628 señala en el artículo 7° que: *"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"*. En consecuencia, el deber de secreto es aplicable a quienes trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados. Respecto de los primeros, la Ley vuelve a repetir este deber en el artículo 21 inciso 2º, al preceptuar que los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias deberán guardar respecto de esa información la debida reserva o secreto.

En cuanto a qué se entiende por personas que trabajen en el tratamiento de datos personales, la ley no lo señala. Por nuestra parte, creemos que debiera incluirse dentro de esta categoría a todas aquellas personas que directa o indirectamente, en razón de su oficio, han participado del proceso denominado tratamiento de datos personales, para lo cual deberá tenerse presente lo preceptuado por el artículo 2º letra o) que señala: *"Para los efectos de esta ley se entenderá por (…) o) Tratamiento de datos, cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado 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 en cualquier otra forma"*. Es decir, toda persona que realice alguna labor que implique cualquiera de las acciones recién señaladas, debería estar afecta al deber de secreto, aunque haya dejado de prestar servicios.

En resumen, puede afirmarse que la ley chilena establece un deber de secreto con un campo de aplicación restringido; sólo a quienes trabajen en el tratamiento de datos personales, sean organismos privados como públicos sin extenderse este deber a terceros ajenos a esa actividad. En este punto, estimamos que el término *"trabajan"* debería ser interpretado de manera extensiva y, por lo tanto, incluir a aquellas personas que tienen una relación laboral contractual propiamente tal, a las que sólo prestan servicios, así como también a aquéllas que realizan labores de práctica profesional u otras labores semejantes.

6º. Principio del consentimiento para la cesión de los datos

En lo tocante a este principio, la Ley chilena dispone en el artículo 4º inciso 2º que la

persona que autoriza el tratamiento de datos personales, debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y *"su posible comunicación al público".* Al respecto, se ha señalado por Herrera que en nuestro ordenamiento jurídico "no existe una obligación general de requerir el consentimiento inequívoco y específico del titular para efectuar una comunicación a terceros, salvo excepciones, sino, por el contrario, la comunicación de datos exige únicamente una obligación de informar la posible ocurrencia de este hecho, al momento de recolectar los datos" [250] . Entre estas excepciones podemos mencionar aquella facultad que tienen los responsables de registros o bancos de datos para establecer un procedimiento automatizado de transmisión de datos personales, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes, en cuyo caso deben dejar constancia frente a un requerimiento de datos de lo siguiente: a) La individualización del requirente; b) El motivo y el propósito del requerimiento, y c) El tipo de datos que se transmiten. Con todo, estos requisitos y exigencias no se aplican cuando se trate de datos personales accesibles al público en general y, cuando se transmitan datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes (Art. 5º) [251] .

En suma, podemos afirmar que el principio del consentimiento para la cesión de los datos personales si bien puede visualizarse en la Ley 19.628, su configuración es de carácter tenue y vago, excluyendo además ámbitos generalmente reconocidos en los instrumentos internacionales sobre protección de datos personales, en especial la Directiva europea de 1995.

7º. Principio de la finalidad

El artículo 9 de la Ley 19.628 señala en el inciso 1º que: *"los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público".* También aparece reseñado este principio en el artículo 3º el cual dispone que en toda recolección de datos personales que se realice a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, sin perjuicio de los demás derechos y obligaciones que la Ley regula, 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"*. Asimismo, el artículo 4º inciso 2º prescribe que la persona que autoriza el tratamiento de datos debe ser debidamente informada respecto del *"propósito del*

[250] Herrera Bravo, Rodolfo, *op. cit*., pág. 25.

[251] Herrera señala que otra de las situaciones referidas a la comunicación, a la que alude expresamente la Ley, atañe a los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, los cuales en virtud del artículo 21, no pueden comunicarse a terceros una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena, a menos que les sea solicitada por los tribunales de justicia u otros organismos públicos competentes. Agrega finalmente este autor que, la comunicación también es tratada en los artículos 17 a 19, con relación a los datos personales de carácter económico, financiero, bancario o comercial, respecto de los cuales dicha comunicación está limitada en el tiempo, bajo la figura que la doctrina denomina derecho al olvido (*op. cit*., págs. 25 y 26).

almacenamiento de sus datos personales (…)". En estos dos casos el término 'propósito' entendemos que ha sido utilizado como sinónimo de finalidad.

Por otra parte, el artículo 5º inciso 1º, dispone que el responsable del registro o banco de datos personales 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"*. El inciso 4º, también hace una referencia directa a los fines de la transmisión digital de datos, al señalar que quien reciba datos personales a través de un procedimiento automatizado o red electrónica *"sólo puede utilizar los datos personales para los fines que motivaron la transmisión".*

Regulando los derechos de los titulares de los datos, la Ley 19.628 dispone en el artículo 12 que toda persona tiene derecho a exigir a quien sea responsable de un banco de datos personales, que se dedique en forma pública o privada al tratamiento de éstos, 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"*. Lo anterior, sin duda es una herramienta que permite controlar directamente la finalidad del banco de datos.

A propósito del tratamiento de datos por los organismos públicos, el artículo 22 prescribe que el Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos, el cual tendrá carácter público. En éste deberá constar, respecto de cada uno de esos bancos de datos, el fundamento jurídico de su existencia, *"su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende, todo lo cual será definido en un reglamento".* A continuación, el inciso 2º precisa que el organismo público responsable del banco de datos proporcionará esos antecedentes al Servicio de Registro Civil e Identificación *"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".* El Reglamento respectivo (Decreto Nº 779/2000 Min. Justicia) dispone a su vez en el artículo 3º que: *"la inscripción en el Registro de Bancos de Datos Personales deberá contener, a lo menos, las siguientes menciones: (…) 5. La finalidad del banco de datos (…)".* Respecto de estas disposiciones, lamentamos que el legislador no haya señalado sanción específica para el caso que no se cumplan los plazos de inscripción o modificación.

Comentando aspectos relacionados con las definiciones utilizadas por la Ley, Jijena ha señalado que el artículo 9, establece *a contrario sensu*, "que los datos personales que provengan o se hayan recolectado de fuentes accesibles al público pueden usarse para fines diversos de aquéllos con que fueron recolectados" [252] . Esta aseveración cobra real dimensión si es concordada con la conclusión a que llega este mismo autor; en Chile todas las fuentes de datos personales serán en principio, por regla general y legalmente, de acceso al público, no restringido o reservado a los solicitantes, salvo que una ley especial, o una norma o resolución administrativa o una cláusula de confidencialidad establezcan expresamente lo contrario. Lo anterior, en razón a los amplísimos términos

[252] Jijena Leiva, Renato, *op. cit*., pág. 99.

en que ha sido concebido por el legislador el concepto de *"fuentes accesibles al público"* [253] . Herrera, refiriéndose directamente al principio de la finalidad, ha dicho que éste se desarrolla a lo largo de la Ley sin fuerza suficiente, no sólo porque las fuentes accesibles al público puedan ser numerosas en la práctica, sino más bien, "porque no exige que la finalidad sea determinada y explícita, y porque, a nuestro juicio, abre la posibilidad de que los datos puedan seguir una finalidad distinta a la que motivó la recogida, al exigir que, respecto de la transmisión de datos a través de una red digital, dicha comunicación guarde relación con las finalidades tanto del cedente como del cesionario. Así, sin existir una limitación legislativa, el tenor literal de la Ley admite la posibilidad de que el organismo requirente persiga un propósito diverso al del responsable del registro que almacena el dato" [254] . En relación con los planteamientos recién expuestos, concordamos con la interpretación de ambos autores, tanto en lo relativo a las excepciones que se deducen del artículo 9, como de la deficiente configuración del artículo 5º. La forma cómo ha sido estructurada la Ley, efectivamente abre la puerta para que eventualmente pueda tergiversarse lo señalado por aquélla y dejar sólo de manera nominal establecido otro principio que puede ser vaciado de todo contenido.

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

En la ley chilena sobre protección de datos personales, se constatan diversos aspectos en los cuales el legislador regula de forma diferenciada al sector público y al sector privado en la materia. Esa normativa legal, a su vez debe entenderse complementada por dos disposiciones reglamentarias; el Decreto Supremo Nº 779/2000 del Ministerio de Justicia [255] y el Decreto Supremo Nº 950/1928 del Ministerio de Hacienda [256] . Sin embargo, debe tenerse presente que el ámbito de vigencia del DS 950 de 1928 es restringido, pues se entiende que las disposiciones contrarias a la Ley 19.628 han sido derogadas tácitamente por ésta, según se deduce de lo señalado por el artículo 3º transitorio de la propia Ley.

[253] El razonamiento de este autor se basa en los amplísimos términos en que concibió la Ley a las fuentes accesibles al público, a saber, como aquellos *"registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes"* (Art. 2 letra i). Señala Jijena que con lo anterior, las fuentes accesibles al público han sido trasformadas en la regla general y la consecuencia práctica que de ello se deriva consiste en que "al ser los datos personales estimados por regla general como legalmente públicos, cualquiera puede procesarlos y comercializarlos porque el acceso está permitido por ley y sin restricciones, validándose el negocio del procesamiento y la venta de datos personales". Por el contrario, los datos personales cuyo acceso no sea permitido sin restricciones o sea prohibido por la ley, constituirán fuentes reservadas o no accesibles al público (*Ídem*, págs. 98 y 99).

[254] Herrera Bravo, Rodolfo, *op. cit.*, pág. 28.

[255] Este Decreto fue publicado en el Diario Oficial el 11 de Noviembre de 2000. Su ámbito de aplicación está restringido a los organismos públicos a cargo de banco de datos personales, excluyéndose a los bancos de datos de carácter privado, en concordancia con lo señalado por al artículo 22 de la Ley 19.628.

5.1 Consentimiento para el Tratamiento de los Datos

En lo que respecta a este tema, si bien la regla general es el consentimiento expreso del titular de los datos, se ha señalado por parte de la doctrina chilena que ésta sólo constituiría una mera declaración de principios, atendido el sinnúmero de excepciones establecidos por la Ley. Ahora bien, dentro de las excepciones a ese principio encontramos diferencias de tratamiento entre el sector público y privado.

En cuanto a las excepciones en materia de consentimiento aplicables al sector público, el artículo 20 de la Ley preceptúa que no se necesita el consentimiento del titular de los datos personales, cuando el Estado, a través de sus organismos públicos, recabe datos respecto de las materias de su competencia y sujetándose a la Ley 19.628. Para dilucidar el ámbito de aplicación de la norma anterior, en especial descifrar qué se entiende por *"materias de su competencia*", nos remitiremos a lo señalado por la Comisión Mixta durante la tramitación de la Ley. Se expuso por dicha Comisión, que "si bien esta disposición puede estimarse innecesaria, al tenor del artículo 7º de la Constitución, presta utilidad en un cuerpo legal, que por primera vez, da reglas sistemáticas sobre los datos personales, más aún si se considera que numerosos organismos públicos tienen solamente normas de carácter reglamentario sobre la materia o, incluso, ni siquiera de esa jerarquía" [257] . Luego, en lo relativo a la facultad de los organismos públicos para tratar datos personales sin el consentimiento de los titulares de éstos, se señaló por la misma Comisión que "se desecha la exigencia adicional planteada en el texto del tercer trámite constitucional, en cuanto a que, además de la habilitación legal general para realizar su cometido, cada organismo público requiriese otra, específica, que le permitiese organizar y mantener bancos de datos personales. Entendió la Comisión Mixta y los señores representantes del Ejecutivo que la existencia de un registro general de bancos de datos personales del sector público, prevista en el artículo 22 de la misma proposición del Ejecutivo, así como los diferentes derechos sustantivos y mecanismos procesales que consulta este cuerpo legal son suficiente garantía para las personas frente a los actos que la Administración realice en la materia" [258] . En este punto, creemos que el legislador pecó de ingenuo, pues tal como está configurada la

[256] El Decreto Supremo Nº 950 de 1928, publicado el 28 de Marzo de 1928, ha sido modificado en diversas oportunidades desde la fecha de su dictación. Este Decreto, establece en general el deber de informar por ciertos organismos tanto públicos como privados a la Cámara de Comercio de Santiago, datos de diversa especie para su registro y publicación. Así por ejemplo, los Notarios deben enviar: a) Estados que contengan la nómina de las letras protestadas durante el día, indicando si el protesto es por falta de aceptación o de pago, el monto de la letra, el nombre y domicilio del librado o aceptante y el nombre del girador; b) Lista de las compraventas, remates y adjudicaciones de bienes raíces, indicando los nombres de las partes contratantes, la ubicación de la propiedad y el precio de venta; c) Lista de los mutuos hipotecarios, con indicación de los nombres del deudor y del acreedor, la ubicación de la propiedad y monto del préstamo; d) Lista de las cancelaciones; e) Nómina de las nuevas sociedades comerciales organizadas y de las modificaciones y disoluciones de éstas y, f) Convenios extrajudiciales entre comerciantes (Art. 1º Nº 1).

[257] Informe de la Comisión Mixta recaído en el Proyecto de Ley sobre Protección de la Vida Privada, sesión ordinaria del 2 de Junio de 1999. Diario de Sesiones del Senado, pág. 131.

[258] *Ibídem*.

obligación de inscripción en el Registro de Bancos de Datos a cargo de Organismos Públicos, no se garantiza en absoluto que todos los bancos de datos llevados por organismos públicos se inscriban, pues el Servicio de Registro Civil carece de facultades sancionatorias y de control en esta materia. Consecuencia de lo anterior es la existencia de diversos organismos públicos chilenos que aún no cumplen el mandato legal de inscribir sus bases de datos personales en el Registro respectivo [259] . En suma, en esta materia se dejó en manos de los propios organismos públicos la facultad de determinar cuándo pueden éstos realizar un tratamiento de datos personales sin el consentimiento de los titulares de los datos. Con todo, serán los jueces los que en definitiva determinarán si un organismo público ha realizado un tratamiento de datos que se ajuste al mandato legal del artículo 20, es decir, realizado respecto de las materias de su competencia y, respetando las demás normas de la Ley 19.628 [260] .

En relación al sector privado o particulares, entendemos que los incisos 5º y 6º del artículo 4º serían aplicable a aquéllos. Al efecto, se dispone por el legislador que no requiere autorización el tratamiento de datos personales:

a) Provenientes o recolectados de fuentes accesibles al público: i) Cuando sean de carácter económico, financiero, bancario o comercial; ii) Cuando 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; iii) Cuando sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios (Art. 4 inciso 5º) y,

b) Que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos (Art. 4 inciso 6º).

5.2 Consentimiento para la Transmisión o Cesión de Datos Personales

En lo relativo al consentimiento del titular para la transmisión de sus datos personales, la Ley no se refiere en particular a uno u otro sector. Así, el artículo 4º inciso 2º, preceptúa de manera bastante vaga que la persona que autoriza el tratamiento de sus datos personales debe ser debidamente informada, entre otros aspectos, sobre la *"posible comunicación al público"* de éstos.

En el caso de transmisiones de datos por vías electrónicas, la Ley establece ciertas

[259] Ejemplos en Chile de organismos públicos que a la fecha no han inscrito sus bases de datos personales en el Registro son: el Servicio de Impuestos Internos, Investigaciones de Chile, Superintendencia de Bancos, Superintendencia de Isapres, Cámara de Diputados de la República, Senado de la República, Corte Suprema, entre otros. Todo lo anterior [en línea] < http://rbdp.srcei.cl/rbdp/html/Consultas/consultas.htm > [consulta: 16 de Mayo 2003].

[260] Esta situación podría complicarse en la eventualidad que la Contraloría General de la República se haya pronunciado por la legalidad del tratamiento de datos personales ante una consulta realizada por un organismo público y, la justicia civil a su vez, estime lo contrario al resolver una contienda en que una de las partes sea precisamente el organismo público que efectuó la consulta a la Contraloría.

condiciones para que éstas puedan llevarse a efecto respecto de algunas clases de datos. En esta materia, el legislador ha omitido toda referencia al consentimiento del titular de los datos que se transmiten, y en consecuencia, tampoco podría hablarse de trato diferenciado. A pesar de lo anterior y, para una comprensión adecuada de lo preceptuado por el legislador en materia de transmisión electrónica de datos, nos detendremos en la norma respectiva, a saber, el artículo 5º. Esta disposición señala que el responsable del registro o banco de datos personales 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. En este caso, y frente a un requerimiento de datos personales mediante una red electrónica, deberá dejarse constancia de lo siguiente: a) La individualización del requirente; b) El motivo y el propósito del requerimiento, y c) El tipo de datos que se transmiten. A su vez, la admisibilidad del requerimiento será evaluada por el responsable del banco de datos que lo recibe, pero la responsabilidad por dicha petición será de quien la haga. La Ley dispone además que el receptor de los datos sólo puede utilizarlos para los fines que motivaron la transmisión. Finalmente, se preceptúa que: *"no se aplicará este artículo cuando se trate de datos personales accesibles al público en general ni cuando se transmitan datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes"*.

Como se puede apreciar, no existe ninguna referencia al consentimiento del titular de los datos en esta materia regulada de manera bastante confusa. Renato Jijena, comentando las condiciones legales establecidas por la norma anterior, ha interpretado esta disposición en un sentido que puede parecer extremo. Señala que sólo serían aplicables las condiciones para la transmisión de datos personales a través de redes electrónicas al tratamiento de datos que sean de acceso restringido o reservado. Lo anterior, a consecuencia de las excepciones establecidas por la Ley en los incisos 5º y 6º del artículo 5º. El razonamiento es el siguiente: "la Ley establece que no se aplicarán las limitantes de este artículo cuando se transmitan datos personales a organizaciones internacionales en cumplimiento de tratados y convenios vigentes, ni cuando se trate de datos personales accesibles al público en general; es decir, y entendiendo que éstos son la regla general, en la práctica no se aplicará nunca. Además que al efecto Chile no ha suscrito a la fecha tratado alguno" [261] .

Como ya lo señalamos, concordamos con las conclusiones a que llega este autor, dados los amplios términos en que la Ley concibe a los datos personales accesibles al público en general. En base a la interpretación anterior, estimamos que de lo dispuesto por el artículo 5º puede concluirse que serían aplicables tanto a los organismos públicos como privados las condiciones para la transmisión de datos a través de redes electrónicas, sólo en los casos en que se tratara de datos de acceso restringido o reservado, como por ejemplo, los datos sujetos al secreto bancario y al secreto tributario; el primero aplicable tanto al sector público como privado y, el segundo sólo respecto de aquél. En suma, en materia de consentimiento para la transmisión de datos a través de redes electrónicas, el legislador no exige el consentimiento del titular de los datos, por lo

[261] Jijena Leiva, Renato, *op. cit*., pág. 108. El razonamiento de este autor se explicó al analizar el principio de la finalidad (ver *supra* punto Nº 4, 7º de este análisis).

que no podría hablarse de diferencias de tratamiento entre el sector público y privado en cuanto a ese requisito-principio.

Una diferencia de tratamiento en materia de excepción al consentimiento para la transmisión de datos, es aquélla que beneficia sólo al sector público, y que está implícita en la regulación de la transmisión de los datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias (Art. 21); éstos pueden ser comunicados, no obstante estar prescrita la acción penal o administrativa o cumplida o prescrita la pena o sanción, sin límite temporal a los tribunales de justicia u otros organismos públicos dentro del ámbito de su competencia (Art. 21 inc. 2º). Aquí, nuevamente la ley chilena muestra su poca claridad en este punto al referirse a organismos del Estado en general, sin determinarlos, lo que en la práctica conlleva a que existan registros de antecedentes penales sin límite temporal de uso exclusivo de algunas instituciones, como por ejemplo de las policías.

Otra diferencia de tratamiento entre el sector público y privado, la cual beneficia en la práctica a los responsables de archivos o bancos de datos de carácter privado, es aquélla regla que importa una excepción al requisito del consentimiento para la transmisión de datos y que autoriza la comunicación de información que verse sobre algunas obligaciones de carácter económico, financiero, bancario o comercial (Art. 17). Las obligaciones que pueden ser objeto de publicidad sin el consentimiento de sus titulares son la siguientes: 1) Las que consten en letras de cambio y pagarés protestados; 2) Las que consten en cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa y, 3) Las obligaciones incumplidas que deriven de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales.

En suma, el tratamiento diferenciado entre el sector público y el privado se aprecia en materia de excepciones al requisito-principio del consentimiento para la cesión de datos personales.

5.3 Tratamiento de los Datos Sensibles

Esta categoría de datos, es definida por la ley como aquellos 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". La ley chilena se refiere a ellos además en el artículo 10, el cual señala que: *"no pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares"*. De lo anterior, se desprende que la regla general sería la prohibición de tratamiento de los datos sensibles. Las excepciones estarían dadas por: 1) Una autorización legal; 2) El consentimiento del titular y, 3) El hecho de ser necesarios para establecer u otorgar beneficios de salud a los titulares de los datos [262] .

La Ley, en la excepción del Nº 3 recién señalada se está refiriendo tanto a las Instituciones de Salud Previsional que son privadas (Isapres), como al Fondo Nacional de Salud (Fonasa) que es público, por lo que ambas instituciones estarían autorizadas para tratar datos sensibles, relativos a la salud de las personas.

Por otra parte, la Ley establece normas solamente aplicables al sector público. Este es el caso del tratamiento de datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, los cuales sólo pueden ser tratados por organismos públicos [263] . En cuanto a la transmisión de esta categoría especial de datos, se señala por el legislador que no podrán comunicarse una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena. No obstante lo anterior, existen dos casos de excepción: 1) Cuando la información sea solicitada por los Tribunales de Justicia y 2) Cuando la información sea solicitada por otros organismos públicos dentro del ámbito de su competencia. En ambos casos, se deberá guardar respecto de esa información la debida reserva o secreto. La Ley, en el segundo caso de excepción, no señala cuál o cuáles sean esos organismos, por lo que en definitiva deberán ser los jueces quienes determinen cuando se está frente a esta excepción.

5.4 Derechos de los Titulares de los Datos

La normativa chilena de 1999 dedica el Título II a reglamentar los derechos de los titulares de datos. La disposición que encabeza este Título (Art. 12) señala que: *"Toda persona tiene derecho a exigir a quien sea responsable de un banco, 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"*. El inciso 2º agrega que: *"En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen"*. Por su parte, el inciso 3º señala que: *"Sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos.* Añade el inciso 4º del artículo 12 que: *"Igual exigencia de eliminación, o la de bloqueo de los datos, en su caso, podrá hacer 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"* [264] .

El artículo 13 a su turno dispone que: *"El derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención"*. Finalmente, el artículo 14 de la Ley señala que: *"Si*

[262] En este caso, no obstante la falta de distinción del legislador, parecería razonable que la excepción debiera restringirse solamente a los datos relativos a la salud y en ningún caso ser extensibles a otros tipos de datos sensibles.

[263] A este respecto cabe señalar que el Registro Nacional de Condenas así como también el Registro de Violencia Intrafamiliar, de Consumo y Tráfico de Estupefacientes y los demás que encomiende la ley, son de competencia exclusiva del Servicio de Registro Civil e Identificación, el cual debe formar y mantener actualizado, por los medios y en la forma que el Reglamento determine (Art. 4, Ley Orgánica del Servicio de Registro Civil e Identificación Nº 19.477, de 19 de Octubre de 1996).

los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos".

Como ha podido apreciarse, de las disposiciones que hemos transcrito, hasta el momento no se perciben diferencias de trato entre el sector público y el privado Por lo tanto, el ámbito de aplicación de tales normas sería indiferenciado y afectaría tanto a los responsables de bancos de datos públicos como privados. Empero, el ejercicio de los derechos reconocidos por la Ley a los titulares de los datos puede verse limitado por las situaciones de excepción señaladas por el legislador en la misma normativa, las cuales se analizarán en el siguiente punto.

5.5 Excepciones al Ejercicio de los Derechos de los Titulares de Datos

Las excepciones que establece la ley chilena a los derechos de información, modificación, cancelación o bloqueo de datos personales operan, en general, respecto de los organismos públicos. En este sentido se enmarca el artículo 15, el cual dispone que no procederá el ejercicio de los derechos de información, modificación, cancelación o bloqueo de datos en los siguientes casos: 1) Cuando se impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido; 2) Cuando se afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias; 3) Cuando afecte la seguridad de la Nación, 4) Cuando se afecte el interés nacional y, 5) Cuando los datos personales sean almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva. En esta hipótesis, se reconoce por la Ley que sólo podrá ejercerse el derecho de información (Art. 15 inciso final).

En el ámbito del sector privado, los derechos de acceso, rectificación, actualización y supresión de datos personales operan sin excepción (Art. 13). No obstante lo anterior, cabría dentro de las excepciones señaladas en el artículo 15, reseñadas a propósito del sector público (ver punto anterior), la causal que dispone la no procedencia del ejercicio de los derechos por el titular, cuando "*afecte la reserva o secreto establecidas en disposiciones legales o reglamentarias"*.

5.6 Creación y Registro de los Archivos, Registros o Bancos de Datos Personales

En cuanto a los requisitos para la creación y registro de los bancos de datos, puede señalarse que la ley chilena sólo se ocupa de aquéllos cuyos responsables sean

[264] Continúa el artículo 12 señalado que: *"En el caso de los incisos anteriores, la información, modificación o eliminación de los datos serán absolutamente gratuitas, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente. Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, 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. El derecho a obtener copia gratuita sólo podrá ejercerse personalmente"* (Inciso 5º). *"(…) Si los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos deberá avisarles a la brevedad posible la operación efectuada. Si no fuese posible determinar las personas a quienes se les hayan comunicado, pondrá un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos"* (Art. 12 inciso final).

organismos del Estado. Al efecto, se dispone que el tratamiento de datos personales por parte de un organismo público sólo puede efectuarse respecto de las materias de su competencia y con sujeción a las normas de la Ley 19.628, agregándose que en esas condiciones, no se necesitará del consentimiento del titular para el tratamiento de sus datos (Art. 20).

Por otra parte, la Ley prescribe en el artículo 22 que el Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de los organismos públicos, el cual tendrá carácter público. En este registro deberá hacerse constar respecto de cada uno de los bancos de datos: 1) El fundamento jurídico de su existencia; 2) Su finalidad; 3) Los tipos de datos almacenados y, 4) Una descripción del universo de personas que comprende. La ley ordena a su vez, que todo lo anterior debe ser definido por reglamento [265] . Agrega finalmente la Ley, que el organismo público responsable del banco de datos debe proporcionar esos antecedentes al Servicio de Registro Civil e Identificación cuando se inicien las actividades del banco, y comunicar cualquier cambio de los elementos indicados en los números anteriores dentro de los quince días desde que se produzca (Art. 22 inciso final).

Respecto de los particulares o sector privado, la ley no contempla la creación de un registro de bancos de datos personales, ni menos la obligación de inscribirlos por los particulares que sean responsables de esos bancos de datos. Sin duda, puede afirmarse que esta situación milita en contra de los titulares de los datos, porque para lograr una efectiva protección de los derechos de las personas es indispensable conocer la mayor cantidad de información que permita la identificación del registro o banco de datos, así como su finalidad, contenido y personas responsables de éste. Sin esta información se dificulta en gran medida el ejercicio de los derechos de información, modificación, cancelación y bloqueo de datos personales.

5.7 Archivos, Registros o Bancos de Datos relativos a Encuestas, Estudios de Mercado o Sondeos de Opinión Pública

En lo que se refiere a estos archivos, registros o bancos de datos, cabe decir que la ley chilena los trata en el artículo 3º dentro de las disposiciones generales, pero sin hacer referencia explícita a un sector u otro como ámbito objetivo de aplicación. Aunque en apariencia pudiera pensarse que en razón del carácter de estos bancos sólo serían aplicables estas normas a los particulares, ello debería ser descartado, pues tanto la

[265] El reglamento respectivo (Decreto Nº 779/2000, del Ministerio de Justicia) si bien establece plazos para la respectiva inscripción de los registros o bancos de datos públicos, no dispone sanción alguna en caso de no realizarse la inscripción. Pensamos que no obstante esta omisión, en ningún caso podría significar la indefensión de los particulares, por lo que ante falta o deficiencia del servicio en este aspecto, cabe sin duda la responsabilidad patrimonial del Estado por los perjuicios causados. En este sentido, sería aplicable lo preceptuado en el inciso 2º del artículo 23, el cual señala que: "*En todo caso, las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario"*. Por otra parte la Ley 18.745, Orgánica de Bases de la Administración del Estado señala que: *"El Estado será responsable por los daños que causen los órganos de la Administración en el ejercicio de sus funciones, sin perjuicio de las responsabilidades que pudieren afectar al funcionario que los hubiere ocasionado"* (Artículo 4º). Como se sabe, esta disposición tiene su fuente directa en el artículo 38 de la Constitución Política.

ubicación de estas normas (Título Preliminar. Disposiciones Generales), como las actividades de esta clase de bancos de datos, no son exclusivas de los particulares. En virtud de lo anterior estimamos que las disposiciones del artículo 3º de la Ley son aplicables tanto al sector público como al privado. Este artículo, señala al efecto que: *"en toda recolección de datos personales que se realice a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, sin perjuicio de los demás derechos y obligaciones que esta ley regula, 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"*. Se agrega que la comunicación de los resultados debe omitir las señas que puedan permitir la identificación de las personas consultadas, es decir, deben utilizarse para su tratamiento procedimientos de disociación de datos. Finalmente, se prescribe en el inciso 2º que el titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión (Art. 3º inciso 2º).

5.8 Tratamiento Manual o Automatizado de Datos

La Ley chilena define el tratamiento de datos como: *"cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado 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 en cualquier otra forma"* (Art. 2º letra o). Lo recién anotado, a su vez es concordante con la definición legal de registro o banco de datos, el cual es entendido como *"el 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 de datos"*.

Por otra parte, el tantas veces señalado artículo 5º autoriza a los responsables de registros o bancos de datos personales para 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 sin distinguir entre el carácter público o privado del registro o banco de datos.

De las normas recién vistas se desprende que el ámbito objetivo de aplicación de la ley chilena abarca tanto a los registros o bancos de datos de carácter manuales como automatizados, sin establecer diferencias en cuanto al carácter de éstos, es decir, si son públicos o de carácter privados.

5.9 Personas Jurídicas como Titulares de Datos

El artículo 2º letra f de la Ley 19.628, al definir lo que se entenderá por datos de carácter personal o datos personales, sólo los circunscribe a la información concerniente a personas naturales, con lo cual expresamente se ha dejado fuera de la protección de la Ley a los datos o información relativa a las personas jurídicas o morales. En este sentido, la exclusión es amplia e incluye tanto a las personas jurídicas de derecho privado como de derecho público.

5.10 Transmisión Internacional de Datos Personales

Esta materia no ha sido regulada por la ley chilena de protección de datos personales sino que por el contrario, la tarea ha sido dejada a la regulación vía tratados internacionales (Art. 5º inc. final).

6. Modelos de Tutela

El ordenamiento jurídico chileno, a través de la Ley 19.628 ha dispuesto mecanismos específicos de protección a los derechos de los titulares de datos personales a través de una acción de amparo a esos derechos, la que en general se asemeja a la denominada acción de hábeas data o acción de protección de datos. Cabe hacer presente que la Ley chilena en ninguna parte utiliza estos términos para referirse al mecanismo de tutela, sino que habla de *"reclamación"* y -como ya se dijo- de *"amparo a los derechos"*.

Comentando esta acción, Corral Talciani ha dicho que la tutela judicial a través de una sola acción de amparo, no necesariamente obliga a pensar que estamos frente a un solo derecho, siguiendo la regla clásica de que a todo derecho corresponde una acción. Para este autor "la acción de amparo digital o *hábeas data* es una forma de tutela judicial amplia que cubre la protección de un conjunto de derechos que, aunque con fisonomías propias, tiene en relación que responden al mismo interés" [266].

Según la Ley, los derechos amparados por la acción chilena de "hábeas data" son: el derecho de información, modificación, cancelación o bloqueo de datos personales, salvo los casos de excepción señalados en el artículo 15 ya visto (Art. 16). Debemos hacer presente que previo al ejercicio de la acción de amparo o hábeas data, el legislador exige primeramente que el afectado haya agotado la vía administrativa o extrajudicial ante el responsable del registro o banco de datos, salvo el caso en que la reclamación se funde en infracciones a la Ley distintas a las previstas en los artículos 16 y 19 que se analizarán más adelante. Conjuntamente con el ejercicio de los derechos ya señalados, se faculta al titular de los datos para demandar dentro del mismo procedimiento, la indemnización de los perjuicios causados a consecuencia de la infracción de las disposiciones legales. Asimismo, en caso de acogerse *"la reclamación"* por el tribunal que conoce de la acción, éste *"podrá aplicar una multa"* (Art. 16 inciso 5º).

6.1 La Acción de Amparo de los Derechos de los Titulares o Acción de Hábeas Data

La Ley 19.628 contempla dentro de su Título II "De los derechos de los titulares de datos", en el artículo 16, una acción de amparo a los derechos de información, modificación, cancelación y bloqueo de datos, la que doctrinalmente ha sido denominada como de hábeas data o acción de protección de datos. Llama la atención el hecho que la Ley se refiera a ésta como una "reclamación" y no derechamente como una demanda (Art. 16 incisos; 2º letras a, b y h; 3º; 4º y 5º). El término utilizado por la ley chilena, tiene una

[266] Corral Talciani, Hernán, *op. cit*., pág. 58.

connotación más bien administrativa que judicial, por lo que creemos hubiera sido más adecuado el uso el término "demanda" en vez de "reclamación", dado que en definitiva se entrega a los jueces civiles el conocimiento y la resolución, tanto de la acción de hábeas data como de las eventuales indemnizaciones de perjuicios y aplicación de multas. A continuación se señalarán los aspectos más relevantes de la acción de protección de datos.

6.1.1) Procedencia de la Acción

La acción de amparo de los derechos de los titulares de datos o acción de hábeas data chilena, según los artículos 16 y 19 procede en los siguientes supuestos:

1º) En caso que el responsable del registro o banco de datos no se pronunciare sobre la solicitud efectuada por el titular de los datos -de información, modificación, cancelación o bloqueo de datos personales- dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional. En este caso, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil, solicitando el amparo a sus derechos. Respecto de lo anterior, cabe destacar el carácter subsidiario que tiene esta acción, pues previo al ejercicio de ella es preciso agotar la vía informal o prejudicial. Es decir, primero debe dirigirse la petición de información, modificación, cancelación o bloqueo de los datos personales ante el responsable del registro o banco de datos y, sólo en caso que éste no se pronunciare acerca de la solicitud, o la denegare por causa distinta a las legales, queda abierta la vía para la acción de hábeas data (Art. 16 inciso 1º).

2º) Cuando quienes efectúen el tratamiento de datos personales, relativos a obligaciones de carácter económico, financiero, bancario o comercial no modifiquen los datos del titular en un plazo máximo de tres días, contados desde que se ha comunicado el pago o la extinción de la obligación por la fuente accesible al público, o no bloqueen los datos del titular hasta que les sea posible actualizar la información, en el caso de no ser posible su modificación inmediata (Art. 19 inciso 3º).

3º) Cuando un acreedor de alguna de las obligaciones señaladas en el número anterior, una vez que se le haya efectuado el pago o extinguida la deuda por otro modo en que él intervenga directamente, no avisare tal hecho dentro de los siguientes siete días hábiles al responsable del registro o banco de datos accesible al público que en su oportunidad comunicó el protesto o la morosidad, salvo que el deudor hubiere optado expresamente por requerir directamente la modificación al banco de datos (Art. 19 inciso 2º).

6.1.2) Legitimación Activa

Está legitimado activamente para ejercer la acción del artículo 16, todo titular de datos personales que haya sido afectado en sus derechos reconocidos por la Ley. Debemos recordar que en nuestra legislación, la titularidad para accionar de hábeas data está reservada sólo a las personas naturales, pues la propia definición legal de datos de carácter personal, señala que ellos son *"los relativos a cualquier información concerniente a personas naturales, identificadas o identificables"* (Art. 1º, letra f).

6.1.3) Legitimación Pasiva

El sujeto pasivo de la acción de hábeas data es el responsable del registro o banco de datos personales, el cual puede ser tanto un organismo público como privado, sea persona natural o jurídica (Art. 16 en relación con artículo 12).

6.1.4) Competencia

La Ley chilena establece en materia de competencia una regla de carácter general y otra de carácter excepcional:

a)La regla general, está dada por la competencia en primera instancia del juez de letras en lo civil del domicilio del responsable del registro o banco de datos, que se encuentre de turno según las reglas correspondientes (Art. 16 inciso 1º).

b)La regla de excepción, se da cuando la causal invocada por el responsable del registro o banco de datos personales para denegar la solicitud del requirente sea la *"seguridad de la Nación o el interés nacional"*. En estos casos será competente para conocer de la "reclamación" la Corte Suprema, en sala y en única instancia (Art. 16 inciso 3º).

6.1.5) Procedimiento Aplicable

El procedimiento general aplicable a la acción de hábeas data se contempla en el artículo 16, destacando de aquél el carácter breve y sumario. Las etapas más importantes del procedimiento son las siguientes:

1)*Reclamación (demanda*): ésta deberá señalar brevemente la infracción cometida y los hechos que la configuran. Conjuntamente deberá acompañarse los medios de prueba que los acrediten, en su caso;

2) *Notificación :* la ley señala que ésta deberá hacerse por cédula. Esta misma forma de notificación se aplicará para la sentencia que se dicte;

3)*Defensa :* el responsable del banco de datos deberá presentar sus descargos dentro del quinto día hábil y adjuntar los medios de prueba que acrediten los hechos en que se funda. En caso de no disponer de ellos deberá expresar esta circunstancia, en este evento, el tribunal fijará una audiencia para que dentro del quinto día hábil se reciba la prueba ofrecida y no acompañada. La sentencia definitiva se dictará dentro del tercer día de vencido el plazo de cinco días ya señalado, se hayan o no presentado descargos.

4)*Resoluciones:* todas las resoluciones, a excepción de la sentencia definitiva, se dictarán en única instancia y se notificarán por el estado diario.

5)*Apelación :* la sentencia definitiva será apelable en ambos efectos. Recibidos los autos por el tribunal de apelación, el Presidente de la Corte ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes. El fallo que se pronuncie sobre la apelación no será susceptible de los recursos de casación.

Por otro lado, el procedimiento de excepción aplicable a la tramitación de la acción de hábeas data se presenta en el caso que la causal invocada para denegar la solicitud

del requirente fuere la seguridad de la Nación o el interés nacional. En este evento, la 'reclamación' deberá deducirse ante la Corte Suprema, la que 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. En caso que la Corte estime procedente la recepción de 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 (Art. 16 inciso 3º).

Reglas comunes: la sala de la Corte Suprema que conozca la reclamación conforme al procedimiento excepcional, o la sala de la Corte de Apelaciones que conozca la apelación, tratándose del procedimiento general, si lo estima conveniente o se le solicita con fundamento plausible, podrá ordenar traer 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. En las reclamaciones que se hagan ante la Corte Suprema el Presidente del Tribunal dispondrá que la audiencia no sea pública.

De las reglas anteriores, llama la atención que la Ley por una parte diga que la resolución de la acción de hábeas data tenga la naturaleza jurídica de una sentencia definitiva (Art. 16 inciso 3º letra f) y por otra, que establezca de manera excepcional el derecho de las partes- a través de sus abogados- de alegar ante los estrados de apelación y ante la Corte Suprema, pues la regla general aplicable en materia procesal civil es la procedencia de los alegatos cuando se trate de sentencias definitivas (Art. 199 del Código de Procedimiento Civil *a contrario sensu*). Lo anterior, es una inconsistencia sistemática dentro del derecho procesal chileno, pues estaría tratando a la sentencia definitiva como si fuera una sentencia interlocutoria, cuya apelación se ve en cuenta, salvo que las partes soliciten alegar. En el caso de la apelación de la sentencia definitiva que resuelve el hábeas data, la Ley señala que el tribunal de alzada *"si lo estima conveniente o se le solicita con fundamento plausible podrá ordenar traer los autos en relación para oír a los abogados de las partes"* y sólo en este caso la causa se agregará extraordinariamente a la tabla respectiva de la misma sala. Creemos que esta situación creada por la Ley 19.628, no sólo se aleja de las reglas generales del procedimiento civil, sino que más grave aún, incluso estaría limitando los derechos en su esencia (Art. 19 Nº 26), pues la propia ley estaría imponiendo requisitos o condiciones para hacer procedente el derecho de la defensa de las partes. Incluso podría plantearse una acción de inconstitucionalidad en base a lo preceptuado por la Convención Americana de Derechos Humanos, la cual dispone en el artículo 8.1 que: *"toda persona tiene derecho a ser oída, con las debidas garantías y dentro de un plazo razonable, por un juez o tribunal competente, independiente e imparcial, establecido con anterioridad por la ley, en la sustanciación de cualquier acusación penal formulada contra ella, o para la determinación de sus derechos y obligaciones de orden civil, laboral, fiscal o de cualquier otro carácter".*

En razón de lo anterior, estimamos que la ley chilena limita las garantías del debido proceso establecidas tanto en la Constitución chilena como en el Pacto de San José de Costa Rica, al condicionar y dejar al arbitrio judicial el derecho de alegar ante los estrados de apelación la sentencia definitiva de hábeas data dictada por el juez de letras. Con ello, cobra relevancia la discusión de una eventual modificación constitucional que consagre el derecho a la autodeterminación informativa, que no lo haga depender de otro derecho

fundamental y, que contemple una acción de tutela propia, no sujeta a plazo de caducidad y cuya sentencia sea de efectos *erga omnes.* Cabe agregar que ante la dificultad planteada, mayores argumentos tendrán las personas para optar por la acción de protección, que como dijimos, estimamos sólo aplicables en los casos no previstos en la Ley 19.628 o en los eventos que el procedimiento de reclamación ante el juez civil (o de apelación) no sea el más rápido y efectivo remedio para proteger las garantías de la vida privada e intimidad, que ciertamente subyacen en la ley chilena de protección de los datos personales.

6.1.6) La Sentencia

La sentencia definitiva que acoja la reclamación, deberá fijar un plazo prudencial para dar cumplimiento a lo resuelto y podrá aplicar una multa de una a diez unidades tributarias mensuales, o de diez a cincuenta unidades tributarias mensuales si se tratare de una infracción a las disposiciones del Título III de la ley que trata *"De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial".*

6.2 Otras Acciones

La Ley 19.628, además de las acciones de hábeas data previstas en los artículos 16 y 19, contempla en el artículo 23 una acción genérica que tiene por finalidad abarcar toda infracción a la Ley que no se halle comprendida en aquéllas disposiciones. Es decir, sería una especie figura residual aplicable a toda violación de disposiciones legales no contemplada en los artículos 16 y 19. Al efecto, se dispone que: *"(…) las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario. El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece. La prueba se apreciará en conciencia por el juez".* Si bien la disposición anterior pareciera completar el régimen sancionatorio establecido por la Ley, ello no es tan así, pues el legislador no previó sanciones aplicables a tales eventos, cuestión que no ocurre tratándose de la violaciones a los artículos 16 y 19 para las cuales se establecen multas, e incluso suspensión del cargo a los funcionarios públicos que desobedezcan ciertas órdenes del Tribunal.

Comentando la disposición del artículo 23, Corral Talciani ha señalado que si la responsabilidad surge por una conducta infraccional que no es de las señaladas en los artículos 16 y 19 se ve muy difícil que pueda articularse esa responsabilidad pues "no se indica quién es el juez competente ni tampoco las sanciones que proceden por estas infracciones (…). Podría sí ejercerse en forma separada la acción de responsabilidad civil, y en este caso será competente el juez de letras en lo civil del domicilio del demandado y se aplicará el procedimiento sumario" [267] . En nuestra opinión, y atendido el tenor de la disposición del artículo 23, en tales supuestos sólo cabría demandar la indemnización de perjuicios, siendo constitutivas de culpa infraccional la violación de cualquiera de las normas de la Ley 19.628, debiendo probarse por el actor al efecto, cada

[267] Corral Talciani, Hernán, *op. cit*., págs. 56 y 57.

uno de los elementos restantes para configurar la responsabilidad civil extracontractual. En materia de competencia estimamos que deben aplicarse las reglas generales del procedimiento civil a falta de disposición legal expresa que altere dichas normas.

En materia constitucional, específicamente en lo que se refiere a la acción de protección, puede decirse que desde la vigencia de la Ley 19.628 no ha existido uniformidad jurisprudencial para determinar la procedencia o improcedencia de la tutela de los derechos de las personas afectadas por el tratamiento de sus datos personales por esta vía. Así, algunas sentencias han rechazado los recursos de protección interpuestos aduciendo que existe un procedimiento especial contemplado en la Ley 19.628 para hacer valer los derechos que este estatuto legal reconoce [268] . Otras sentencias se han pronunciado en sentido contrario, argumentando que el afectado en sus derechos y garantías constitucionales tutelables por el recurso de protección puede accionar a través de esta vía, *"sin perjuicio de los demás derechos que pueda hacer valer ante la autoridad o los tribunales correspondientes"* (Art. 20 C. Pol.) [269] . Esta última interpretación es defendida por Corral Talciani, para quien la acción de protección puede interponerse fundado en las amenazas, privaciones o perturbaciones del derecho al respeto y protección a la vida privada, e incluso del derecho a la identidad (vía respeto de la vida pública) "en los casos de infracciones a la ley 19.628 si el atentado al derecho se comete a través del tratamiento de datos de carácter personal. La deducción del recurso y su fallo no obstará a que posteriormente el particular pueda ejercer la acción de amparo digital o *hábeas data* (…)" [270] . Como ya lo adelantamos, en nuestra opinión, el ejercicio de la acción de protección habría quedado restringida a dos amplios supuestos: a) Todo ámbito no regulado o no contemplado por la Ley Nº 19.628 en que se afectaren los bienes jurídicos intimidad, vida privada e incluso la honra de las personas a consecuencia

[268] En este sentido se ha pronunciado la Corte de Apelaciones de Santiago, en sentencia de protección Rol Nº 4.581-2000, considerando 7º, el cual señala: "Que, a mayor abundamiento, esta Corte estima que existiendo en la Ley 19.628 un procedimiento especial, pormenorizado en su artículo 16, la recurrente debió comparecer ante el juzgado civil respectivo, una vez transcurrido el plazo que la recurrida tenía para evacuar la respuesta a su carta; debiendo, concluirse que el especial procedimiento allí diseñado debe preferirse a la vía excepcional que constituye el recurso de protección". En otra sentencia de protección se lee también en el considerando 7º que: "(…) conviene agregar que el actor debió seguir, en todo caso, respecto de la señalada recurrida el procedimiento estatuido en el antes indicado artículo 16 de la ley N° 19.628, que debe entenderse que prevalece sobre la vía excepcional constituida por la acción de protección" (Corte de Apelaciones de Santiago., Rol Nº 3.558-2000, apelación pendiente).

[269] Sigue esta línea interpretativa la Corte de Apelaciones de Concepción en la sentencia de protección Rol Nº 2.381-2001, considerando 2º, el cual señala: "Que en lo concerniente a la improcedencia del recurso basada en que la ley 19.628, sobre protección de la vida privada, contempla un procedimiento propio para la aclaración y eliminación de los antecedentes incorporados en el registro del individuo, es lo cierto que la presente acción constitucional procede sin perjuicio de los demás derechos que el interesado pueda hacer valer ante la autoridad o tribunales, como lo prescribe expresamente el artículo 20 del texto constitucional, razón por la cual esta otra alegación tampoco puede ser acogida". En este mismo sentido se ha pronunciado la Corte de Apelaciones de Santiago, aceptando tácitamente su competencia en sede de protección para conocer materias comprendidas en la Ley 19.628, señalando: "(…) 3º.- Que la normativa que rige en la actualidad este tipo de materia está contenida en la Ley 19.628, a cuya luz debe necesariamente examinarse la queja de ilegalidad" (Rol Nº 2.456-2000).

[270] Corral Talciani, Hernán, *op. cit*., pág. 59.

del tratamiento de sus datos personales y, b) A las situaciones en que, no obstante estar cubiertas por la Ley 19.628 y, atendidas las circunstancias del caso, el procedimiento de reclamación ante el juez civil competente (o de apelación) no apareciera como el más expedito y efectivo remedio para proteger los bienes jurídicos ya señalados, que ciertamente subyacen en la ley chilena de protección de los datos personales. Para fundamentar esto último nos basamos en los artículos 8.1 [271] y 25 de la Convención Americana de Derechos Humanos la cual se ha incorporado al ordenamiento jurídico chileno en virtud del artículo 5º inciso 2º de nuestra Constitución [272] . Al efecto, el artículo 25 de la Convención dispone que: "*Toda persona tiene derecho a un recurso sencillo y rápido o a cualquier otro recurso efectivo ante los jueces o tribunales competentes, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la Constitución, la ley o la presente Convención, aun cuando tal violación sea cometida por personas que actúen en ejercicio de sus funciones oficiales"*. Con todo, y dada la complejidad del tema en estudio, estimamos que a nivel de tutela constitucional, debería seguirse el camino de la consagración independiente y autónoma del derecho a la protección de datos y la acción de hábeas data, lo que para muchos podrá parecer un exceso. Nosotros pensamos todo lo contrario, pues dadas las condiciones actuales de constante desarrollo de las tecnologías de la información y su influencia en la vida de las personas, urge actuar y reconocer jurídicamente que estamos en presencia de un fenómeno en el que no basta la tutela tradicional. Más aún, no es posible abarcarla con la sola configuración de un derecho a la intimidad o a la vida privada entendida como facultad de exclusión o libertad negativa, sino que es preciso reconocer un nuevo derecho fundamental, la autodeterminación informativa. En este sentido, concordamos con el planteamiento del profesor Nogueira, quien ya en el año 1997 sostenía que debería constitucionalizarse el instituto del hábeas data basado en la necesidad de delimitar el núcleo esencial del derecho protegido, "garantizándolo ante cualquier desnaturalización o limitación que los órganos instituidos puedan realizar de él bajo pretexto de regularlo, ya que este contenido esencial del derecho queda fijado por la propia Constitución y garantizado por la normativa del artículo 19 Nº 26 de la Carta Fundamental, sin perjuicio que el legislador complemente tal normativa" [273] .

7. Mecanismos de Control

La legislación chilena de protección de datos personales no contempla la creación un órgano de control que vele por el resguardo de los derechos consagrados en ella, y que supervise la gestión de los responsables de los registros o bancos de datos de carácter personal. El único órgano al cual la ley de protección de datos personales chilena le encomienda alguna función relacionada con el tratamiento de esos datos es el Servicio de Registro Civil, el cual debe mantener un Registro de todos los bancos de datos

[271] Ver *supra,* punto Nº 6.1.5 de este análisis.

[272] Sobre esta materia ver *supra* punto Nº 2.1 del presente análisis.

[273] Nogueira Alcalá, Humberto, 1997, *op. cit*, pág. 275.

personales a cargo solamente de organismos públicos (Art. 22). Cabe aclarar al respecto que el Servicio de Registro Civil, carece de toda facultad coactiva respecto de los responsables de los bancos de datos a cargo de organismos públicos, por lo que no puede obligar a éstos a que inscriban sus bases de datos, es decir, su rol queda reducido a ser un ente meramente registral [274] . Como ya se adelantó, el Decreto Nº 779/2000, del Ministerio de Justicia, se encarga de reglamentar ese Registro.

La falta de un órgano de control en la materia, quita fuerza y coherencia al sistema de protección de datos chileno, pues se ha entendido que éste cumple un rol fundamental para la efectiva eficacia de las leyes de *data protection* [275] **.** Por otra parte, no se entiende que sólo se obligue inscribir (nominalmente pues no hay sanción) los bancos de datos a cargo de organismos públicos y se deje fuera a los que están bajo la responsabilidad de privados o particulares. Ciertamente este es un tema pendiente y mientras no se resuelva, nuestra legislación carecerá de una efectiva supervisión y control, donde cada banco de datos privado y sus responsables operarán en el más absoluto secreto, frente a nuestras narices pero sin que podamos detectarlos.

8. Transmisión Internacional de Datos

En materia de transmisión internacional de datos personales, la ley chilena sólo se refiere a ella en dos disposiciones; en la primera de manera más bien vaga, al definir que se entiende por transmisión de datos [276] y, en la segunda directamente, a propósito de las excepciones a las condiciones para la transmisión electrónica de datos personales, prescribiendo que: "*esta disposición tampoco es aplicable cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes"*(Art. 5º inciso final). En relación a lo anterior, se ha señalado por Magliona que el Proyecto de Ley originario que fue presentado por la Cámara de Diputados, contenía un artículo que establecía la prohibición de la transferencia internacional de datos personales desde países o con destino a países cuya legislación no ofrezca garantías análogas a las previstas en la ley. La Comisión Mixta rechazó el precepto señalado por considerar que la regulación de la transferencia internacional de datos debe ser regulada por tratados internacionales sobre la materia [277] . Por lo tanto, la Ley se desentendió del tema y prefirió dejarlo entregado al derecho internacional.

[274] Se ha señalado que la falta de un organismo de control en la legislación chilena redunda en mayores costos, tanto económicos como de tiempo de espera para las víctimas, pues al no existir este órgano (con atribuciones y poderes para la gestión y para la solución de los eventuales conflictos que se susciten entre los titulares de los datos y los responsables de los bancos o registros de datos), las víctimas se ven obligadas a recurrir a los tribunales ordinarios de justicia: González Hoch, Francisco *op. cit*., pág. 177.

[275] Ver Directiva 95/46 CE, artículos 18-22.

[276] El artículo 2º letra o) dispone que para los efectos de esta ley se entenderá por: Tratamiento de datos, *"cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado 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 en cualquier otra forma"* (negrita nuestra).

En el ámbito legal sectorial, debemos señalar que el Código Tributario chileno, faculta al Director de Impuestos Internos en el artículo 6 letra A, Nº 6º a: "*Mantener canje de informaciones con Servicio de Impuestos de otros países para los efectos de determinar la tributación que afecte a determinados contribuyentes. Este intercambio deberá solicitarse a través del Ministerio que corresponda y deberá llevarse a cabo sobre la base de reciprocidad, quedando amparado por las normas relativas al secreto de las declaraciones tributarias".* Lo anterior eventualmente podría entrar en contradicción con lo señalado por la Ley 19.628, pues tanto de la historia fidedigna del establecimiento de ella como de lo previsto en el artículo 5º, se desprendería que todo lo relativo a la transmisión internacional de datos personales debe regularse vía tratados internacionales y no a través de convenios entre organismos tributarios administrativos. En definitiva, estimamos que la disposición del artículo 6º letra A Nº 6, eventualmente habría sido derogada tácitamente por el artículo 5º inciso final de la Ley 19.628.

9. Régimen de Responsabilidad

En materia de responsabilidad, la Ley 19.628 sólo se ocupa del ámbito civil y administrativo mas no del penal; en materia civil se establece como regla general la responsabilidad por culpa o negligencia. En el ámbito administrativo, se contemplan para algunas situaciones sanciones de multa y suspensión del cargo al jefe de servicio público responsable del banco de datos. En materia penal la ley de protección de datos chilena no intervino, por lo cual en principio puede afirmarse que en esta materia no existen delitos.

Fuera del ámbito de la Ley 19.628, las demás normas legales contenidas en estatutos sectoriales que protegen indirectamente los datos personales, contemplan sanciones administrativas para el caso de infracción a ellas. En materia penal, como se dijo, no existen tipos específicos que sancionen violaciones a la Ley 19.628. Con todo, al igual que en los demás análisis, se reseñaran las normas que establecen delitos por violación a algunos de los bienes jurídicos que subyacen en la Ley 19.628, en particular el derecho a la intimidad y a la vida privada (ver *supra* puntos Nº 2.2.4 y siguientes de este análisis).

9.1 Responsabilidad Administrativa

El legislador chileno no ha establecido claramente un régimen de sanciones administrativas en la Ley 19.628, como tampoco un órgano de control que se encargue de velar por el cumplimiento y aplicación de la ley de protección de datos personales. No es claro el régimen, pues se establecen sanciones consistentes en multas cuya naturaleza jurídica es bastante incierta y que además sólo se aplican cuando se violan los artículos 16 y 19, y cuando el juez lo estime procedente (Art. 16 inciso 5º) [278] . Además de estas sanciones, la Ley ha señalado la siguiente regla en el inciso 6º del artículo 16: *"la falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la*

[277] Magliona M, Claudio: *"Hábeas Data y Protección de Datos Personales en Chile"*. [En línea] < http://www.adi.cl/pdf/magliona2.pdf > [consulta: 30 de Octubre 2002], pág. 7.

forma que decrete 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". De lo recién dicho, se desprende que la sanción de suspensión de funciones sólo es aplicable a quien tenga la especial calidad que se indica (jefe de Servicio de una repartición pública). Respecto de las multas, no es tan claro el punto, pues no se señala a quienes serían aplicables, si sólo a los particulares o también a los funcionarios públicos. Con todo, y dado que la Ley establece perentoriamente -sin distinguir si el responsable del banco de datos es un organismo público o un particular-, que en caso de desobediencia a ciertas órdenes específicas dictadas por el Tribunal *"serán castigados con multa"*, estimamos que estas sanciones deberían aplicarse tanto a uno como a otro responsable. Ahora bien, si el infractor ha sido un organismo público, además el juez *"podrá sancionar al jefe del Servicio"* con la suspensión de su cargo. Si se optara por interpretar que sólo pueden ser sancionados con multa los responsables de bancos de datos que no tuvieran el carácter de organismo público, se daría la injusta situación en la cual el jefe del Servicio a cargo del banco de datos solamente 'podría' ser sancionado por desobedecer la orden de un Tribunal, en cambio el responsable de un banco de datos que no tenga esa calidad 'debería' serlo. No creemos que existan razones de fondo para hacer diferencias en esta materia.

En cuanto a la naturaleza jurídica de la disposición del artículo 16 inciso 6º ya señalado, estimamos que ésta constituiría una figura especial de desacato a la autoridad judicial, la cual debe ser conocida y resuelta por el mismo Tribunal que decreta la medida incursa. Lo anterior, en razón a que la conducta sancionada es precisamente una desobediencia a las órdenes específicas decretadas dentro de un proceso por el Tribunal que conoce de una acción de hábeas data, lo que constituye jurídicamente desacato. Asimismo, creemos que esas sanciones aplicables en sede civil a los infractores deberían entenderse sin perjuicio de la disposición contemplada en el Título XIX del Libro I del Código de Procedimiento Civil intitulado "De la Ejecución de las Resoluciones", cuyo artículo 240 inciso 2º prescribe que: *"El que quebrante lo ordenado cumplir será sancionado con reclusión menor en su grado medio a máximo"*.

Por otra parte, en el caso de los funcionarios públicos que no sean "jefe de Servicio", e incurran en conductas que infrinjan la Ley 19.628 en el ejercicio de sus funciones, la normativa general aplicable sería la Ley Orgánica Constitucional de Bases Generales de

278 El artículo 16 inciso 5º de la Ley señala que: *"En caso de acogerse la reclamación, la misma sentencia fijará un plazo prudencial para dar cumplimiento a lo resuelto y podrá aplicar una multa (…)"*. Por lo que esta sanción es de carácter facultativa. Los montos de éstas pueden ir de 1 a 10 U.T.M, en caso de infracciones al artículo 16, y de 10 a 50 U.T.M, en caso de infracciones a los artículos 17 y 18 cometidas por los responsables de los registros o bancos de datos de información de carácter financiera, económica, bancaria o comercial. En nuestra opinión, el carácter facultativo de la aplicación de la multa en caso de acogerse una reclamación (acción de hábeas data), no permite que ésta cumpla su rol disuasivo (si es que éste fuera realmente), pues si no existe certeza acerca de la aplicación de aquélla, no incentiva a tomar medidas que eviten la violación de las normas de la Ley. Creemos que, verificada una infracción a las disposiciones de los artículos 16, 17 y 18, las sanciones 'deben ser aplicadas' dentro del marco establecido por la Ley. Para ello, basta una actitud activa por parte de los jueces, quienes deberían desestimar toda defensa (muy común en nuestro país) fundada en 'errores involuntarios', 'errores del sistema', salvo obviamente el caso fortuito, el cual excluye la culpa.

la Administración del Estado. Esta Ley establece en el artículo 18 la responsabilidad funcionaria, señalando que: "*el personal de la administración del Estado estará sujeto a responsabilidad administrativa, sin perjuicio de la responsabilidad civil y penal que pueda afectarle. En el ejercicio de la potestad disciplinaria, se asegurará el derecho a un racional y justo procedimiento*" [279] .

Fuera del ámbito de los estatutos ya señalados, en materia de responsabilidad administrativa se contemplan ciertas normas sectoriales que sancionan la violación a los deberes generales de confidencialidad de ciertas informaciones. A continuación se señalaran tales normas.

9.1.1) Código Tributario

El artículo 101 de este cuerpo legal dispone que serán sancionados con suspensión de su empleo hasta por dos meses, los funcionarios del Servicio que cometan algunas de las siguientes infracciones: *"(…)5º.- Infringir la obligación de guardar el secreto de las declaraciones en los términos señalados en este Código"*. Luego se agrega en el inciso 4º que: *"la reincidencia en cualquiera de las infracciones señaladas en los números 1º, 4º y 5º, será sancionada con la destitución de su cargo del funcionario infractor".*

En suma, puede señalarse que en el caso de la violación al deber de secreto por parte de funcionarios del Servicio de Impuestos Internos, éstos pueden ser suspendidos de sus funciones o destituidos, sin perjuicio de las normas penales y civiles aplicables.

9.1.2) Ley General de Bancos

En este estatuto sectorial, se establecen sanciones administrativas generales para quienes violen el secreto bancario (Art. 154), caso en el cual, sin perjuicio de las responsabilidades civiles y penales deben ser sancionados administrativamente por la Superintendencia de Bancos e Instituciones Financieras. Al respecto se señala en el artículo 19 del cuerpo legal en comento que: *"las instituciones sometidas a la fiscalización de la Superintendencia que incurrieren en alguna infracción a la ley que las rige, a sus leyes orgánicas, a sus estatutos o a las órdenes legalmente impartidas por el Superintendente, que no tenga señalada una sanción especial, podrán ser amonestadas, censuradas o penadas con multa hasta por una cantidad equivalente a cinco mil unidades de fomento"*. Luego, en el inciso 2º de este artículo se preceptúa que: *"igualmente podrá amonestar, censurar o multar hasta por una cantidad equivalente a 1.000 unidades de fomento a los directores, gerentes y funcionarios en general que resulten responsables de las infracciones cometidas. La multa se comunicará al infractor y al gerente general de la empresa".*

En definitiva, la violación del deber de secreto bancario puede sancionarse administrativamente, afectando tanto a la empresa directamente, como a los funcionarios involucrados en el ilícito.

[279] D. F. L. Nº 1/ 19.653. Ministerio Secretaría General de la Presidencia, Santiago, 13 de Diciembre de 2000. Fija texto refundido, coordinado y sistematizado de la Ley 18.575, L.O.C. de Bases Generales de la Administración del Estado.

9.1.3) Código Sanitario

El artículo 127 de este Código dispone que: *"las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados"* y sólo puede revelarse el contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Luego agrega que: *"en ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expendieron, ni datos que sirvan para identificarlos"*. Ahora bien, las sanciones a las normas anteriores se prevén en el artículo 174 del cuerpo legal citado, el cual prescribe que: *"La infracción de cualquiera de las disposiciones de este Código o de sus reglamentos y de las resoluciones que dicten los Directores de los Servicios de Salud o el Director del Instituto de Salud Pública de Chile, según sea el caso, salvo las disposiciones que tengan una sanción especial, será castigada con multa de un décimo de unidad tributaria mensual hasta mil unidades tributarias mensuales. Las reincidencias podrán ser sancionadas hasta con el doble de la multa original".*

Por otra parte, las infracciones antes señaladas pueden ser sancionadas además, con la clausura de los establecimientos, locales, lugares de trabajo donde se cometiere la infracción; con la cancelación de la autorización de funcionamiento o de los permisos concedidos, entre otras. (Art. 174 inciso 2º).

9.1.4) Código del Trabajo

Como se recordará, tanto la Ley 19.759 como la 19.628 introdujeron en el Código del Trabajo disposiciones relacionadas con la materia de nuestro estudio. Por una parte, la primera de las leyes citadas, agregó el artículo 154 bis al código del ramo el cual señala que: *"el empleador deberá mantener reserva de toda la información y datos privados del trabajador a que tenga acceso con ocasión de la relación laboral"*. A su vez, la Ley 19.628, que tuvo por finalidad evitar la discriminación de los trabajadores a consecuencia de sus antecedentes comerciales, agregó un inciso 5º al artículo 2º del Código del Trabajo, el cual dispone que: *"Ningún empleador puede condicionar la contratación de trabajadores a la ausencia de obligaciones de carácter económico, financiero, bancario o comercial que, conforme a la ley, puedan ser comunicadas por los responsables de registros o bancos de datos personales; ni exigir para dicho fin declaración ni certificado alguno"* (Art. 2º inciso 6º). Ahora bien, las infracciones a las normas ya mencionadas deben ser castigadas según las reglas del artículo 477 de la ley laboral chilena, el cual prescribe que: *"las infracciones a este Código y a sus leyes complementarias, que no tengan señalada una sanción especial, serán sancionadas con multa de una a veinte unidades tributarias mensuales, según la gravedad de la infracción".* Con todo, dependiendo de la cantidad de trabajadores que laboren en la empresa la multa puede llegar hasta las sesenta U.T.M (si la empresa cuenta con más de 200 trabajadores).

9.2 Responsabilidad Civil

En materia de responsabilidad civil, el artículo 11 de la Ley prescribe 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". Más adelante, en el artículo 23 la Ley dispone que: *"La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal".*

En cuanto a la naturaleza de la responsabilidad civil establecida por la ley chilena, ha señalado Corral que se trata de un supuesto de responsabilidad civil extracontractual, aunque la presencia de una autorización expresa y por escrito de un titular de datos para la utilización de éstos podría hacer surgir dudas sobre si hay un contrato que fija el marco de actuación entre las partes. Para este autor dicha autorización sería un acto unilateral y no la aceptación de un acuerdo contractual, agregando que, por lo demás, la ley se refiere a la responsabilidad civil como aneja a la responsabilidad infraccional (Art. 23 inciso 2º), lo que sólo se condice con la responsabilidad civil extracontractual [280] . Por nuestra parte, compartimos íntegramente la interpretación de este autor, pues se aviene tanto con el tenor de la Ley como con las reglas generales sobre obligaciones y contratos.

En lo relativo al deber de diligencia exigido a los responsables de los bancos de datos, nada se ha dicho por el legislador. No obstante lo anterior, esta omisión es suplida por las reglas generales de la responsabilidad extracontractual, las cuales disponen que el correspondiente estándar de diligencia es el de un buen padre de familia, por lo que se responderá de culpa leve (Art. 44 del Código Civil). En el caso que medie un contrato entre el titular de los datos y el responsable del registro o banco de datos personales, cabría aplicar las reglas de la responsabilidad contractual, por lo que el nivel de diligencia exigido será el pactado por las partes (por lo que habría que ser cuidadoso con las condiciones grales. o letra chica de algunos contratos) y, en subsidio, el determinado por el legislador civil (Art. 1.547 del Código Civil).

Cabe destacar de la Ley chilena la directa alusión a la indemnización del daño moral en esta materia, la cual es procedente tanto en la responsabilidad civil extracontractual como en la contractual. En cuanto a esta última ella es completamente justificable en atención a la previsibilidad del daño. Es decir, a que puede claramente preverse por el responsable del banco de datos, que cualquier acción u omisión negligente en el tratamiento de los datos personales es apta para causar daños morales a los titulares de éstos, dado que están en juego importantes derechos de la personalidad.

Por otra parte, la Ley prescribe que la acción de indemnización de perjuicios podrá ser interpuesta conjuntamente con la reclamación destinada a establecer la infracción cometida, sin perjuicio que las partes puedan reservarse el derecho de discutir sobre la especie y el monto de los perjuicios en la ejecución del fallo o en otro juicio diverso (Art. 23 inciso 2º) [281] .

Cabe agregar que en lo relativo a la tramitación de estos juicios, el legislador ha señalado que la indemnización de perjuicios se sujetará al procedimiento sumario. Para tal efecto, el juez tomará todas las providencias que estime convenientes para hacer

[280] Corral Talciani, Hernán , *op. cit*., pág. 55.

efectiva la protección delos derechos que esta ley establece (Art. 23 inc. 2º). De lo anterior se desprende que en estos casos procederán todo tipo de medidas cautelares, sin limitación, cumpliéndose los requisitos generales del *periculum in mora* y del *fumus bonis juris.* Finalmente, la ley dispone que la prueba se apreciara en conciencia por el juez y que el monto de la indemnización será establecido prudencialmente, considerando las circunstancias del caso y la gravedad de los hechos(Art. 23 inc. 3º) [282] .

9.3 Responsabilidad Penal

Ni la Ley 19.628, ni el Código Penal chileno contemplan delitos penales que sancionen conductas atentatorias contra los derechos de los titulares de los datos personales. Sin embargo, y como ya lo hemos hecho en los demás análisis, reseñaremos a modo ilustrativo aquellos tipos penales chilenos que tutelan algunos de los bienes jurídicos directamente relacionados con la protección de los datos personales; el derecho a la intimidad y a la vida privada, lo cual en ningún caso significa que estimemos que éstos pudieran aplicarse en defensa de ataques a los derechos reconocidos en la Ley.

A continuación revisaremos los delitos relacionados con el bien jurídico intimidad y vida privada contemplados por el Código Penal, Ley 19.223 sobre delitos informáticos, Código Tributario y Ley General de Bancos.

9.3.1) Código Penal

a) Allanamiento ilegal y registro ilegal de papeles por funcionarios públicos:

El artículo 155 dispone que: *"El empleado público que abusando de su oficio, allanare un templo o la casa de cualquiera persona o hiciere registro en sus papeles, a no ser en los casos y forma que prescriben las leyes, será castigado con la pena de reclusión menor en sus grados mínimo a medio o con la de suspensión en cualquiera de sus grados".*

Por su parte, el artículo 156 preceptúa que: *"Los empleados en el Servicio de Correos y Telégrafos u otros que prevaliéndose de su autoridad interceptaren o abrieren la correspondencia o facilitaren a tercero su apertura o supresión, sufrirán la pena de reclusión menor en su grado mínimo y, si se aprovecharen de los secretos que contiene o los divulgaren, las penas serán reclusión menor en cualquiera de sus grados y multa de once a veinte sueldos vitales.* El inciso 2º agrega que: *"en los casos de retardo doloso en*

[281] El artículo 23 de la Ley 19.628 se remite al artículo 173 del Código de Procedimiento Civil, para señalar que será aplicable la denominada reserva de la determinación del monto y la especie de los perjuicios en un juicio diverso al de determinación de responsabilidad civil por parte del demandante.

[282] De lo dispuesto por el art. 23 inciso 3º de la Ley, surge una interesante interrogante digna de estudio, cual es, si eventualmente se estaría abriendo camino en Chile al establecimiento de los denominados daños punitivos o *punitive damages*, dada la facultad entregada a los jueces de acoger demandas de indemnización de perjuicios por daños morales, en que se tenga en cuenta las circunstancias del caso y la gravedad de los hechos, dentro de las cuales podría caber una interminable lista de elementos de reproche subjetivo a la conducta del autor del daño, dejándose de lado la construcción del estándar de conducta debido, prescindiendo de esa subjetividad.

el envío o entrega de la correspondencia epistolar o de partes telegráficos, la pena será reclusión menor en su grado mínimo".

b) Violación de domicilio:

Este delito se encuentra tipificado en el artículo 144 del Código Penal y señala en su primera parte que: "*el que entrare en morada ajena contra la voluntad de su morador, será castigado con reclusión menor en su grado mínimo o multa de seis a diez sueldos vitales".*

c) Violación de correspondencia *:*

El artículo 146 a su vez dispone: *"El que abriere o registrare la correspondencia o los papeles de otro sin su voluntad, sufrirá la pena de reclusión menor en su grado medio si divulgare o se aprovechare de los secretos que ellos contienen, y en el caso contrario la de reclusión menor en su grado mínimo.* El inciso 2º agrega que *"esta disposición no es aplicable entre cónyuges, ni a los padres, guardadores o quienes hagan sus veces, en cuanto a los papeles o cartas de sus hijos o menores que se hallen bajo su dependencia* El inciso final prescribe a su vez que *"tampoco es aplicable a aquellas personas a quienes por leyes o reglamentos especiales, les es lícito instruirse de correspondencia ajena".*

d) Delitos contra el respeto y protección a la vida privada y pública de la persona y su familia:

El Código Penal chileno designa de esta manera a los delitos contenidos en el parágrafo 5 del Título III, Libro II, los cuales se encuentran tipificados en dos artículos, el 161-A y 161-B. Sólo haremos referencia al primero de éstos.

Artículo 161-A.- "*Se castigará con la pena de reclusión menor en cualquiera de sus grados y multa de 50 a 500 Unidades Tributarias Mensuales al que, en recintos particulares o lugares que no sean de libre acceso al público, sin autorización del afectado y por cualquier medio, capte, intercepte, grabe o reproduzca conversaciones o comunicaciones de carácter privado*; *sustraiga, fotografíe, fotocopie o reproduzca documentos o instrumentos de carácter privado; o capte, grabe, filme o fotografíe imágenes o hechos de carácter privado que se produzcan, realicen, ocurran o existan en recintos particulares o lugares que no sean de libre acceso al público.*

Igual pena se aplicará a quien difunda las conversaciones, comunicaciones, documentos, instrumentos, imágenes y hechos a que se refiere el inciso anterior.

En caso de ser una misma la persona que los haya obtenido y divulgado, se aplicarán a ésta las penas de reclusión menor en su grado máximo y multa de 100 a 500 Unidades Tributarias Mensuales.

Esta disposición no es aplicable a aquellas personas que, en virtud de ley o de autorización judicial, estén o sean autorizadas para ejecutar las acciones descritas".

Cabe comentar de la disposición anterior, que si bien ésta protege los bienes

jurídicos vida privada e intimidad de las personas, resulta de difícil aplicación para tutelar el derecho a la autodeterminación informativa. Primero, porque ese derecho fue excluido expresamente por el legislador chileno en la Ley 19.628, y segundo, porque igual situación ocurrió en materia penal, es decir, no se estimaron dignos de tutela penal los derechos reconocidos por la Ley. No obstante lo anterior, podría darse en la práctica el caso en que alguien sustrajera documentos en alguna de las formas tipificadas por el artículo 161-A, que contengan información que pudiera calificarse de reservada o incluso datos sensibles y que luego procediera a divulgar tal información. La situación anterior, eventualmente podría ser subsumible en la hipótesis del inciso 2º y/o 3º del artículo señalado. Con todo, el límite a cualquier conclusión a este respecto viene dado por el principio de legalidad, el cual debe ser siempre tenido a la vista [283] .

e) Violación de secretos:

El parágrafo 8 del Título V, Libro II del Código Penal lleva el título anterior, dentro del cual se contemplan dos artículos. Éstos son los siguientes:

Art. 246.-"*El empleado público que revelare los secretos de que tenga conocimiento por razón de su oficio o entregare indebidamente papeles o copia de papeles que tenga a su cargo y no deban ser publicados, incurrirá en las penas de suspensión del empleo en sus grados mínimo a medio o multa de seis a veinte sueldos vitales, o bien en ambas conjuntamente".*

"Si de la revelación o entrega resultare grave daño para la causa pública, las penas serán reclusión mayor en cualquiera de sus grados y multa de veintiuno a treinta sueldos vitales".

A continuación, el artículo 247 preceptúa que: *"El empleado público que, sabiendo por razón de su cargo los secretos de un particular, los descubriere con perjuicio de éste, incurrirá en las penas de reclusión menor en sus grados mínimo a medio y multa de seis a diez sueldos vitales".* El inciso 2º de esta norma tipifica el delito de violación de secretos, haciendo aplicable las mismas penas del inciso 1º *"a los que, ejerciendo alguna de las profesiones que requieren título, revelen los secretos que por razón de ella se les hubieren confiado".*

Ley N º 19.223 que Tipifica Figuras Penales Relativas a la Informática

Esta ley del año 1993, señala en su artículo 2º que: "*El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio".* Más adelante, el artículo 4º dispone: "*El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado*".

Los artículos anteriores plantean una serie de dudas interpretativas cuya dilucidación

[283] El principio de legalidad en materia penal tiene cuatro consecuencias de máxima importancia, las cuales se traducen en que no hay crimen ni pena sin ley escrita (*scripta)*, estricta (*stricta*), previa (*praevia*) y cierta (*certa*).

exceden con todo la finalidad de esta memoria, por lo tanto, no nos aventuraremos en esta materia y dejamos entregada la discusión de una eventual aplicación de estos tipos para la protección de los datos personales a los estudiosos del derecho penal y a la jurisprudencia.

9.3.3) Código Tributario

El artículo 30 inciso 4º del Código Tributario prescribe que las personas que, a cualquier título, reciban o procesen las declaraciones o giros quedan sujetas a obligación de reserva absoluta de todos aquellos antecedentes individuales de que conozcan en virtud del trabajo que realizan. La infracción a este deber *"será sancionada con reclusión menor en su grado medio y multa de 5 a 100 UTM".*

9.3.4) Ley General de Bancos

El artículo 154 de esta ley señala que: *"Los depósitos y captaciones de cualquiera naturaleza que reciban los bancos están sujetos a secreto bancario y no podrán proporcionarse antecedentes relativos a dichas operaciones sino a su titular o a quien haya sido expresamente autorizado por él o a la persona que lo represente legalmente".* A continuación tipifica un delito, señalado que "*El que infringiere la norma anterior será sancionado con la pena de reclusión menor en sus grados mínimo a medio".* Por lo tanto, la infracción a este deber de secreto es constitutiva de delito penal.

10. Códigos de Conducta

La legislación chilena, no contempla la creación ni fomenta el desarrollo de códigos deontológicos de buena práctica profesional por parte de las asociaciones o entidades representativas de responsables o usuarios de bancos de datos, que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información que realizan tratamiento de datos personales. Cabría entonces analizar en profundidad la conveniencia o no de propender a la autorregulación en materia de protección de datos en Chile, pues para que pueda funcionar adecuadamente se necesitaría de la confluencia de diversos factores uno de los cuales lamentablemente se ve cada vez más mermado, nos referimos a la confianza.

11. Conclusiones

El ordenamiento jurídico chileno no contempla constitucionalmente el derecho a la protección de datos personales. Sólo reconoce la protección y defensa de la vida privada, de la cual deriva toda la protección legal a los datos personales plasmada en la Ley 19.628. Esta tutela legal, si bien ha significado un avance en la materia, no es suficiente para poder garantizar efectivamente los derechos de las personas ante el tratamiento de sus datos personales, pues faltan diversos elementos para que se pueda hablar de un sistema de protección de datos, tales como, principios más consistentes y explícitos, un deber general de inscripción de los bancos de datos y la existencia de un órgano de

control, entre otros. Al respecto, alguna doctrina ha sido crítica en este punto señalando que es necesaria una modificación legal que se ajuste a los modelos comparados de protección de datos, en especial al europeo. Cabe agregar a lo dicho, que hace falta una legislación sistemática que se haga cargo de todas aquellas disposiciones legales aisladas contempladas en estatutos especiales, con la finalidad de lograr una ley armónica y ordenada, que pretenda ser autosuficiente y evite tener que remitirse *ad infinitum* a estatutos especiales.

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN COLOMBIA

1. Generalidades

El ordenamiento jurídico colombiano consagra una protección constitucional a los datos personales a través del artículo 15 de la Carta Fundamental de 1991. No obstante esta previsión, no cuenta Colombia a nivel legal con una ley de protección de datos personales. Ha sido la jurisprudencia constitucional la que ha tenido que llenar los vacíos legales a través de la revisión de las acciones de tutela constitucional. Sin embargo, existe consenso general en todos los estamentos colombianos de la necesidad de una ley estatutaria que regule la materia en estudio. A este respecto puede mencionarse que existen actualmente dos proyectos de ley que se tramitan conjuntamente en el Senado colombiano en materia de protección de datos.

2. Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional

La Constitución colombiana [284] señala en su artículo 15 que todas las personas tienen derecho a su "*intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas".* Luego agrega que: *"en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución".* De esta forma, el Constituyente colombiano ha consagrado como derecho al hábeas data (lo que en nuestro concepto sería equivalente al derecho a la protección de datos) sin indicar remedio judicial específico que tutele de manera exclusiva los derechos de acceso, actualización y rectificación de las informaciones recogidas en los bancos de datos o archivos. Esta falta de previsión

[284] [En línea] < http://www.georgetown.edu/pdba/Constitutions/Colombia/col91.html > [consulta: 6 de Noviembre 2002].

constitucional es suplida por la aplicación del artículo 86 de la Constitución, el cual se señala que: *"toda persona tendrá acción de tutela para reclamar ante los jueces, en todo momento y lugar, mediante un procedimiento preferente y sumario, por sí misma o por quien actúe a su nombre, la protección inmediata de sus derechos constitucionales fundamentales, cuando quiera que éstos resulten vulnerados o amenazados por la acción o la omisión de cualquier autoridad pública*". Luego, el inciso final de este mismo artículo señala el camino a seguir en caso que sea un particular el que afecte el derecho, diciendo que: "*la ley establecerá los casos en los que la acción de tutela procede contra particulares encargados de la prestación de un servicio público o cuya conducta afecte grave y directamente el interés colectivo, o respecto de quienes el solicitante se halle en estado de subordinación o indefensión".*

Comentando el hábeas data colombiano, Cifuentes ha señalado que "aunque en estricto rigor el hábeas data corresponde a un específico proceso constitucional ideado para cumplir diversos propósitos, en la Constitución se enuncian, a título de derecho sustantivo, varias facultades de la persona concernida por los datos y se confía a la acción de tutela, en principio, su protección judicial" [285] . Esto se ha dicho a propósito del análisis de la naturaleza jurídica y ubicación del derecho en cuestión, pues dada la redacción del texto constitucional, en principio podría parecer que sólo se comprenderían las facultades enunciadas en éste. Lo anterior no es tan así, pues se ha señalado que la Corte Constitucional colombiana nunca ha puesto en duda que el hábeas data ostente la condición de derecho fundamental [286] .

2.2 Protección Legal de los Datos Personales

A nivel legal, el ordenamiento jurídico colombiano no dispone de una ley de protección de datos personales. Este vacío ha sido suplido en parte por la vía jurisprudencial. Sin embargo, para Palazzi, esa vía casuística, no es capaz de contemplar el conjunto de eventos y asuntos que normalmente integran una norma exhaustiva en esta materia. Así, ha señalado que no se puede negar que la jurisprudencia de la Corte se ha generado en torno de los bancos de datos financieros, y sólo marginalmente se ha referido a otros bancos de datos" [287] .

Cabe anotar que existe amplio consenso tanto en la doctrina como en la jurisprudencia para que se dicte a la brevedad una ley de protección de los datos personales. Al respecto, tenemos que hacer presente que en la actualidad se tramita en el Senado un proyecto de ley estatutaria presentado por el Poder Ejecutivo, el cual pretende regular el derecho de acceso a la información de interés público, en particular la de carácter comercial y financiero. Asimismo, propone regular aquella información

[285] Cifuentes Muñoz, Eduardo: *"El Hábeas Data en Colombia"*. En Revista Ius Et Praxis, Universidad de Talca, año 3 Nº 1, Talca, 1997, pág. 87. En este mismo sentido Puccinelli, quien señala que "el hábeas data debiera ser reconocido como un proceso constitucional en vez de como derecho" (Puccinelli, Óscar, *op cit*., pág. 375).

[286] Puccinelli, Óscar, *Ibídem.*

[287] Palazzi Pablo,2002, *op. cit*., pág. 67.

relacionada con el cumplimiento de obligaciones fiscales y parafiscales, y con el pago de servicios públicos domiciliarios, además de otras disposiciones [288] .

En otros ámbitos más específicos, como el relativo a las informaciones de carácter financiero o el secreto fiscal, existen algunas normas sectoriales que se refieren a la protección de los datos personales. En materia de secreto bancario, siguiendo a Del Villar y otros, cabe mencionar que en Colombia no existe en materia financiera una ley que expresamente se refiera al secreto bancario. A pesar de lo anterior, se señala que tanto la doctrina como la jurisprudencia admiten unánimemente la existencia de ese deber de discreción, el cual es considerado como un principio que deben respetar la banca y los profesionales de los negocios bancarios. Se agrega por estos autores que, existen diversos textos u ordenamientos legales, que aún cuando no sean leyes, consagran el secreto bancario. Ejemplo de lo anterior lo constituye la Circular Externa 07 de 1996 de la Superintendencia Bancaria que establece la reserva bancaria como una de las obligaciones especiales de las entidades vigiladas por ésta, definiéndola como el deber que tienen los funcionarios de las entidades financieras y aseguradoras de guardar reserva y discreción sobre los datos de sus clientes o sobre aquellos relacionados con la situación propia de la compañía, que conozcan en desarrollo de su profesión u oficio. Sin embargo, se agrega, que la Corte Constitucional colombiana ha establecido que el derecho al secreto bancario no debe impedir que fluya información hacia quienes otorgan crédito [289] . A continuación revisaremos la normativa legal sectorial específica colombiana.

2.2.1) Ley Nº 550-1999 que establece un Régimen que Promueva y Facilite la Reactivación Empresarial [290]

Esta ley dispone en su artículo 76 que: *"las personas que dentro de los diez (10) meses siguientes a la vigencia de la presente ley se pongan al día en obligaciones por cuya causa hubieren sido reportadas a los bancos de datos de que trata este artículo, tendrán un alivio consistente en la caducidad inmediata de la información negativa, sin importar el monto de la obligación e independientemente de si el pago se produce judicial o extrajudicialmente. La Defensoría del Pueblo velará por el cumplimiento de esta norma"*. Esta disposición establece la caducidad de los registros de morosidades en los bancos de datos que suministren regularmente datos financieros o sobre solvencia patrimonial y crediticia, los cuales sólo pueden tratar automatizadamente datos personales obtenidos de fuentes accesibles al público o procedentes de informaciones recogidas mediante el consentimiento libre, expreso, informado y escrito de su titular. Con todo, del tenor de las

[288] El Proyecto de Ley Estatutaria es el Nº 71 y fue presentado en Septiembre de 2002. Actualmente se encuentra aprobado por la Comisión Primera del Senado con fecha 22 de Octubre de 2002. Cabe hacer presente que conjuntamente con este Proyecto se tramita el Proyecto de Ley Estatutaria Nº 75 de 2002, el cual ha sido acumulado al primero. [En línea] < http://www.superbancaria.gov.co/gobierno/Proynorma/proyectosley.htm > [consulta: 14 de Enero 2003].

[289] Todo lo anterior en Del Villar, Rafael "et al", *op. cit*., págs. 53 y 54.

[290] [En línea] < http://www.supersociedades.gov.co/ss/drvisapi.dll?MIval=sec&dir=96 > [consulta: 3 de Febrero 2003].

disposiciones transcritas se deduce el carácter excepcional que tiene la normativa, coyuntural a la situación económica colombiana.

2.2.2) Ley Nº 510 de 1999 [291]

El artículo 114 de la Ley Nº 510 de 1999, establece algunas reglas para el tratamiento de datos de carácter financiero señalando que: *"previo el pago de la tarifa que autorice la Superintendencia Bancaria y la solicitud escrita de su titular, el responsable del banco de datos deberá comunicarle las informaciones difundidas y el nombre y dirección del cesionario. Sólo se podrán registrar y ceder los datos que, según las normas o pautas de la Superintendencia Bancaria y de conformidad con el artículo 15 de la Constitución, se consideren relevantes para evaluar la solvencia económica de sus titulares. Los datos personales que recojan y sean objeto de tratamiento deben ser pertinentes, exactos y actualizados, de modo que correspondan verazmente a la situación real de su titular"*. No obstante lo recién expuesto, surgen dudas acerca de la eficacia con que se esté aplicando tanto el artículo 114 de la Ley Nº 510 como el artículo 76 de la Ley Nº 550, dado que la Corte Constitucional tiene facultades para declarar inexequible las normas que no se ajusten a la Constitución. En este sentido la Alta Corte ha sostenido que las leyes que regulen el derecho constitucional del hábeas data, deben tener el carácter de Ley Estatutaria, es decir, ley aprobada con quórum más alto que el de simple ley, entre otras diferencias, especial calidad que no tiene la ley recién citada [292] .

2.2.3) Ley General de Procedimiento Tributario [293]

El artículo 583 de este cuerpo legal establece el carácter reservado de las declaraciones tributarias, disponiendo que: *"la información tributaria respecto de las bases gravables y la determinación privada de los impuestos que figuren en las declaraciones tributarias, tendrá el carácter de información reservada; por consiguiente, los funcionarios de la Dirección General de Impuestos Nacionales sólo podrán utilizarla para el control, recaudo, determinación, discusión y administración de los impuestos y para efectos de informaciones impersonales de estadística"*. Más adelante agrega que: "*los bancos y demás entidades que en virtud de la autorización para recaudar los impuestos y recibir las declaraciones tributarias, de competencia de la Dirección General de Impuestos Nacionales, conozcan las informaciones y demás datos de carácter tributario de las declaraciones, deberán guardar la más absoluta reserva con relación a ellos y sólo los podrán utilizar para los fines del procesamiento de la información, que demanden los*

291 [En línea] < http://www.secretariasenado.gov.co/leyes/L0510_99.HTM > [consulta: 7 de Enero 2003].

292 Este fue el razonamiento para declarar inconstitucional el Proyecto de Ley 127/93 que establecía algunas disposiciones relativas a la actividad de recolección, manejo, conservación y divulgación de información comercial, cuyo objetivo central era restringir al máximo el hábeas data referido a los bancos de datos financieros. Sentencia C-008 del 17 de Enero de 1995 (citado por Puccinelli, *op. cit*., pág. 369).

293 [En línea] < http://www.ciat.org/doc/docu/leg/cod/lal_colom_02_ley_procedimiento_tributario.doc >, [consulta: 3 de Enero 2003].

reportes de recaudo y recepción, exigidos por el Ministerio de Hacienda y Crédito Público".

En las disposiciones recién transcritas se puede apreciar la regla general que rige en materia tributaria, cual es el deber de reserva por parte de los funcionarios fiscales y de aquellas personas que en razón de su oficio tienen conocimiento de las declaraciones impositivas.

El parágrafo de este artículo, señala además que para fines de control al lavado de activos, la Dirección de Impuestos y Aduanas Nacionales deberá remitir, a solicitud de la dependencia encargada de investigar el lavado de activos, la información relativa a las declaraciones e investigaciones de carácter tributario, aduanero y cambiario, que posea en sus archivos físicos y/o en sus bases de datos (Parágrafo adicionado por el art. 89 de la Ley 488 de 24/12/98). Con ello, se establece una excepción a la regla, la cual debe ser justificada sólo en base a la investigación por lavado de dinero.

Por otra parte, el artículo 585 señala que para los efectos de los impuestos nacionales, departamentales o municipales se puede *"intercambiar información sujeta a secreto".* Asimismo, para los efectos de liquidación y control de impuestos nacionales, departamentales o municipales, podrán intercambiar información sobre los datos de los contribuyentes, el Ministerio de Hacienda y las Secretarias de Hacienda Departamentales y Municipales. El artículo 586 por su lado, hace extensiva la garantía de la reserva a las entidades contratadas para el manejo de información tributaria [294] .

Finalmente el artículo 587 establece otras excepciones al secreto fiscal. En estos casos es la Dirección General de Impuestos Nacionales la que podrá levantar la reserva de las declaraciones de impuestos en relación con los pagos laborales objeto del aporte, para efectuar cruces de información con el Instituto de Seguros Sociales, el Instituto Colombiano de Bienestar Familiar, el Servicio Nacional de Aprendizaje, y las respectivas cajas de compensación familiar, así como sus asociaciones o federaciones, tendientes a verificar el cumplimiento del pago de los aportes a dichas entidades a petición de cualesquiera de estos organismos. Como es obvio, en virtud de esta autorización el Estado se facilita a sí mismo los deberes de fiscalización tributaria al permitirse el cruce de informaciones entre distintas reparticiones del Estado.

2.2.4) Ley Nº 546-1999 que Regula el Financiamiento de las Viviendas

El artículo 52 de esta ley, también responde a una situación excepcional relativa a la coyuntura económica del país, pues en lo relativo al registro en centrales de riesgo de los

[294] Artículo 586.- Garantía de la reserva por parte de las entidades contratadas para el manejo de información tributaria. *"Cuando se contrate para la Dirección General de Impuestos Nacionales, los servicios de entidades privadas para el procesamiento de datos, liquidación y contabilización de los gravámenes por sistemas electrónicos, podrá suministrarles informaciones globales sobre la renta y el patrimonio bruto de los contribuyentes, sus deducciones, rentas exentas, exenciones, pasivos, bienes exentos, que fueren estrictamente necesarios para la correcta determinación matemática de los impuestos, y para fines estadísticos. (…) Las entidades privadas con las cuales se contraten los servicios a que se refiere el inciso anterior, guardarán absoluta reserva acerca de las informaciones que se les suministren, y en los contratos respectivos se incluirá una caución suficiente que garantice tal obligación".*

deudores de créditos de vivienda individual a largo plazo, dispone que aquellas personas que reestructuren sus créditos hipotecarios según esta Ley "*tendrán derecho a exigir que sus nombres se retiren como deudores morosos de las centrales de riesgo, una vez hayan cumplido puntualmente con el pago de las tres primeras cuotas de la obligación reestructurada*". Este mismo beneficio se extiende a los deudores hipotecarios de viviendas entregadas en dación en pago con posterioridad al 1° de enero de 1997, los que tendrán derecho a que las entidades financieras los declaren a paz y en salvo por el crédito respectivo y retiren sus nombres de las centrales de riesgo (inciso 2º). En suma, el fin de esta norma es incentivar la repactación de deudas, otorgando un premio para quienes lo hagan en la forma que la ley prescribe. Este parece ser un buen ejemplo legislativo de las poco utilizadas sanciones premiales.

3. Bienes Jurídicos Protegidos por la Legislación de Datos Personales

Como ya se ha dicho, el ordenamiento jurídico colombiano no dispone de una legislación que se ocupe de la protección de datos personales, sólo la Constitución reconoce de manera confusa el hábeas data, para algunos en carácter de derecho fundamental, pero sin regular su forma de tutela. A pesar del vacío legal ya constatado, es pertinente detenerse a analizar el bien jurídico protegido por las normas constitucionales.

Se ha señalado por la doctrina que en relación al hábeas data propio la cuestión presenta aristas particulares por cuanto la jurisprudencia de la Corte Constitucional ha tenido una evolución destacada. En un primer momento -el cual puede situarse a partir de la reforma constitucional de 1991- se señaló por la Corte que el bien jurídico protegido era la intimidad, pero sin desconocer la honra ni la libertad contra los abusos del poder informático [295] . Cifuentes Muñoz ha expresado que "la Corte Constitucional, en un primer momento, no dudó en acomodar conceptualmente el Hábeas Data dentro del ámbito del derecho a la intimidad. En esa oportunidad se precisó que la intimidad se proyectaba en dos dimensiones: como secreto de la vida privada (sentido estricto) y como libertad (sentido amplio). La primera dimensión ofrecería la visión tradicional de la intimidad marcadamente individualista y portadora de facultades de exclusión de signo negativo. La segunda, conferiría a la intimidad el carácter de libertad pública y la habilitaría para enfrentar las amenazas que en el mundo moderno se ciernen sobre ella" [296] .

Posteriormente, la Corte constató que el denominado 'derecho de hábeas data' no solo protege la intimidad, sino que algo más que ésta. Así, se arriba a un criterio unificador interpretativo el cual señala que el núcleo esencial del hábeas data estriba en la defensa del derecho a la autodeterminación informática, el que faculta al titular de los

[295] Así, se dijo en un primer momento por la Corte Constitucional que: "la Sala estima conveniente señalar en forma muy somera algunos alcances de esta nueva disposición con la cual el Constituyente ha querido, en buena medida, proteger la intimidad, la honra y al libertad contra los abusos del poder vinculado estrechamente, según se verá, con los adelantos tecnológicos (…)". Citado por Puccinelli, *op. cit*., pág. 385.

[296] Cifuentes Muñoz, Eduardo, *op. cit*., pág. 87.

datos que constan en archivos públicos o privados, para autorizar la conservación, uso y circulación de los mismos. Cifuentes agrega al respecto, que dos consecuencias principales se seguirían de esa caracterización del hábeas data como derecho fundamental; "de una parte, la regulación de este derecho y la determinación de los procedimientos y recursos para su protección sólo pueden consagrarse a través de leyes estatutarias (se aprueban por mayoría absoluta de los miembros del Congreso dentro de una sola legislatura y su trámite comprende la revisión previa de la constitucionalidad del proyecto por parte de la Corte Constitucional). De otra parte, entre los mecanismos de defensa judicial del derecho, se destaca la acción de tutela que puede reclamarse ante cualquier juez, en todo momento y lugar, mediante un procedimiento preferente y sumario" [297] . Una tercera posición respecto al bien jurídico protegido señala que es la dignidad aquel objeto jurídico merecedor de tutela [298] . Finalmente, se ha afirmado también por Puccinelli que los bienes dignos de protección jurídica serían la honra, la reputación y la imagen, los cuales se encuentran contenidos en el artículo 15 de la Constitución colombiana [299] .

En suma, la consideración del bien jurídico protegido por las disposiciones constitucionales que brindan protección a los datos personales, no ha sido uniforme en el tiempo en Colombia. En la actualidad, sin embargo, es posible afirmar que rige sin contrapeso la idea que el bien jurídico protegido es el derecho a la autodeterminación informativa o libertad informática a partir de la consideración del hábeas data como un derecho fundamental [300] .

4. Principios Informativos de la Legislación de Protección de Datos Personales

En atención a la falta de ley de protección de datos personales en el ordenamiento jurídico colombiano, no nos referiremos a esta materia.

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

Dada la inexistencia de una ley general de protección de datos personales en el ordenamiento jurídico colombiano, tampoco nos detendremos en este punto.

6. Modelos de Tutela

297 Cifuentes Muñoz, Eduardo, *op. cit*., pág. 88.

298 Puccinelli, *op. cit*., pág. 388.

299 *Ídem*, pág. 391.

300 Para una explicación más detallada y con referencias jurisprudenciales, Puccinelli, *op. cit*., págs. 384-392.

Para la protección del derecho consagrado en el artículo 15 de la Constitución colombiana denominado hábeas data, se dispone de la "*acción de tutela constitucional"* de los derechos fundamentales, establecida en el artículo 86 de la propia Carta y no de una acción propia de hábeas data [301] . Como ya se señaló, esta acción procede sin restricciones en contra de actos u omisiones de autoridades públicas, lo cual no ocurre en caso de ser un privado quien amenace, perturbe o lesione un derecho fundamental. A continuación nos referiremos a ambas, señalando en cada caso las diferencias entre una y otra.

6.1 La Acción de Tutela

Como ya se ha dicho, esta acción se consagra en el artículo 86 de la Constitución. Su regulación procedimental así como también su procedencia respecto de actos u omisiones de particulares, ha sido entregada al Poder Ejecutivo (Decreto Nº 2.591 de 1991) [302] . Éste, a su vez se encuentra reglamentado por otro Decreto, el Nº 306 de 19 de febrero de1992.

6.1.1) Procedencia de la Acción

La Constitución concede la acción de tutela sin restricciones cuando la vulneración o amenaza de los derechos fundamentales proviene de la acción u omisión de cualquier *autoridad pública*, con lo que en principio esta acción tendría como sujeto pasivo sólo a los funcionarios del Estado. Luego, el inciso 4º del artículo 86, se encarga de ampliar la procedencia de la acción de tutela respecto de los particulares pero dejando la determinación de las circunstancias y los casos de procedencia al legislador. El texto reza así: *" La ley establecerá los casos en los que la acción de tutela procede contra particulares encargados de la prestación de un servicio público o cuya conducta afecte grave y directamente el interés colectivo, o respecto de quienes el solicitante se halle en estado de subordinación o indefensión".* La disposición normativa que regula la acción de tutela en este caso es el artículo 42 del Decreto Nº 2.591 de 1991, el cual señala los casos en los cuales es procedente la acción de tutela contra particulares [303] . En razón de lo anterior y, para analizar adecuadamente la procedencia de la acción de tutela es preciso hacer una distinción:

a) *Acción de tutela en contra de actos u omisiones de autoridades públicas*: la acción tiene por objeto la protección inmediata del derecho constitucional fundamental de hábeas data (según la concepción mayoritaria), cuando quiera que resulte vulnerado o amenazado por la acción o la omisión de cualquier autoridad pública, cuando el afectado no disponga de otro medio de defensa judicial (Art. 86 C. Pol. y Art. 5 Decreto 2.591).

[301] Esta situación se produce dada la consagración del hábeas data como derecho y no como garantía constitucional, en cuanto no indica remedio alguno específicamente diseñado para tutelar de manera exclusiva los derechos que confiere el hábeas data. En Puccinelli, *op. cit*., págs. 371 y 373.

[302] Cifuentes Muñoz, Eduardo, *op. cit*., pág. 168.

[303] *Ibídem.*

b) *Acción de tutela en contra de actos u omisiones de particulares*: la acción de tutela procederá para la protección inmediata del derecho constitucional fundamental de hábeas data, cuando quiera que resulte vulnerado o amenazado por la acción o la omisión de particulares, cuando el afectado no disponga de otro medio de defensa judicial (Art. 42 Decreto 2.591).

En cuanto al carácter subsidiario que presenta esta acción, se ha señalado tanto por la jurisprudencia como por el Decreto 2.591 de 1991, que es necesario que "el medio alternativo sea idóneo y eficaz atendidas las circunstancias en que se encuentre el demandante" [304] . Por lo tanto, el requisito para la procedencia de la acción de tutela de no disponer de otro medio de defensa judicial, ha sido interpretado de manera que no haga ilusoria una protección que pueda llegar muy tarde, o con menores alcances de eficacia, lo que parece del todo razonable.

6.1.2) Legitimación Activa

La acción de tutela del hábeas data, tiene como sujetos activos a todas las personas (Art. 86 C. Pol. y 42 del Decreto 2.591). Se ha discutido la titularidad de las personas jurídicas al respecto, pero en general se admite que éstas puedan accionar por ésta vía para resguardar sus derechos [305] . También podrá ejercerla el Defensor del Pueblo y los personeros municipales (Art. 10, Decreto 2.591).

6.1.3) Legitimación Pasiva

Legitimados pasivos de esta acción pueden serlo tanto "las personas naturales o jurídicas, públicas o privadas, que organicen bancos de datos diseñados con el fin de poner en circulación los datos que almacenen o con aptitud para hacerlo (sic) y generar información a terceros" [306] .

6.1.4) Competencia

Los tribunales encargados de conocer y fallar estas acciones son todos aquellos "con jurisdicción en el lugar donde hubiere ocurrido la violación o amenaza de vulneración del derecho fundamental, quienes son competentes a prevención" (sic) [307] (Arts. 37 y 40 Decreto 2.591).

6.1.5) Procedimiento Aplicable

Señala la Constitución que en cuanto al procedimiento aplicable a la acción de tutela,

[304] Cifuentes Muñoz, Eduardo: *"La Acción de Tutela en Colombia"*. En Revista Ius et Praxis, Universidad de Talca, año 3 Nº 1, Talca, 1997, pág. 170.

[305] En este sentido la jurisprudencia, Cifuentes y Dueñas Ruiz. Todo lo anterior en Puccinelli, *op. cit*., págs. 392 y 393.

[306] *Ídem*, pág. 393.

[307] Cifuentes, Eduardo, 1997 (2), *op. cit.*, pág. 173.

éste tendrá el carácter de preferente y sumario. Luego el Decreto 2.591 se encarga de regularlo.

1)*Demanda*: el escrito de demanda no requiere de mayores formalidades, incluso se autoriza la interposición verbal cundo el solicitante sea menor de edad, no sepa escribir o en casos urgentes [308] . La acción puede interponerse por cualquier persona sin necesidad de intervención de un abogado. La agencia oficiosa también es admitida. El Defensor del Pueblo y los Personeros también están facultados para interponerla en nombre de personas que así lo soliciten o se encuentren en situación de desamparo o indefensión [309] .

2) *Tramitación*: ella estará a cargo del juez, del presidente de la sala o magistrado a quien éste designe, en turno riguroso, y será sustanciada con prelación para lo cual se pospondrá cualquier asunto de naturaleza diferente (Art. 15). En cuanto al plazo para la resolución del asunto, se señala que éste no puede exceder los 10 días desde que se haya solicitado la tutela (Art. 86 C. Pol.).

3) *Informe*: el juez podrá requerir informes al órgano o a la autoridad contra quien se hubiere hecho la solicitud y pedir el expediente administrativo o la documentación donde consten los antecedentes del asunto. La omisión injustificada de enviar esas pruebas al juez acarreará responsabilidad. El plazo para informar será de uno a tres días, y se fijará según sea la índole del asunto, la distancia y la rapidez de los medios de comunicación(Art. 19 Decreto 2.591). Además, el juez cuenta con amplias facultades para decretar las diligencias que estime necesarias, incluso puede fallar aún sin que se hayan realizado todas las diligencias ordenadas, en tanto el juez haya logrado la convicción para fallar en un determinado sentido (Art. 22 Decreto 2.591) [310] .

4) *Medidas cautelares*: el juez está facultado para decretar medidas cautelares, entre las cuales destaca la suspensión temporal de la aplicación del acto causante de la lesión así como las medidas de conservación o seguridad que eviten daños o los aminoren (Art. 8 Decreto 2.591).

6.1.6) La Sentencia

[308] Al respecto, el artículo 14 del Decreto 2.591 señala que: *"En la solicitud de tutela se expresará, con la mayor claridad posible, la acción o la omisión que la motiva, el derecho que se considera violado o amenazada o del agravio, y la descripción de las demás circunstancias relevantes para decidir la solicitud. También contendrá el nombre y el lugar de residencia del solicitante. (…) No será indispensable citar la norma constitucional infringida, siempre que se determine claramente el derecho violado o amenazado. La acción podrá ser ejercida, sin ninguna formalidad o autenticación, por memorial, telegrama u otro medio de comunicación que se manifieste por escrito, para lo cual se gozará de franquicia. No será necesario actuar por medio de apoderado. (…) En caso de urgencia o cuando el solicitante no sepa escribir o sea menor de edad, la acción podrá ser ejercida verbalmente. El juez deberá atender inmediatamente al solicitante, pero, sin poner en peligro el goce efectivo del derecho, podrá exigir su posterior presentación personal para recoger una declaración que facilite proceder con el trámite de la solicitud, u ordenar al secretario levantar el acta correspondiente sin formalismo alguno".*

[309] *Ídem*, pág. 171.

[310] *Ídem*, pág. 172.

El artículo 23 del Decreto estudiado señala que: *"cuando la solicitud se dirija contra una acción de la autoridad el fallo que conceda la tutela tendrá por objeto garantizar al agraviado el pleno goce de su derecho, y volver al estado anterior a la violación, cuando fuere posible".* Cuando lo impugnado hubiere sido la denegación de un acto o una omisión, este mismo artículo señala que: *"el fallo ordenará realizarlo o desarrollar la acción adecuada, para lo cual se otorgará un plazo prudencial perentorio. Si la autoridad no expide el acto administrativo de alcance particular u lo remite al juez en el término de 48 horas, éste podrá disponer lo necesario para que el derecho sea libremente ejercido sin más requisitos. Si se hubiere tratado de una mera conducta o actuación material, o de una amenaza, se ordenará su inmediata cesación, así como evitar toda nueva violación o amenaza, perturbación o restricción".* Si la violación o amenaza tiene origen en la aplicación de una disposición de rango legal, el juez podrá decretar la inaplicabilidad de la norma, invocando la "excepción de inconstitucionalidad" (sic)" [311] .

Finalmente, la sentencia que resuelve la acción de tutela es apelable, debiendo elevarse los autos dentro de los tres días siguientes a su notificación [312] . El tribunal *ad quem* está obligado a fallar dentro de los 20 días siguientes al de haber recibido el expediente. Dictada la sentencia de apelación, ésta se envía a la Corte Constitucional para su revisión, la cual es discrecional, pues las sentencias son seleccionadas unilateralmente por la Corte. En el caso de avocarse la revisión de una sentencia, la Corte tiene tres meses para pronunciarse desde que se seleccionó ésta para su revisión [313] .

Cabe comentar respecto de la revisión de la sentencia que falla la acción de tutela y que no es impugnada, que el mecanismo contemplado por el ordenamiento jurídico colombiano de revisión discrecional por parte de la Corte Constitucional, no parece ser el más adecuado, pues debieran explicitarse, al menos, las motivaciones objetivas que deben estar presentes para elegir entre un caso y otro. En otras palabras, creemos que la elección debiera basarse en consideraciones explicitadas por la propia ley, y no en criterios que no pueden conocerse por la ciudadanía.

7. Mecanismos de Control

En el ordenamiento jurídico colombiano no se contempla la existencia de un órgano de control que vele por la aplicación de una normativa de protección a los datos personales, máxime si ésta no existe.

311 *Ídem*, pág., 173.

312 Al respecto se señala por el artículo 31 que: *"dentro de los tres días siguientes a su notificación el fallo podrá ser impugnado por el Defensor del Pueblo, el solicitante, la autoridad pública o el representante del órgano correspondiente, sin perjuicio de su cumplimiento inmediato. Los fallos que no sean impugnados serán enviados al día siguiente a la Corte Constitucional para su revisión.".*

313 Cifuentes, Eduardo, 1997 (2), *op. cit.*, pág. 174.

8. Transmisión Internacional de Datos

En cuanto a este punto, nada puede decirse por el momento en atención a la falta de legislación en la materia en el ordenamiento jurídico colombiano.

9. Régimen de Responsabilidad

En materia de responsabilidad, y dada la falta de ley de protección de datos, las normas eventualmente aplicables para la tutela de los derechos de los titulares de los datos deben buscarse en otros estatutos jurídicos. A continuación señalaremos dos ámbitos en los cuales podría hacerse efectiva la responsabilidad por infracción a las normas constitucionales que reconocen derechos a los titulares de los datos personales; el administrativo y el civil. En materia penal revisaremos algunas disposiciones contenidas en el código del ramo pero sólo a modo ilustrativo, la razón de ello ya la hemos explicitado.

9.1 Responsabilidad Administrativa

El ordenamiento jurídico colombiano -como ya se ha dicho- no cuenta dentro de su legislación con una ley de protección a los datos personales, ni menos con un órgano de control que vele por el cumplimiento de aquélla. Por lo tanto, creemos que a lo menos podrían aplicarse las normas establecidas en los estatutos administrativos, que sancionan las violaciones a los deberes de cargo relativos a la confidencialidad y secreto de ciertas informaciones.

En concordancia con lo recién señalado, el estatuto tributario colombiano dispone en el artículo 679 intitulado “Incumplimiento de deberes” que sin perjuicio de las sanciones por la violación al régimen disciplinario de los empleados públicos y de las sanciones penales, por los delitos, cuando fuere del caso, *“son causales de destitución de los funcionarios públicos con nota de mala conducta, las siguientes infracciones: a) La violación de la reserva de las declaraciones de renta y complementarios y de los documentos relacionados con ellas (…)”.*

Por otra parte, debemos hacer presente que el estatuto genérico colombiano aplicable a los funcionarios públicos es el Código Contencioso Administrativo, el cual dispone en el artículo 76 que son causales de mala conducta que motivarán multas hasta de un millón de pesos, o la destitución del responsable, las siguientes: *“(…) 1a) Negarse a recibir las peticiones, a expedir constancias sobre ellas, o a sellar sus copias, cuando se presenten en los días, horas y sitios que indiquen los reglamentos;(…) 4a) No dar traslado de los documentos recibidos a quien deba decidir, dentro del término legal;(…) 6a) Resolver sin motivación siquiera sumaria, cuando sea obligatoria y (…) 8a) Dilatar o entrabar el cumplimiento de las decisiones en firme o de las sentencias”* [314] .

[314] Las disposiciones anteriores pueden consultarse [en línea] < http://www.leyesnet.com/Classic/Codigos2.asp?NombreCodigoID=4 > [consulta: 8 de Febrero 2003].

9.2 Responsabilidad Civil

En materia civil, no existen normas especiales de protección de datos que contemplen la reparación de los daños causados por la violación del derecho a la protección de datos o hábeas data constitucional. Sin embargo, ello no es obstáculo para que operen ampliamente las reglas generales de la responsabilidad civil, tanto en sede contractual como en la extracontractual. Respecto de esta última, cabe aplicar el artículo 2.341 del Código Civil colombiano, el cual dispone lo siguiente: "*El que ha cometido un delito o culpa, que ha inferido a otro un daño, es obligado a la indemnización*" [315] .

En cuanto al Estado, éste también queda obligado a reparar los perjuicios si ha causado daño injusto. A esta materia se refiere el artículo 90 de la Constitución que señala: *"El Estado responderá patrimonialmente por los daños antijurídicos que le sean imputables, causados por la acción o la omisión de las autoridades públicas".* En relación a este punto, se ha dicho que esta responsabilidad se explica hoy mediante una teoría autónoma que no tiene su equivalente en el derecho civil. "Para llegar a ella la doctrina y jurisprudencia ha recorrido un largo camino que parte del reconocimiento de responsabilidad en el Estado, la que durante épocas fue negada por la jurisprudencia" [316] . Por lo tanto, el Estado también es sujeto pasivo de la acción de daños y perjuicios si éste vulnera el derecho consagrado en el artículo 15 de la Constitución.

9.3 Responsabilidad Penal

En materia penal, tampoco existen tipos delictivos que protejan directamente el bien jurídico libertad informática o el hábeas data. Sólo es posible encontrar delitos que se refieren a los otros ámbitos del derecho a la intimidad o vida privada consagrados en la Constitución. A continuación se señalan las disposiciones penales correspondientes contempladas en el Código Penal colombiano [317] .

a) Delitos contra la inviolabilidad de habitación o sitio de trabajo:

Artículo 189.-*"Violación de habitación ajena. El que se introduzca arbitraria, engañosa o clandestinamente en habitación ajena o en sus dependencias inmediatas, o que por cualquier medio indebido, escuche, observe, grabe, fotografíe o filme, aspectos de la vida domiciliaria de sus ocupantes, incurrirá en multa".*

Artículo 190.-*"Violación de habitación ajena por servidor público. El servidor público que abusando de sus funciones se introduzca en habitación ajena, incurrirá en multa y pérdida del empleo o cargo público".*

Artículo 191.-"*Violación en lugar de trabajo. Cuando las conductas descritas en este*

315 En García-Herreros, Orlando: *"Lecciones de Derecho Administrativo"*, Institución Universitaria Sergio Arboleda, Santa Fe de Bogotá, 1994, pág. 256.

316 *Ídem*, pág. 249 y 250.

317 [En línea] http://www.unifr.ch/derechopenal/legislacion/co/l2t3c1-9.htm#4 [consulta: 10 de Febrero 2003].

capítulo se realizaren en un lugar de trabajo, las respectivas penas se disminuirá hasta en la mitad, sin que puedan ser inferior a una unidad multa".

b) Violación a la intimidad, reserva e interceptación de comunicaciones:

Artículo 192.-*"Violación ilícita de comunicaciones. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, incurrirá en prisión de uno (1) a tres (3) años, siempre que la conducta no constituya delito sancionado con pena mayor".*

"Si el autor de la conducta revela el contenido de la comunicación, o la emplea en provecho propio o ajeno o con perjuicio de otro, la pena será prisión de dos (2) a cuatro (4) años".

Artículo 194.-*"Divulgación y empleo de documentos reservados. El que en provecho propio o ajeno o con perjuicio de otro divulgue o emplee el contenido de un documento que deba permanecer en reserva, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor".*

Artículo 195.-*"Acceso abusivo a un sistema informático. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa".*

Como comentario único en esta materia, diremos que parece difícil la aplicación de los tipos penales contemplados en el Código Penal a conductas que atenten en contra del derecho constitucional de hábeas data o derecho a la protección de datos, pues se requiere ley expresa que específicamente tenga como finalidad sancionar conductas que atenten en contra de ese bien jurídico específico.

10. Conclusiones

La protección de los datos personales en Colombia si bien tiene rango constitucional, adolece de una falta de legislación que regule tanto el derecho de hábeas data como todo lo relativo al tratamiento de datos. Hasta el momento, ha sido la jurisprudencia constitucional la que ha tenido que llenar los vacíos legales a través de la revisión de las acciones de tutela, interpuestas a partir de la modificación a la Constitución del año 1991 en materia de hábeas data. Cabe destacar de la magistratura y de la doctrina, la actual la visión que tienen acerca del bien jurídico protegido por la disposición del artículo 15 constitucional, señalando que el núcleo fundamental de éste es la libertad informática o derecho a la autodeterminación informativa. Con todo, existe consenso general dentro de la doctrina y dentro de la propia magistratura de la necesidad de una ley estatutaria que regule la materia en estudio. Por ahora las esperanzas están puestas en dos Proyectos de Ley que actualmente se tramitan conjuntamente en el Senado colombiano. Uno de ellos presentado por el propio gobierno quien también ha visto la necesidad de legislar sobre la materia.

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN COSTA RICA

1. Generalidades

El ordenamiento jurídico costarricense no contempla disposición constitucional ni estatuto legal que proteja especialmente los datos personales. Sólo se hace referencia por el Constituyente al derecho a la intimidad, libertad y secreto de las comunicaciones. A pesar de lo anterior, a nivel infraconstitucional es posible encontrar algunas disposiciones que se relacionan en mayor o menor medida con la protección de los datos personales. En el ámbito legislativo, puede señalarse que en la actualidad se tramitan dos Proyectos de Ley que pretenden introducir la acción de hábeas data a modo de acción de carácter constitucional, lo cual permitiría suplir en parte el vacío legal en la materia. Sin embargo, debemos señalar que ha sido la jurisprudencia constitucional la que en definitiva ha tenido que pronunciarse acerca de la protección de los datos personales. El mecanismo a través del cual se han podido tutelar ciertos derechos ha sido hasta ahora, la acción de amparo.

2. Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional

A nivel constitucional puede señalarse que en el ordenamiento jurídico costarricense, no existe norma expresa que reconozca el derecho a la autodeterminación informativa ni su acción de tutela específica, el hábeas data. Sólo establece una protección general al derecho a la intimidad, libertad, y vida privada a través del secreto de las comunicaciones. Al efecto, el artículo 24 señala lo siguiente: *"Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones*" [318] . Se agrega en el inciso 2º de este mismo artículo que "*son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República"*. A continuación, dispone que será materia de ley -aprobada por los votos de dos tercios de los Diputados de la Asamblea Legislativa- aquella que señale los casos en que podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento. El inciso 3º del artículo 24 prescribe que de la misma forma, la ley determinará en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuanto tiempo,

[318] [En línea] < http://www.georgetown.edu/pdba/Constitutions/Costa/costa2.html > [consulta: 3 de Noviembre 2002].

señalando las responsabilidades y sanciones en que incurrirán los funcionarios que apliquen ilegalmente esta excepción.

Más adelante, la Constitución establece que: "*la ley fijará los casos en que los funcionarios competentes del Ministerio de Hacienda y de la Contraloría General de la República podrán revisar los libros de contabilidad y sus anexos para fines tributarios y para fiscalizar la correcta utilización de los fondos públicos* (Art. 24 inciso 5º). Finalmente, dentro del ámbito de la protección a la vida privada, el Constituyente señala que: "*No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación*" (Art. 24 inciso final).

En relación a lo anterior se ha dicho por Carvajal que la Constitución no reconoce en forma expresa el derecho a la autodeterminación informativa y que la previsión del artículo 24 lo hace en forma casi tangencial, "a partir de la prohibición de prácticas que alteren la confidencialidad de las comunicaciones privadas" [319] .

En otro ámbito, el artículo 30 reconoce y garantiza: *"el libre acceso a los departamentos administrativos con propósitos de información sobre asuntos de interés público. Quedan a salvo los secretos de Estado"*. Lo anterior, sin duda que podría fundamentar una acción de hábeas data impropio (en principio ajena a la protección de datos personales) a través de la acción de amparo, restringida a informaciones de "interés público".

En materia de tutela de los derechos y garantías constitucionales, el Constituyente ha previsto entre otros mecanismos, la acción de amparo, la cual tiene por finalidad mantener o restablecer el goce de los derechos reconocidos por la Constitución y por los tratados internacionales sobre Derechos Humanos. A este respecto, el artículo 48 señala: "*Toda persona tiene derecho al recurso de hábeas corpus para garantizar su libertad e integridad personales, y al recurso de amparo para mantener o restablecer el goce de los otros derechos consagrados en esta Constitución, así como de los de carácter fundamental establecidos en los instrumentos internacionales sobre derechos humanos, aplicables en la República"*. Agrega esta disposición, que ambos recursos serán de competencia de una Sala especializada de la Corte Suprema de Justicia.

En base al texto constitucional, se ha explicado por Carvajal cómo se ha llegado a una protección de los datos personales por vía jurisprudencial. Señala este autor que en un comienzo, conociendo acciones de amparo tendientes a la tutela de los datos personales, "la Sala Constitucional declaró la confidencialidad de los registros en los archivos criminales, restringiendo su uso apenas a las autoridades policiales y al sujeto registrado, y determinando la destrucción de la ficha en caso de que se vieran desvirtuados los indicios que tuvieron a dicha persona como sospechosa de haber delinquido". Luego agrega que, en casos en que en expedientes públicos consten informaciones o documentos que no sean confidenciales (íntimos), formalmente declarados secretos de Estado, o exista un marcado interés general en su preservación, declarado en acto administrativo motivado, "debe, de conformidad con los términos del

[319] Carvajal Pérez, Marvin: *"La protección de los datos personales en Costa Rica",* [en línea] < http://www.democraciadigital.org/derechos/arts/0207datos.html > [consulta: 6 de Febrero 2003].

artículo 30 de la Constitución, garantizarse su pleno e irrestricto acceso, sin que quepa a la Administración la posibilidad de excusarse en razones de mera conveniencia a fin de impedir que las personas accedan a dicha información" [320] .

De lo anterior puede concluirse que, si bien el texto constitucional costarricense no contempla disposiciones expresas que protejan los datos personales, ha sido la jurisprudencia la que ha brindado protección a éstos, basada en el precepto que consagra el derecho a la intimidad, logrando ampliar los ámbitos de protección tradicional que a este derecho se le ha atribuido.

En cuanto a iniciativas legislativas en la materia, cabe hacer presente que en 1997 se presentó un proyecto de ley para reformar la Ley de la Jurisdicción Constitucional (que regula el ejercicio de la acción de hábeas corpus, amparo e inconstitucionalidad), iniciativa del entonces Diputado Constantino Urcuyo, el cual pretendía incorporar el recurso de hábeas data en Costa Rica. Lamentablemente dicho Proyecto fue archivado [321] . El año 2002 nuevamente se planteó formalmente la necesidad de introducir la acción de hábeas data en Costa Rica. En este sentido se enmarcan dos Proyectos de Ley que actualmente se tramitan en la Asamblea Legislativa costarricense, ambos circunscritos solamente a la acción de hábeas data, mas no a la regulación legal del derecho a la protección de datos [322] .

2.2 Protección Legal de los Datos Personales

En lo que respecta a la protección legal de los datos personales, poco puede decirse en esta materia, pues no existe normativa especial que se ocupe de ella. En razón de lo anterior sólo nos referiremos a algunas disposiciones sectoriales aisladas que tratan de

[320] Este autor agrega que en los últimos años la Sala Constitucional superó el umbral de protección de los datos íntimos, desarrollando en forma paulatina una extensa doctrina en materia de protección de los datos personales desde una perspectiva mucho más amplia, una serie de fallos enfocados en la misma dirección, ha ido delineando los aspectos fundamentales de la protección de datos personales. Así, las sentencias números 5802-99 y 4347-99 reconocieron la existencia de un derecho a la tutela jurisdiccional privilegiada de los datos personales (hábeas data), desarrollando una serie de principios atinentes al acopio, almacenamiento y empleo de bases de datos, lista que ha sido ampliada y delimitada por diversos fallos posteriores, hasta llegar al 00754-02, última resolución de fondo dictada en la materia" (*Ibídem*).

[321] Expediente 12.827 de la Asamblea Legislativa, Junio de 1997.

[322] El primero de estos Proyectos de Ley es el contenido en el Expediente Nº 14.778, de 12 de junio de 2002, denominado "Adición de un Capítulo IV a la Ley de Jurisdicción Constitucional (Recurso de Hábeas Data)", y fue presentado por los Diputados Rocío Ulloa Solano, Carlos Avendaño Calvo y Laura Chinchilla Miranda. Actualmente el Proyecto se encuentra en la Comisión Permanente de Asuntos Jurídicos para su estudio e informe. El texto de este proyecto de ley puede ser consultado [en línea] < http://www.racsa.co.cr/asamblea/proyecto/tx_base/14778.doc > [consulta: 6 de Febrero de 2003]. El segundo proyecto de ley, fue presentado por el Diputado Rolando Laclé Castro, el 18 de junio de 2002, expediente Nº 14.785, intitulado "Adición de un Nuevo Capítulo IV, denominado Del Recurso de Hábeas Data, al Título III de la Ley de Jurisdicción Constitucional, Ley Nº 7.135, de 11 de octubre de 1989". Al igual que el Proyecto anterior, éste pasó a estudio e informe de la Comisión Permanente de Asuntos Jurídicos. Su texto se encuentra disponible [en línea] < http://www.racsa.co.cr/asamblea/proyecto/tx_base/14785.doc > [consulta: 6 de Febrero 2003].

un modo indirecto la protección de estos datos, estableciendo deberes de secreto o confidencialidad respecto de ciertas informaciones. A continuación revisaremos algunas de estas disposiciones.

2.2.1) Código de Comercio [323]

El artículo 615 del Código de Comercio consagra el secreto bancario en los siguientes términos: "*Las cuentas corrientes bancarias son inviolables y los Bancos sólo podrán suministrar información sobre ellas a solicitud o con autorización escrita del dueño, o por orden de autoridad judicial competente. Se exceptúa la intervención que en cumplimiento de sus funciones determinadas por la ley haga la Superintendencia General de Entidades Financieras".* Luego agrega en el inciso 2º que: *"queda prohibida la revisión de cuentas corrientes por las autoridades fiscales"*.

Del tenor de la disposición anterior se desprende que el secreto bancario al cual se refiere sólo es aplicable a las cuentas corrientes y no a otra clase de operaciones bancarias.

2.2.2) Código Tributario [324]

La Ley tributaria costarricense establece en dos artículos normas sobre el uso de la información recibida por la autoridad tributaria y el carácter secreto de éstas. El artículo 115 preceptúa que la información obtenida o recabada por la Administración Tributaria sólo podrá usarse para fines tributarios de la propia institución, la cual está impedida para trasladarla o remitirla a otras oficinas, dependencias o instituciones públicas o privadas. A renglón seguido la norma señala que, en caso de no cumplirse con el mandato legal, esta acción será constitutiva del delito de divulgación de secretos, tipificado en el artículo 337 del Código Penal (inc. 2º). Luego dispone que la prohibición indicada en este artículo no impide trasladar ni utilizar toda la información necesaria requerida por los tribunales comunes (inc. 3º). Finalmente, este mismo artículo establece el carácter de prueba ilegal de aquella obtenida con infracción a lo dispuesto en esta disposición señalando que: "*La información y la prueba general obtenidas o recabadas como resultado de actos ilegales realizados por la Administración Tributaria, no producirán ningún efecto jurídico contra el sujeto fiscalizado"* (Art. 115 inc. 4º).

Por otra parte, el artículo 117 establece el carácter confidencial de las informaciones recibidas por la Administración Tributaria, ordenando que: "*Las informaciones que la Administración Tributaria obtenga de los contribuyentes, responsables y terceros, por cualquier medio, tienen carácter confidencial; y sus funcionarios y empleados no pueden divulgar en forma alguna la cuantía u origen de las rentas, ni ningún otro dato que figure en las declaraciones, ni deben permitir que estas o sus copias, libros o documentos, que*

[323] **El Código de Comercio se encuentra disponible [En línea] < http://www.pgr.go.cr/leyes-usuales/Ley%20N%203284%20Codigo%20de%20Comercio.htm > [consulta: 3 de Febrero 2003].**

[324] **El Código Tributario está contenido en la Ley Nº 4.755 de 1971 y puede consultarse [en línea] < http://www.nexos.co.cr/cesdepu/nbdp/cotri.htm > [consulta: 3 de Febrero 2003].**

contengan extractos o referencia de ellas sean vistos por otras personas que las encargadas en la Administración de velar por el cumplimiento de las disposiciones legales reguladoras de los tributos a su cargo".

La prohibición que señala este artículo no impide la inspección de las declaraciones por los Tribunales Comunes (Art. 117 inc. 2º). Tampoco impide el secreto de las declaraciones, la publicación de datos estadísticos o del registro de valores de los bienes inmuebles, así como de la jurisprudencia tributaria conforme a lo previsto en ése Código, o el suministro de informes a los personeros de los Poderes Públicos, siempre que se hagan en tal forma que no pueda identificarse a las personas (Art. 117 inc. 3º).

Finalmente señala la Ley que las prohibiciones y las limitaciones establecidas en este artículo alcanzan también a los miembros y empleados del Tribunal Fiscal Administrativo, así como a los servidores de los bancos del Sistema Bancario Nacional, las sociedades financieras de inversión y crédito especial de carácter no bancario y las demás entidades reguladas por la Auditoria General de Entidades Financieras (Art. 117 inc. 4º).

2.2.3) Código de la Niñez y la Adolescencia [325]

Este cuerpo legal que busca ser concordante con la Convención sobre los Derechos del Niño, señala en materia de protección a la vida privada lo siguiente: "*las personas menores de edad tendrán derecho a no ser objeto de injerencia en su vida privada, familia, domicilio y correspondencia; sin perjuicio de los derechos y deberes inherentes a la patria potestad"* (Art. 25). Por lo tanto, se asegura el ámbito relativo a la vida privada de los menores de edad, teniendo debidamente en cuenta los derechos y obligaciones de los padres relativos a la educación y cuidado de sus hijos.

2.2.4) Ley sobre Justicia Penal Juvenil (Ley Nº 7.576) [326]

La Ley sobre Justicia Penal Juvenil dispone en el articulo 20 titulado "Derecho a la privacidad" que: "*Los menores de edad tendrán derecho a que se les respete su vida privada y la de su familia. Consecuentemente, se prohíbe divulgar la identidad de un menor de edad sometido a proceso".* A su turno, el artículo 21 titulado "Principio de confidencialidad"señala que: *"serán confidenciales los datos sobre los hechos cometidos por menores sometidos a esta ley"*. Además, en todo momento deberá respetarse la identidad y la imagen del menor de edad. Luego agrega que: *"los Jueces Penales Juveniles deberán procurar que la información que brinden, sobre estadísticas judiciales, no contravenga el principio de confidencialidad ni el derecho a la privacidad, consagrados en esta ley".*

[325] **La Ley Nº 7.739 de 1998 que contiene a este Código. puede consultarse [en línea] < http://www.pgr.go.cr/scripts/TextoCompleto.dll > [consulta: 2 de Febrero 2003].**

[326] **Esta ley se encuentra disponible [en línea] < http://www.pgr.go.cr/scripts/TextoCompleto.dll > [consulta 2 de Febrero 2003].**

2.2.5) Ley que Crea el Sistema de Emergencias 911 (Ley Nº 7.566) [327]

Esta Ley tiene por objetivo participar oportuna y eficientemente en la atención de situaciones de emergencia para la vida, libertad, integridad y seguridad de los ciudadanos o casos de peligro para sus bienes (Art. 1º). En materia de protección a la vida privada, se dispone que: "*por las características de la información generada al operar el Sistema, los funcionarios de las instituciones involucradas deberán manejarla con la confidencialidad necesaria para salvaguardar la seguridad de los usuarios"* (Art. 12). A renglón seguido, se dispone que *"el Sistema de Emergencias 9-1-1 no podrá utilizar ningún equipo para intervenir llamadas telefónicas ni violar la privacidad de los ciudadanos, excepto si lo usa únicamente para identificar el número telefónico del cual se llama al Sistema"* (Art. 13).

3. Bienes Jurídicos Protegidos por la Legislación de Datos Personales

Dada la inexistencia de legislación que se ocupe en particular de la protección de los datos personales en Costa Rica, se hace imposible poder esbozar cuáles serían los bienes jurídicos protegidos. Sin embargo, es posible afirmar que en base al artículo 24 de la Constitución podría desarrollarse una legislación de protección de datos basado en el derecho a la intimidad. Al respecto, se ha dicho que la Sala Constitucional de la Corte Suprema de Justicia, al conocer de recursos de amparo, ha ido ampliando el concepto clásico de intimidad, "extrayendo de éste un derecho no solo a la privacidad en las comunicaciones, sino incluso imponiendo la preservación de los datos sensibles y delineando las reglas básicas para la recolección, almacenamiento y empleo de informaciones personales no pertenecientes al fuero íntimo del individuo" [328].

Respecto de los casos particulares de normas que indirectamente protegerían los datos personales, los bienes jurídicos protegidos parecieran ser distintos a la autodeterminación informativa y más bien pueden enmarcarse dentro del ámbito del derecho a la intimidad o de la vida privada.

4. Principios Informativos de la Legislación de Protección de Datos Personales

En cuanto a los principios informativos en materia de protección de datos personales, no es posible constatarlos, dada la inexistencia de ley al respecto.

5. Regulación Diferenciada o Indiferenciada del Sector Público y

[327] **[En línea] < http://www.pgr.go.cr/scripts/TextoCompleto.dll > [consulta 2 de Febrero 2003].**

[328] Carvajal Pérez, Marvin, *op. cit*., [en línea].

Privado

En atención a la inexistencia de una ley general de protección de datos personales en el ordenamiento jurídico costarricense, no nos detendremos en este punto.

6. Modelos de Tutela

La protección de los datos personales en el ordenamiento jurídico costarricense ha quedado entregada en definitiva a la Sala Constitucional de la Corte Suprema de Justicia, la cual conoce de los recursos de amparo de los derechos y libertades consagrados por la Constitución y los Derechos Humanos reconocidos por el Derecho Internacional vigente en Costa Rica. A este respecto se ha señalado por Carvajal, que dos serían las razones fundamentales que explicarían el hecho de que las personas hayan recurrido mayoritariamente a la vía del amparo constitucional, y menos a otras instancias administrativas y jurisdiccionales para la protección del derecho a la autodeterminación informativa. La primera, se basa en la carencia de una adecuada regulación positiva, lo cual genera una frecuente reiteración de infracciones a ese derecho fundamental por parte del Estado y de los sujetos privados. En segundo lugar, este fenómeno se explicaría por la aceptación popular del recurso de amparo como mecanismo más efectivo para la defensa de los derechos de las personas [329] . Agrega este mismo autor que es procedente el recurso de amparo, tanto para la protección de los datos personales contenidos en bases de datos públicas como para los almacenados en archivos privados. De esta manera "las agencias particulares que almacenan este tipo de datos (empresas protectoras de crédito, por ejemplo), pueden ser accionadas por entenderse que se encuentran, respecto del particular, en una situación fáctica de poder, debido a la enorme cantidad y calidad de datos que pueden almacenar en medios cada vez más eficientes y difíciles de rastrear" [330] .

6.1 La Acción de Amparo

Esta acción se encuentra regulada en la Ley de la Jurisdicción Constitucional (en adelante LJC) [331] . Para analizarla nos apoyaremos en la exposición de Marvin Carvajal. Señala este autor -en base a la Ley- que el mal llamado recurso de amparo, es un proceso jurisdiccional previsto para la defensa de los derechos fundamentales contenidos en la Constitución, así como los derechos reconocidos por del Derecho Internacional de los Derechos Humanos contra actos u omisiones cometidos por autoridades públicas o por particulares en ejercicio de funciones públicas o situados en posiciones jurídicas o fácticas de poder, frente a los cuales los remedios ordinarios resulten tardíos o insuficientes (Art. 2 letra a LJC).

329 Todo lo anterior, en Carvajal Pérez, Marvin, *op. cit*. [en línea].

330 *Ibídem*.

331 El texto de esta Ley está disponible [en línea] < http://www.pgr.go.cr/scripts/TextoCompleto.dll,fecha > [consulta: 2 de Febrero 2003].

6.1.1) Procedencia de la Acción

Para analizar la procedencia de la acción de amparo, es preciso distinguir entre el amparo en contra de órganos o servidores públicos y el amparo en contra de sujetos de derecho privado:

i) *Amparo contra órganos o servidores públicos*: respecto de ellos, procede la acción contra toda disposición, acuerdo o resolución y, en general, contra toda acción, omisión o simple actuación material no fundada en un acto administrativo eficaz, que haya violado, viole o amenace violar cualquiera de los derechos fundamentales contenidos tanto en la Constitución, como en los pactos internacionales sobre Derechos Humanos. El amparo procederá no sólo contra los actos arbitrarios, sino también contra las actuaciones u omisiones fundadas en normas erróneamente interpretadas o indebidamente aplicadas (Art. 29 LJC). No obstante lo anterior, no procederá el amparo: a) Contra las leyes u otras disposiciones normativas salvo cuando se impugnen conjuntamente con actos de aplicación individual de aquellas, o cuando se trate de normas de acción automática, de manera que sus preceptos resulten obligatorios inmediatamente por su sola promulgación, sin necesidad de otras normas o actos que los desarrollen o los hagan aplicables al perjudicado; b) Contra las resoluciones y actuaciones jurisdiccionales del Poder Judicial; c) Contra los actos que realicen las autoridades administrativas al ejecutar resoluciones judiciales, siempre que esos actos se efectúen con sujeción a lo que fue encomendado por la respectiva autoridad judicial; ch) Cuando la acción u omisión hubiere sido legítimamente consentida por la persona agraviada y, d) Contra los actos o disposiciones del Tribunal Supremo de Elecciones en materia electoral (Art. 30 LJC).

ii) *Amparo contra sujetos de derecho privado*: respecto de ellos, procede la acción de amparo cuando actúen o deban actuar en ejercicio de funciones o potestades públicas, o se encuentren, de derecho o de hecho, en una posición de poder frente a la cual los remedios jurisdiccionales comunes resulten claramente insuficientes o tardíos para garantizar los derechos o libertades fundamentales a que se refiere el artículo 2 letra a de esta Ley (los derechos y libertades consagrados por la Constitución Política y los derechos humanos reconocidos por el Derecho Internacional vigente en Costa Rica). La LJC agrega que: *"no se podrán acoger en sentencia, recursos de amparo contra conductas legítimas del sujeto privado"* (Art. 57 LJC). La Ley dispone por otra parte que: "*no será necesaria la reposición ni ningún otro recurso administrativo para interponer el recurso de amparo"* (Art. 31).

Finalmente, cabe anotar que la acción de amparo puede interponerse en cualquier tiempo mientras subsista la violación, amenaza, perturbación o restricción, y hasta dos meses después de que hayan cesado totalmente sus efectos directos respecto del perjudicado. Sin embargo, cuando se trate de derechos puramente patrimoniales u otros cuya violación pueda ser válidamente consentida, el recurso deberá interponerse dentro de los dos meses siguientes a la fecha en que el perjudicado tuvo noticia fehaciente de la violación y estuvo en posibilidad legal de interponer el recurso (Articulo 35).

6.1.2) Legitimación Activa

Los artículos 33 y 58 de la LJC señalan que: "*cualquier persona podrá interponer el recurso de amparo".* Carvajal señala al respecto que la acción de amparo puede ser interpuesta por cualquier persona a favor de sí misma o de un tercero [332] .

6.1.3) Legitimación Pasiva

Al respecto la Ley distingue entre el amparo contra órganos del Estado y contra particulares:

i) *Amparo contra órganos públicos* **:** se señala que el recurso se dirigirá en contra del servidor o del titular del órgano que aparezca como presunto autor del agravio. Si uno u otro hubiesen actuado en cumplimiento de órdenes o instrucciones impartidas por un superior, o con su autorización o aprobación, se tendrá por establecido el amparo contra ambos, sin perjuicio de lo que se decida en sentencia. De ignorarse la identidad del servidor, el recurso se tendrá por establecido contra el jerarca (Articulo 34 LJC).

ii) *Amparo contra particulares*: se dirigirá la acción contra el presunto autor del agravio, si se tratare de persona física en su condición individual; si se tratare de una persona jurídica, contra su representante legal; y si lo fuere de una empresa, grupo o colectividad organizados, contra su personero aparente o el responsable individual (Articulo 59 LJC).

6.1.4) Competencia

Tiene competencia para conocer de estas acciones la Sala Constitucional de la Corte Suprema de Justicia (Art. 4º LJC).

6.1.5) Procedimiento Aplicable

El procedimiento aplicable a la tramitación de la acción de amparo costarricense puede resumirse de la siguiente manera:

1) *Demanda*: para la interposición de esta acción, no se requieren más requisitos que un documento escrito donde se consignen con meridiana claridad los datos de identificación del actor y el amparado, el acto impugnado y la autoridad responsable por el mismo.

2) *Audiencia oral*: el artículo 10 de la LJC, aplicable al amparo contra órganos del Estado, preceptúa que la Sala dispondrá que los trámites se realicen en lo posible, en forma oral, y ordenará una comparecencia oral para que los interesados formulen conclusiones antes de la sentencia, necesariamente en las acciones de inconstitucionalidad, y facultativamente en los demás casos.

3) *Informe:* en cuanto al trámite del informe hay que distinguir nuevamente:

i) Amparo contra órganos públicos: admitida a tramitación la acción, se pedirá informe al recurrido, fijándole un plazo para ello de uno a tres días, según sean la índole del asunto, la distancia y la rapidez de los medios de comunicación. Los informes se

[332] Carvajal Pérez, Marvin, *op. cit*., [en línea].

considerarán dados bajo juramento. Por consiguiente, cualquier inexactitud o falsedad hará incurrir al funcionario en las penas del perjurio o del falso testimonio, según la naturaleza de los hechos contenidos en el informe (Articulo 44 LJC).

ii) Amparo contra particulares: si no corresponde rechazar de plano el recurso, se dará traslado a la persona o entidad que se indique como autora del agravio, amenaza u omisión, por un plazo de tres días, para lo cual se hará uso de la vía escrita más rápida posible. Ese plazo podrá aumentarse si resultare insuficiente por razón de la distancia (Art. 61 LJC).

6.1.6) La Sentencia

La sentencia del recurso es obligatoria con efectos *erga omnes*, e implica -en caso de ser acogida la pretensión- la responsabilidad del accionado por los daños y perjuicios ocasionados con el acto impugnado [333] . A este respecto, el artículo 13 de la LJC dispone que: *"la jurisprudencia y los precedentes de la jurisdicción constitucional son vinculantes erga omnes, salvo para sí misma".*

7. Mecanismos de Control

La legislación costarricense no contempla una ley de protección de datos personales, ni menos un órgano de control que vele por el cumplimiento de ésta.

8. Transmisión Internacional de Datos

El ordenamiento jurídico en estudio tampoco contempla normas que regulen la transmisión internacional de datos personales.

9. Régimen de Responsabilidad

Como ya se señaló, la protección jurídica de los datos personales en Costa Rica está entregada a la Sala Constitucional de la Corte Suprema, la cual a través del conocimiento y fallo de las acciones de amparo ha ido delineando principios de protección en materia de datos personales. Cabe destacar que el mismo procedimiento de amparo es idóneo para la determinación en abstracto de la responsabilidad civil. En este caso la liquidación de los daños y perjuicios y de las costas se reservará a la vía civil de ejecución de la sentencia (Art. 62 inciso final LJC).

9.1 Responsabilidad Administrativa

[333] Carvajal Pérez, Marvin, *op. cit*., [en línea]. Comentando este instituto, este autor señala que "la carencia de formalismos propios de otras instancias jurisdiccionales, así como la competencia en manos de un órgano de máximo rango del Poder Judicial y la celeridad con que la Sala resuelve sus asuntos comparada con la jurisdicción común han hecho que las personas empleen cada vez más este mecanismo procesal, con un crecimiento sostenido a lo largo de los más de doce años de existencia del Tribunal Constitucional".

El ordenamiento jurídico costarricense no contempla una ley de protección de los datos personales, por lo que tampoco existen sanciones administrativas específicas a conductas que lesionen los derechos de los titulares de datos. Con todo, a falta de ley especial entendemos que deberían aplicarse los estatutos particulares de cada repartición funcionaria, o en su defecto, las reglas generales de responsabilidad administrativa, respecto de las cuales no tenemos información.

9.2 Responsabilidad Civil

En el ámbito de la responsabilidad civil, no existen normas especiales en materia de protección de datos. Sin embargo, está reconocido como un derecho constitucional la reparación y compensación de los daños injustamente causados. Al efecto, el artículo 41 constitucional dispone que: "*ocurriendo a las leyes, todos han de encontrar reparación para las injurias o daños que hayan recibido en su persona, propiedad o intereses morales. Debe hacérseles justicia pronta, cumplida, sin denegación y en estricta conformidad con las leyes".*

Concordante con lo anterior, el Código Civil [334] ha señalado reglas generales en materia de responsabilidad extracontractual en los artículos 1.045 y 1.046. El primero de éstos dispone que: "*Todo aquel que por dolo, falta, negligencia o imprudencia, causa a otro un daño, está obligado a repararlo junto con los perjuicios".* A su turno, el artículo 1.046 prescribe que: *"la obligación de reparar los daños y perjuicios ocasionados con un delito o cuasi-delito, pesa solidariamente sobre todos los que han participado en el delito o cuasi-delito, sea como autores o cómplices y sobre sus herederos".*

9.3 Responsabilidad Penal

El ordenamiento jurídico costarricense, no contempla normas penales que protejan directamente el derecho a la autodeterminación informativa o a la protección de datos, máxime si éste no se encuentra reconocido explícitamente en él. En razón de lo anterior, sólo nos referiremos a los tipos penales contemplados en el Código Penal [335] que tutelan los bienes jurídicos vida privada e intimidad. De éstos, destaca el artículo 196 bis que sanciona la violación de las comunicaciones electrónicas. A continuación revisaremos las disposiciones correspondientes.

a) Violación de las comunicaciones:

Artículo 196.-*"Será reprimido, con prisión de uno a tres años, quien abra o se imponga del contenido de una comunicación destinada a otra persona, cualquiera que sea el medio utilizado".*

334 El texto del Código Civil puede consultarse [en línea] < http://www.pgr.go.cr/leyes-usuales/Ley%20N%2063%20Codigo%20Civil.htm > [consulta: 3 de Febrero 2003].

335 El Código Penal de Costa Rica está disponible [En línea] < http://www.pgr.go.cr/leyes-usuales/Ley%20N%204573%20Codigo%20de%20Penal.htm > [consulta: 2 de Febrero 2003].

b) Violación de las comunicaciones electrónicas:

El artículo 196 bis, dispone que será reprimida con pena de prisión de seis meses a dos años, la persona que, *"para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos"*. Luego, agrava la sanción de uno a tres años de prisión, si las acciones descritas, son realizadas por las personas encargadas de los soportes electrónicos, informáticos, magnéticos y telemáticos.

c) Sustracción, desvío o supresión de correspondencia *:*

En cuanto a la sustracción, desvío o supresión de correspondencia, el artículo 197 preceptúa que: *"será reprimido, con prisión de uno a tres años, quien se apodere de una carta o de otro documento privado, aunque no esté cerrado, o al que suprima o desvíe de su destino una correspondencia que no le esté dirigida".*

d) Captación indebida de manifestaciones verbales *:*

El legislador también contempla el delito de captación indebida de manifestaciones verbales. Se señala en el artículo 198 que: "*será reprimido, con prisión de uno a tres años, quien grabe sin su consentimiento, las palabras de otro u otros, no destinadas al público o que, mediante procedimientos técnicos, escuche manifestaciones privadas que no le estén dirigidas, excepto lo previsto en la Ley sobre registro, secuestro y examen de documentos privados e intervención de las comunicaciones".* El inciso segundo agrega a su vez que: *"La misma pena se impondrá a quien instale aparatos, instrumentos, o sus partes, con el fin de interceptar o impedir las comunicaciones orales o escritas, logren o no su propósito".*

Por otra parte, se contemplan agravantes para los casos de los delitos de los artículos 196 bis, 197 y 198, disponiendo al efecto que se impondrá prisión de dos a seis años si la acción se perpetra: a) Por funcionarios públicos, en relación con el ejercicio de sus funciones; b) Por quien ejecute el hecho, prevaliéndose de su vinculación con una empresa o institución pública o privada encargada de las comunicaciones y, c) Cuando el autor publique la información obtenida o aún sin hacerlo, tenga carácter privado, todo a juicio del Juez. Cabe comentar respecto a esto último, que a primera vista, en cuanto a la agravante de la letra c), no se ve mayor desvalor de injusto si la información obtenida no se hace pública, más bien no habría mayor diferencia con las acciones penadas en los artículos a que accede el agravante.

e) Uso indebido de correspondencia *:*

Más adelante, el artículo 201 tipifica el uso indebido de correspondencia, prescribiendo que: *"Será reprimido con prisión de seis meses a un año, el que usare indebidamente en cualquier forma, cartas, papeles, grabaciones, despachos telegráficos, telefónicos, cablegráficos o de otra naturaleza que hubieren sido sustraídos o reproducidos".*

El artículo 202 por su lado, sanciona con treinta a sesenta días multa, si el hecho pudiere causar perjuicio: *"Al que hallándose legítimamente en posesión de una correspondencia, de papeles o grabaciones no destinadas a la publicidad, las hiciere públicas sin la debida autorización, aunque le hubieren sido dirigidas"*. La pena será de treinta a cien días multa, si la información propagada tuviere carácter privado, aun cuando no causare perjuicio.

f) Divulgación de secretos:

Finalmente, dos artículos se ocupan de estos delitos; el 203 y el 339. El primero de ellos señala que: "*Será reprimido con prisión de un mes a un año o de treinta a cien días multa, el que teniendo noticias por razón de su estado, oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño, lo revele sin justa causa. Si se tratare de un funcionario público o un profesional se impondrá, además inhabilitación para el ejercicio de cargos y oficios públicos, o de profesiones titulares, de seis meses a dos años".* El artículo 339, por su parte prescribe que: *"Será reprimido con prisión de tres meses a dos años el funcionario público que divulgare hechos, actuaciones o documentos, que por la ley deben quedar secretos"*. Esta última disposición es aplicable a la violación del secreto tributario por expresa remisión del artículo 115 del Código Tributario. Empero, debemos hacer presente que el señalado artículo 115 se remite al artículo 337 del Código Penal, el cual en la actualidad ya no figura en el Código con esa numeración sino que con la del artículo 339. Lo anterior, es consecuencia de la modificación de la numeración hecha por la Ley Nº 7.732 de 17 de diciembre de 1997 (Art.185, inciso a) que lo traspasó del 337 al 339. Nos queda la duda acerca de la actual situación penal de la violación del secreto tributario, pues la disposición del Código Tributario (ley penal en blanco) ha quedado sin sustento, dado que el nuevo artículo 337 castiga los "Nombramientos ilegales".

Como comentario final a las disposiciones penales, cabe señalar que si bien algunos de estos delitos parecieren a primera vista aplicables a situaciones en que exista una utilización indebida de datos personales y divulgación de ellos, habrá que tener siempre presente el límite impuesto por el principio de legalidad en materia penal. [336]

10. Conclusiones

El sistema jurídico costarricense carece de normativa tanto a nivel constitucional como legal que proteja directamente los datos personales. En el ámbito de la Constitución sólo se dispone de la protección al derecho a la intimidad (Art. 24), y su respectiva garantía, la acción de amparo. Es precisamente a través de esa acción que se ha logrado tutelar los datos personales por parte de la Sala Constitucional de la Corte Suprema, la cual ha aplicado extensivamente la disposición del artículo 24, logrando lineamientos jurisprudenciales de eficacia general en virtud el artículo 13 de la Ley de la Jurisdicción

[336] De este principio, se derivan cuatro consecuencias; la prohibición de analogía, la prohibición de derecho consuetudinario, la prohibición de retroactividad y la prohibición de leyes penales y penas indeterminadas (Roxin, Claus: *"Derecho Penal Parte General, T.I, Fundamentos. La Estructura de la Teoría del Delito"*, tr. Luzón Peña, Diego-Manuel "'et al'", Ed. Civitas, Madrid, 1997, págs. 140 y 141).

Constitucional. Finalmente, cabe hace presente que en la actualidad existen en tramitación legislativa dos Proyectos de Ley que buscan incorporar en la Ley de Jurisdicción Constitucional la acción de hábeas data.

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN CUBA

1. Generalidades

El sistema jurídico cubano no contempla normas que protejan a nivel constitucional ni legal los datos personales. Si bien existen algunos estatutos sectoriales que establecen una protección a cierta información bancaria o tributaria, éstos son insuficientes para tutelar adecuadamente los derechos de las personas en relación a sus datos personales.

Por otra parte, debemos mencionar que el estudio de la protección de datos personales en Cuba se hace aún más complejo que en otros ordenamientos jurídicos latinoamericanos, dado que el sistema cubano se aparta de los estándares institucionales democráticos modernos, lo cual se traduce en definitiva en un mermado respeto por los derechos fundamentales de las personas lo que repercute directamente en el tema de fondo de nuestro análisis, cual es la protección de las personas frente al tratamiento de sus datos personales. Ello, en atención a que los bienes jurídicos que subyacen al instituto en estudio no se constatan de manera clara dentro las escasas normas jurídicas a las que hemos tenido acceso a través de la Internet. A pesar de lo anterior, hemos tratado de buscar indicios que pudiesen justificar en la actualidad una protección al menos teórica en la materia.

2. Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional

En el ordenamiento jurídico cubano no existe disposición constitucional alguna que garantice la protección a los datos personales [337] . Tampoco contempla norma alguna que reconozca explícitamente el derecho a la intimidad o la vida privada. Sin embargo, se reconocen ciertos derechos engarzados con el derecho a la vida privada, como lo son la inviolabilidad de domicilio y de la correspondencia. Con todo, la propia Constitución se encarga de poner límites a esas garantías fundadas en los ideales institucionales del Estado cubano. A continuación se señalarán aquellos preceptos que consideramos relacionados con la protección de la vida privada e intimidad.

[337] La Constitución cubana de 1976 (reformada en 1992) esta disponible [en línea] < http://www.georgetown.edu/pdba/Constitutions/Cuba/cuba1992.html > [consulta: 3 de Febrero 2003].

El artículo 9 de la Carta cubana señala que el Estado: *"a) (…) garantiza la libertad y la dignidad plena del hombre, el disfrute de sus derechos, el ejercicio y cumplimiento de sus deberes y el desarrollo integral de su personalidad".*

Más adelante, dentro del Capítulo VII denominado "Derechos, deberes y garantías fundamentales", se insertan dos artículos; el 56 que garantiza la inviolabilidad de domicilio, y el 57 que garantiza la inviolabilidad de la correspondencia. El primero de éstos prescribe: "*El domicilio es inviolable. Nadie puede penetrar en el ajeno contra la voluntad del morador, salvo en los casos previstos por la ley*". A su turno, el artículo 57 dispone que: "*La correspondencia es inviolable. Sólo puede ser ocupada, abierta y examinada en los casos previstos por la ley. Se guardará secreto de los asuntos ajenos al hecho que motivare el examen. El mismo principio se observara con respecto a las comunicaciones cablegráficas, telegráficas y telefónicas".*

Más adelante, el artículo 62 constitucional señala que: "*ninguna de las libertades reconocidas a los ciudadanos puede ser ejercida contra lo establecido en la Constitución y las leyes, ni contra la existencia y fines del Estado socialista, ni contra la decisión del pueblo cubano de construir el socialismo y el comunismo. La infracción de este principio es punible"*. De lo anterior, se desprende una seria limitación a las garantías señaladas más arriba con lo cual las debilita.

A renglón seguido, el artículo 63 consagra el derecho de petición, en el cual podría eventualmente fundarse una petición de hábeas data impropio, al decir que: *"t odo ciudadano tiene derecho a dirigir quejas y peticiones a las autoridades y a recibir la atención o respuestas pertinentes y en plazo adecuado, conforme a la ley"*.

En otro ámbito de materias, y con la finalidad de ilustrar someramente la particular institucionalidad cubana, nos referiremos a la configuración constitucional de los órganos del Estado que directamente están llamados a tutelar los derechos de las personas, con el fin de dimensionar la inexistencia de una verdadera separación de poderes, pilar básico de una república constitucional moderna. En lo relativo al Poder Judicial cubano, cabe consignar que la Constitución cubana establece una independencia puramente nominal respecto de los otros órganos del Estado. Al efecto, si bien se dispone que los Tribunales constituyen un sistema de órganos estatales estructurado con independencia funcional de cualquier otro órgano, en definitiva el Poder Judicial está "*subordinado jerárquicamente a la Asamblea Nacional del Poder Popular y al Consejo de Estado"* (Art. 121). Por otra parte, existe un órgano estatal encargado de velar por el respeto de la Constitución y las leyes, así como también de ejercer la acción penal pública en Cuba. Ese órgano es la Fiscalía General de la República. Según la Constitución, ésta tiene los siguientes objetivos fundamentales: el control y la preservación de la legalidad, sobre la base de la vigilancia del estricto cumplimiento de la Constitución, las leyes y demás disposiciones legales, por los organismos del Estado, entidades económicas, sociales y por los ciudadanos. Asimismo, le corresponde a la Fiscalía, la promoción y el ejercicio de la acción penal pública en representación del Estado (Art. 127). Lo recién señalado debe, sin embargo, ser concordado con lo preceptuado por el Constituyente en el artículo siguiente, el cual dispone que: "*la Fiscalía General de la República constituye una unidad orgánica subordinada únicamente a la Asamblea Nacional del Poder Popular y al Consejo de Estado. El Fiscal General de la República recibe instrucciones directas del Consejo de*

Estado" (Art. 128). De lo anterior, puede concluirse que la Fiscalía tampoco es un órgano independiente, sino que al igual que el Poder Judicial se encuentra subordinada al Consejo de Estado, cuyo Presidente ejerce el gobierno (Art. 93 a).

2.2 Protección Legal de los Datos Personales

A nivel legal, Cuba no posee una ley de protección de datos personales. Sólo en algunos ámbitos particulares podemos encontrar normas señoriales que aluden a la protección de la intimidad y la vida privada. Estas normas se señalarán a continuación.

2.2.1) Decreto-Ley Nº 169 de 1997, sobre Normas Generales y Procedimientos Tributarios [338]

En materia tributaria este Decreto Ley consagra el secreto fiscal en el artículo 22 de la siguiente forma: *"Tendrán carácter reservado las declaraciones e informaciones que la Administración Tributaria obtenga de los sujetos pasivos, responsables y demás personas obligadas por cualquier medio y sólo podrán ser utilizadas para los fines propios de dicha Administración, en los casos establecidos y cuando lo dispongan los Tribunales y la Fiscalía"*. Agrega el inciso 2º que: "*se exceptúa, la publicación de datos estadísticos que, por su generalidad, no permitan la individualización de declaraciones, informaciones o personas"*. En suma, puede afirmarse Cuba dispone de una normativa legal que resguarda el secreto de las declaraciones de los contribuyentes e informaciones obtenidas por la Administración Tributaria.

2.2.2) Estatutos del Banco Central de Cuba [339]

Los Estatutos del Banco Central de Cuba establecen entre otras materias, las funciones de ese organismo, de las cuales destaca la de supervisión. Al efecto, el artículo 15º señala: *"Las funciones de supervisión del Banco Central de Cuba son: (…) recopilar, procesar y organizar toda la información que de forma periódica las instituciones financieras deben remitir a la Central de Información de Riesgos del Banco Central de Cuba sobre: clientes morosos, clientes que violan los principios de cobros y pagos de forma consuetudinaria, personas naturales o jurídicas procesadas judicialmente por fraudes, malversación u otro tipo de delito incompatibles con la actividad financiera, casos de lavado de activos u otros delitos o contravenciones de carácter grave y diseminar esta información de manera periódica al resto de las instituciones financieras del país, organismos de la Administración Central del Estado y otras instituciones que así lo requieran".* De lo anterior, se desprenden a lo menos dos cosas; primero, que el Banco Central cubano posee una Central de Información de Riesgos a través de la cual realiza un tratamiento de datos personales de diversa especie, tales como los relativos a deudores morosos, infractores de leyes penales, entre otros. Segundo, que la información

[338] **El estatuto jurídico tributario cubano está disponible [En línea] < http://www.ciat.org/doc/docu/leg/cod/cuba_dto_169_procedimientos_tributarios.DOC > [consulta: 2 de Marzo 2003].**

[339] **[En línea] < http://www.bc.gov.cu/Espanol/regulaciones_bancarias/EstatutosBCC.htm > [consulta: 3 de Febrero 2003].**

tratada debe diseminarse y estar a disposición de toda institución que así lo requiera. Lo anterior, sin duda que es preocupante dado que no existen los mecanismos jurídicos para controlar la calidad y el tipo de información a tratar por este organismo del Estado.

Por otra parte, la disposición 35º de los Estatutos titulada "Del Secreto Bancario", dispone que este organismo está *"obligado a guardar secreto sobre sus cuentas, depósitos y operaciones en general y no podrá dar noticias e informes más que al depositante, heredero, beneficiario, a sus representantes legales o a quién tenga poder para disponer de la cuenta o intervenir en la operación, salvo por disposición judicial dictada en proceso en que el depositante sea parte demandante o acusado o en los casos en que la ley lo autorice expresamente".* Luego agrega, que el Banco Central de Cuba queda liberado de su obligación de mantener el Secreto Bancario en los casos expresamente autorizados por las disposiciones vigentes, de las cuales no tenemos noticia. En suma, puede afirmarse que en principio se encuentra resguardado el secreto de las operaciones bancarias. El alcance de éste, al parecer es amplio pues habla de las "operaciones en general", por lo que en principio cubriría tanto las de carácter activas como pasivas.

2.2.3) Decreto-Ley Nº 173 sobre Bancos e Instituciones Financieras no bancarias [340]

El artículo 81 de este Decreto Ley, insertado dentro del Capitulo VIII, dispone de manera casi idéntica al artículo trigésimo quinto de los Estatutos del Banco Central que: "*las instituciones financieras están obligadas a guardar secreto sobre sus cuentas, depósitos y operaciones en general, y no podrán dar noticias e informes más que al depositante, heredero, beneficiario, a sus representantes legales o a quien tenga poder para disponer de la cuenta o intervenir en la operación, salvo por disposición judicial dictada en proceso en que el depositante sea parte demandante o acusado o en los casos en que la ley lo autorice expresamente".* El inciso 2º de este artículo agrega que: *"Los dirigentes, funcionarios y demás trabajadores de las instituciones financieras no bancarias son responsables por las violaciones de dicho secreto*".

Por lo tanto, esta norma establece el secreto bancario de manera amplia, al igual que la disposición 35º del Estatuto del Banco Central. Conjuntamente con ello introduce una regla de responsabilidad funcionaria aplicable a quienes trabajen en instituciones financieras "no bancarias" y que violen el deber de secreto. De lo anterior, entendemos que la norma de secreto establecida en el Estatuto del Banco Central sólo sería aplicable a las entidades financieras de carácter "bancarias" y la disposición del artículo 81 del DL 173 a las instituciones financieras "no bancarias".

3. Bienes Jurídicos Protegidos por la Legislación de Datos Personales

En razón de la inexistencia de legislación de protección de datos personales en Cuba, no

[340] **[En línea] < http://www.bc.gov.cu/Espanol/regulaciones_bancarias/DL173.HTM > [consulta: 3 de Febrero 2003].**

es posible encontrar bienes jurídicos protegidos. A pesar de esa carencia, sí puede avistarse en las normas jurídicas especiales, como la bancaria, una protección a la vida privada. Lo mismo podría decirse del secreto fiscal en materia tributaria.

En cuanto a los delitos establecidos en el Código Penal, como la violación de domicilio, violación de correspondencia y de secretos, puede afirmarse que los bienes jurídicos protegidos por esas normas se vinculan directamente con la vida privada e intimidad de las personas.

4. Principios Informativos de la Legislación de Protección de Datos Personales

Dada la inexistencia de una ley de protección de datos personales, no podremos referirnos a este punto.

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

En atención a la falta de ley general de protección de datos personales en el ordenamiento jurídico cubano, tampoco nos detendremos en este punto.

6. Modelos de Tutela

En lo relativo a esta materia nada podemos señalar, pues no tenemos conocimiento de normativa general ni especial que proteja, al menos, las escuálidas garantías constitucionales.

7. Mecanismos de Control

No encontramos en la legislación cubana mecanismo de control alguno a la protección de los datos personales.

8. Transmisión Internacional de Datos

En lo relativo a la transmisión internacional de datos, vale lo dicho anteriormente, pues no sabemos de disposiciones que se encarguen de regular la materia.

9. Régimen de Responsabilidad

En materia de responsabilidad fundada en ley especial de protección de datos, nada puede decirse por el momento. A pesar de ello, sí podemos citar algunas reglas dispersas en el ordenamiento jurídico cubano.

9.1 Responsabilidad Administrativa

Al parecer no existe normativa que contemple sanciones administrativas por infracción a una ley de protección de datos, pues no tenemos conocimiento de la existencia de ella. Por lo tanto, en esta materia, y en caso que sea un funcionario del Estado el que vulnere los derechos a la vida privada o intimidad, entendemos que deberían aplicarse los estatutos propios de cada repartición pública y, en subsidio, la normativa general o estatuto administrativo respectivo. Dado que hemos accedido a la normativa específica, para efectos de este análisis consideraremos esta materia como 'sin información'.

9.2 Responsabilidad Civil

Tampoco estamos al tanto del régimen de responsabilidad civil general cubano, ni de eventuales sanciones civiles por violación al derecho a la intimidad o a la vida privada al cual remitir la protección eventual de los datos personales. No obstante lo anterior, la Constitución establece una regla que consagra la responsabilidad patrimonial del Estado. Esta norma es el artículo 26 y dispone que: "*toda persona que sufriere daño o perjuicio causado indebidamente por funcionarios o agentes del Estado con motivo del ejercicio de las funciones propias de sus cargos, tiene derecho a reclamar y obtener la correspondiente reparación o indemnización en la forma que establece la ley".* Por lo tanto, en el eventual caso que pudiere acreditarse un acto ilegal que cause daño en materia de datos personales, en principio, puede decirse que existiría al menos una reparación o compensación patrimonial.

9.3 Responsabilidad Penal

El Código Penal cubano contempla diversos delitos que protegen bienes jurídicos como la intimidad y la vida privada, pese a que éstos no hayan sido reconocidos explícitamente por el Constituyente. Al respecto podemos mencionar los siguientes [341] .

a) Violación de domicilio:

El artículo 287 tipifica el delito de violación de domicilio, disponiendo al efecto que:

"1. El que, fuera de los casos autorizados en la ley penetre en domicilio ajeno sin la voluntad, expresa o tácita del morador o permanezca en él contra su voluntad manifiesta incurre en sanción de privación de libertad de tres meses a un año o multa de cien a trescientas cuotas o ambas.

2. Si el delito se ejecuta de noche o en despoblado o empleando violencia o intimidación en las personas, o fuerza en las cosas, o usando armas o con el concurso de dos o más personas la sanción es de privación de libertad de dos a cinco años.

3. Se considera domicilio, a los efectos de este artículo, la casa que sirve de morada, así como los locales cerrados que la integran y espacios patios y jardines cercados contiguos a ella".

[341] [En línea] < http://www.unifr.ch/derechopenal/legislacion/cu/cpcuba7.htm > [consulta: 2 de Marzo 2003].

b) Registro ilegal:

El artículo 288, de la Sección Segunda, tipifica el delito de registro ilegal y dispone: *"El que, sin autorización legal o sin cumplir las formalidades legales efectúe un registro en un domicilio incurre en sanción de privación de libertad de tres meses a un año o multa de cien a trescientas cuotas o ambas".*

c) Violación del secreto de la correspondencia *:*

Más adelante, en el artículo 289 la ley tipifica el delito de violación del secreto de la correspondencia disponiendo que:

"*1. El que sin estar autorizado abra carta telegrama despacho o cualquier correspondencia perteneciente a otro es sancionado con privación de libertad de tres meses a un año o multa de cien a trescientas cuotas.*

2. En igual sanción incurre el que sin estar autorizado viola el secreto de las comunicaciones telefónicas.

3. Si el delito se comete por un funcionario o empleado público con abuso de su cargo la sanción es de privación de libertad de seis meses a dos años o multa de doscientas a quinientas cuotas".

d) Revelación del secreto de la correspondencia *:*

El artículo 290 por su parte tipifica la revelación del secreto de la correspondencia preceptuando que: *"E1 que con el propósito de perjudicar a otro o de procurar para sí o para un tercero un beneficio revele un secreto que conoce a través de carta telegrama despacho o cualquiera otra correspondencia no dirigida a él es sancionado con privación de libertad de tres meses a un año o multa de cien a trescientas cuotas o ambas.* Ahora bien, si el delito se comete por un funcionario o empleado público con abuso de su cargo *"la sanción es de privación de libertad de seis meses a dos años o multa de doscientas a quinientas cuotas"* (Art. 290 Nº 2).

En suma, puede afirmarse que en materia de protección penal de la vida privada e intimidad, el ordenamiento jurídico cubano contempla reglas generalmente reconocidas en las legislaciones latinoamericanas, pero su eventual idoneidad de aplicación para proteger los datos personales, parece cuestionable a la luz del principio de legalidad en materia penal.

10. Conclusiones

El sistema jurídico cubano no presenta normativa ni constitucional ni legal que se ocupe de la protección de los datos personales. Sólo cuenta Cuba con reglas comúnmente reconocidas de funcionamiento de algunas instituciones, como la tributaria por parte del Estado y, la bancaria. En cuanto a las normas penales que sancionan violaciones de aspectos de la vida privada e intimidad, estas aparecen como reglas mínimas de respeto por los derechos esenciales de las personas, de las cuales, no obstante, no pueden

sacarse fácilmente principios de protección a los datos personales.

Finalmente, y a modo de prevención, cabe señalar que el análisis del ordenamiento jurídico cubano en materia de datos personales se hace doblemente difícil; por una parte, no existe legislación especial que regule la materia en estudio, y por otra, existe una gran dificultad para la obtención del material jurídico vigente en este país. Por lo tanto, las conclusiones a que hemos llegado sólo pueden ser tenidas como meros indicios de esa realidad jurídica.

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN ECUADOR

1. Generalidades

El ordenamiento jurídico ecuatoriano cuenta con una nueva normativa constitucional que reconoce la acción de hábeas data. Junto con ella, existen diversas normas de tutela a los derechos humanos. De todo lo anterior se desprende una configuración constitucional favorable a la protección de los datos personales. Sin embargo, en la práctica, la operatividad del instituto del hábeas data se ha visto mermada a consecuencia de discusiones doctrinarias y jurisprudenciales que giran en torno a la interpretación de la norma constitucional en relación a la ley que fija el procedimiento judicial para hacer efectiva la acción de hábeas data.

En el ámbito legal, Ecuador no dispone de una ley de protección de datos personales que desarrolle las normas constitucionales, sino sólo de una normativa de carácter procedimental que regula la acción constitucional de hábeas data (Ley de Control Constitucional), cuya vigencia ha sido puesta en duda actualmente en el Ecuador. A nivel legal sectorial, hemos encontrado normas que regulan ciertos aspectos específicos de algunos tipos de datos personales, destacando la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, la cual establece algunas normas en materia de protección de datos.

2. Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional

La nueva Constitución ecuatoriana del año 1998 [342] establece expresamente en la Sección Segunda de su Capítulo 6 titulado “De las garantías de los derechos”, la garantía del hábeas data, la cual se desarrolla en el solo artículo 94. Cabe hacer presente en esta materia que la Constitución anterior de 1996 ya contemplaba esta garantía y la regulaba en el artículo 30. La nueva disposición del artículo 94 presenta diferencias con la de la

[342] [En línea] < http://www.georgetown.edu/pdba/Constitutions/Ecuador/ecuador98.html > [consulta: 3 de Noviembre 2002].

anterior Constitución; en la actualidad, y como resultado del cambio normativo señalado, se han originado controversias en cuanto a la determinación de los órganos competentes para conocer y resolver las acciones de hábeas data, cuestión en la que aún no existe acuerdo doctrinario ni del máximo órgano de justicia constitucional, el Tribunal Constitucional del Ecuador.

Siguiendo dentro del ámbito constitucional ecuatoriano, podemos señalar que también se reconoce y garantiza el derecho a la honra, la buena reputación familiar y a la intimidad personal y familiar (Art. 23 Nº 8). Asimismo ocurre en relación a la inviolabilidad de domicilio (Art. 23 Nº 12) y la inviolabilidad y secreto de la correspondencia (Art. 23 Nº 13).

En el Nº 21 del artículo 23 constitucional, se contempla una disposición directamente relacionada con la protección a los datos personales específicamente circunscrita a los datos sensibles, en la cual se señala que sin perjuicio de los derechos establecidos en la Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes: *"(…) 21. El derecho a guardar reserva sobre sus convicciones políticas y religiosas. Nadie podrá ser obligado a declarar sobre ellas. En ningún caso se podrá utilizar la información personal de terceros sobre sus creencias religiosas y filiación política, ni sobre datos referentes a salud y vida sexual, salvo para satisfacer necesidades de atención médica".*

La disposición anterior es de trascendental importancia pues de ella claramente se desprendería una prohibición de tratamiento de los datos sensibles, al hablar de *"utilizar la información personal de terceros"*, salvo el tratamiento o utilización de éstos para la satisfacción de necesidades de atención médica. Esta norma llama la atención, pues no es común que se trate esta materia a nivel constitucional, sino más bien dentro de una ley de protección de datos personales. Con todo, estimamos que no está demás, por el contrario fortalece la configuración constitucional del hábeas data, la cual como se ha dicho aún no se ha desarrollado a nivel legal.

Además de las disposiciones ya mencionadas, el Constituyente ecuatoriano ha contemplado otras que vienen a complementar el sistema de protección a los derechos humanos. Así, el artículo 16 dispone que: *"El más alto deber del Estado consiste en respetar y hacer respetar los derechos humanos que garantiza esta Constitución".* El artículo 17 a su vez preceptúa que el Estado garantizará a todos sus habitantes, sin discriminación alguna, el libre y eficaz ejercicio y el goce de los derechos humanos establecidos en la *"Constitución y en las declaraciones, pactos, convenios y más instrumentos internacionales vigentes. (…) Adoptará, mediante planes y programas permanentes y periódicos, medidas para el efectivo goce de estos derechos".*

A renglón seguido se encuentra a nuestro juicio una de las disposiciones más importantes de la Carta ecuatoriana, el artículo 18, el cual dispone:

Art. 18.- *"Los derechos y garantías determinados en esta Constitución y en los instrumentos internacionales vigentes, serán directa e inmediatamente aplicables por y ante cualquier juez, tribunal o autoridad".*

En materia de derechos y garantías constitucionales, se estará a la interpretación que más favorezca su efectiva vigencia. Ninguna autoridad podrá exigir condiciones o

requisitos no establecidos en la Constitución o la ley, para el ejercicio de estos derechos.

No podrá alegarse falta de ley para justificar la violación o desconocimiento de los derechos establecidos en esta Constitución, para desechar la acción por esos hechos, o para negar el reconocimiento de tales derechos.

Las leyes no podrán restringir el ejercicio de los derechos y garantías constitucionales".

Finalmente, el artículo 19 señala que los derechos y garantías señalados en la Constitución y en los instrumentos internacionales, *"no excluyen otros que se deriven de la naturaleza de la persona y que son necesarios para su pleno desenvolvimiento moral y material".*

De todo lo anterior, puede concluirse que el Constituyente ecuatoriano establece de manera expresa la supremacía de los derechos inherentes a las personas, limitando el ejercicio de su soberanía a éstos aunque no se plasmen ni en la Constitución ni en tratados internacionales de Derechos Humanos. Al mismo tiempo, obliga a la interpretación más favorable a esos derechos, entre los cuales se encuentran sin duda aquéllos que subyacen a la protección de los datos personales, como la intimidad y vida privada, lo cual se garantiza instrumentalmente a través de la acción constitucional de hábeas data.

A continuación, analizaremos la disposición que consagra la garantía del hábeas data haciendo referencia en primer lugar a la norma constitucional anterior a la actual, a fin de apreciar las consecuencias prácticas que han devenido de tal cambio normativo.

a) El Hábeas Data en la Constitución de 1996

La derogada Constitución ecuatoriana de 1996 disponía en esta materia lo siguiente:

Artículo 30.- *"Toda persona tiene derecho a acceder a los documentos, bancos de datos e informes que sobre si misma o sobre sus bienes consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su* ***finalidad*** *".*

"Igualmente, podrá solicitar ante el funcionario ***o juez competente*** *la actualización, rectificación, eliminación o anulación de aquéllos si fueren erróneos o afectaren ilegítimamente sus derechos".*

"Se exceptúan los documentos reservados por razones de seguridad nacional" (negrita nuestra).

b) El Hábeas Data en la Constitución actual de 1998

A este respecto la Constitución ecuatoriana señala:

Artículo. 94.- *"Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su* ***propósito*** *".*

"Podrá solicitar ante el ***funcionario respectivo*** *, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus*

derechos" ***.***

"Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización".

"La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional" (negrita nuestra).

De la comparación de los textos anteriores saltan a la vista importantes diferencias. Algunas de éstas, han causado problemas interpretativos que han dividido tanto a la doctrina como a la jurisprudencia constitucional ecuatoriana, en particular, en lo referido a la tramitación de la acción de hábeas data. Esta controversia se reseña a continuación.

El inciso 2º del artículo 30 de la derogada Constitución de 1996, establecía que toda persona podía solicitar ante el *"funcionario o juez competente"* la actualización, rectificación, eliminación o anulación de aquellos datos que fueren erróneos o afectaren ilegítimamente los derechos del titular. Sin embargo, la Ley de Control Constitucional de 1997 [343] (en adelante LCC), señala en el artículo 37 que la acción de hábeas data "*deberá interponerse ante cualquier juez o tribunal"* de primera instancia del domicilio del poseedor de la información o datos requeridos, omitiendo la mención al *"funcionario"*, al cual la Constitución de 1996 hacía referencia. Por otra parte, la LCC señala que *"la resolución que deniegue el hábeas data será susceptible de apelación ante el Tribunal Constitucional* (…)". Finalmente, según el artículo 41 de la LCC es el Tribunal Constitucional el órgano jurisdiccional llamado a conocer y fallar en última instancia la acción de hábeas data. Esta configuración del hábeas data, no causó mayor discusión en materia de competencia para conocer de esas acciones, pues se aplicaba la disposición del artículo 37 de la LCC, por lo cual las acciones de hábeas data eran conocidas y falladas por los jueces de primera instancia. Lo anterior cambió radicalmente luego de la entrada en vigencia de la nueva Constitución y del texto del artículo 94 que consagra el hábeas data; la discusión se centra fundamentalmente en cuanto al rol que le cabe al "*funcionario respectivo"* en la tramitación de las acciones hábeas data, materia en la cual la Ley de Control Constitucional de 1997 no se pronuncia.

En relación con lo anterior, se ha sostenido por una parte de la doctrina que luego de la dictación de la nueva Constitución, el texto que consagra el hábeas data (Art. 94) habría derogado a la LCC en lo que respecta a la tramitación de esta acción, por lo que se les habría quitado competencia en primera instancia a los jueces para conocer de esas acciones, siendo los únicos autorizados para tal efecto, los "*funcionarios respectivos".* En este sentido, se ha pronunciado Galo Chiriboga para quien "la jurisdicción nace de la Ley. En este caso, de la Constitución. El texto actual del Artículo 94 le quitó jurisdicción a los jueces" (sic). Agrega este autor, que en caso de existir discrepancia entre la Constitución y la Ley de Control Constitucional debe aplicarse en cada caso que conozcan los jueces, lo dispuesto en el artículo 274 de la Constitución [344] ,

[343] Esta Ley, vigente en la actualidad, fue dictada de conformidad a la derogada Constitución de 1996 y fue publicada en el Registro Oficial con fecha 2 de Julio 1997. Ésta regula conjuntamente diversos aspectos relativos al Tribunal Constitucional, al hábeas corpus, al hábeas data y al amparo constitucional. Puede consultarse [en línea] < http://www.cajpe.org.pe/rij/bases/legisla/ecuador/lh-25.HTMl > [consulta: 3 de Febrero 2003].

declarando inaplicables todas las normas que contradigan a la Constitución. Finaliza señalando que "la Reforma de la Constitución de 1998, es norma posterior a la Ley de Control Constitucional, por lo tanto, cronológicamente, la ley posterior deroga a la anterior" [345] . La doctrina contraria, sostiene que el artículo 94 de la Constitución Política es claro y determinante al elevar a la categoría de norma constitucional el derecho de las personas al acceso de documentos, bancos de datos e informes que sobre si mismas o sobre sus bienes, consten en entidades públicas o privadas. Por su parte, el inciso segundo de esta norma faculta a las personas a recurrir directamente al funcionario poseedor de la información. En este sentido, Gordón ha dicho que en el caso de optarse por esta vía informal, a más de desaparecer como acción el hábeas data, "se perdería la capacidad de apelación ante el Tribunal Constitucional; y, lo que es peor, en caso de la existencia de un evidente daño moral en contra de las personas, no podría recurrirse a la justicia ordinaria para el reconocimiento de los daños y perjuicios que tal interrogante ha causado a la persona. En suma, el Hábeas Data, no es un recurso, es una acción, que tiene como elemento principal la intervención del juez" (sic) [346] .

La Jurisprudencia Constitucional por su parte, ha hecho suya la discusión señalada reproduciendo en general las posiciones interpretativas, aunque al parecer, se inclinaría por la última doctrina. En relación a ella, se ha señalado por Gordón que "el Pleno del Tribunal Constitucional ha tomado cartas en el asunto y en el ejercicio de sus facultades, ha determinado que la Acción de Hábeas Data, debe incoarse ante el juez o tribunal de

344 El artículo 274 de la Constitución dispone que: "*cualquier juez o tribunal, en las causas que conozca, podrá declarar inaplicable, de oficio o a petición de parte, un precepto jurídico contrario a las normas de la Constitución o de los tratados y convenios internacionales, sin perjuicio de fallar sobre el asunto controvertido. (…)Esta declaración no tendrá fuerza obligatoria sino en las causas en que se pronuncie. El juez, tribunal o sala presentará un informe sobre la declaratoria de inconstitucionalidad, para que el Tribunal Constitucional resuelva con carácter general y obligatorio".*

345 Chiriboga Zambrano, Galo: *"La acción de amparo y de hábeas data: garantías de los derechos constitucionales y su nueva realidad jurídica"*. [En línea] < http://www.ildis.org.ec/amparo/hab.htm > [consulta: 18 de Noviembre 2002]. En este mismo sentido se pronuncia Roldós Aguilera, quien sostiene que en la Constitución de 1998, la Asamblea eliminó la competencia de los jueces, quedando el segundo inciso solamente con la mención del funcionario, eliminando la del juez, estableciendo que si no se atiende el pedido del reclamante "el afectado podrá demandar indemnización", lo cual sería ante el Tribunal Contencioso Administrativo de tratarse de funcionario público o ante los jueces de lo Civil de ser relativo a particular, esto es con las instancias que permite la defensa del que reclama y de la administración. En Roldós Aguilera, León: *"El Hábeas Data",* citado por Chiriboga, *op. cit*. (anexo).

346 Gordón Ormaza, Fredy: "*El hábeas data en la legislación ecuatoriana"*, [en línea] < http://www.dlh.lahora.com.ec/paginas/judicial/paginas/D.Constitucional.172.htm > [consulta: 27 de Febrero 2003]. En este mismo sentido se pronuncia García Ponce, quien señala que el precepto constitucional que establece la garantía del hábeas data, se complementa con el Titulo II De las garantías de los derechos de las personas, Capítulo II, artículo 34 y siguientes de la Ley de Control Constitucional, en lo atinente a la substanciación de este recurso, en donde no cabe la inhibición del Juez o tribunal de primera instancia, que conozca del recurso, excepto cuando haya incompatibilidad de parentesco hasta cuarto grado de consanguinidad y segundo de afinidad u otros impedimentos legales. Luego agrega, consecuente con lo afirmado anteriormente que "es competente para conocer del recurso de hábeas data cualquier juez o tribunal de primera instancia del domicilio del poseedor de la información". García Ponce, Temístocles: *El recurso de Hábeas Data*. [En línea] < http://www.dlh.lahora.com.ec/paginas/judicial/paginas/D.Constitucional.122.htm > [consulta: 16 de Noviembre 2002].

instancia" [347] . En sentido contrario a la postura anterior, es decir, la minoritaria, podemos citar la opinión dos Magistrados del Tribunal Constitucional, los cuales han señalado que "la codificación de la Constitución, publicada en el Registro Oficial No. 1 de 11 de agosto de 1998, en su artículo 94, no otorga competencia a los jueces para efectos de la interposición de la acción de hábeas data, siendo este Tribunal, de conformidad con el número 3 del artículo 276 de la Constitución, quien debe conocer las *resoluciones de las entidades* que denieguen el acceso a la información o a los documentos que requiere el peticionario(…) [348] (cursiva nuestra).

En definitiva, puede afirmarse que el punto no es claro ni en la doctrina ni en la jurisprudencia constitucional ecuatoriana, por lo que sería adecuado un pronunciamiento a través de una reforma al artículo 94 de la Constitución o a través de una interpretación auténtica por parte del Constituyente. Por nuestra parte haremos dos comentarios al respecto:

1º) De una primera lectura al texto del artículo 94 constitucional, pareciera desprenderse que el Constituyente habría quitado competencia a los jueces para conocer de una petición de acceso, actualización, rectificación, eliminación o anulación de datos erróneos o lesivos de los derechos de las personas, pues ya no se refiere a ellos, sino sólo al "*funcionario respectivo*". Luego, el artículo 276 de la Constitución actual señala que: "*Competerá al Tribunal Constitucional: (…) 3. Conocer las resoluciones que denieguen el hábeas corpus, el hábeas data y el amparo, y los casos de apelación previstos en la acción de amparo"*. Por lo tanto, dado que la competencia del Tribunal Constitucional en el numeral 3º del artículo 276 de la Constitución, se circunscribe al conocimiento de "*resoluciones"* denegatorias de tres acciones constitucionales de máxima importancia (amparo, hábeas corpus y hábeas data), parecería difícil argumentar que cualquier funcionario tuviera competencia para dictar ese tipo de *"resoluciones"*. Más aún, cabría preguntarse antes, si esos funcionarios están facultados legal y constitucionalmente para ejercer jurisdicción. Al respecto, pensamos que la respuesta es clara, la Constitución no otorga jurisdicción al "*funcionario respectivo*". Luego, la competencia del Tribunal Constitucional para conocer de las resoluciones que denieguen el hábeas data se refiere exclusivamente a aquéllas dictadas por jueces. Una interpretación ajustada a derecho debería concluir que sólo pueden ejercer jurisdicción aquellos órganos constitucional y legalmente investidos de esa potestad. No vemos que éste sea el caso de los 'funcionarios respectivos'.

A pesar de lo anterior, estimamos que podría llegarse a una solución interpretativa que armonizara el texto constitucional con la Ley de Control Constitucional y que no excluyera ni al *"funcionario respectivo"* ni mucho menos al juez en el procedimiento de hábeas data. El razonamiento es el siguiente: 1) Al señalar la Constitución que podrá solicitarse la información al "*funcionario respectivo*", parecería razonable pensar que se

[347] *Ídem*.

[348] Voto salvado de los doctores Marco Morales Tobar y Hernán Rivadeneira Jativa, en la resolución Nº 095-2001-TP, del Caso Nº 004-2001-HD. [En línea] < http://www.dlh.lahora.com.ec/paginas/judicial/paginas/T.Constitucional.65.html > [consulta: 16 de Diciembre 2002].

está refiriendo al eventual sujeto pasivo de una también eventual acción de hábeas data. O sea, el *"funcionario respectivo"* sería cualquier persona que tenga a su cargo, jurídica o fácticamente, un archivo, registro o banco de datos personales, el que, en caso de no satisfacer los requerimientos del titular de los datos, se convierte en eventual sujeto pasivo de la acción de hábeas data a seguirse ante el juez competente. Luego, el titular de datos personales "*podrá"* optar por seguir un procedimiento informal o vía extrajudicial ante el *"funcionario respectivo"* responsable del banco de datos o archivo, el cual deberá pronunciarse sobre la petición del titular de los datos no como juez, sino en su calidad de responsable del archivo, registro o banco de datos personales, no importando si éste ejerce un cargo en un organismo público o privado; 2) En concordancia con lo anterior, estimamos que la Constitución no podría estarse refiriéndose jamás con el término *"funcionario respectivo"* a un tercero imparcial que dirima un conflicto entre partes y que esté investido con facultades de imperio para hacer ejecutar su decisión (un juez), pues para ello debería otorgársele expresamente jurisdicción. Creemos que la referencia al *"funcionario respectivo"*, debe interpretarse o ser leído como sujeto responsable del archivo, registro o banco de datos personales, sea de carácter público o privado, ante el cual los titulares de datos personales podrán recurrir informal o administrativamente para solicitar la actualización, rectificación, eliminación o anulación de éstos y, 3) En cuanto a la obligatoriedad o no de recurrir al procedimiento informal o administrativo para ejercer los derechos de titular de datos personales, cabría señalar que, éste sólo tendría el carácter de 'facultativo', pues podría el titular de los datos personales, optar por la directa intervención del juez, en razón a que el propio Constituyente señala que "*podrá solicitar ante el funcionario respectivo"*,lo cual en ningún caso obligaría a hacerlo ante él.

Estimamos que con la interpretación propuesta, podría sostenerse jurídicamente que la competencia de los jueces habría quedado intacta, siendo ellos competentes para conocer y resolver de manera exclusiva y excluyente las acciones de hábeas data en virtud del artículo 37 de la LCC que señala perentoriamente que "*la acción de hábeas data deberá interponerse"* ante cualquier juez o tribunal de primera instancia. Luego, en caso que el juez competente rechace la acción de hábeas data, se abre la posibilidad para el actor de elevar el conocimiento del asunto ante el Tribunal Constitucional (Art. 276 Nº 3). En suma, el rol del "*funcionario respectivo"* quedaría reducido a responder satisfactoriamente las solicitudes de los titulares de datos personales y, en caso de no ser así, convertirse en eventual sujeto pasivo de la acción de hábeas data a interponerse por el titular de los datos ante el juez competente. Finalmente, y en caso que erróneamente se ejerza la acción constitucional de hábeas data ante cualquier otro ente distinto de un juez, todo acto pronunciado por éste que emule una sentencia, no tendría existencia jurídica alguna, sería una no sentencia (*nicht turteil*), que jamás podría tener efecto jurídico alguno, por lo que sería imposible que pudiere llegar a conocerse por el Tribunal Constitucional, el cual sólo puede pronunciarse respecto de resoluciones denegatorias de hábeas data fallados por los jueces y no por entes carentes de jurisdicción.

En síntesis, creemos que la Constitución ecuatoriana de 1998 no ha derogado tácitamente en ninguna de sus partes a las normas que regulan la tramitación de la acción de hábeas data contenida en la LCC de 1997. La entidad de los bienes jurídicos que protege la acción constitucional del hábeas data, exige que sea interpretada de manera más favorable a su efectiva vigencia, esto es lo que precisamente dispone el

Constituyente en el artículo 18 inciso 2 de la Ley Fundamental del Ecuador.

2º) En lo que se refiere a otras diferencias apreciables en el texto del nuevo artículo 94 de la Constitución, podemos señalar:

a) En primer lugar, llama la atención la sustitución del término finalidad por *propósito.* Para nosotros este último, poseería una connotación más subjetiva que el término finalidad, pues la voz "*propósito*" denota un ánimo o intencionalidad al realizar o hacer algo [349] , en cambio el vocablo finalidad, denota un objeto perseguido o motivo con que se ejecuta una cosa [350] . No estamos al tanto de las discusiones en el seno de la Comisión Constituyente a la hora de sustituir un término por otro, pero creemos que es más preciso utilizar el término finalidad que propósito, pues en la materia de protección a los datos personales se adecua mejor a las disposiciones comparadas sobre el tema, en particular al artículo 10 de la Directiva 94/46 CE [351] . Las consecuencias prácticas de esta modificación aún están por verse en la jurisprudencia constitucional ecuatoriana, nosotros sólo llamamos la atención sobre el punto.

b) En segundo lugar, y dentro el ámbito de la responsabilidad, cabe hacer presente que la Constitución de 1998 se hace cargo de sentar el principio de responsabilidad funcionaria, uno de los pilares del Estado de Derecho. En nuestro concepto, la inteligencia del precepto nos dice que el término *"funcionario respectivo"* comprende tanto al encargado del banco de datos público como privado, pues no cabría hacer distinción a este respecto, según la interpretación que hemos sostenido al efecto.

c) Finalmente, el Constituyente encomienda a la ley el establecimiento de un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional. En este punto puede decirse que se avanzó normativamente, pues con anterioridad se establecía la improcedencia del ejercicio del hábeas data informativo, respecto de los datos personales que constaran en documentos reservados por motivos de seguridad nacional. Con todo, no tenemos conocimiento de que la señalada ley exista en el sistema legal ecuatoriano.

2.2 Protección Legal de los Datos Personales

El ordenamiento jurídico ecuatoriano no dispone de una legislación de protección de datos personales. No obstante lo anterior, cuenta con normas legales de carácter sectorial, que en general se ocupan de tutelar ciertos datos personales de carácter económico, relacionados con algunas operaciones bancarias y con información proporcionada al Estado a efectos impositivos. Junto con este tipo de normas cabe destacar la reciente Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos, la cual se ocupa entre otras cosas, de la protección a los datos personales circunscrita a

349 Diccionario de la Lengua Española, RAE, 21º Edición, Tomo II, pág. 1679.

350 *Ídem*, Tomo I, págs. 970 y 971.

351 Este artículo señala que los responsables del tratamiento de datos personales o su representante deberán comunicar a la persona de quién se recaben los datos, entre otros: *"b) los fines del tratamiento de que van a ser objeto los datos".*

la mensajería de datos. Esta ley establece algunos principios en la materia, así como también deberes para aquellos que traten esos datos e introduce algunos delitos en el Código Penal. A continuación revisaremos las normas que ya se han mencionado.

2.2.1) Codificación de la Ley General de Instituciones del Sistema Financiero [352]

El artículo 88 de esta Ley establece el secreto bancario en los siguientes términos: *"Los depósitos y demás captaciones de cualquier índole que se realicen en las instituciones del sistema financiero, estarán sujetos a sigilo bancario, por lo cual las instituciones financieras receptoras de los depósitos y captaciones, sus administradores, funcionarios y empleados no podrán proporcionar información relativa a dichas operaciones sino a su titular o a quien lo represente legalmente"*. Agrega el inciso 2º que: *"las firmas auditoras externas tendrán acceso al conocimiento detallado de las operaciones anteriores y sus antecedentes, las que también quedarán sometidas al sigilo bancario"* (Art. 88 inciso 2º). El inciso 3º por su parte, dispone que las instituciones del sistema financiero podrán dar a conocer las operaciones anteriores, en términos globales, no personalizados ni parcializados, sólo para fines estadísticos o de información (Art. 88 inciso 3º). Finalmente, se señala que las instituciones financieras también *"podrán proporcionar información general respecto del comportamiento de clientes en particular, para fines de evaluación de crédito a requerimiento de otra institución del sistema financiero o de establecimientos comerciales autorizados por aquellos, sin que ello implique la facultad de revelar transacciones individualizadas"* (Art. 88 inciso 4º).

De lo señalado con anterioridad se desprende que sólo quedarían cubiertas por el secreto bancario las operaciones pasivas, ya que la Ley habla de depósitos y demás captaciones de cualquier índole. Este deber de secreto se extiende además a las firmas auditoras externas. Llama la atención de esta normativa, que se faculte a las instituciones financieras a otorgar información a otras instituciones o a establecimientos comerciales acerca del comportamiento de clientes en particular a efectos de evaluación del crédito. Con ello se legaliza el mercado de la venta de informes comerciales, sin mayor regulación legal.

El artículo 89 de esta Ley, dispone por su parte que las instituciones del sistema financiero *"están obligadas a mantener sistemas de control interno que permitan una adecuada identificación de las personas que efectúan transacciones con la institución".* Lo anterior se relaciona con la obligación que estas instituciones tienen de proporcionar a la Superintendencia información sobre operaciones determinadas por ésta, que por su naturaleza y monto, requieran de un informe especial (Art. 89 inciso 2º). A su vez, la Ley señala que la Superintendencia *"proporcionará esta información a otras autoridades que por disposición legal expresa, previa determinación sobre su causa y fines, puedan requerirla, quienes también estarán sujetas al sigilo bancario hasta que se utilice la información en los fines para los cuales se la requirió"* (Art. 89 inciso 2º).

A renglón seguido, el artículo 90 dispone que: *"los informes de inspección y análisis*

[352] **[En línea] < http://www.superban.gov.ec/pages/e_leyes_sist-financiero_ley.htm > [consulta: 3 de Marzo 2003].**

que emitan los funcionarios y empleados de la Superintendencia, en el ejercicio de las funciones de control y vigilancia, serán escritos y reservados". También aclara este artículo que las operaciones activas y contingentes de las instituciones financieras no están sujetas a reserva, señalando que el sigilo sólo es aplicable a las operaciones pasivas (Art. 90 inciso 2º). Se agrega en esta materia que: *"a todo funcionario o empleado de la Superintendencia se le prohíbe revelar los datos contenidos en dichos informes, o dar a personas no relacionadas con las funciones de control y vigilancia información alguna respecto a los negocios o asuntos de la institución, obtenida en ejercicio de sus deberes oficiales"* (Art. 90 inciso 4º). En último lugar, se señala que cuando se hubiese iniciado un proceso de investigación en una institución del sistema financiero, *"los informes de auditoría no tendrán el carácter de reservados ni gozarán de sigilo bancario ante el Congreso Nacional, Fiscalía General de la Nación, Contraloría General del Estado y Comisión de Control Cívico de la Corrupción"* (Art. 90 inciso final) [353] .

Finalmente, debemos señalar en esta materia que el artículo 94 se encarga de establecer las sanciones correspondientes, disponiéndose al efecto que la violación a las disposiciones de este Capítulo será reprimida con uno a cinco años de prisión correccional, pudiéndose reclamar a los tribunales de justicia las indemnizaciones que correspondan por los daños que causasen las violaciones al sigilo y al carácter de reservado.

En suma, podemos decir que en cuanto a las normas jurídicas que rigen el funcionamiento del mercado bancario, es posible constatar en general estrictos deberes de sigilo o secreto respecto de las operaciones bancarias pasivas. Dentro de este ámbito, se aseguraría al menos una protección de carácter civil y penal en caso de violarse por los particulares o por funcionarios públicos los deberes de secreto de las operaciones bancarias, sanciones que se analizarán más adelante en el punto Nº 9.

[353] Como excepciones al deber se sigilo o secreto, el artículo 91 señala que "*se exceptúan de las prohibiciones contempladas en este Capítulo: a) Los informes y pruebas requeridos por los jueces y el Ministerio Público a la Superintendencia de Bancos y a las instituciones del sistema financiero privado, en las causas que estuviesen conociendo; b) La especificación del titular de cuentas corrientes cerradas por giro de cheques sin provisión de fondos; c) Los informes requeridos por el Directorio del Banco Central del Ecuador, el Banco Central del Ecuador, la Superintendencia de Compañías y la administración tributaria, en el ámbito de sus competencias, que serán tramitados por intermedio de la Superintendencia de Bancos; d) Los informes requeridos a la Superintendencia de Bancos por gobiernos o por autoridades competentes de los países con los que el Ecuador mantenga convenios legítimamente celebrados para combatir la delincuencia y en los términos de dichos convenios; e) Las informaciones financieras que constituyan intercambio con autoridades de control bancario y financiero de otros países, siempre que existan convenios vigentes legítimamente celebrados; f) La información que debe entregar la Superintendencia para dar a conocer al público la situación patrimonial y financiera de las instituciones del sistema financiero; y, g) Cuando la información sea requerida a las instituciones financieras, bajo control de la Superintendencia de Bancos, por el Secretario Ejecutivo del Consejo Nacional de Control de Sustancias Estupefacientes y Psicotrópicas, CONSEP, en el ámbito de su competencia"*. A renglón seguido, el artículo 92 viene a reforzar la regla general del deber de sigilo señalando que: *"todo funcionario público y toda persona, natural o jurídica, que en razón de su empleo, profesión u oficio, llegase a tener conocimiento de información sometida al sigilo o que tenga el carácter de reservada de conformidad con esta Ley, no podrá divulgarla en todo o en parte, salvo en los casos exceptuados en esta Ley. El incumplimiento de estas disposiciones acarreará las sanciones civiles y penales previstas en el artículo 94 de esta Ley".* En cuanto a las excepciones al deber se secreto bancario relativas a las facultades de transmisión internacional de datos en materia financiera, y los eventuales convenios celebrados por Ecuador y otros países, no tenemos información al respecto.

2.2.2) Código Tributario

El artículo 99 del Código Tributario ecuatoriano, titulado "Carácter de la Información Tributaria", señala que: *"Las declaraciones e informaciones de los contribuyentes, responsables o terceros, relacionadas con las obligaciones tributarias, serán utilizadas para los fines propios de la administración tributaria". (…) "La administración tributaria, deberá difundir anualmente los nombres de los sujetos pasivos y los valores que hayan pagado o no por sus obligaciones tributarias".*

Este artículo fue modificado en 1999 por el artículo 1º de la Ley 99-24 publicada en el Registro Oficial Nº S-181 / 30 de abril de 1999 [354] . Con anterioridad a la modificación legal, el citado precepto establecía expresamente el deber de reserva o secreto fiscal y señalaba que *"las declaraciones e informes que la Administración Tributaria obtenga de los contribuyentes, responsables o terceros, por cualquier medio, tendrán carácter reservado y sólo podrán ser utilizados para los fines propios de dicha Administración, salvo las excepciones legales"* [355] .

En suma, puede afirmarse que la actual normativa derogó el deber de secreto tributario o fiscal contemplado hasta el año 1999. En la actualidad, sólo existe la limitación a la utilización de la información entregada a la Administración Tributaria, fundada en los **"** *fines propios de la administración tributaria"*. Además de lo anterior, se establece expresamente la facultad de aquél organismo del Estado para difundir información relativa al cumplimiento e incumplimiento de las obligaciones tributarias, con lo cual eventualmente se estaría legalizando indirectamente la venta de este tipo de información.

2.2.3) Ley de Comercio Electrónico, Firmas y Mensajes de Datos [356]

La reciente Ley de Comercio Electrónico ecuatoriana (en adelante Ley) tiene por objeto la regulación de diversas materias, a saber: los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas (Art. 1º). Dentro del complejo ámbito de regulación que prevé esta Ley, podemos destacar la expresa normativa que se ocupa de la protección de los usuarios de los sistemas que son objeto de aquélla (mensajería de datos, firma electrónica, contratación electrónica etc.). A propósito de esa normativa, se

354 [En línea] < http://webs.demasiado.com/eculegal/ecu1/011.htm > [consulta: 2 de Marzo 2003].

355 *Ibídem*.

356 Ley Nº 67. Registro Oficial, Suplemento 557 de 17 de Abril del 2002. [En línea] < http://www.corpece.org.ec/documentos/ley/ley_ce.doc > [consulta: 2 de Marzo 2003]. Resulta paradójico que en este país se haya legislado sobre un tema tan importante en la actualidad siendo que al mes de Mayo del 2002, el Ecuador tenía menos de cuatro personas suscritas a Internet por cada 1.000, es decir, presentaba una penetración de Internet del 0,3% respecto a su población total, el nivel más bajo del área andina. [En línea] < http://www.delitosinformaticos.com/noticias/99199121038851.shtml > [consulta: 2 de Marzo 2003].

establecen diversas normas que revisten especial interés, pues se relacionan directamente con la protección de los datos personales. A continuación señalaremos esas disposiciones.

El Título I de esta Ley, denominado "De los Mensajes de Datos", establece en su Capítulo I los "Principios Generales". De estos principios destaca el de "*Confidencialidad y reserva"*, contemplado en el artículo 5º el cual dispone que: *"Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia".* Esta disposición entendemos que es una extensión del tradicional derecho a la inviolabilidad de las comunicaciones, ahora materializada a través de medios digitales [357] .

Por otra parte, el artículo 9 intitulado "Protección de datos" establece importantes reglas de las cuales claramente se desprenden algunos de los principios generales para el tratamiento de los datos personales. Señala este artículo al efecto que:

"Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros".

"La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente".

"No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato".

"El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo".

El artículo anterior recoge, al menos, dos principios generales para el tratamiento de datos personales establecidos en la Directiva europea 95/46/CE; se visualiza el principio del consentimiento del titular tanto para el tratamiento de sus datos, como para la transmisión o cesión de éstos a terceros. Interpretada la disposición del artículo 9 de la Ley Nº 67-2002 en armonía con el artículo 21 Nº 23 de la Constitución, podría plantearse eventualmente un conflicto de hermenéutica, pues ésta señala que: *"en ningún caso se podrá utilizar"* la información personal de terceros sobre sus creencias religiosas y

[357] Esta Ley define el mensaje de datos como *"toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos"* (Disposición Gral. 9ª Ley Nº 67-2002).

filiación política, ni sobre datos referentes a salud y vida sexual, salvo para satisfacer necesidades de atención médica. Dada la redacción de la norma podría estimarse que, no obstante, el titular pueda prestar su consentimiento para la utilización de sus datos sensibles, éste carecería de eficacia jurídica por expresa disposición constitucional. Finalmente, el legislador establece los límites al tratamiento de los datos personales, los cuales están dados por el respeto del derecho a la privacidad, intimidad y confidencialidad (Art. 9 inciso 2º Ley 67-2002).

Más adelante, en el Capítulo III denominado "De las Entidades de Certificación de Información", se señala por el artículo 32º que: *"las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta ley".* De lo dispuesto en este artículo, de restringida aplicación, se visualiza el principio de la seguridad de los datos.

Finalmente, cabe agregar que la Ley dentro de su Disposición General "*Novena*", contempla un *"Glosario de términos"*, de los cuales destacan para nuestro estudio los siguientes:

1) Intimidad: *"El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados".* Esta definición sin duda que resulta aclaratoria para una eventual integración de la ley en los casos no legislados, teniendo presente que la Ley 67-2002 sólo abarca un ámbito del tratamiento de los datos, el relativo al uso y transmisión de los mensajes de datos.

2) Datos personales: *"Son aquellos datos o información de carácter personal o intimo, que son materia de protección en virtud de esta ley".*

3) Datos personales autorizados: *"Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicite , solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular"*. De esta disposición se desprende claramente tanto el principio de la finalidad como el consentimiento informado del titular de los datos.

En suma, podríamos concluir que si bien esta Ley tiene un ámbito de aplicación restringido, las reglas que establece siguen la línea de principios generales considerados como adecuados para una efectiva de protección de los titulares de datos personales. En nuestro concepto, la falta de ley especial de protección de datos personales, puede ser suplida por vía jurisprudencial, aplicando por analogía los principios que informan esta Ley, teniendo además en vista la configuración constitucional que se le ha dado a la materia. En este sentido, este estatuto legal vendría a aclarar una opción del legislador que no deja de sorprender, pues se adelanta a regular temas tan actuales y complejos, saltándose una regulación básica que desarrolle de manera general la protección de los datos y la garantía del hábeas data constitucional.

3. Bienes Jurídicos Protegidos por la Legislación de Datos Personales

Como ya se ha señalado, el ordenamiento jurídico ecuatoriano no dispone de una ley de protección de datos personales, no obstante contar con una Constitución que reconoce en el artículo 94 la acción de hábeas data, y que prohíbe el uso de los denominados datos sensibles (Art. 23 Nº 21). A pesar de la falta de legislación general ya anotada, ello no es óbice para analizar el bien jurídico tutelado tanto por la Carta Fundamental como por legislador en materia de mensajes de datos (Ley 67-2002).

En opinión de Temístocles García la acción de hábeas data "tiende a proteger varios derechos como el de la intimidad, el honor, la imagen, la identidad, la libre elección sexual, etc." [358] . Para Aída García "es más claro, dentro del contexto de las relaciones sociales y económicas actual, el pensar en que el hábeas data, tal como lo concibe nuestra Ley Suprema, protege el derecho a la honra y a la buena reputación" [359] . Por su parte, Galo Chiriboga refiriéndose también al hábeas data, señala que ésta es una "garantía que protege varios derechos, tales como, la honra, la buena reputación, la intimidad y también el derecho a la información" [360] . Finalmente, Gordón señala que el hábeas data es un "instrumento elevado a la categoría de verdadera garantía constitucional llamada a proteger los derechos a la información a través del acceso a documentos, bancos de datos e informes que reposen en manos de particulares o del Estado" [361] .

En base a lo anterior, se puede afirmar que no existe unanimidad de pareceres en la doctrina a la hora de señalar cuáles serían los bienes jurídicos tutelados por la normativa constitucional que establece la garantía del hábeas data. Llama la atención de las opiniones anteriores, la nula referencia a la autodeterminación informativa como bien jurídico protegido, siendo que en nuestro concepto, de lo preceptuado por el Constituyente aparecería meridianamente claro que ese bien jurídico si estaría tutelado al menos implícitamente.

Diversas razones podrían explicar la ausencia de referencia a la autodeterminación informativa por parte de los autores y del propio Constituyente. Una posibilidad sería entender derechamente que no se han referido a ella los autores ni la Ley Fundamental; esta opción es la que más dudas plantea, pues sería extraño que dentro del ordenamiento jurídico ecuatoriano, el cual establece disposiciones expresas relacionadas con la protección de datos personales (Arts. 23 Nº 21 y 94 C. Pol.), no se tomara en

358 García, Temístocles, *op. cit*. [en línea].

359 García Berni, Aída: *"La acción de Hábeas Data"* [en línea] < http://www.dlh.lahora.com.ec/paginas/judicial/paginas/D.Constitucional.18.htm > [consulta: 28 de Febrero 2003].

360 Chiriboga Zambrano, Galo, *op. cit*., [en línea].

361 Gordón Ormaza, Fredy, *op. cit*., [en línea].

cuenta todo el desarrollo jurídico comparado tras el instituto del hábeas data. Otra opción sería entender implícito este derecho en otro o como parte de otro. Esta última idea desarrollaremos a continuación.

Estimamos que en el ordenamiento jurídico ecuatoriano, se ha entendido al hábeas data como una garantía de diversos derechos que pueden ser lesionados por el tratamiento de los datos personales. En base al artículo 94 de la Constitución, en verdad lo que se pretende consagrar es la 'garantía de un derecho de hábeas data' que no se desarrolla. Por lo tanto, sería en la configuración de ese 'derecho de hábeas data' donde radicaría parte del problema, pues se confundiría el o los derechos fundamentales (que no es el hábeas data propiamente tal) con su garantía específica (la acción de hábeas data). La situación anterior a la vez, podría ser consecuencia de una confusión en la utilización de los términos para referirse al derecho a la protección de datos (terminología seguida en este estudio), dado que -como se señaló en el Capítulo I-, no existe unanimidad de criterio lexicológico ni en la doctrina ni en la jurisprudencia comparada para referirse de forma genérica a la protección de los datos personales. Algunos, se refieren a ella con el término libertad informática, autodeterminación informativa e incluso hábeas data. Pensamos al mismo tiempo, que si efectivamente se ha contemplado el derecho a la protección de datos o hábeas data, debería estar presente a lo menos el derecho a la autodeterminación informativa, sea que se lo conciba como derecho autónomo, o como un derecho nuevo desgajado del derecho a la intimidad.

Como ya se señaló, a la configuración constitucional actual, se ha agregado a nivel legal la Ley 67 sobre comercio electrónico, la cual dentro de su glosario de términos (Disposición Novena) da un concepto de intimidad amplísimo, señalando que: *"el derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados".* Ahora bien, lo señalado por el legislador, vendría en parte a aclarar la opción normativa constitucional, pues aparecería meridianamente claro que al menos implícitamente el derecho a la autodeterminación informativa estaría contenido dentro del derecho a la intimidad, dado que los derechos y facultades entendidas como pertenecientes a ésta se acercan demasiado a una configuración de la intimidad mirada desde un punto de vista de derecho de control sobre la propia información. En definitiva, estimamos que el legislador reconocería el derecho a la autodeterminación informativa entendido como contenido del amplísimo derecho a la intimidad. Ahora bien, si esta interpretación la extrapolamos en sede constitucional, podríamos eventualmente aventurar una conclusión con más sentido que la sola afirmación a que el derecho a la libertad informática esta implícitamente reconocido por el Constituyente en el artículo 94 y 23 Nº 21. Ahora podría señalarse que, a pesar de no existir referencia explícita a este derecho el se encontraría contenido específicamente en el derecho a la intimidad.

En suma, creemos que podría afirmarse que de la configuración constitucional ecuatoriana se desprende el derecho a la autodeterminación informativa, el cual estaría contenido implícitamente en el derecho a la intimidad; señalado de manera no exclusiva por la doctrina y por la ley como objeto de tutela tanto de la garantía constitucional del

hábeas data, como del tratamiento y uso de los datos personales obtenidos a través de la mensajería de datos.

4. Principios Informativos de la Legislación de Protección de Datos Personales

La legislación del Ecuador si bien no cuenta con una ley de protección de datos personales al cual referirnos, si contempla una ley de carácter procesal que establece la tramitación de la acción de hábeas data (Ley de Control Constitucional) y, por otra parte también dispone de una Ley de Comercio Electrónico, Contratación Electrónica y Mensajería de Datos (Ley 67-2002), la cual contiene algunas disposiciones que dicen relación con la protección de los datos personales circunscrita al tema de la mensajería de datos. A continuación se señalarán los principios que hemos podido constatar a la luz de esas disposiciones.

1º. Principio de licitud y lealtad de los archivos de datos

El artículo 39 de la Ley de Control Constitucional señala que declarado con lugar el recurso de hábeas data, las entidades o personas requeridas entregarán, dentro del plazo de ocho días toda la información y, bajo juramento, *"una explicación detallada que incluya por lo menos, lo siguiente: a) Las razones y fundamentos legales que amparen la información recopilada (…)".* Creemos que en la referencia a las razones y fundamentos legales de la existencia del archivo se visualizaría implícitamente el principio de licitud de los archivos de datos.

Por su parte, el artículo 9 de la Ley 67-2002 dispone en el inciso 1º, que para la *"elaboración"*, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el *"consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros".* Asimismo el inciso 2º prescribe que la *"recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley*". Estimamos que en la referencia a la facultad del titular de decidir qué información podrá ser compartida y en el límite expreso impuesto por los derechos de privacidad intimidad y confidencialidad al tratamiento de datos estaría implícito el principio en comento.

2º. Principio del consentimiento informado del titular de los datos

Este principio se desprende del artículo 9 inciso 1º ya señalado, a propósito del principio de licitud de los archivos. También se contiene directamente en la definición legal de los 'datos personales autorizados' (Disposición Novena), entendidos como aquellos datos personales que *"el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicite, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular".*

3º. Principio de la seguridad de los datos

El ya señalado artículo 39 de la Ley de Control Constitucional, dispone que declarado con lugar el recurso, las entidades requeridas entregarán, dentro de ocho días toda la información y, bajo juramento, explicación detallada de: *"(…) e) El tipo de tecnología que se utiliza para almacenar la información; y, f) Las medidas de seguridad aplicadas para precautelar dicha información".* Con esta disposición indirectamente se está señalando que el juez evaluará los mecanismos de seguridad empleados en el tratamiento y conservación de los datos personales.

Por otra parte, el principio de la seguridad de los datos pareciera vislumbrarse en el artículo 32 de la Ley 67-2002, disposición contenida en el Capítulo III denominado "De las Entidades de Certificación de Información", el cual señala que: *"las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta ley".*

4º. Principio de confidencialidad de los datos

La Ley de Comercio Electrónico señala expresamente en el artículo 5 intitulado "Confidencialidad y reserva" que: *"Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia".*Luego, el inciso 2º del artículo 9º dispone que la recopilación y uso de datos personales *"responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley".* Por último, la Ley al definir la intimidad en la disposición general novena, indirectamente estaría consagrando este principio al señalar que el derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta ley, comprende también el derecho a la privacidad, *"a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados".*

5º. Principio del consentimiento para la cesión de los datos

Entendemos que este principio se contiene en el artículo 9 de la Ley 67-2002 al señalar que para la elaboración, *transferencia* o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el *"consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros"* (Art. 9 inc 1º). Lo anterior se refuerza en el inciso 2º, el cual dispone que la recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales *"podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente".* Finalmente, entendemos que

este principio tendría tutela a nivel penal toda vez que se sanciona a quien *"obtuviere información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares"* (Art. 58 inciso 5º). Queda planteada la duda en cuanto al ámbito de aplicación de la respectiva norma, pues ella está circunscrita a la mensajería de datos.

6º. Principio de la finalidad

El artículo 39 de la Ley de Control Constitucional, implícitamente reconocería en parte el principio de la finalidad al disponer que declarado con lugar el recurso (de hábeas data) las entidades o personas requeridas entregarán, dentro del plazo de ocho días toda la información y, bajo juramento, una explicación detallada que incluya por lo menos: *"(…) c) El uso dado y el que se pretenderá dar a ella; d) Las personas o entidades a quienes se les haya suministrado los referidos datos, la fecha del suministro y las razones para hacerlo"*.

Por otra parte, consideramos que este principio también estaría contenido en la disposición novena de la Ley 67-2002, al definir los 'datos personales autorizados' como aquellosen que el titular ha accedido a entregar o proporcionar de forma voluntaria, *"para ser usados por la persona, organismo o entidad de registro que los solicite solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular"*.

En suma, podemos señalar que en el ámbito de la Ley de Control Constitucional, si bien ésta es de carácter procedimental, contiene importantes disposiciones que avalan la existencia de principios generales para el tratamiento de datos que deben ser respetados por los responsables de bancos de datos, y tomados en cuenta por el juez a la hora de determinar responsabilidades. En lo que respecta a la Ley 67-2002, el único principio que no se visualiza en ella es paradójicamente el de la calidad de los datos, el cual se encuentra estrechamente ligado a los derechos de actualización, rectificación y eliminación contemplados en el artículo 94 de la Constitución.

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

Como consecuencia de la inexistencia de una ley general de protección de datos personales en el Ecuador, no nos podemos referir a las eventuales diferencias entre la regulación del sector público y privado.

6. Modelos de Tutela

El ordenamiento jurídico ecuatoriano contempla constitucionalmente la acción de hábeas data. Cabe recordar al respecto, que en este punto existe una discusión doctrinal y jurisprudencial en cuanto a la vigencia o no de la Ley de Control Constitucional, la cual regula el procedimiento para la tramitación de la acción de hábeas data. En este sentido y, dado que hemos optado por una interpretación que haga operativa la Ley de Control Constitucional, en lo que sigue se abordará la tramitación de la acción de hábeas data según el procedimiento establecido en esta Ley.

6.1 La Acción de Hábeas Data

La acción de hábeas data se encuentra consagrada en el artículo 94 de la Constitución y regulada en la cuestionada Ley de Control Constitucional de 1997 (en adelante LCC), artículos 34 y siguientes. Como se recordará, el artículo 94 constitucional dispone que: *"Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito (…) Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. (…) Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización. (…)La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional".*

6.1.1) Procedencia de la Acción

El artículo 34 de la LCC dispone que: *"Las personas naturales o jurídicas, nacionales o extranjeras, que deseen tener acceso a documentos, bancos de datos e informes que sobre sí mismas o su bienes están en poder de entidades públicas, de personas naturales o jurídicas privadas, así como conocer el uso y finalidad que se les haya dado o se les esté por dar, podrán interponer el recurso de hábeas data para requerir las respuestas y exigir el cumplimiento de las medidas tutelares prescritas en esta Ley, por parte de las personas que posean tales datos o informaciones".*

El artículo 35 por su parte señala que el hábeas data tendrá por objeto:

a) Obtener del poseedor de la información que éste la proporcione al recurrente, en forma completa, clara y verídica;

b) Obtener el acceso directo a la información;

c) Obtener de la persona que posee la información que la rectifique, elimine o no la divulgue a terceros; y,

d) Obtener certificaciones o verificaciones sobre que la persona poseedora de la información la ha rectificado, eliminado, o no la ha divulgado.

6.1.2) Legitimación Activa

Están legitimados para accionar de hábeas data *"toda persona"* [362] , sea natural o jurídica, nacional o extranjera (Art. 34 LCC).

6.1.3) Legitimación Pasiva

Son legitimados pasivos de la acción, *"las personas que posean tales datos o informaciones"* que consten en entidades tanto públicas como privadas [363] .

[362] Artículo 94 Constitución Política del Ecuador.

[363] Artículo 34 Ley de Control Constitucional.

6.1.4) Competencia

Es competente para conocer y fallar la acción de hábeas data, cualquier juez o tribunal de primera instancia del domicilio del poseedor de la información o datos requeridos (Art. 37 LCC).

6.1.5) Procedimiento Aplicable

El procedimiento aplicable para la tramitación de la acción de hábeas data en el Ecuador se explica a continuación:

1)*Audiencia*: el juez o tribunal, en el día hábil siguiente al de la presentación de la demanda, convocará a las partes a audiencia que se realizará dentro de un plazo de ocho días, diligencia de la cual se dejará constancia escrita. La respectiva resolución deberá dictarse en el término máximo de dos días, contados desde la fecha en que tuvo lugar la audiencia, aun si el demandado no asistiere a ella (Art. 38).

2)*Entrega de información*: declarado con lugar el recurso, las entidades o personas requeridas entregarán, dentro del plazo de ocho días toda la información y, bajo juramento, una explicación detallada que incluya por lo menos, lo siguiente:

a)Las razones y fundamentos legales que amparen la información recopilada;

b)La fecha desde la cual tienen esa información;

c)El uso dado y el que se pretenderá dar a ella;

d)Las personas o entidades a quienes se les haya suministrado los referidos datos, la fecha del suministro y las razones para hacerlo;

e)El tipo de tecnología que se utiliza para almacenar la información; y,

f)Las medidas de seguridad aplicadas para precautelar dicha información (Art. 39).

3) *Verificación de información entregada*: de considerarse insuficiente la respuesta, podrá solicitarse al juez que disponga la verificación directa, para la cual, se facilitará el acceso del interesado a las fuentes de información, proveyéndose el asesoramiento de peritos si así se solicitare (Art. 40).

6.1.6) La Sentencia

La LCC dispone en cuanto al contenido de ésta, que si de la información obtenida el demandante considera que uno o más datos deben ser eliminados, rectificados, o no darse a conocer a terceros, pedirá al juez que ordene al poseedor de la información que así proceda. El Juez ordenará tales medidas, salvo cuando claramente se establezca que la información no puede afectar el honor, la buena reputación, la intimidad o irrogar daño moral al solicitante. Asimismo se señala que el depositario de la información dará estricto cumplimiento a lo ordenado por el juez, lo cual certificará bajo juramento, sin perjuicio de que ello se verifique por parte del propio interesado, solo o acompañado de peritos, previa autorización del juez del trámite.

La resolución que niegue el hábeas data, será susceptible de apelación ante el

Tribunal Constitucional, en el término de ocho días a partir de la notificación de la misma (Art. 41 inciso final).

6.2 Otras Acciones

No se contemplan otras acciones encaminadas a proteger los datos personales en el ordenamiento jurídico ecuatoriano.

7. Mecanismos de Control

El sistema jurídico del Ecuador no contempla órgano de control alguno en materia de protección de datos personales.

8. Transmisión Internacional de Datos

En esta materia, tampoco existe en Ecuador legislación que se ocupe del tema.

9. Régimen de Responsabilidad

A pesar de la inexistencia de una ley de protección de datos personales, la Ley de Control Constitucional, de carácter procedimental, establece sanciones aplicables a quienes desobedezcan las órdenes impartidas por el Tribunal que conoce de un proceso de hábeas data. En otro ámbito, diversas normas sectoriales contemplan una protección específica a ciertos datos personales estableciendo su propio régimen sancionatorio. Junto con éstas, cabe tener presente las reglas de carácter civil y penal contenidas en los estatutos respectivos que tutelan los bienes jurídicos que fundamentarían la protección a los datos personales.

9.1 Responsabilidad Administrativa

A continuación revisaremos las sanciones administrativas previstas por algunos de los estatutos sectoriales señalados en el punto Nº 2.2 de este análisis.

9.1.1) Ley de Control Constitucional

La Ley de Control Constitucional, la cual consideraremos como ley especial en la materia, señala en el artículo 42 que: *"Los representantes legales de las personas jurídicas de derecho privado o las naturales que incumplieren las resoluciones expedidas por jueces o Tribunales que concedan el hábeas data, no podrán ejercer ni directa ni indirectamente, las actividades que venían desarrollando y que dieron lugar al hábeas data, por el lapso de un año".* Se agrega curiosamente por esta Ley que: *"Esta disposición será comunicada a los órganos de control y demás entidades públicas y privadas que sean del caso".* Sin duda que el legislador de la época (1997) previó la dictación de una ley de carácter sustantivo en la materia, acorde a lo preceptuado por la Constitución de 1996, derogada dos años más tarde, pues se refiere expresamente a "los órganos de control",

inexistentes hasta la fecha en el Ecuador.

Por otra parte, el artículo 43 prescribe ahora en el ámbito de los funcionarios públicos que aquéllos *"de libre remoción que se nieguen a cumplir con las resoluciones que expidan los jueces o tribunales dentro del procedimiento de hábeas data serán destituidos inmediatamente de su cargo o empleo, sin más trámite, por el respectivo juez o tribunal, salvo cuando se trate de los funcionarios elegidos por el Congreso Nacional, quienes deberán ser destituidos por éste, a pedido fundamentado del juez o tribunal y previo el correspondiente juicio político".* El inciso 2º agrega que la sanción de destitución se comunicará inmediatamente a la Contraloría General del Estado y a la autoridad nominadora correspondiente.

9.1.2) Ley General de Instituciones del Sistema Financiero

Dentro de las leyes sectoriales, cabe señalar y comentar la disposición contenida en la ley de instituciones financieras, dentro del capítulo titulado "Central de Riesgos". El artículo 95 de esta Ley señala en su primera parte que la Superintendencia establecerá un sistema de registro denominado Central de Riesgos, que permita contar con información individualizada debidamente consolidada y clasificada sobre los deudores principales de las instituciones del sistema financiero ecuatoriano, incluyendo los casos en que éstas actúen en su nombre por cuenta de una institución bancaria o financiera del exterior. Luego en el inciso 2º, prescribe que: "*La institución financiera que proporcione deliberadamente información falsa o maliciosa a la Central de Riesgos será sancionada por el Superintendente de Bancos con una multa de dos mil unidades de valor constante (2000 UVCs) cada vez y, la destitución del funcionario responsable en caso de reincidencia, sin perjuicio de la correspondiente responsabilidad penal"* (Art. 95 inciso 2º).

La disposición anterior parece de gran utilidad, pues cubriría aquellos casos en que los bancos enviaran información falsa a la Central de Riesgo, es decir, datos sobre los deudores principales de las instituciones del sistema financiero que no cumplieran con el principio general de la calidad de los datos. Por lo tanto, el titular de esos datos personales falsamente transmitidos a esa Central, tendría asegurada una acción en contra de los responsables, para la cual es competente el Superintendente de Bancos, es decir, a la autoridad administrativa. Con todo, para que sea procedente la responsabilidad administrativa en esos casos, el legislador exige que exista dolo, por lo que no sería aplicable este inciso 2º si lo que existe es falta de diligencia o culpa por parte de la institución financiera.

9.1.3) Código Tributario

Por su parte, la Ley tributaria ecuatoriana establece sanciones genéricas a las infracciones a ella. En efecto, el artículo 101 inciso final dispone que los funcionarios o empleados de la Administración Tributaria, en el ejercicio de sus funciones, son responsables, personal y pecuniariamente, por todo perjuicio que por su acción u omisión dolosa causaren al Estado o a los contribuyentes. Luego agrega que: *"La inobservancia de las leyes, reglamentos, jurisprudencia obligatoria e instrucciones escritas de la Administración, será sancionada con multa de diez unidades de valor constante (10*

UVC's) a setenta unidades de valor constante (70 UVC's). En caso de reincidencia, serán sancionados con la destitución del cargo por la máxima autoridad de la respectiva Administración Tributaria, sin perjuicio de la acción penal a que hubiere lugar. La sanción administrativa podrá ser apelada de conformidad con la Ley de Servicio Civil y Carrera Administrativa". Por lo tanto, entendemos que la violación del deber de reserva que pesa sobre los funcionarios de la Administración Tributaria se sanciona en virtud del artículo recién señalado.

En los demás casos en que un funcionario público cometa un acto que atente contra los derechos constitucionales del hábeas data, deberá estarse al particular estatuto funcionario y en defecto o ausencia de éste, a las reglas generales sobre responsabilidad funcionaria respecto de las cuales no tenemos información.

9.2 Responsabilidad Civil

En materia de responsabilidad civil, la propia Constitución dispone en el inciso 3º del artículo 94 que si la falta de atención de los responsables de los archivos, o registros de datos personales causare perjuicio al ejercitar los derechos de acceso, rectificación, eliminación o anulación, el afectado podrá demandar indemnización. Asimismo, el artículo 44 de la Ley de Control Constitucional señala que las sanciones contempladas en ésta, se impondrán sin perjuicio de las respectivas responsabilidades civiles y penales a que hubiere lugar. En suma, el Constituyente ha establecido una regla de responsabilidad en materia de hábeas data, la cual ha sido seguida por la Ley de Control Constitucional, la que a falta de regulación especial debe regirse por las reglas generales establecidas en el Código Civil [364] . Estas reglas son:

1º)Artículo 1.480.- *"Las obligaciones nacen, (...) ya a consecuencia de un hecho que ha inferido injuria o daño a otra persona, como en los delitos y cuasidelitos"* y,

2º)Artículo 2.241.- *"El que ha cometido un delito o cuasidelito que ha inferido daño a otro, está obligado a la indemnización; sin perjuicio de la pena que le impongan las leyes por el delito o cuasidelito".*

9.3 Responsabilidad Penal

El Código Penal ecuatoriano tipifica al igual que la generalidad de las legislaciones delitos relacionados con los bienes jurídicos vida privada e intimidad, tales como, la violación de domicilio, de correspondencia y violación de secretos [365] . Además de estos delitos, la Ley Nº 67-2002 sobre comercio electrónico incluyó ciertos tipos penales en el Código Penal sin darles una numeración determinada, y la Ley de Instituciones Financieras establece un delito de violación de secreto. A continuación, se señalaran las normas respectivas.

9.3.1) Código Penal

[364] [En línea] < http://www.dlh.lahora.com.ec/paginas/judicial/paginas/CodcivilTP.html > [consulta: 2 de Marzo 2003].

[365] El Código Penal ecuatoriano se encuentra disponible [en línea] < http://www.dlh.lahora.com.ec/paginas/judicial/paginas/Codpenal.2.html#anchor1728504 > [consulta: 2 de Marzo 2003].

a) Violación de domicilio:

Artículo 191.- *"Los empleados del orden administrativo o judicial, los oficiales de justicia o de policía, los comandantes o agentes de la fuerza pública que, obrando como tales, se hubieren introducido en el domicilio de un habitante, contra la voluntad de éste, fuera de los casos previstos y sin las formalidades prescritas por la ley, serán reprimidos con prisión de seis meses a dos años y multa de cuarenta a cien sucres".*

Artículo 192.- *"Será reprimido con prisión de un mes a dos años y multa de cuarenta a ochenta sucres, el que sin orden de la autoridad y fuera de los casos en que la ley permite entrar en el domicilio de los particulares, contra la voluntad de éstos, se hubiere introducido en una casa, departamento, pieza o vivienda, habitada por otro, o sus dependencias cercadas, ya por medio de amenazas o violencias, ya por medio de fractura, escalamiento o ganzúas".*

b) Violación de correspondencia:

Artículo 197.- *"Serán reprimidos con prisión de dos meses a un año y multa de cuarenta a cien sucres, los empleados o agentes del Gobierno y los del servicio de estafetas y telégrafos que hubieren abierto o suprimido cartas confiadas al correo, o partes telegráficos, o que hubieren facilitado su apertura o supresión".*

Artículo 198.- *"Los que, siendo depositarios de partes telegráficos, hubieren revelado su existencia o contenido, a excepción de los casos en que fueren llamados a declarar en juicio y de aquellos en que la ley les obligue a hacer conocer la existencia o contenido de dichos despachos, serán reprimidos con prisión de quince días a seis meses y multa de cuarenta a ochenta sucres".*

Artículo 199.- *"El que hallándose en posesión de una correspondencia no destinada a la publicación, la hiciera publicar, o presentare en juicio sin orden judicial, aunque haya sido dirigida a él, será reprimido con multa de cuarenta a doscientos sucres, si el acto puede causar perjuicio a terceros; a no ser que se trate de correspondencia en que consten obligaciones a favor del tenedor de ella, caso en el que puede presentarse en juicio"*

c) Violación de secretos:

Artículo 200.- *"En la misma pena incurrirá el que, sin ser empleado público, divulgare actuaciones o procedimientos de que haya tenido conocimiento y que, por ley, deben quedar reservados".*

Artículo 201.-*" El que teniendo noticia, por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación puede causar daño, lo revelare sin causa justa, será reprimido con prisión de seis meses a tres años y multa de cincuenta a quinientos sucres".*

Ley de Comercio Electrónico, Firmas y Mensajes de Datos

En lo que se refiere al régimen de sanciones establecido por la Ley de Comercio

Electrónico, cabe señalar que el Título V, denominado "De las Infracciones Informáticas", dispone en el artículo 57 que: *"Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley"*. A continuación se señalaran cuáles son esos delitos que reformaron el Código Penal.

El artículo 58de la Ley de Comercio Electrónicodispone que a continuación del artículo 202 del Código Penal, se incluyan "*los siguientes artículos innumerados*: *Artículo ....- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad , será reprimido con prisión de seis meses a un alío y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica"* (sic)(Art. 58 inciso 1º).

Más adelante, establece una sanción penal para aquella persona o personas encargadas de la custodia o utilización legítima de la información, que cometiendo las acciones descritas en el inciso 1º del artículo 58º, la divulgaren o la utilizaren fraudulentamente, exponiéndolas a la pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica (Art. 58 inciso 4º).

Luego, la Ley, nuevamente tipifica delitos sin señalar una numeración específica para su inclusión en el Código Penal disponiendo textualmente: *"Art. –Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica"* (sic) (Art. 58 inciso 5º).

En la Disposición General "Décima" de la Ley, se señala que: *"Para la fijación de la pena en los delitos tipificados mediante las presentes reformas al Código Penal, contenidas en el Titulo V de esta ley, se tomarán en cuenta los siguientes criterios: el importe de lo defraudado, el quebranto económico causado, los medios empleados y cuantas otras circunstancias existan para valorar la infracción".*

De las disposiciones anteriores cabe comentar que ciertamente ellas se enmarcan dentro de una finalidad protectora de la intimidad y vida privada de las personas, sancionándose duramente la violación a los principios tanto del consentimiento para el tratamiento como para la transmisión de datos. Asimismo, destaca que se castigue la utilización fraudulenta de los datos por quienes están encargados de la custodia de éstos.

9.3.3) Ley General del Sistema de Instituciones Financieras

Finalmente, y en cuanto al régimen de sanciones penales contempladas por la Ley General del Sistema de Instituciones Financieras (secreto bancario), debemos señalar que el artículo 94 prescribe lo siguiente: *"La violación a las disposiciones de este Capítulo será reprimida con uno a cinco años de prisión correccional. Se podrán reclamar a los tribunales de justicia las indemnizaciones que correspondan por los daños que causasen*

las violaciones al sigilo y al carácter de reservado".

10. Conclusiones

Del examen del ordenamiento jurídico ecuatoriano, podemos concluir que, si bien la Constitución reconoce un 'derecho de hábeas data' o derecho a la protección de datos y su correspondiente garantía, ésta no tiene su consecuente desarrollo legal que se plasme en una normativa general de protección a los datos personales. En esta materia existe una Ley de Control Constitucional que regula aspectos procedimentales de la acción constitucional del hábeas data, estableciendo además algunas sanciones administrativas. Con todo, la vigencia de esta ley al amparo de la nueva Constitución ha sido cuestionada en Ecuador tanto por la doctrina como por la jurisprudencia constitucional. Sin embargo, es posible encontrar determinadas normas legales sectoriales referidas a la protección de los datos personales. De éstas, destaca la Ley de Comercio Electrónico, Firma y Mensajes de Datos de 2002 (Ley 67), la cual contempla no sólo normas de protección a los datos personales referidos a las operaciones de mensajería de datos, sino que establece ciertos principios generales para el tratamiento de esos datos personales, los cuales pueden ser de mucha utilidad al momento de solucionar vacíos legales en la materia. Finalmente, no conocemos proyecto legal alguno que pretenda regular de manera general y concordante con la Constitución de 1998 el tema de nuestro estudio.

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN EL SALVADOR

1. Generalidades

El sistema jurídico salvadoreño no dispone de reglas especiales que se refieran a la protección de los datos personales. A nivel constitucional, sólo se ocupa de consagrar entre otros, el derecho a la intimidad y a la vida privada. A su vez, la propia Constitución garantiza el ejercicio de estos derechos a través de la acción de amparo, la cual se encuentra reglamentada por la Ley de Procedimiento Constitucional. En el plano legal, El Salvador solamente dispone de algunas normas sectoriales que tratan aspectos relacionados con la protección de los datos personales en el ámbito del deber de secreto tanto en materia bancaria como impositiva fiscal.

2. Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional [366]

A nivel constitucional podemos señalar que si bien no se encuentra reconocido el

derecho a la autodeterminación informativa, ni tampoco la acción de hábeas data, el Constituyente reconoce diversos derechos que pudieran fundamentar una protección a los datos personales. En este sentido, el inciso 2º del artículo 2 dispone que: *"Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen".* Agrega por su parte el inciso final que: *"Se establece la indemnización, conforme a la ley, por daños de carácter moral".*

Llama la atención que en el inciso 2º del artículo 2, no se haya referido al derecho a la vida privada, sino sólo a la intimidad personal y familiar y, a la propia imagen, pero luego en otro artículo, y a propósito del derecho a la libertad de expresión si lo contemple como límite al ejercicio de éste. La disposición en comento es la del artículo 6 el cual señala que: *"toda persona puede expresar y difundir libremente sus pensamientos siempre que no subvierta el orden público, ni lesione la moral, el honor, ni la vida privada de los demás"*. Lo anterior, podría ser interpretado como que en definitiva, el derecho a la vida privada estaría reconocido implícitamente en la disposición del artículo 2, siempre que entendamos por intimidad un ámbito específico del derecho a la vida privada.

En relación con el inciso 3º del artículo 2, creemos que resulta destacable la consideración constitucional que se tiene respecto del daño moral y su compensación. En este sentido, la fundamentación de esa compensación por daño moral se acercaría a la doctrina que considera el elemento daño, no como 'el precio del dolor', sino más bien como una lesión a un derecho de la personalidad, cuestión que aparece medianamente clara al situar el Constituyente ese reconocimiento a continuación de los derechos de la personalidad.

Más adelante, el artículo 18 reconoce el derecho de petición en los siguientes términos: "*Toda persona tiene derecho a dirigir sus peticiones por escrito, de manera decorosa, a las autoridades legalmente establecidas; a que se le resuelvan, y a que se le haga saber lo resuelto".* Esta disposición podría fundamentar, tanto una petición de hábeas data propio como impropio; este último con el fin de obtener información de público interés relativo a las actividades y gestión de los organismos públicos.

A renglón seguido, el artículo 20 reconoce la inviolabilidad del domicilio y prescribe que su violación genera responsabilidad. Al efecto se dispone: *"La morada es inviolable y sólo podrá ingresarse a ella por consentimiento de la persona que la habita, por mandato judicial, por flagrante delito o peligro inminente de su perpetración, o por grave riesgo de las personas".* El inciso 2º agrega que la violación de este derecho *"dará lugar a reclamar indemnización por los daños y perjuicios ocasionados".*

Por su parte, el artículo 24 reconoce la inviolabilidad del domicilio en los siguientes términos: *"La correspondencia de toda clase es inviolable, interceptada no hará fe ni podrá figurar en ninguna actuación, salvo en los casos de concurso y quiebra. Se prohíbe la interferencia y la intervención de las comunicaciones telefónicas"*.

Más adelante, en el Título IX, denominado "*Alcances, Aplicación, Reformas y Derogatorias"*, establece el artículo 246 que: *"Los principios, derechos y obligaciones*

366 La Constitución Política salvadoreña puede consultarse [en línea] <

http://www.georgetown.edu/pdba/Constitutions/ElSal/ElSal83.html > [consulta: 6 de Noviembre 2002].

establecidos por esta Constitución no pueden ser alterados por las leyes que regulen su ejercicio". Añade el inciso 2º que: *"La Constitución prevalecerá sobre todas las leyes y reglamentos. El interés público tiene primacía sobre el interés privado".*

Finalmente, cabe hacer presente que, a renglón seguido, el inciso 1º del artículo 247 consagra la acción de amparo en los siguientes términos: *"Toda persona puede pedir amparo ante la Sala de lo Constitucional de la Corte Suprema de Justicia por violación de los derechos que otorga la presente Constitución".* Esta disposición es de trascendental importancia, pues consagra la efectiva tutela de los derechos constitucionales. Por lo tanto, a falta de una acción de hábeas data, entendemos que debería recurrirse a la acción de amparo para solicitar la tutela del máximo tribunal de justicia salvadoreño ante acciones u omisiones que como consecuencia de un tratamiento de datos personales vulneren los derechos de las personas, sea la intimidad, sea la vida privada e incluso el honor. La competencia de la Corte Suprema en esta materia está a su vez confirmada por el artículo 174 el cual dispone: *"La Corte Suprema de Justicia tendrá una Sala de lo Constitucional, a la cual corresponderá conocer y resolver las demandas de inconstitucionalidad de las leyes, decretos y reglamentos, los procesos de amparo, el habeas corpus, las controversias entre el Órgano Legislativo y el Órgano Ejecutivo".*

En suma, la Constitución de El Salvador, no contempla normas que se refieran expresamente a la protección de los datos personales, sólo dispone el reconocimiento de los derechos a la intimidad personal y familiar, al honor, la propia imagen y, a la vida privada, como límite al ejercicio de la libertad de expresión. Por otra parte también reconoce la inviolabilidad del domicilio y de las comunicaciones. En base a esas disposiciones, creemos que es posible fundamentar una protección de datos personales, especialmente a través de la acción de amparo, no regulada por el Constituyente de 1983.

2.2 Protección Legal de los Datos Personales

En el ámbito legal de protección a los datos personales, no tenemos conocimiento de ley alguna que se ocupe de esta materia. A pesar de lo anterior, El Salvador cuenta con algunas normas sectoriales que protegen el secreto bancario, establecen un sistema de información de crédito de los usuarios de sistema financiero y otras relativas a la reserva de información tributaria. A continuación revisaremos esas disposiciones legales.

2.2.1) Ley de Bancos [367]

La Ley de Bancos salvadoreña señala en el artículo 61, insertado dentro del título "Sistema de Información", lo siguiente: *"La Superintendencia mantendrá un servicio de información de crédito sobre los usuarios de las instituciones integrantes del sistema financiero, con el objeto de facilitar a las mismas la evaluación de riesgos de sus operaciones, el cual podrá ser delegado en una entidad privada. (…) Los bancos y demás instituciones que fiscalice la Superintendencia, estarán obligados a proporcionar la información que requiera la misma".*

[367] **Decreto Nº 697, [en línea] < http://www.ssf.gob.sv/frm_marco/frm_marco.htm > [consulta: 4 de Marzo 2003].**

En este caso, es el propio órgano administrativo el encargado de prestar la información de crédito sobre los usuarios, en base a la propia información entregada a su vez por las instituciones financieras. El objetivo específico de este sistema es la evaluación de riesgos de las operaciones que lleven a cabo los bancos. En cuanto a la facultad de delegar al sector privado el señalado servicio, y si ésta se ha ejercido o no, no es posible pronunciarnos pues no tenemos mayor información al respecto. Con todo, estimamos que en ese caso debiera contemplarse una regulación muy precisa dada la cantidad y calidad de la información manejada.

Más adelante, en el artículo 232 esta Ley consagra el secreto bancario, disponiendo que: *"Los depósitos y captaciones que reciben los bancos están sujetos a secreto y podrá proporcionarse informaciones sobre esas operaciones sólo a su titular o a la persona que lo represente legalmente".* Se agrega por la Ley que: *"Las demás operaciones quedan sujetas a reserva y sólo podrán darse a conocer a las autoridades a que se refiere el Artículo 201 de esta Ley y a quien demuestre un interés legítimo, previa autorización de la Superintendencia"* (Art. 232 inc. 2º). El inciso 3º por su parte aclara que tanto el deber de secreto como la reserva: *"(…) es sin perjuicio de la información que debe solicitar la Superintendencia para cumplir con lo dispuesto en el Artículo 61 de esta Ley y con la información detallada que debe dar a conocer al público en virtud del literal f) del Artículo 21 de su Ley Orgánica".* Finalmente se señala que el secreto bancario no será obstáculo para esclarecer delitos, ni para impedir el embargo sobre bienes (Art. 232 inc. final).

Cabe comentar de este artículo que, en general, se parece mucho a la disposición del artículo 154 de la Ley General de Bancos chilena, la cual establece el secreto bancario sólo respecto de los depósitos y captaciones (operaciones pasivas), y respecto de las demás operaciones, prescribe que ellas quedarán sujetas al deber de reserva. Respecto de esta última, la disposición salvadoreña es más precisa y resguarda mejor los derechos de los titulares de los datos, dado que para el otorgamiento de esa clase de información a un tercero quedemuestre un interés legítimo, debe contarse previamente con la autorización de la Superintendencia.

Por otra parte, las excepciones tanto al deber de secreto como a la reserva señaladas en el inciso 3º del artículo 232, son concordantes con las funciones asignadas al Servicio de Información de Crédito establecido en el artículo 61 de la Ley. Finalmente, y en lo relativo al régimen de excepciones al deber de secreto bancario, éste cede en pos de la justicia tanto penal como civil, lo cual aparece como regla de excepción uniforme en las demás legislaciones. Las sanciones administrativas por la violación a estas disposiciones se verán más adelante en el punto Nº 9.1

2.2.2) Código Tributario [368]

El Código Tributario salvadoreño consagra la denominada reserva tributaria en el extenso artículo 28 titulado "Reserva de la información". Éste dispone lo siguiente:

Artículo 28.-*"La información respecto de las bases gravables y la determinación de*

[368] ***Decreto Nº 230 de 14 de diciembre de 2000, [en línea] < http://www.ciat.org/doc/docu/leg/cod/lal_elsal_02_codigo_tributario.doc > [consulta: 4 de Marzo 2003].***

los impuestos que figuren en las declaraciones tributarias y en los demás documentos en poder de la Administración Tributaria, tendrá el carácter de información reservada. Por consiguiente, los empleados y funcionarios que por razón del ejercicio de sus cargos tengan conocimiento de la misma, sólo podrán utilizar para el control, recaudación, determinación, emisión de traslados, devolución y administración de los tributos, y para efectos de informaciones estadísticas impersonales, sin perjuicio de las sanciones penales a que hubiere lugar" [369] .

De las disposiciones anteriores queda claro que el deber de reserva compete tanto a los funcionarios de la Administración Tributaria, como aquellos terceros u otros funcionarios que tuvieren acceso a los datos o informaciones en virtud de disposiciones generales, con lo que se amplían los sujetos pasivos del deber de confidencialidad en esta materia. Destaca de la normativa en comento la limitación del uso de la información tributaria a las finalidades propias de la Administración Tributaria, como lo son, el control, recaudación, determinación, emisión de traslados, devolución y administración de los tributos, así como también para efectos de informaciones estadísticas impersonales (Art. 28 inc. 1º).

3. Bienes Jurídicos Protegidos por la Legislación de Datos Personales

Dada la inexistencia de una ley de protección de datos personales, no podremos desarrollar este punto. A pesar de ello, cabe recordar que la configuración constitucional adoptada en el ordenamiento jurídico salvadoreño permitiría fundamentar una protección de éstos en base al derecho a la vida privada, intimidad e incluso el honor (Artículos 2 y 6 C. Pol.).

4. Principios Informativos de la Legislación de Protección de Datos Personales

Por la misma razón señalada en el punto anterior, no podremos detenernos a analizar

[369] Se agrega por la disposición que: "No obstante lo anterior, la Administración Tributaria podrá proporcionar a las instituciones que desempeñen funciones que constituyan un servicio público, el número de identificación tributaria de sus administrados, que le requieran en cumplimiento de sus atribuciones. La restricción contenida en esta disposición legal no inhibe a la Administración Tributaria de publicar los nombres de contribuyentes deudores, de conformidad a lo establecido en el artículo 277 de este Código. (…) Aquellas personas o entidades que, sin pertenecer a la Administración Tributaria, en cumplimiento de disposiciones especiales tuvieren acceso a los datos o informaciones a que se hace referencia, deberán guardar absoluta reserva y sólo podrán utilizarlos para efectos del cumplimiento de sus obligaciones. La contravención a la obligación establecida en este artículo, será sancionada de conformidad con las disposiciones legales o contractuales que resulten aplicables. (…) Las declaraciones tributarias sólo podrán ser examinadas por el propio sujeto pasivo, o a través de cualquier persona debidamente autorizada al efecto por aquél, en la Administración Tributaria y en las dependencias de la misma. (…) La reserva de información dispuesta en este artículo no le es aplicable a la Fiscalía General de la República y a los jueces, respecto de aquellos casos que estén conociendo judicialmente a quienes la Administración Tributaria deberá proporcionar la información que requieran en el cumplimiento de las atribuciones que les corresponden en la investigación de los delitos y en defensa de los intereses fiscales" (Art. 28 incisos 2º, 3º,4º y 5º).

este punto.

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

En atención a la inexistencia de una ley general de protección de datos personales en el ordenamiento jurídico de El Salvador, no desarrollaremos esta materia.

6. Modelos de Tutela

El ordenamiento jurídico salvadoreño no dispone de mecanismos específicos que tutelen los derechos de las personas ante el tratamiento de sus datos personales. Dado lo anterior, estimamos que para suplir esa falta de protección debería recurrirse a la acción de amparo de los derechos constitucionales, consagrada en el artículo 247 de la Constitución salvadoreña y regulada por la Ley de Procedimientos Constitucionales.

6.1 La acción de Amparo

El artículo 247 de la Constitución -como se recordará- dispone que: *"toda persona puede pedir amparo ante la Sala de lo Constitucional de la Corte Suprema de Justicia por violación de los derechos que otorga la presente Constitución".* A efectos de hacer aplicable esta disposición, se dicta la Ley de Procedimientos Constitucionales (en adelante LPC) [370] , la cual tiene por objeto regular las acciones de inconstitucionalidad, de hábeas corpus y de amparo de los derechos consagrados constitucionalmente. Por lo tanto, a falta de norma especial la acción de amparo sería el medio jurídico idóneo para obtener la tutela a los datos personales, en base a los derechos a la intimidad, vida privada e incluso honor. Con todo, cabe señalar una importante limitación, cual es que la acción de amparo regulada por la LPC sólo contempla como sujetos pasivos de ésta a los funcionarios del Estado, sin mencionar a los particulares.

6.1.1) Procedencia de la acción

La acción de amparo procede en contra de toda clase de acciones u omisiones de cualquier autoridad, funcionario del Estado o de sus órganos descentralizados y de las sentencias definitivas pronunciadas por la Sala de lo Contencioso Administrativo que violen los derechos consagrados en la Constitución u obstaculicen su ejercicio (Art. 12 LPC) [371] . Asimismo, la acción de amparo *"únicamente podrá incoarse cuando el acto contra el que se reclama no puede subsanarse dentro del respectivo procedimiento mediante otros recursos"*.

Por lo tanto, queda claro que la acción es procedente ante acciones u omisiones por parte de cualquier autoridad del Estado que viole los derechos constitucionales, debiendo

370 Esta ley puede ser consultada [en línea] < http://www.uc3m.es/uc3m/inst/MGP/JCI/02-elsalvador-leydeprocedimientosconstitucionalesl.htm > [consulta: 15 de Marzo 2003].

previamente agotarse la vía administrativa.

6.1.2) Legitimación Activa

El artículo 3º y 12º de la LPC señalan que toda persona puede pedir amparo ante la Sala de lo Constitucional de la Corte Suprema de Justicia, por violación de los derechos que le otorga la Constitución. Por lo tanto, no existiría restricción respecto del sujeto activo.

6.1.3) Legitimación Pasiva

El artículo 16º de la LPC dispone al respecto que: *"son partes en el juicio de amparo: (…) 2. La autoridad contra quien se interpone la demanda".* Por consiguiente, la acción deberá dirigirse en contra de la autoridad pública que viole los derechos consagrados en la Constitución u obstaculice su ejercicio.

6.1.4) Competencia

Es competente para conocer de la acción de amparo, la Sala Constitucional de la Corte Suprema de Justicia (Artículos 3 y 12 LPC).

6.1.5) Procedimiento Aplicable

La tramitación de la acción de amparo puede sintetizarse de la siguiente forma:

1)*Demanda*: el artículo 14 de la LPC señala que la demanda de amparo podrá presentarse por la persona agraviada, por sí o por su representante legal o su mandatario, por escrito y deberá expresar: *"1)- El nombre, edad, profesión u oficio y domicilio del demandante y, en su caso, los de quién gestiona por él. Si el demandante fuere una persona jurídica, además de las referencias personales del apoderado, se expresará el nombre, naturaleza y domicilio de la entidad; 2)- La autoridad o funcionario demandado; 3)- El acto contra el que se reclama; 4)- El derecho protegido por la Constitución que se considere violado u obstaculizado en su ejercicio; 5)- Relación de las acciones u omisiones en que consiste la violación; 6)- Las referencias personales del tercero a quien benefició el acto reclamado, caso de que lo haya; y, 7)- El lugar y fecha del escrito y firma del demandante o de quien lo hiciere a su ruego".* Luego añade en el artículo 15 que iniciado el amparo, no será necesaria la solicitud de las partes para su continuación, debiendo el Tribunal pronunciar de oficio todas las resoluciones hasta la sentencia.

[371] El articulo 12 señala que: *"Toda persona puede pedir amparo ante la Sala de lo Constitucional de la Corte Suprema de Justicia, por violación de los derechos que le otorga la Constitución. (…) La acción de amparo procede contra toda clase de acciones u omisiones de cualquier autoridad, funcionario del Estado o de sus órganos descentralizados y de las sentencias definitivas pronunciadas por la Sala de lo Contencioso Administrativo que violen aquellos derechos u obstaculicen su ejercicio. Cuando el agraviado fuere el Estado, la Sala de lo Constitucional tendrá obligación de mandar a suspender el acto reclamado. (…) La acción de amparo únicamente podrá incoarse cuando el acto contra el que se reclama no puede subsanarse dentro del respectivo procedimiento mediante otros recursos. (…) Si el amparo solicitado se fundare en detención ilegal o restricción de la libertad personal de un modo indebido, se observará lo que dispone el Título IV de la presente ley".*

2)*Suspensión del acto reclamado*: el artículo 19 de la LPC dispone que al admitir la demanda, la Sala en el mismo auto *"resolverá sobre la suspensión del acto contra el que se reclama, aún cuando el peticionario no la hubiere solicitado"*, agregando que para estos efectos será procedente ordenar la suspensión provisional inmediata del acto reclamado cuando su ejecución pueda producir un daño irreparable o de difícil reparación por la sentencia definitiva(Art. 20). De lo anterior, se entiende claramente que se está frente a medidas cautelares que evitan el *periculum in mora.* Cabe agregar en esta materia que la Ley señala que en todo caso, la suspensión sólo procede respecto de actos que produzcan o puedan producir efectos positivos (Art. 19 LPC).

3)*Informe*: la LPC dispone que ordenada o no la suspensión provisional inmediata, *"se pedirá informe a la autoridad o funcionario demandado, quien deberá rendirlo dentro de veinticuatro horas"* (Art. 21).

4)*Audiencia al Fiscal*: el artículo 23 señala que recibido el informe o transcurrido el plazo sin que el demandado lo rindiere, se mandará oír en la siguiente audiencia al Fiscal de la Corte.

5)*Término probatorio*: el artículo 29 dispone que concluidos los términos de los traslados y audiencia en su caso, se abrirá el juicio a pruebas por ocho días, si fuera necesario.

6.1.6) La Sentencia

El artículo 32 prescribe que devueltos los traslados y transcurrida la audiencia ya señalada, se pronunciará la sentencia. En ésta, *"se relacionarán los hechos y cuestiones jurídicas que se controviertan, dando las razones y fundamentos legales que se estimen procedentes y citando las leyes y dictámenes que se consideren aplicables. La Sala podrá omitir la relación de la prueba y los alegatos de las partes, pero hará la apreciación jurídica de la prueba en caso necesario"* (Art. 33). Añade el artículo 35 que: *"en la sentencia que concede el amparo, se ordenará a la autoridad demandada que las cosas vuelvan al estado en que se encontraban antes del acto reclamado*. *Si éste se hubiere ejecutado en todo o en parte, de un modo irremediable, habrá lugar a la acción civil de indemnización por daños y perjuicios contra el responsable personalmente y en forma subsidiaria contra el Estado".* El inciso 2º de este artículo, agrega que cuando el amparo sea procedente porque un funcionario o autoridad ha obstaculizado en cualquier forma con sus actos, dilaciones u omisiones el ejercicio de un derecho que otorga la Constitución, *"la sentencia determinará la actuación que deberá seguir la autoridad o el funcionario responsable, quien estará obligado a dictar sus providencias en el sentido indicado, y si no lo hace dentro del plazo que se le señale, incurrirá en el delito de desobediencia y el Tribunal lo mandará procesar".*

Por otro lado, la LPC señala que la sentencia contendrá además, *"la condena en las costas, daños y perjuicios del funcionario que en su informe hubiere negado la existencia del acto reclamado, o hubiese omitido dicho informe o falseado los hechos en el mismo. Esta parte de la sentencia se ejecutará conforme al procedimiento común".* Si la sentencia deniega el amparo, *"se condenará en las costas, daños y perjuicios al demandante; también se condenará en costas, daños y perjuicios al tercero que*

sucumbiere en sus pretensiones" (Art. 35 incisos 3º y 4º).

En cuanto a los efectos la sentencia de amparo, el artículo 81, ubicado dentro de las "Disposiciones generales" de la LPC, señala que la sentencia definitiva de amparo produce los efectos de cosa juzgada contra toda persona o funcionario, haya o no intervenido en el proceso, sólo en cuanto a que el acto reclamado es o no *"violatorio de preceptos constitucionales. Con todo, el contenido de la sentencia no constituye en sí declaración, reconocimiento o constitución de derechos privados subjetivos de los particulares o del Estado; en consecuencia la resolución dictada no puede oponerse como excepción de cosa juzgada a ninguna acción que se ventile posteriormente ante los Tribunales de la República"*. De lo anterior, se deduce que la sentencia de amparo tiene efecto de cosa juzgada material sólo en cuanto a la declaración de que un acto viola o no la constitución, pero en cuanto al reconocimiento, declaración o constitución de derechos subjetivos de los particulares o del Estado, sólo tiene efecto de cosa juzgada formal, por lo que podrá discutirse ante los tribunales ordinarios en un proceso diverso toda las cuestiones ya señaladas.

6.2 Otras Acciones

Al respecto no se observan otras de acciones que puedan ser idóneas para tutelar los datos personales en El Salvador.

7. Mecanismos de Control

En el Salvador, no se aprecian mecanismos de control a la protección de datos personales, más aún si no existe una ley general en la materia.

8. Transmisión Internacional de Datos

En lo referente a la regulación de la transmisión internacional de datos personales, tampoco podemos pronunciarnos pues no se observa legislación al respecto.

9. Régimen de Responsabilidad

En materia de responsabilidad y, a falta de normas especiales, sólo nos referiremos a algunas disposiciones sectoriales y generales que hemos podido constatar a este respecto. A continuación se enunciarán las diversas clases de sanciones que el ordenamiento jurídico salvadoreño contempla para casos específicos relacionados con la afectación de bienes jurídicos como la intimidad y la vida privada.

9.1 Responsabilidad Administrativa

En esta materia, y a falta de normas especiales, entendemos que debería recurrirse a las reglas generales que establecen la responsabilidad administrativa de los funcionarios del Estado, cuando por un acto u omisión de éstos se causa daño a los particulares.

Lamentablemente, en este ámbito no disponemos de la información legal particular.

De los estatutos sectoriales, podemos mencionar a la Ley Orgánica de la Superintendencia del Sistema Financiero de El Salvador [372] . Este cuerpo legal dispone en el artículo 37 que: *"Las entidades sujetas a la fiscalización de la Superintendencia que incurran en infracciones a las Leyes, Reglamentos, Estatutos y demás normas que las rijan o les sean aplicables o en el incumplimiento de las instrucciones u órdenes que les imparta aquella dentro de sus facultades legales, estarán sujetas a la imposición de multas hasta del dos por ciento sobre el capital y reservas de capital sin perjuicio de las sanciones establecidas específicamente en otros cuerpos legales o reglamentarios".*

9.2 Responsabilidad Civil

En materia de responsabilidad civil, a falta de normas especiales entendemos que deberían aplicarse las reglas generales. En el caso de la responsabilidad civil extracontractual, cabría aplicar las normas del Título XXV, "De los delitos y cuasidelitos" del Código Civil, en especial los artículos 2.067 y 2.080 los cuales señalan respectivamente que: *"Es obligado a la indemnización el que hizo el daño (...)"* y, que: *"Por regla general todo daño que pueda imputarse a malicia o negligencia de otra persona, debe ser reparado por ésta"* [373] . Según la propia jurisprudencia salvadoreña "el Código no distingue a qué clase de daño se refiere y donde la ley no distingue no puede distinguir el intérprete; y en la segunda, de carácter más general, señala 'todo daño', expresión que no puede ser más amplia y por lo tanto, una decisión que diera lugar al resarcimiento por daño moral perfectamente puede asimilarse en el mencionado Título" [374] . De lo anterior deducimos también que es procedente la compensación de los daños morales causados. Por otra parte, si el daño tiene por antecedente un contrato, deberán aplicarse las reglas generales de la responsabilidad contractual.

9.3 Responsabilidad Penal

El Código Penal salvadoreño [375] contempla diversos delitos que protegen tanto la intimidad como la vida privada, los cuales de señalan a continuación.

a) Allanamiento sin autorización legal:

El artículo 300 dispone que: "*El funcionario o empleado público, agente de autoridad o autoridad pública que ingresare a morada ajena, sin el consentimiento del morador o de quien haga sus veces, no estando legalmente autorizado o lo ordenare o permitiere, será*

[372] Decreto Nº 628. [En línea] < http://www.ssf.gob.sv/frm_marco/frm_marco.htm > [consulta: 15 de Marzo 2003].

[373] Estas normas legales las tomamos como cita de jurisprudencia salvadoreña. [En línea] < http://www.csj.gob.sv/bar_infe.htm > [consulta: 15 de Marzo 2003].

[374] *Ídem*.

[375] [En línea] < http://www.unifr.ch/derechopenal/legislacion/sv/cp_elsalvador15.htm > [consulta: 4 de Marzo 2003].

sancionado con prisión de uno a tres años e inhabilitación especial para el ejercicio del cargo o empleo respectivo por el mismo tiempo".

b) Inviolabilidad de la correspondencia *:*

El artículo 301 por su parte señala que: *"El funcionario o empleado público, agente de autoridad o autoridad pública que fuere de los casos previstos por la Constitución de la República y en el transcurso de una investigación policial o judicial, violare correspondencia privada, o lo ordenare o permitiere, será sancionado con prisión de uno a tres años e inhabilitación especial para el ejercicio del cargo o empleo respectivo por igual tiempo"*.

c) Violación de comunicaciones privadas:

Dentro de los delitos establecidos por el Código Penal salvadoreño los artículos 184 y 185 sin duda que muestran un acercamiento a lo menos indirecto a la protección d los datos personales. En efecto, el artículo 184 dispone: *"El que con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apoderare de comunicación escrita, soporte informático o cualquier otro documento o efecto personal que no le esté dirigido o se apodere de datos reservados de carácter personal o familiar de otro, registrados en ficheros, soportes informáticos o de cualquier otro tipo de archivo o registro público o privado, será sancionado con multa de cincuenta a cien días multa.(…) Si difundiere o revelare a terceros los datos reservados que hubieren sido descubiertos, a que se refiere el inciso anterior, la sanción será de cien a doscientos días multa. (…) El tercero a quien se revelare el secreto y lo divulgare a sabiendas de su ilícito origen, será sancionado con multa de treinta a cincuenta días multa".*

A continuación, el artículo 185 dispone que: *"Si los hechos descritos en el artículo anterior se realizaren por las personas encargadas o responsables de los ficheros, soportes informáticos, archivos o registros, se impondrá, además de la pena de multa, inhabilitación del respectivo cargo o empleo público de seis meses a dos años"*. En estos casos, si la obtención ilícita y posterior divulgación de datos personales es realizada por los encargados o responsables de los ficheros, soportes informáticos, archivos o registros, la pena se agrava.

Los dos artículos recién señalados, sin duda contemplan una protección al derecho a la intimidad y la vida privada, la cual puede ser puesta en peligro o lesionada a través de las acciones descritas por las normas. Entendemos que en estos casos, indirectamente se protegerían los datos personales en el caso que éstos se obtengan de manera ilícita. Si ellos se divulgaren la pena se aumenta. Además se sanciona al tercero receptor de la divulgación se datos personales obtenidos ilícitamente.

d) Captación de comunicaciones:

Luego, el artículo 186 preceptúa: *"El que con el fin de vulnerar la intimidad de otro, interceptare, impidiere o interrumpiere una comunicación telegráfica o telefónica o utilizare instrumentos o artificios técnicos de escucha, transmisión o grabación del sonido, la imagen o de cualquier otra señal de comunicación, será sancionado con prisión de seis*

meses a un año y multa de cincuenta a cien días multa.(…) Si difundiere o revelare a terceros los datos reservados que hubieren sido descubiertos, a que se refiere el inciso anterior, la sanción será de prisión de seis meses a un año y multa de cien a ciento cincuenta días multa. (…) El tercero a quien se revelare el secreto y lo divulgare, a sabiendas de su ilícito origen, será sancionado con multa de treinta a cincuenta días multa".

En este caso, podría considerarse a los datos reservados como un género de datos que vulneren la intimidad y, a algunos datos personales, como una especie de éstos, por ejemplo, a los datos sensibles. La disposición anterior tutelaría indirectamente los datos personales y directamente el derecho a la intimidad de su titular.

e) Revelación de secreto profesional:

En materia de revelación de secretos, el artículo 187 dispone: *"El que revelare un secreto del que se ha impuesto en razón de su profesión u oficio, será sancionado con prisión de seis meses a dos años e inhabilitación especial de profesión u oficio de uno a dos años.*

f) Allanamiento de morada:

En materia de violación de domicilio el artículo 188 consigna lo siguiente: *"El particular que, sin habitar en ella, se introdujere en morada ajena o en sus dependencias, sin el consentimiento de quien la habitare, de manera clandestina o con engaño o permaneciere en la misma contra la voluntad del morador, pese a la intimación para que la abandonare, será sancionado con prisión de seis meses a dos años y multa de treinta a cincuenta días multa. (…) Si la introducción o permanencia se hiciere con violencia en las personas, la sanción será de uno a tres años de prisión y multa de cincuenta a cien días multa"*.

g) Allanamiento de lugar de trabajo o establecimiento abierto al público:

Por su parte el artículo 189 dispone : *"El que ingresare o se mantuviere contra la voluntad de su titular en el lugar reservado de trabajo de una persona o en establecimiento o local abierto al público fuera de las horas de apertura, será sancionado con prisión de seis meses a dos años y multa de treinta a cincuenta días multa".*

De lo señalado en los artículos recién transcritos, se desprende que el legislador penal salvadoreño ha tomado en cuenta diversos bienes jurídicos tales como la intimidad y la vida privada. No se divisa que pudiera referirse directamente a la protección del derecho a la autodeterminación informativa o derecho a la protección de datos, aunque reconocemos que lo señalado por los artículos 184 y 185 pudiera generar alguna duda al respecto.

10. Conclusiones

Como se pudo constatar, el ordenamiento jurídico salvadoreño no contempla norma expresa constitucional referida a la protección de los datos personales. En este nivel, lo

más próximo a la materia es el reconocimiento de los derechos a la intimidad personal y familiar, el derecho a la propia imagen, al honor a al vida privada. En el plano infraconstitucional, tampoco se dispone de una ley especial en la materia. Sólo existen en ese país, normas aisladas y sectoriales que se ocupan de ámbitos relacionados con deberes de secreto de cierta información. Con todo, estimamos que esa falta de previsión normativa no es obstáculo para la tutela de los derechos de las personas afectados por el tratamiento de sus datos personales. La vía más efectiva al efecto, sería la acción de amparo constitucional la cual es conocida y resuelta por la Corte Suprema de Justicia de El Salvador.

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN GUATEMALA

1. Generalidades

El sistema jurídico guatemalteco de protección de los datos personales es precario. Si bien cuenta con una disposición constitucional que consagra el derecho de acceso, corrección, rectificación y actualización de los datos personales, éste sólo se puede ejercer respecto de organismos del Estado y, eventualmente en contra de algunas entidades de carácter privado, si se aplican extensivamente las normas sobre la acción de amparo. En el ámbito legal, Guatemala no cuenta con una ley de protección de datos personales. Sólo dispone de normas sectoriales relacionadas con la protección a los datos de las personas, que en general están presentes en los ordenamientos jurídicos latinoamericanos, como lo son: el secreto bancario y el secreto fiscal. Cabe señalar por último, que en la actualidad se discute por el Poder Legislativo un Proyecto de Ley de acceso a la información.

2. Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional

En el ordenamiento jurídico guatemalteco se contemplan a nivel constitucional diversas disposiciones relacionadas con la protección de los datos personales. Ciertamente la más importante de éstas es la contemplada en el artículo 31, la cual reconoce el derecho de todas las personas para acceder, corregir, rectificar y actualizar los datos personales que de ellas conste en fichas o registros estatales disponiendo al efecto lo siguiente:

Artículo 31. *"Acceso a archivos y registros estatales. Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación*

política, excepto los propios de las autoridades electorales y de los partidos políticos" [376] .

De la disposición anterior, se desprende la consagración de un derecho de control sobre la propia información en manos del Estado, pero sin especificar la acción específica de su tutela. Tampoco es clara la consideración del o los bienes jurídicos tutelados, pues al igual que en la Constitución ecuatoriana y colombiana pareciera que estuviera reconociendo un 'derecho de hábeas data', pero en este caso de carácter limitado, pues sólo podría hacerse valer en contra de los responsables de los archivos, fichas o cualquier otra forma de registro de carácter estatal. Conjuntamente con la disposición anterior, se señala como regla general la prohibición de los registros y archivos de filiación política, salvo los pertenecientes a las autoridades electorales y los de los propios partidos políticos. Es decir, se establece expresamente una prohibición de creación y tratamiento de una especie particular de datos sensibles.

Llama la atención la opción del Constituyente de dejar fuera de la protección a los datos personales en manos de sujetos de derecho privado o particulares. A falta de antecedentes fidedignos sobre el establecimiento de la disposición del artículo 31, no podemos analizar las motivaciones del Constituyente. A pesar de ello, intuímos que esa opción normativa guardaría estrecha relación con sucesos históricos relacionados con el débil respeto a los derechos humanos por parte del Estado guatemalteco a lo largo de los últimos cuarenta años. Al respecto, se ha señalado que en la actualidad la organización política del Estado si bien es de orden democrático, aún no ha podido consolidarse como un verdadero estado de derecho [377] . Por lo tanto, creemos que sólo se previó por el Constituyente el peligro para los derechos de las personas derivados del uso y abuso sin control alguno, de parte del Estado y de sus organismos de los datos personales recolectados y tratados por éste, en particular los datos relacionados con la filiación política de los ciudadanos guatemaltecos, pues en ese ámbito se experimentó, entre otros, el abuso de poder y violaciones a los derechos de las personas.

Por otra parte, la Constitución dispone en el artículo 22 que: *"los antecedentes penales y policiales no son causa para que a las personas se les restrinja en el ejercicio de sus derechos que esta Constitución y las leyes de la República les garantiza, salvo cuando se limiten por ley, o en sentencia firme, y por el plazo fijado en la misma".*

La disposición anterior puede parecernos una perogrullada si la analizamos desde nuestra perspectiva jurídica nacional. En verdad, pareciera ser que no es suficiente que la sola ley se encargue de fijar los efectos que puedan tener las condenas penales o

376 [En línea] < http://www.georgetown.edu/pdba/Constitutions/Guate/reforms99.html > [consulta: 17 de Enero 2003].

377 Al respecto se ha dicho por una autora que "Después de 36 años de guerra civil en Guatemala, hoy día los ciudadanos siguen todavía luchando por derechos humanos básicos. Los derechos que están prometidos en la constitución del país y de todo el mundo, derechos de libertad, vida, justicia e igualdad, son solamente sueños para esta población que sufre de injusticia, racismo, y pobreza. La población Guatemalteca se está muriendo de hambre. Es una población con pocas esperanzas. En Guatemala, hay un dicho amargo circulando: "Cuidado con la paz, porque, ahora, el gobierno está luchando contra todos." Guatemala ha sobrellevado los abusos humanos más inimaginables en nuestra historia moderna. Y hoy, aunque no está en guerra, Guatemala sigue luchando". En *"La protección de los derechos humanos en Guatemala"*, Rodríguez Reichberg, Tamara. [En línea] < http://hcs.harvard.edu/~haciadem/summit/bulletins/Reichberg-CdG-Bulletin.pdf > [consulta: 16 de Marzo 2003].

infraccionales en un país como Guatemala. En nuestra opinión, lo preceptuado por la norma refleja claramente una intención de evitar el abuso y la discriminación, ciertamente vivida quizá por cuanto tiempo por los habitantes de ese país.

A renglón seguido, la Constitución reconoce en el artículo 23 la inviolabilidad de la vivienda, señalando al respecto que: *"la vivienda es inviolable. Nadie podrá penetrar en morada ajena sin permiso de quien la habita, salvo por orden escrita de juez competente en la que se especifique el motivo de la diligencia y nunca antes de las seis ni después de las dieciocho horas, Tal diligencia se realizará siempre en presencia del interesado, o de su mandatario".*

El artículo 24 por su parte, reconoce en el inciso 1º la inviolabilidad de la correspondencia y documentos privados, señalando que: *"la correspondencia de toda persona, sus documentos y libros son inviolables. Sólo podrán revisarse o incautarse, en virtud de resolución firme dictada por juez competente y con las formalidades legales".* Asimismo se reconoce la inviolabilidad de las comunicaciones en los siguientes términos: *"Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna".* Dada la amplitud de lo recién señalado, estaría cubierta toda comunicación privada, independiente del medio a través del cual pueda llegar a establecerse esa comunicación.

A su vez, el inciso 2º del artículo 24 eleva a rango constitucional el deber de secreto fiscal o tributario, situación del todo inusual en este nivel normativo. Se señala al respecto que: "*Los libros, documentos y archivos que se relacionan con el pago de impuestos, tasa, arbitrios y contribuciones, podrán ser revisados por la autoridad competente de conformidad con la ley. Es punible revelar el monto de los impuestos pagados, utilidades, pérdidas, costos y cualquier otro dato referente a las contabilidades revisadas a personas individuales o jurídicas, con excepción de los balances generales, cuya publicación ordene la ley".*

De lo anterior, se deduce la importancia asignada por el Constituyente a la protección de los datos personales relacionados con los deberes impositivos, señalando que constituirá delito la revelación de los datos referentes a los estados financieros de las personas naturales y jurídicas a excepción de los balances generales. Con todo, la tipificación de estos delitos queda entregada a la ley.

Cabe destacar además del artículo 24, la regla probatoria que establece en su último inciso y que dispone: *"Los documentos o informaciones obtenidas con violación de este artículo no producen fe ni hacen prueba en juicio".* Por lo tanto, además de la sanción propia por la violación a las normas ya señaladas, se establece el carácter de prueba ilegal, y por lo tanto inadmisible, de aquélla obtenida con infracción a lo dispuesto en el artículo 24.

A su turno, el artículo 25 dispone que el registro de las personas y de los vehículos, sólo podrá efectuarse por elementos de las fuerzas de seguridad cuando se establezca causa justificada para ello. Para ese efecto, los elementos de las fuerzas de seguridad deberán presentarse debidamente uniformados y pertenecer al mismo sexo de los requisados, *"debiendo guardarse el respeto a la dignidad, intimidad y decoro de las personas".* Hacemos referencia a este artículo, dado que es la única disposición respecto

de la cual el Constituyente guatemalteco hace alusión al derecho a la intimidad de las personas. A pesar de lo anterior, estimamos que si bien no se contempla explícitamente a la intimidad como derecho fundamental, sí aparece configurada como límite al ejercicio de los derechos de registro de las personas y los vehículos por los funcionarios de seguridad competentes. Al estar limitado tal facultad por el derecho a la intimidad, se manifiesta en toda su magnitud la entidad de este derecho, razón por la cual debería estimarse incluida la intimidad dentro de los derechos resguardados por la Constitución y tutelada por la acción de amparo.

Más adelante, en el artículo 35, ocurre una situación similar a la recién señalada con el derecho a la intimidad, pero ahora con el derecho a la vida privada. En esta disposición, se reconoce la libertad de expresión señalando que: *"es libre la emisión del pensamiento por cualesquiera medios de difusión, sin censura ni licencia previa. Este derecho constitucional no podrá ser restringido por ley o disposición gubernamental alguna. Quien en uso de esta libertad faltare al respeto a la vida privada o a la moral, será responsable conforme a la ley. Quienes se creyeren ofendidos tienen derechos a la publicación de sus defensas, aclaraciones y rectificaciones".*

La disposición anterior es la única que hace referencia al derecho a la vida privada en el ordenamiento constitucional guatemalteco. Pese a ello, creemos que su configuración como límite al ejercicio del derecho a la libertad de expresión no es obstáculo para proclamar su consagración de derecho fundamental susceptible de ser tutelado por la acción de amparo. Por consiguiente, si bien el derecho a la vida privada no se encuentra reconocido de manera explícita en una disposición especial, si está presente al momento de establecer límites a otros derechos reconocidos constitucionalmente. Luego, si se le reconoce el carácter de límite, es porque se tiene en consideración la entidad del derecho que fundamenta tal limitación. En suma, pensamos que el derecho a la vida privada tiene configuración constitucional directa al igual que el derecho a la intimidad, y por lo tanto, su tutela quedaría entregada igualmente a la acción de amparo.

Más adelante, el artículo 44 de la Constitución prescribe que: *"los derechos y garantías que otorga la Constitución no excluyen otros que, aunque no figuren expresamente en ella, son inherentes a la persona humana. (…) El interés social prevalece sobre el interés particular. (…) Serán nulas ipso jure las leyes y las disposiciones gubernativas o de cualquier otro orden que disminuyan, restrinjan o tergiversen los derechos que la Constitución garantiza".*

La disposición recién transcrita cobra relevancia toda vez que se quisiera desconocer derechos fundamentales no contemplados expresamente por el Constituyente guatemalteco. Creemos que la limitada configuración constitucional del hábeas data en el artículo 31 podría ser suplida a través de este precepto y hacer extensivos los derechos de acceso, corrección y actualización a los titulares de datos personales respecto de los responsables de los archivos, registros o bancos de datos personales no estatales, es decir, en contra de los responsables de los archivos de datos que sean particulares o pertenezcan al sector privado. No vemos inconveniente en lo anterior, pues las lesiones a los derechos de las personas, obviamente pueden ser cometidas por cualquiera y no sólo por el Estado y sus organismos. De no seguirse este razonamiento, estimamos que no se

estaría aplicando el principio básico constitucional de la igualdad ante la ley. En el caso del derecho a la intimidad y la vida privada, el artículo 44 reforzaría aún más la consideración de éstos como derechos inherentes a la persona humana, con lo que se hace más fácil poder argumentar la tutela de estos derechos a través de la acción de amparo. Por último, la disposición en comento señala que son nulas de pleno derecho todas las leyes y disposiciones gubernativas que tergiversen o restrinjan los derechos que la Constitución establece. Este es un claro límite impuesto tanto al legislador como al Poder Ejecutivo en sus actividades normativas.

Por otra parte, y en cuanto a los derechos consagrados por la Constitución de Guatemala cabe mencionar lo señalado por el artículo 46, el cual establece la preeminencia del Derecho Internacional por sobre el derecho interno en materia de Derechos Humanos, prescribiendo que: *"se establece el principio general de que en materia de derechos humanos, los tratados y convenciones aceptados y ratificados por Guatemala, tienen preeminencia sobre el derecho interno".* Esta disposición viene a completar el sistema de protección a los Derechos Humanos en Guatemala, pues a pesar de las omisiones de que pueda adolecer la Constitución, y de los posibles conflictos interpretativos que puedan suscitarse al respecto, finalmente deberá prevalecer lo dispuesto en esos tratados ratificados por Guatemala. Entre éstos se encuentra la Convención Americana de Derechos Humanos [378] .

En lo relativo al mecanismo de tutela constitucional para hacer respetar los derechos consagrados en la Ley Fundamental, cabe hacer presente que el artículo 265 establece la acción de amparo. Al respecto dispone la norma que: *"Se instituye el amparo con el fin de proteger a las personas contra las amenazas de violaciones a sus derechos o para restaurar el imperio de los mismos cuando la violación hubiere ocurrido. No hay ámbito que no sea susceptible de amparo, y procederá siempre que los actos, resoluciones, disposiciones o leyes de autoridad lleven implícitos una amenaza, restricción o violación a los derechos que la Constitución y las leyes garantizan".* El artículo 276 por su parte dispone que: *"una ley constitucional desarrollará lo relativo al amparo, a la exhibición personal a la constitucionalidad de las leyes".* Al efecto, la Ley de Amparo, Exhibición Personal y Constitucionalidad de 1986 desarrolla el procedimiento de amparo constitucional.

Relacionado con lo anterior, debe consignarse que el artículo 272 señala entre las funciones de la Corte de Constitucionalidad: *"(…) b. Conocer en única instancia en calidad de Tribunal Extraordinario de Amparo en las acciones de amparo interpuestas en contra del Congreso de la República, la Corte Suprema de Justicia, el Presidente y el Vicepresidente de la República; c. Conocer en apelación de todos los amparos interpuestos ante cualquiera de los tribunales de justicia (…)".*

Finalmente, debemos señalar que la Constitución establece la designación de un Procurador de los Derechos Humanos el cual es *"un comisionado del Congreso de la República para la defensa de los Derechos Humanos que la Constitución garantiza. Tendrá facultades de supervisar la administración; ejercerá su cargo por un período de*

[378] Guatemala fue signataria de la Convención Americana el 22 de Noviembre de 1969 y ratifico ésta el 25 de Mayo de 1978. [En línea] < http://www.oas.org/juridico/spanish/firmas/b-32.html > [consulta: 18 de Marzo 2003].

cinco años, y rendirá informe anual al pleno del Congreso, con el que se relacionará a través de la Comisión de Derechos Humanos" (Art. 274) [379] .

En suma, podríamos afirmar que a primera vista el sistema constitucional guatemalteco contempla una protección parcial a los datos personales a través de los derechos reconocidos en el artículo 31, sólo ejercitable respecto de los órganos del Estado, a través de la acción de amparo constitucional. No obstante lo anterior, creemos que es posible ampliar el ámbito de protección a los datos personales. En este sentido el artículo 31 serviría de base para desarrollar un sistema general de protección jurídica a los datos personales, teniendo en cuenta las demás disposiciones constitucionales que resguardan tanto el derecho a la vida privada como a la intimidad y, fundamentalmente teniendo presente las normas contempladas en la Convención Americana de Derechos Humanos, la cual no sólo reconoce derechos fundamentales de las personas, sino que también obliga a los Estados a crear las condiciones favorable para el debido cumplimiento del Pacto.

Además de lo recién expuesto, la remisión a la Convención Americana nos permite sostener que es posible eludir el obstáculo a la tutela del derecho a la protección de datos o hábeas data que plantea la Ley de Amparo, la cual sólo procede respecto de actos u omisiones cometidas por funcionarios de la administración del Estado y por entidades privadas. En concreto, el artículo 25.1 de la Convención Americana de Derechos Humanos permitiría salvar la deficiencia normativa al establecer que*: "(…) 1. Toda persona tiene derecho a un recurso sencillo y rápido o a cualquier otro recurso efectivo ante los jueces o tribunales competentes, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la Constitución, la ley o la presente Convención, aun cuando tal violación sea cometida por personas que actúen en ejercicio de sus funciones oficiales (…)".* Esta disposición jurídicamente, tiene preeminencia sobre el derecho interno guatemalteco (Art. 43 C. Pol.).

2.2 Protección Legal de los Datos Personales

Si bien el ordenamiento jurídico guatemalteco contempla en el artículo 31 de la Constitución el derecho a la protección de datos o hábeas data limitado a los archivos y registros que posea la administración del Estado, no cuenta con una ley de protección de datos personales. Sin embargo, podemos señalar que existen al menos tres estatutos sectoriales legales que se ocupan de resguardar la confidencialidad de ciertos datos personales; la Ley de Bancos, que consagra la confidencialidad de las operaciones bancarias, la Ley Orgánica del Banco de Guatemala y el Código Tributario en lo que se refiere al secreto fiscal o tributario.

Por otra parte, cabe destacar que en la actualidad se encuentra en discusión

379 A su vez, el artículo 275 señala que entre las atribuciones de este procurador competerá: *"(…) b. Investigar y denunciar comportamientos administrativos lesivos a los intereses de las personas; c. Investigar toda clase de denuncias que le sean planteadas por cualquier persona, sobre violaciones a los Derechos Humanos; d. Recomendar privada o públicamente a los funcionarios la modificación de un comportamiento administrativo objetado; e. Emitir censura pública por actos o comportamientos en contra de los derechos constitucionales; f. Promover acciones o recursos, judiciales o administrativos, en los casos en que sea procedente; y g. Las otras funciones y atribuciones que le asigne la ley".*

legislativa un Proyecto de Ley de acceso a la información, el cual pretende regular tanto el hábeas data propio como el impropio. En relación a éste se ha dicho que tiene dos finalidades; por una parte "(…) regular el acceso a las personas al conocimiento de los actos de la administración con el fin de garantizar el pleno ejercicio del derecho de los interesados en cuando a la publicidad de esos actos (…)", y por otra parte "(…) regular el acceso a datos personales, el uso y tratamiento de los mismos, contenidos en archivos, registros, fichas, bases, bancos o cualquier otra forma de almacenamiento de datos, con el fin de garantizar el pleno ejercicio de los derechos de los titulares de los datos" [380] .

A continuación revisaremos las disposiciones legales pertinentes que se relacionan con la protección de loa datos personales en Guatemala.

2.2.1) Ley de Bancos y Grupos Financieros [381]

El artículo 63 de esta Ley dispone en el Capítulo II "Confidencialidad de las operaciones" que, salvo las obligaciones y deberes establecidos por la normativa sobre lavado de dinero u otros activos, *"los directores, gerentes, representantes legales, funcionarios y empleados de los bancos, no podrán proporcionar información, bajo, bajo cualquier modalidad, a ninguna persona, individual o jurídica, pública o privada, que tienda a revelar el carácter confidencial de la identidad de lo depositantes de los bancos, instituciones financieras y empresas de un grupo financiero, así como las informaciones proporcionadas por los particulares a estas entidades".*

Hacen excepción al deber de confidencialidad: *"la información que los bancos deban proporcionar a la Junta Monetaria, al Banco de Guatemala y a la Superintendencia de Bancos, así como la información que se intercambie entre bancos e instituciones financieras"* (Art. 63 inciso 2º). El inciso 3º del artículo 63 señala por su parte que: "*los*

[380] Información obtenida de artículo de prensa en el Diario La Hora de Guatemala: *"Congreso inicia ronda de discusión sobre la Ley de libre acceso a la información"*. [En línea] < http://www.lahora.com.gt/02/10/17/paginas/nac_2.htm#n1 > [Consulta: 17 de Enero 2003]. Se señala en este mismo artículo que "con esta ley se busca otorgar a todos los habitantes de la República un procedimiento legal, sin formalismos y de fácil aplicación, a efecto que puedan conocer todo lo que de ellos conste y su finalidad de los datos personales que obran en archivos y registros estatales y privados; así como la identidad de los responsables y usuarios de dichos datos. Se establece que todos los jueces o tribunales de la República son competentes para conocer el proceso de Hábeas Data a solicitud del interesados (sic) que la podrá plantear verbalmente o por escrito y sin necesidad del auxilio de abogado. En un plazo de 72 horas las autoridades judiciales jurisdiccionales emitirán auto para dictar las medidas cautelares o de urgencia que consideren pertinentes y ordenará al responsable del archivo la exhibición de los datos personales del interesado. El proyecto de ley se sustenta en la Declaración Universal de los Derechos Humanos, declaración Americana de los Derechos y Deberes del Hombre, Convención Americana sobre Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos, así como en el Acuerdo de Paz sobre el Fortalecimiento del Poder Civil y función del Ejército en una Sociedad Democrática". Cabe hacer presente que al 18 de marzo de 2003 se ha señalado que el "Congreso de la República aprobó por unanimidad en tercer debate el proyecto de Ley de Libre Acceso a la Información, un compromiso expreso establecido en los acuerdos de paz y demás convenios ratificados por Guatemala en materia de derechos humanos, que desarrolla los artículos 30 y 31 constitucionales". [En línea] < http://www.congreso.gob.gt/Noticias/marzo/180303/11-2003.htm > [consulta: 19 de Marzo 2003].

[381] Esta ley está contenida en el Decreto Nº 19-2002, publicado en el Diario Oficial el 15 de Mayo de 2002. [En línea] < http://www.banguat.gob.gt/leyes/2002/bancos.pdf > [consulta: 18 de Marzo 2003].

miembros de la Junta Monetaria y las autoridades, funcionarios y empleados del Banco de Guatemala y de la Superintendencia de Bancos no podrán revelar la información a que se refiere el presente artículo, salvo que medie orden del juez competente".

Llama la atención del artículo 63, el ámbito cubierto por el deber de confidencialidad de las operaciones bancarias, pues del tenor de la ley pareciera desprenderse que sólo quedarían a resguardo tanto la identidad de quien realiza los depósitos como las informaciones proporcionadas por los particulares a esas instituciones. Opinamos que la norma apunta a resguardar la confidencialidad no sólo de la identidad de quien realiza una operación de depósito bancario, sino que también el monto de ella, pues si no fuera de esta manera, no tendría sentido intitular el Capítulo II tal como lo hace la ley. Además, es norma general en las legislaciones latinoamericanas que el secreto bancario abarque no sólo la identidad del cliente u interviniente en una operación en el sistema bancario, sino también se extienda a los depósitos y captaciones (operaciones pasivas).

Finalmente, en relación a la excepción al deber de confidencialidad de las operaciones bancarias relativa al traspaso de información confidencial entre bancos e instituciones financieras, no queda claro el tratamiento de esa información cuando se está frente a bancos que son filiales o agencias de otros extranjeros. Entendemos que en este caso como toda excepción, debe dársele una interpretación restrictiva y sólo aplicarla al traspaso de información a nivel nacional.

2.2.2) Ley Orgánica del Banco de Guatemala [382]

Esta ley, dentro de su Capítulo IV denominado "La Superintendencia de Bancos", contempla una disposición relacionada con la protección de los datos personales. El artículo 49 inciso 2º señala que: *"las informaciones de particulares obtenidas por la Superintendencia de Bancos, en el ejercicio de sus funciones, incluyendo de accionistas, directores, funcionarios y empleados de las entidades sujetas a su vigilancia e inspección, serán estrictamente confidenciales, por considerarse datos suministrados por particulares bajo garantía de confidencia. En consecuencia, las autoridades, funcionarios y empleados de la Superintendencia de Bancos no podrán revelar ni comentar los datos obtenidos, ni los hechos observados, salvo que medie orden de juez competente".*

De lo anterior, se desprende claramente el deber de confidencialidad de los funcionarios de la Superintendencia respecto de las informaciones de particulares obtenidas en el ejercicio de sus funciones, así como también el deber de secreto en relación a los hechos presenciados por éstos. Cabe la duda en relación a lo que la ley entiende por *"informaciones de particulares".* Creemos que éstas se refieren a toda información relativa a las operaciones efectuadas por las personas en el mercado bancario así como también sus respectivas identidades. La interpretación anterior la basamos en la amplitud del término utilizado por el legislador, a diferencia de lo señalado por la Ley de Bancos de reciente data, la cual dispone la confidencialidad de la identidad de los depositantes así como las informaciones proporcionadas por los particulares. Finalmente, el artículo 50 señala las sanciones aplicables en caso de violarse la disposición anterior, las cuales se analizarán en el punto Nº 9 relativo al régimen de

[382] **[En línea] < http://www.sib.gob.gt/banguat/index_2.php > [consulta 19 de Marzo 2003].**

responsabilidad.

2.2.3) Código Tributario [383]

Antes de señalar la normativa del Código Tributario relacionada con la protección de los datos personales, cabe recordar el texto del artículo 24 de la Constitución el cual dispone que: *"Los libros, documentos y archivos que se relacionan con el pago de impuestos, tasa, arbitrios y contribuciones, podrán ser revisados por la autoridad competente de conformidad con la ley. Es punible revelar el monto de los impuestos pagados, utilidades, pérdidas, costos y cualquier otro dato referente a las contabilidades revisadas a personas individuales o jurídicas, con excepción de los balances generales, cuya publicación ordene la ley".* Teniendo en cuenta lo anterior, el artículo 30 del Código Tributario señala en el inciso 1º que la Administración Tributaria podrá requerir de cualquier entidad o persona, ya sea individual o jurídica, información referente a actos, contratos u otros hechos o relaciones mercantiles con terceros, generadores de tributos, *"siempre que no se viole la garantía de confidencialidad establecida en la Constitución Política de la República y las leyes especiales, el secreto profesional y lo dispuesto en este Código".*

Luego en el inciso 2º dispone que: *"las informaciones de personas individuales o jurídicas obtenidas por la Administración Tributaria en el ejercicio de su función de fiscalización a que se refieren las literales a) e i) del artículo 3 de la Ley Orgánica de la Superintendencia de Administración Tributaria, Decreto Número 1-98 del Congreso de la República, serán estrictamente confidenciales, por considerarse datos suministrados bajo garantía de confidencialidad. En consecuencia, las autoridades, funcionarios y empleados de la Administración Tributaria no podrán revelar ni comentar los datos obtenidos, ni los hechos observados, salvo que medie orden de Juez competente".*

En definitiva, el ordenamiento jurídico guatemalteco establece el deber de secreto respecto de los montos de los impuestos pagados, utilidades, pérdidas, costos y cualquier otro dato referente a las contabilidades revisadas por la Administración Tributaria, así como también los datos suministrados bajo garantía de confidencialidad a ese organismo por los contribuyentes y terceros requeridos de cooperación por la Administración Tributaria. La excepción al deber de secreto está configurada por la intervención de una orden judicial emanada de un Tribunal competente. Este Código, también establece sanciones para quienes violen las disposiciones recién señaladas, las cuales se reseñaran más adelante en el punto relativo al régimen de responsabilidad (Nº 9).

3. Bienes Jurídicos Protegidos por la Legislación de Datos Personales

Si bien el ordenamiento jurídico guatemalteco no dispone de una ley de protección de datos personales, en el ámbito constitucional si se contempla una disposición

383 [En línea] < http://www.ciat.org/doc/docu/leg/cod/lgt_02_codigo_tributario_guatemala.doc > [consulta: 18 de Marzo 2003].

directamente relacionada con la materia de estudio [384] . Sin embargo, la configuración del derecho de control sobre los datos en poder de los organismos del Estado (Art. 31) suscita dudas en cuanto a los bienes jurídicos que éste tutelaría. Al respecto, el Constituyente no utiliza ningún término que pudiera vincularse al derecho a la protección de datos sino que sólo se refiere al *"Acceso a archivos y registros estatales"*. En nuestra opinión, si bien no se habla de hábeas data, pensamos que el objeto del derecho reconocido en el artículo 31, es similar al objeto perseguido por la acción de hábeas data, cual es acceder a los registros y conocer lo que en ellos consta así como también la finalidad para la cual se utilizan los datos, y eventualmente, solicitar la corrección, rectificación y actualización de ellos en el evento de inexactitud, error o caducidad de la información. En razón de ello, creemos que el Constituyente estaría reconociendo un derecho a la protección de datos limitado -dado que sólo tutela el tratamiento de datos realizado por el Estado- sin especificar el medio de tutela idóneo para tal derecho. Ahora bien, en nuestro concepto, los bienes jurídicos que se tutelarían, serían la intimidad y vida privada de las personas, aunque estos derechos no aparezcan reconocidos directamente por el Constituyente y, deban por lo tanto fundamentarse en una interpretación sistemática del texto constitucional en relación a la Convención Americana de derechos Humanos o Pacto de san José de Costa Rica, la cual tiene primacía sobre el derecho interno guatemalteco en virtud del artículo 46 de la Constitución.

4. Principios Informativos de la Legislación de Protección de Datos Personales

En este punto no nos detendremos, dada la falta de legislación general de protección de datos personales.

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

En esta materia tampoco podemos adentrarnos, en atención a la falta de ley general de protección de datos personales en el ordenamiento jurídico de Guatemala.

6. Modelos de Tutela

El ordenamiento jurídico guatemalteco no contempla una acción especial destinada a la protección de los datos personales. En materia constitucional, si bien posee Guatemala una norma que consagra el derecho de acceso, corrección, rectificación y actualización de los datos personales que consten en fichas o registros estatales, no establece el mecanismo específico para la tutela de éstos. A falta de esa previsión, estimamos que es

[384] Cabe recordar que en la actualidad se encuentra en tramitación ante el Congreso Nacional de Guatemala un Proyecto de Ley de Acceso a la Información, cuyos fundamentos se encuentran en el artículo 30 de la Constitución que establece la publicidad de los actos administrativos y el 31, que consagra un derecho a la protección de datos que nosotros hemos llamado limitado.

necesario remitirse al artículo 265 el cual consagra la acción de amparo.

A continuación analizaremos la acción de amparo, pues creemos que dada la inexistencia de un medio procesal específico que se ocupe de regular el ejercicio del derecho consagrado en el artículo 31 de la Constitución Guatemalteca, ésta sería la más adecuada -pero no la mejor- para proteger los derechos de las personas ante el tratamiento de sus datos personales. No obstante lo anterior, cabe señalar que la configuración legal de la propia acción de amparo no la haría procedente respecto de actos u omisiones que provengan de cualquier particular, sino sólo de aquéllos señalados exhaustivamente por el legislador. Con todo, entendemos que el marco jurídico constitucional permitiría fundamentar una protección respecto de los actos de particulares y lograr suplir la deficiencia normativa en esta materia, lo cual ya hemos señalado más arriba (ver punto Nº 2.1 de este análisis).

6.1 La Acción de Amparo

El artículo 265 de la Constitución guatemalteca consagra la acción de amparo, cuyo objeto es: *"proteger a las personas contra las amenazas de violaciones a sus derechos o para restaurar el imperio de los mismos cuando la violación hubiere ocurrido".* El artículo 276, por su parte dispone que: *"una ley constitucional desarrollará lo relativo al amparo, a la exhibición personal a la constitucionalidad de las leyes"*. Esa ley constitucional es la Ley de Amparo, Exhibición Personal y Constitucionalidad, la cual está contenida en el Decreto Nº 1 de 1986 [385] .

6.1.1) Procedencia de la Acción

Antes de señalar la regulación específica del amparo, debemos recordar la exclusión por el artículo 31 de la Constitución del derecho a la protección de datos respecto del sector privado. Del tenor tal disposición, se desprende que los derechos de acceso, corrección, rectificación y actualización de datos sólo pueden ser ejercitados respecto de los archivos o registros del sector público, representado por el Estado y sus organismos. Lo anterior, atendido el silencio en relación a los responsables de archivos o bancos de datos que no pertenezcan a la administración del Estado. Tal diferencia, nos parece atentatoria al principio de igualdad ante la ley. Sin embargo, la Ley de Amparo amplía el sujeto pasivo de la acción al señalar en el artículo 9 que puede solicitarse amparo en contra de entidades a las que debe ingresarse por mandato legal y otras reconocidas por ley, tales como: los partidos políticos, asociaciones, sociedades, sindicatos, cooperativas y otras semejantes. Junto con ello, debe tenerse presente lo dispuesto en el artículo 46 de la Constitución, lo cual permitiría suplir la estrechez normativa del artículo 31 haciendo aplicación directa de los tratados sobre Derechos Humanos ratificados por Guatemala los que tienen primacía sobre el ordenamiento jurídico guatemalteco.

En cuanto a la regulación propiamente tal del amparo la Constitución dispone al efecto que: *"(…) No hay ámbito que no sea susceptible de amparo, y procederá siempre*

385 Este Decreto está disponible [en línea] < http://www.minugua.guate.net/derhum/CDROM/Normativa/Leyes%20Guate/leydeamparo.htm,fecha > [consulta: 17 de Enero 2003].

que los actos, resoluciones, disposiciones o leyes de autoridad lleven implícitos una amenaza, restricción o violación a los derechos que la Constitución y las leyes garantizan" (Art. 265). Por su parte, la Ley de Amparo, Exhibición Personal y Constitucionalidad (en adelante LAEPC), preceptúa -de manera similar al texto constitucional- en el artículo 8 que: *"el amparo protege a las personas contra las amenazas de violaciones a sus derechos o restaura el imperio de los mismos cuando la violación hubiere ocurrido. No hay ámbito que no sea susceptible de amparo y procederá siempre que los actos, resoluciones, disposiciones o leyes de autoridad lleven implícitos una amenaza, restricción o violación a los derechos que la Constitución y las leyes garantizan".*

Luego, el inciso 1º del artículo 10 de la LAEPC agrega a lo ya prescrito que: *"la procedencia del amparo se extiende a toda situación que sea susceptible de un riesgo, una amenaza, restricción o violación a los derechos que la Constitución y las leyes de la República de Guatemala reconocen, ya sea que dicha situación provenga de personas y entidades de derecho público o entidades de derecho privado"* [386] . Por lo tanto, procede esta acción en caso de amenaza, restricción o violación de los derechos garantizados por la Constitución y las leyes, sea que provengan de actos, resoluciones o leyes de autoridad o de "*entidades de derecho privado"*.

Por otra parte, el artículo 19 de la LAEPC señala el carácter subsidiario que se le ha dado al amparo, al decir que: *"para pedir amparo, salvo casos establecidos en esta ley, deben previamente agotarse los recursos ordinarios, judiciales y administrativos, por cuyo medio se ventilan adecuadamente los asuntos de conformidad con el principio del debido proceso".* En el caso del especial derecho a la protección de datos guatemalteco, cabe la duda acerca de la procedencia directa del amparo en razón a lo preceptuado por el texto del artículo 10 de la LAEPC, el cual prescribe que toda persona tiene derecho a pedir amparo, entre otros casos:"*(…) f) Cuando las peticiones y trámites ante autoridades administrativas no sean resueltos en el término que la ley establece, o de no haber tal término, en el de treinta días, una vez agotado el procedimiento correspondiente; así como cuando las peticiones no sean admitidas para su trámite (…)".* En este caso pareciera ser que se requeriría primeramente ejercitar los derechos de acceso, corrección, rectificación y actualización de los datos personales directamente ante los organismos públicos responsables de los archivos o bancos de datos, y vencido el plazo general de 30 días desde que se haya agotado el procedimiento, o desde el rechazo de la petición, recién quedaría expedita la vía para el amparo. Es decir, se exigiría agotar previamente la vía administrativa.

6.1.2) Legitimación Activa

Están legitimados para entablar la acción de amparo *"toda persona"* (Art. 10 inciso 2º LAEPC). Se añade a lo anterior por el artículo 25 que: *"el Ministerio Público y el*

386 El artículo 10 de la LAEPC enumera una serie de casos no exhaustivos en que es procedente el amparo, señalando finalmente que *"(…) lo determinado en los incisos anteriores, no excluye cualesquiera otros casos, que no estando comprendidos en esa enumeración, sean susceptibles de amparo de conformidad con lo establecido por los artículos 265 de la Constitución y 8 de esta ley".*

Procurador de los Derechos Humanos, tienen legitimación activa para imponer amparo a efecto de proteger los intereses que les han sido encomendados".

6.1.3) Legitimación Pasiva

La Constitución da a entender que son legitimados pasivos de esta acción de amparo -para proteger los derechos de los titulares de datos personales-, los responsables de los archivos, bancos de datos o de *"cualquier otra forma de registros estatales"* (Art. 31 C. Política).

Por su parte, la LAEPC amplía el sujeto pasivo al señalar en el artículo 9 que: *"Podrá solicitarse amparo contra (…) entidades a las que debe ingresarse por mandato legal y otras reconocidas por ley, tales como partidos políticos,* ***asociaciones, sociedades*** *,* ***sindicatos, cooperativas*** *y* ***otras semejantes*** *"* (negrita nuestra).

Luego en el inciso 2º del artículo 9, se dispone que: *"el amparo procederá contra las entidades a que se refiere este articulo cuando ocurrieren las situaciones previstas en el articulo siguiente o se trate de prevenir o evitar que se causen daños patrimoniales, profesionales o de cualquier naturaleza".* A este respecto el artículo 10 -como se vio-, señala que procederá el amparo *"(…) ya sea que dicha situación provenga de personas y entidades de derecho público* ***o entidades de derecho privado*** *"* (negrita nuestra).

En suma, la LAEPC ha ampliado el sujeto pasivo de la acción de amparo a las entidades privadas tales como: las sociedades, asociaciones, cooperativas, sindicatos u otra semejantes. Si bien ello es un avance en relación al texto constitucional, esto no es suficiente pues no se refiere a las personas naturales. Con todo, creemos que esa falta se suple por las disposiciones de los tratados internacionales de Derechos Humanos ratificados por Guatemala los cuales tiene primacía sobre ese orden jurídico, entre estos, destaca la Convención Americana de Derechos Humanos. Para este efecto cobra relevancia el artículo 25.1 citado anteriormente.

6.1.4) Competencia

La competencia, se regula en virtud del carácter del sujeto pasivo de la acción de amparo, es decir, en razón de su "dignidad". A este respecto podemos señalar que la regla general, es la competencia de los *"los jueces de primera instancia del orden común"* quienes conocerán de los amparos interpuestos en contra de: a) Los administradores de rentas; b) Los jueces menores; c) Los jefes y demás empleados de policía; d) Los alcaldes y corporaciones municipales no comprendidos en el artículo anterior; e) Los demás funcionarios, autoridades y empleados de cualquier fuero o ramo no especificados en los artículos anteriores y f) Las entidades de derecho privado(Art. 14 LAEPC) [387] .

6.1.5) Procedimiento Aplicable

El procedimiento aplicable a la tramitación de la acción de amparo, puede sintetizarse de la siguiente forma:

1) *Demanda*: la petición de amparo debe hacerse dentro de los treinta días siguientes al de la última notificación al afectado o de conocido por éste el hecho que a su

juicio, le perjudica. El plazo anterior no rige cuando el amparo se promueva en contra del riesgo de aplicación de leyes o reglamentos inconstitucionales a casos concretos; así como ante la posibilidad manifiesta de que ocurran actos violatorios a los derechos del sujeto activo (Art. 20). El amparo se pedirá por escrito, debiendo cumplir ciertos requisitos [388] . No obstante lo anterior, la persona notoriamente pobre o ignorante, el menor y el incapacitado, que no pudieren actuar con auxilio profesional, *"podrán comparecer ante los tribunales en solicitud verbal de amparo (…)"* (Art. 26).

2) *Suspensión provisional*: al momento de interposición del amparo podrá solicitarse la suspensión provisional de la disposición, acto, resolución o procedimiento reclamado (Art. 24).

3) *Informe*: los jueces y Tribunales están obligados a tramitar los amparos el mismo día en que les fueren presentados, mandando pedir los antecedentes o en su defecto informe circunstanciado a la persona, autoridad, funcionario o empleado contra el cual se haya pedido amparo, quienes deberán cumplir remitiendo los antecedentes o informando

[387] Los demás ámbitos de competencia se regulan en los artículos 11 al 13, los que disponen al efecto: "Artículo 11.- Competencia de la Corte de Constitucionalidad. Corresponde a la Corte de constitucionalidad, conocer en única instancia en calidad de Tribunal Extraordinario de Amparo, en los amparos interpuestos en contra del Congreso de la República, la Corte Suprema de Justicia, el Presidente y el Vicepresidente de la República". "Articulo 12.- Competencia de la Corte Suprema de Justicia. La Corte Suprema de Justicia conocerá de los amparos en contra de: a) El Tribunal Supremo Electoral; b) Los Ministros de Estado o Viceministros cuando actúen como Encargados del Despacho; c) Las Salas de la Corte de Apelaciones, Cortes Marciales, Tribunales de Segunda Instancia de Cuentas y de lo Contencioso-Administrativo; d) El Procurador General de la Nación; e) El Procurador de los Derechos Humanos; f) La Junta Monetaria; g) Los Embajadores o Jefes de Misión Diplomática guatemaltecos acreditados en el extranjero; h) El Consejo Nacional de Desarrollo Urbano y Rural". "Artículo 13.- Competencia de la Corte de Apelaciones. Las Salas de la Corte de Apelaciones del orden común, en sus respectivas jurisdicciones, conocerán de los amparos que se interpongan contra: a) Los Viceministros de Estado y los Directores Generales; b) Los Funcionarios Judiciales de cualquier fuero o ramo que conozcan en primera instancia; c) Los alcaldes y corporaciones municipales de las cabeceras departamentales; d) El Jefe de la Contraloría General de Cuentas; e) Los gerentes, jefes o presidentes de las entidades descentralizadas o autónomas del Estado o sus cuerpos directivos, consejos o juntas rectoras de toda clase; f) El Director General del Registro de Ciudadanos; g) Las asambleas generales y juntas directivas de los colegios profesionales; h) Las asambleas generales y órganos de dirección de los partidos políticos; i) Los cónsules o encargados de consulados guatemaltecos en el extranjero; j) Los consejos regionales o departamentales de desarrollo urbano y rural y los gobernadores".

[388] Estos requisitos son los siguientes: a) Designación del tribunal ante el que se presenta; b) Indicación de los nombres y apellidos del solicitante o de la persona que lo represente; su edad, estado civil, nacionalidad, profesión u oficio, domicilio y lugar para recibir notificaciones. Si se gestiona por otra persona deberá acreditarse la representación; c) Cuando quien promueve el amparo sea una persona jurídica, deberán indicarse sucintamente los datos relativos a su existencia y personalidad jurídica; d) Especificación de la autoridad, funcionario, empleado, persona o entidad contra quien se interpone el amparo; e) Relación de los hechos que motivan el amparo; f) Indicación de las normas constitucionales de otra índole en que descansa la petición de amparo con las demás argumentaciones y planteamientos de derecho; g) Acompañar la documentación que se relacione con el caso, en original o en copias, o indicar el lugar en donde se encuentre y los nombres de las personas a quienes les consten los hechos y los lugares donde pueden ser citadas y precisar cualesquiera otras diligencias de carácter probatorio que conduzcan al esclarecimiento del caso; h) Lugar y fecha; i) Firmas del solicitante y del abogado colegiado activo que lo patrocina, así como el sello de éste. Si el solicitante no sabe o no puede firmar, lo hará por él otra persona o el abogado que auxilia; j) Acompañar una copia para cada una de las partes y una adicional para uso del tribunal (Artículo 21).

dentro del perentorio término de cuarenta y ocho horas, más el de la distancia, que fijará el Tribunal en la misma resolución, a su prudente arbitrio (Art. 33).

4) *Audiencia*: recibidos los antecedentes o el informe, el Tribunal deberá confirmar o revocar la suspensión provisional decretada en el auto inicial del procedimiento. De estos antecedentes o del informe dará vista al solicitante, al Ministerio Público y a las que a su juicio también tengan interés en la subsistencia o suspensión del acto, resolución o procedimiento, quienes podrán alegar dentro del término común de cuarenta y ocho horas.

5) *Prueba eventual*: vencido el término de cuarenta u ocho horas recién señalado, hayan o no alegado las partes, el Tribunal estará obligado a resolver, pero si hubiere hechos qué establecer, abrirá a prueba el amparo, por el improrrogable término de ocho días. Los Tribunales de amparo podrán relevar de la prueba en los casos en que a su juicio no sea necesario, pero la tramitarán obligadamente si fuere pedida por el solicitante (Art. 35). Concluido el término probatorio, el Tribunal dictará providencia dando audiencia a las partes y al Ministerio Público por el término común de cuarenta y ocho horas, transcurrido el cual, se hayan o no pronunciado, dictará sentencia dentro de tres días (Art. 37).

6.1.6) La Sentencia

El artículo 42 dispone que, al pronunciar sentencia, el Tribunal de amparo examinará los hechos, analizará las pruebas y actuaciones, y todo aquello que formal, real y objetivamente resulte pertinente; examinará todos y cada uno de los fundamentos de derecho aplicables, hayan sido o no alegados por las partes. Agrega en el inciso 2º que con base en las consideraciones anteriores y aportando su propio análisis doctrinal y jurisprudencial, pronunciará sentencia, *"interpretando siempre en forma extensiva la Constitución, otorgando o denegando amparo, con el objeto de brindar la máxima protección en esta materia, y hará las demás declaraciones pertinentes"*.

Los efectos del amparo, son señalados en el artículo 49, el cual dispone que la sentencia de amparo puede: *"a) Dejar en suspenso, en cuanto al reclamante, la ley, el reglamento, resolución o acto impugnados y, en su caso, el restablecimiento de la situación jurídica afectada o el cese de la medida; b) Fijar un término razonable, para que cese la demora, si el caso fuere de mero retardo en resolver, practicar alguna diligencia o ejecutar algún acto ordenado de antemano; c) Cuando el amparo hubiese sido interpuesto por omisión de la autoridad en la emisión de la reglamentación de la ley, el Tribunal de Amparo resolverá fijando las bases o elementos de aplicación de ésta al caso concreto, según los principios generales del derecho, la costumbre, los precedentes para otros casos, la analogía de otros reglamentos y la equidad, siguiendo el orden que el tribunal decida".*

Finalmente, el artículo 59 prescribe que cuando el tribunal declare que ha lugar al pago de daños y perjuicios, sea en sentencia o en resolución posterior, *"fijará su importe en cantidad líquida o establecerá, por lo menos, las bases con arreglo a las cuales deberá hacerse la liquidación o dejará la fijación de su importe a juicio de expertos (…). Además de los casos establecidos en esta ley, el tribunal, después de la sentencia, a*

petición de parte, condenará el pago de daños y perjuicios cuando hubiere demora o resistencia a ejecutar lo resuelto en la sentencia".

6.2 Otras Acciones

Dentro del ordenamiento jurídico guatemalteco no se observan otras acciones tendientes a resguardar a los titulares de los datos personales.

7. Mecanismos de Control

Dada la inexistencia de una legislación de protección de datos personales, tampoco es posible referirse a eventuales mecanismos de control.

8. Transmisión Internacional de Datos

En esta materia tampoco tenemos conocimiento de legislación especial en Guatemala.

9. Régimen de Responsabilidad

En materia de responsabilidad, y como consecuencia de la inexistencia de una ley de protección de datos personales que prevea reglas en esta materia, sólo queda remitirse a las reglas contempladas en estatutos sectoriales y generales para la protección de algunos ámbitos relacionados con los datos personales. A continuación se reseñaran esas reglas aplicables.

9.1 Responsabilidad Administrativa

En lo tocante a esta clase de responsabilidad, señalaremos las sanciones contempladas en los estatutos ya analizados en el punto Nº 2.2 de este análisis.

a) Ley de Bancos

En materia bancaria el artículo 63 de la Ley respectiva -el cual dispone acerca del deber de confidencialidad bancaria-, señala que la infracción a este deber *"será sancionado como falta grave, y motivará la inmediata remoción de los que incurran en ella, sin perjuicio de las responsabilidades civiles y penales que de tal hecho se deriven".*

b) Ley Orgánica del Banco de Guatemala

Por su parte, el artículo 50 de la Ley Orgánica del Banco de Guatemala, dentro del Capítulo relativo a la Superintendencia de Bancos, señala que la infracción a los deberes de confidencialidad y secreto a que están afectos los funcionarios de ese organismo: *"será considerada como falta grave, y motivará la inmediata remoción de los que incurran en ella, sin perjuicio de las responsabilidades que determine el Código penal".*

c) Código Tributario

En materia tributaria el Código del ramo también establece sanciones administrativas para los funcionarios que incumplan los deberes de secreto a que están afectos. Al respecto, el artículo 96 dispone que: *"Existe incumplimiento de deberes, (…) cuando revele o facilite la revelación de hechos, actuaciones o documentos de los que tenga conocimiento por razón de su cargo y que por disposición de la ley, deban permanecer en secreto o confidencia".* Luego, agrega la norma que: *"Las infracciones anteriores serán sancionadas por la Administración Tributaria, conforme a lo dispuesto en la Ley de Servicio Civil y la Ley de Responsabilidades, sin perjuicio de las sanciones civiles y penales que correspondan"*.

En suma, en caso de existir faltas funcionarias que lesionen los derechos de los titulares de los datos, deberán aplicarse los estatutos sectoriales ya vistos cuando sea procedente, y a falta de éstos, las reglas generales que rigen a los funcionarios de la administración del Estado. Respecto de estas últimas debemos señalar que no disponemos de información.

9.2 Responsabilidad Civil

En lo relativo a la responsabilidad civil no disponemos de información acerca de ella, sin embargo estimamos que quienes infrinjan tanto el derecho a la protección de datos limitado o incompleto reconocido en el artículo 31 de la Constitución, como cualquiera de las normas legales ya señaladas, a falta de normas especiales, deberían responder civilmente por los daños causados. En el caso que sea un organismo del Estado el que afecte el derecho, debería operar la responsabilidad patrimonial de éste sea que el daño se cometa por un acto o una omisión.

9.3 Responsabilidad Penal

Dentro del Código Penal guatemalteco se contemplan diversos delitos que tutelan bienes jurídicos como la intimidad y la vida privada [389] . Su eventual aplicación para la protección de los datos personales parece difícil, pues están pensadas para sancionar conductas que no afectan un bien jurídico como la autodeterminación informativa o el derecho a la protección de datos. No obstante lo anterior, se señalarán las disposiciones relacionadas a los bienes jurídicos intimidad y vida privada, estrechamente vinculados a la protección de datos personales.

a) Allanamiento de morada:

El artículo 206 contempla el delito de allanamiento de morada y señala que: *"El particular que, sin autorización o contra la voluntad expresa o tácita del morador, clandestinamente o con engaño, entrare en morada ajena o en sus dependencias o permaneciere en ella, será sancionado con prisión de tres meses a dos años".*

[389] El Código Penal guatemalteco puede consultarse [en línea] < http://www.unifr.ch/derechopenal/legislacion/gt/cp_guatemala.htm > [consulta: 19 de Marzo 2003].

b) Violación de correspondencia:

Por su otra parte, el artículo 217 tipifica el delito de violación de correspondencia disponiendo que: *"Quien, de propósito o para descubrir los secretos de otro, abriere correspondencia, pliego cerrado o despachos telegráficos, telefónico o de otra naturaleza, que no le estén dirigidos a quien, sin abrirlos, se impusiere de su contenido, será sancionado con multa de cien a un mil quetzales".*

A continuación, el artículo 218 preceptúa que: *"Quien, indebidamente, se apoderare de correspondencia, pliego o despachos, a que se refiere el artículo anterior o de otro papel privado, aunque no estén cerrados o quien los suprimiere o desviare de su destino, será sancionado con multa de cien a un mil quetzales".*

c) Violación de comunicaciones:

El artículo 219, tipifica el delito de violación de comunicaciones disponiendo al efecto que: *"Quien, valiéndose de medios fraudulentos interceptare, copiare o grabare comunicaciones televisadas, radiales, telegráficas, telefónicas u otras semejantes o de igual naturaleza, o las impida o interrumpa, será sancionado con multa de cien a un mil quetzales".*

A su vez, el artículo 220 contempla situaciones especiales de agravamiento del delito disponiendo que: *"Las sanciones señaladas para los hechos delictuosos definidos en los tres artículos que preceden, serán de prisión de seis meses a tres años, en los siguientes casos: 1º. Si el autor se aprovechare de su calidad de funcionario o empleado de la dependencia, empresa o entidad respectivas; 2º. Si se tratare de asuntos oficiales; 3º. Si la información obtenida, el autor la hiciere pública, por cualquier medio".*

Luego el artículo 222 sanciona a: *"Quien, hallándose legítimamente en posesión de correspondencia, de papeles o de grabaciones, fotografías no destinadas a la publicidad, los hiciere públicos, sin la debida autorización, aunque le hubieren sido dirigidos, cuando el hecho cause o pudiere causar perjuicio, será sancionado con multa de doscientos a dos mil quetzales".*

d) Violación de secretos:

Finalmente, el artículo 223 castiga a: *"Quien, sin justa causa, revelare o empleare en provecho propio o ajeno un secreto del que se ha enterado por razón de su estado, oficio, empleo, profesión o arte, sin que con ello ocasionare o pudiere ocasionar perjuicio, será sancionado con prisión de seis meses a dos años o multa de cien a un mil quetzales".*

De las disposiciones anteriores cabe destacar que, en general para los delitos en contra de la intimidad o la vida privada las sanciones consisten en multas y sólo en los casos agravados se sanciona con pena privativa de libertad.

10. Conclusiones

La protección de los datos personales en el ordenamiento jurídico guatemalteco está

consagrada de manera imperfecta en el artículo 31 de la Constitución. En éste, sólo reconoce un derecho a la protección de datos limitado, reclamable sólo respecto de los responsables de archivos o bancos de datos personales pertenecientes al poder estatal, dejando fuera a los particulares que realicen actividades de recolección y tratamiento de datos. A nivel infraconstitucional, no cuenta Guatemala con una ley que regule y desarrolle lo preceptuado en la Carta Fundamental. No obstante lo anterior, en la actualidad existe una propuesta legislativa de acceso a la información que se discute en el Congreso Nacional.

En lo relativo al mecanismo de tutela del derecho a la protección de datos limitado o de hábeas data del artículo 31 constitucional, no existe una acción específica para ese efecto. En la actualidad, la vía más adecuada que visualizamos para otorgar tutela a ese derecho sería la acción de amparo, la cual si bien logra ampliar a los sujetos pasivos señalados por el Constituyente, también aparece como insuficiente para otorgar eficaz protección a los datos personales. Con todo, creemos que muchos de los obstáculos pueden ser salvados por los Tribunales de justicia haciendo aplicación de la importante disposición del artículo 46 de la Constitución, la cual da primacía sobre el derecho interno a las disposiciones contenidas en los tratados sobre Derechos Humanos ratificados por Guatemala. Teniendo a la vista esos preceptos, es posible saltar los escollos que dejan en la indefensión a las personas respecto de particulares que recolectan y tratan datos personales, hasta ahora sin ninguna cortapisa jurídica.

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN HONDURAS

1. Generalidades

El ordenamiento jurídico hondureño no contempla disposiciones que se encarguen de la protección directa a los datos personales. Ni la Constitución ni la ley reconocen un derecho a la protección de datos. En razón de lo anterior, nuestro análisis de centrará en las disposiciones constitucionales que protegen la intimidad y la vida privada, conjuntamente con otras que configuran la protección jurídica de los Derechos Humanos. En éstas trataremos de fundamentar una protección a los datos personales a falta de normas expresas y en especial, a falta de la consideración de la autodeterminación informativa como bien jurídico digno de tutela.

En al ámbito legal sectorial, no hemos encontrado mayores antecedentes que en el ámbito financiero y tributario, los cuales tampoco dan muchas luces como para afirmar que pudiera existir una legislación sectorial fuerte en la materia.

2. Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional

La Constitución hondureña de 1982 no contempla disposiciones que reconozcan el derecho a la protección de datos y por consiguiente que consagren una acción de hábeas data [390] . Sólo posee normas de carácter general que reconocen el derecho a la honra, la intimidad personal y familiar y, el derecho a la imagen. Junto con éstas, existen diversos preceptos que van configurando el marco jurídico de protección a los Derechos Humanos. Las normas relevantes para nuestro estudio las señalaremos a continuación.

El artículo 76 señala que: *"se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen".* De esta disposición se desprende que se reconocen esos derechos fundamentales a través de la consagración de su garantía.

Más adelante, desarrollando el derecho a la intimidad y reconociendo indirectamente el derecho a la vida privada, el artículo 99 garantiza la inviolabilidad de domicilio prescribiendo en el inciso 1º que: *"ningún ingreso o registro podrá verificarse sin consentimiento de la persona que lo habita o resolución de autoridad competente. No obstante, puede ser allanado, en caso de urgencia, para impedir la comisión o impunidad de delitos o evitar daños graves a la persona o a la propiedad".*

En el mismo sentido anterior se enmarca el artículo 100, el cual dispone también en el inciso 1º que: *"toda persona tiene derecho a la inviolabilidad y al secreto de las comunicaciones, en especial de las postales, telegráficas y telefónicas, salvo resolución judicial".* Por su parte, el inciso 3º establece una sanción que al mismo tiempo opera como regla probatoria señalando que: *"las comunicaciones, los libros, comprobantes y documentos a que se refiere el presente artículo, que fueren violados o substraídos, no harán fe en juicio".* Finalmente, el artículo 100 establece un deber de secreto, disponiendo que: *"en todo caso, se guardará siempre el secreto respecto de los asuntos estrictamente privados que no tengan relación con el asunto objeto de la acción de la autoridad".* Entendemos que ese deber recae sobre los funcionarios que hayan tomado parte o conocimiento de diligencias ordenadas por un juez y que constituyan excepción a la regla general de la inviolabilidad de las comunicaciones.

En otro ámbito normativo, el Constituyente hondureño en el Capítulo III, Título I "Del Estado", se refiere al derecho internacional como fuente del derecho hondureño a través de los tratados internacionales. Lo anterior, se plasma en el inciso 2º del artículo 16 el cual dispone que: *"Los tratados internacionales celebrados por Honduras con otros estados, una vez que entran en vigor, forman parte del derecho interno".* Dos artículos más abajo señala que: *"en caso de conflicto entre el tratado o convención y la Ley prevalecerá el primero"* (Art. 18).

De las disposiciones recién transcritas, se desprende una clara voluntad del Constituyente en hacer primar las normas internacionales incorporadas al derecho interno por sobre las nacionales, en caso de conflicto. Esas normas cobran mucha importancia a la hora de interpretar y determinar los alcances de la Constitución. No satisfecho con lo anterior, el Constituyente más adelante establece en tres artículos normas que vienen a

[390] [En línea] < http://www.georgetown.edu/pdba/Constitutions/Honduras/hond82.html > [consulta: 3 de Noviembre 2002].

complementar lo prescrito, ahora desde una perspectiva de la protección de los Derechos Humanos. El primero de éstos es el artículo 59 y dispone que: *"la persona humana es el fin supremo de la sociedad y del Estado. Todos tienen la obligación de respetarla y protegerla. La dignidad del ser humano es inviolable. Para garantizar los derechos y libertades reconocidos por esta Constitución, créase la Institución del Comisionado Nacional de los Derechos Humanos. La organización, prerrogativa y atribuciones del Comisionado Nacional de los Derechos Humanos será objeto de una ley especial"* [391] . Luego, el artículo 63 preceptúa que: *"las declaraciones, derechos y garantías que enumera esta Constitución, no serán entendidos como negación de otras declaraciones, derechos y garantías no especificadas, que nacen de la soberanía, de la forma republicana, democrática y representativa de gobierno y de la dignidad del hombre".* Por último, el artículo 64 prescribe que: *"no se aplicarán leyes y disposiciones gubernativas o de cualquier otro orden, que regulen el ejercicio de las declaraciones, derechos y garantías establecidos en esta Constitución, si los disminuyen, restringen o tergiversan".*

Reseñadas y apreciadas las disposiciones constitucionales en su conjunto, podemos afirmar que el sistema de protección a los Derechos Humanos en Honduras se encuentra garantizado por disposiciones flexibles que no limitan la incorporación de nuevos derechos que nazcan de la *"inviolable" "dignidad del hombre".* En este sentido y, en atención a la incorporación de los tratados internacionales ratificados por Honduras en materia de Derechos Humanos, como lo es la Convención Americana o Pacto de San José de Costa Rica [392] , estimamos que los eventuales vacíos normativos de que pueda adolecer la Constitución en materia de intimidad o vida privada, pueden suplirse aplicando directamente de las normas internacionales sobre Derechos Humanos. Quedaría entregada en definitiva la no fácil tarea tanto al legislador como a los jueces, de deducir de esas normas un derecho como la autodeterminación informativa y fundar en éste una protección integral a los datos personales [393] .

[391] La respectiva normativa es la Ley Orgánica del Comisionado Nacional de los Derechos Humanos, establecida por el Decreto Nº 153-95. El artículo 1º de esa ley señala que el Comisionado Nacional es *"(…) una institución nacional, establecida para garantizar la vigencia de los derechos y libertades reconocidas en la constitución de la república y los tratados y convenios internacionales ratificados por Honduras (…)",* Decreto Nº 153-95. Esta ley puede consultarse sólo parcialmente [en línea] < http://ns.rds.org.hn/participacion_ciudadana/legislacion/leyes_secundarias/ley_organica_del_comisionado_derechos_humanos.html > [consulta: 20 de Marzo 2003].

[392] El Pacto de San José de Costa Rica fue firmado el 22 de Noviembre de 1969 y su ratificación se llevó a cabo el 9 de Mayo de 1977. [En línea] < http://www.oas.org/juridico/spanish/firmas/b-32.html > [consulta: 2 de Enero 2003].

[393] Cabe agregar que la Constitución hondureña consagra la Institución del Comisionado Nacional de los Derechos Humanos, lo cual muestra la importancia asignada a este tema por el Constituyente a pesar de que en la práctica las instituciones no funcionen como se quisiera. En relación a este tema se ha señalado en un informe sobre derechos humanos en Honduras que "conforme se agudiza la crisis de la inseguridad pública y el descontento social, el trabajo de los defensores de derechos humanos es más que urgente, pero al mismo tiempo se dificulta por la falta de garantías para el ejercicio del mismo. Las amenazas, el hostigamiento, los procesos judiciales, vigilancia, intervención de líneas telefónicas, son algunas de las acciones para acosar a quienes activan e investigan las violaciones a los derechos humanos del presente y del pasado (…)". [En línea] < http://www.derechos.org/nizkor/honduras/doc/cofadeh2.html > [consulta: 20 de Marzo 2003].

Por otra parte, debemos consignar que para la tutela de los derechos consagrados en la Constitución se establece por ésta la acción de amparo en el artículo 183, señalando que: *"el Estado reconoce la garantía de Amparo (...)".* Más adelante, dispone en el artículo 319 Nº 8 que la Corte Suprema de Justicia, tendrá las atribuciones para conocer de los recursos de amparo y revisión conforme a la ley.

Finalmente, la Constitución consagra la responsabilidad del Estado para el caso de cometerse daño por personal de éste en ejercicio de sus funciones. Estas reglas se analizarán en el punto Nº 9 relativo al régimen de responsabilidad.

En suma, puede señalarse que el ordenamiento constitucional hondureño no dispone de normas de protección a los datos personales. Creemos que a falta de éstas, deberá recurrirse principalmente a las disposiciones que consagran el derecho a la intimidad y a la vida privada (Artículos 76, 99 y 100) para fundamentar la protección a los derechos de los titulares de datos personales, la cual a falta de acción específica debería quedar cubierta, a lo menos, por la acción de amparo constitucional.

2.2 Protección Legal de los Datos Personales

A nivel legal, el ordenamiento jurídico hondureño no cuenta con una ley de protección de los datos personales. Tampoco hemos podido constatar reglas que protejan las informaciones sobre las operaciones bancarias realizadas por las personas. En materia tributaria las disposiciones existentes establecen ciertos deberes de secreto fiscal, pero conceptualizados de manera ambigua. A continuación se señalarán estas normas.

2.2.1) Ley de Instituciones del Sistema Financiero [394]

Revisada esta ley, llegamos a la conclusión de que curiosamente no existen disposiciones que consagren o establezcan el secreto bancario.

2.2.2) Código Tributario [395]

El artículo 49 de este Código prescribe ciertos deberes de información que obligan a las instituciones del sistema financiero (bancos) para con la administración tributaria, señalando al respecto que aquéllos tendrán las siguientes obligaciones: 1) Proporcionar a la Dirección Ejecutiva de Ingresos, con la periodicidad que ésta determine y previa autorización expresa de las correspondientes personas, información sobre las operaciones que hubiesen hecho con los cuentahabientes, tarjetahabientes, ahorrantes, usuarios, depositantes o clientes que hubiesen implicado movimientos de dinero, esta información podrá proporcionarse por medios magnéticos o electrónicos; 2) Proporcionar a la Dirección Ejecutiva de Ingresos información sobre las operaciones a que se refiere el

[394] **Esta ley puede ser consultada [en línea] < http://www.hondurasri.com/business_honduras_spa/leyes/leysis.html > [consulta: 20 de Marzo 2003].**

[395] **Éste puede ser consultado [en línea] < http://www.ciat.org/doc/docu/leg/cod/lhn_02_codigo_tributario_honduras.doc > [consulta: 20 de Marzo 2003].**

numeral anterior por orden de juez competente; y 3) Las demás que autoricen las leyes generales o especiales.Luego, en el inciso final de este artículo se señala que: *"la información a que se refieren los numerales 1) y 2) precedentes serán confidenciales, su entrega a terceras personas o su divulgación serán constitutivas del delito de abuso de autoridad y violación de los deberes de los funcionarios y se sancionará con reclusión de tres (3) años a seis (6) años".*

De lo prescrito por las normas, se desprende que los deberes de confidencialidad se circunscriben a las informaciones o datos sobre operaciones en dinero realizadas por los clientes o usuarios del sistema financiero, entregadas por las instituciones financieras a la Dirección Ejecutiva de Ingresos previamente autorizadas expresamente por los titulares de éstos, por resolución judicial o en los casos que autoricen las leyes.

En otra de sus normas, el Código Tributario señala en el artículo 61 que los agentes de retención o percepción de tributos *"así como aquéllas a quienes la autoridad tributaria competente les encomiende la realización de investigaciones de cualquier clase, el procesamiento de información tributaria, gestiones de cobro o percepción de impuestos, comprobaciones contables u otras tareas administrativas análogas, estarán obligadas a mantener reserva o confidencialidad sobre tales hechos". (…) "La violación de lo prescrito en esta norma será sancionada de conformidad con lo dispuesto por el artículo 215 del Código Penal".* En lo relativo a las sanciones, nos referiremos a ellas más adelante en el punto Nº 9 de este análisis.

3. Bienes Jurídicos Protegidos Por la Legislación de Datos Personales

Dada la inexistencia de normativa en materia de protección de datos personales en Honduras, no es posible referirnos a eventuales bienes jurídicos.

4. Principios Informativos de la Legislación de Protección de Datos Personales

Al respecto y, en atención a la carencia de normas en la materia, tampoco podemos hacer este análisis.

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

Dada la inexistencia de una ley general de protección de datos personales en el ordenamiento jurídico de Honduras, no nos detendremos en este punto.

6. Modelos de Tutela

En el ordenamiento jurídico hondureño no existen mecanismos específicos de tutela en

materia de protección de datos personales. A pesar de lo anterior y, principalmente en atención a la configuración constitucional del derecho a la intimidad, creemos que la única vía de tutela genérica a los datos personales sería la acción de amparo.

6.1 La Acción de Amparo

Esta acción se encuentra contemplada en el artículo 183 de la Constitución, el cual dispone en el inciso 1º que: *"el Estado reconoce la garantía de Amparo"*. Luego, en el inciso 5º agrega que: *"el Recurso de Amparo se interpondrá de conformidad con la Ley"*. Al respecto, debemos hacer presente que no tenemos información relativa a esa ley, por lo que sólo nos referiremos a lo señalado en la Constitución.

6.1.1) Procedencia de la Acción

La Constitución dispone en el artículo 183, que podrá interponerse esta acción: *"1. Para que se le mantenga o restituya en el goce o disfrute de los derechos o garantías que la constitución establece; (…) 2. Para que se declare en casos concretos que una ley, resolución, acto o hecho de autoridad, no obliga al recurrente ni es aplicable por contravenir, disminuir o tergiversar cualesquiera de los derechos reconocidos por esta Constitución".* Nos parece que esta segunda causal, más bien correspondería a una de acción de inconstitucionalidad que de un amparo propiamente tal.

6.1.2) Legitimación Activa

El Constituyente señala al respecto que: *"toda persona agraviada o cualquiera otra en nombre de ésta, tiene derecho a interponer recurso de amparo"* (Art. 183).

6.1.3) Legitimación Pasiva

En cuanto a la legitimación pasiva, la Constitución no señala contra quien puede dirigirse. A pesar de ello, puede deducirse que a lo menos podría entablarse en contra de cualquier *"autoridad".* En cuanto a los particulares o privados como eventuales sujetos pasivos del amparo, no podemos pronunciarnos pues no conocemos la ley que regula el amparo. A pesar de ello, nos aventuramos a pensar que en virtud del artículo 25.1 de la Convención Americana de Derechos Humanos –la cual se ha incorporado al ordenamiento jurídico hondureño- sí podría dirigirse esta acción en contra de un particular.

6.1.4) Competencia

El artículo 319 Nº 8 de la Constitución, dispone que: *"la Corte Suprema de Justicia"*, tendrá las atribuciones para conocer de los recursos de amparo y revisión conforme a la ley.

6.1.5) Procedimiento Aplicable

En esta materia no tenemos información al respecto.

6.1.6) La Sentencia

Respecto de los requisitos y los efectos de la sentencia de amparo, tampoco tenemos información al respecto.

6.2 Otras Acciones

Al parecer no existirían otras acciones que pudieran tutelar los bienes jurídicos que subyacen a la protección de los datos personales.

7. Mecanismos de Control

Dada la inexistencia de legislación protectora de los datos personales en el ordenamiento jurídico hondureño, tampoco es posible que nos refiramos a éstos.

8. Transmisión Internacional de Datos

Honduras no cuenta con disposiciones especiales en materia de transmisión internacional de datos, por lo que no nos detendremos en este punto.

9. Régimen de Responsabilidad

En materia de responsabilidad no existe ley especial que se ocupe de esta materia. Sin embargo, podemos mencionar algunas normas particulares que establecen sanciones para ciertas conductas relacionadas con la afectación del derecho a la intimidad o vida privada.

9.1 Responsabilidad Administrativa

En materia de sanciones administrativas sólo podemos referirnos a aquellas normas que la Constitución establece, y en las cuales encarga a la ley el desarrollo y regulación de la responsabilidad administrativa de los funcionarios públicos, pues no disponemos de información particular respecto de las normas legales respectivas.

La Constitución Política de Honduras, dispone en el artículo 321 que los servidores del Estado no tienen más facultades que las que expresamente les confiere la ley, agregando que: *"Todo acto que ejecuten fuera de la ley es nulo e implica responsabilidad".* Luego, el artículo 327 señala que: *"La ley regulará la responsabilidad civil del Estado, así como la responsabilidad civil solidaria, penal y administrativa de los servidores del Estado".* El artículo 326 por su parte dispone que: *"Es pública la acción para perseguir a los infractores de los derechos y garantías establecidas en esta Constitución, y se ejercitará sin caución ni formalidad alguna y por simple denuncia".*

Por lo tanto, en esta materia es menester remitirse a los estatutos jurídicos particulares de los funcionarios del Estado y, en su defecto al estatuto común administrativo, cuyas disposiciones desconocemos.

9.2 Responsabilidad Civil

En materia civil no tenemos conocimiento de las reglas generales de la responsabilidad por daño. A pesar de lo anterior, puede deducirse de la Constitución que la regla general sería la responsabilidad por culpa, en atención a que el artículo 324 señala que: *"si el servidor público en el ejercicio de su cargo, infringe la ley en perjuicio de particulares, será civil y solidariamente responsable junto con el Estado o con la institución estatal a cuyo servicio se encuentre, sin perjuicio de la acción de repetición que éstos pueden ejercitar contra el servidor responsable, en los casos de culpa o dolo".* Si bien esta norma es aplicable al Estado y a los funcionarios públicos, de ella se desprenden algunos de los elementos básicos para configurar la responsabilidad civil extracontractual, como lo son el daño o perjuicio y la culpa o dolo en el actuar del agente.

9.3 Responsabilidad Penal

En lo relativo a las sanciones penales, solamente nos referiremos al delito de violación de la reserva tributaria y algunos delitos contra la intimidad y vida privada contemplados en el Código Penal.

9.3.1) Código Tributario

En materia tributaria, el artículo 49 del Código del ramo tipifica como delito la violación del deber de confidencialidad que pesa sobre los funcionarios de la Dirección Ejecutiva de Ingresos respecto de la información que es entregada a ese organismo por las Instituciones Financieras, sobre las operaciones en dinero realizadas por los clientes de éstas, disponiendo al efecto que: *"La información a que se refieren los numerales 1) y 2) precedentes serán confidenciales, su entrega a terceras personas o su divulgación serán constitutivas del delito de abuso de autoridad y violación de los deberes de los funcionarios y se sancionará con reclusión de tres (3) años a seis (6) años".*

9.3.2) Código Penal

Dentro del Código Penal hondureño se insertan algunas típicas figuras que sancionan delitos que atentan en general contra los bienes jurídicos intimidad y vida privada. Estos serán señalados a continuación.

a) Allanamiento de morada:

Artículo 202.- *"El particular que entrare en morada ajena contra la voluntad de su morador o habiendo entrado con el consentimiento expreso o tácito del mismo, permaneciere en ella a pesar de habérsele conminado a abandonarla, será sancionado con tres meses a un año de reclusión (…) Si los hechos anteriores se ejecutaren con violencia o intimidación o simulación de autoridad, la pena será de uno a tres años de reclusión".*

Artículo 203.- *"El agente de la autoridad, funcionario o empleado público que allane una casa sin cumplir los requisitos prescritos por la ley, será sancionado con dos (2) a cinco (5) años de reclusión e inhabilitación especial (…)".*

b) Violación y revelación de secretos:

Artículo 214.- *"Quien sin la debida autorización judicial, con cualquier propósito, se apoderare de los papeles o correspondencia de otro, intercepta o hace interceptar sus comunicaciones telefónicas, telegráficas, soportes electrónicos o computadoras, facsimilares o de cualquier otra naturaleza, incluyendo las electrónicas, será sancionado con seis (6) a ocho (8) años si fuere particular y de ocho (8) a doce (12) años si se tratare de un funcionario o empleado público".*

Creemos que la disposición anterior podría ser la más cercana a una protección directa de la vida privada amenazada por sofisticados medios de ataque.

Artículo 215.-*"Quien revela sin justa causa o emplea en provecho propio o ajeno un secreto del que se ha enterado por razón de su oficio, empleo, profesión o arte y con ello ocasiona perjuicio a alguien, será sancionado con reclusión de tres (3) a seis (6) años".*

10. Conclusiones

Del análisis al ordenamiento jurídico hondureño, se constata una inexistencia de normativa específica que se ocupe de la protección de los datos personales. Ni la Constitución ni la ley consagran un derecho a la protección de datos o autodeterminación informativa, con lo cual la tutela a los datos personales debe fundarse en normas constitucionales que guarden relativa proximidad con algunos de los bienes jurídicos en los que generalmente se ha basado esa protección. En el caso de estudio, creemos que el derecho a la intimidad y el derecho a la vida privada aparecen como los más próximos a falta de un bien jurídico como la autodeterminación informativa. Por ahora, deberá buscarse su tutela a través de la acción constitucional de amparo.

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN MÉXICO

1. Generalidades

El sistema jurídico mexicano no contempla una protección general a los datos personales. Ni la Constitución ni la ley se ocupan de establecer reglas específicas en esta materia, por lo que el estudio que sigue está centrado principalmente, a nivel constitucional, en el análisis de las reglas que puedan brindar protección a los bienes jurídicos intimidad y vida privada y, en materia legal, al análisis de algunas normas sectoriales específicas que contemplan reglas de protección a los datos personales. De éstas algunas establecen derechos de acceso y rectificación, de carácter informal o extrajudicial. No obstante lo dicho, en la actualidad se encuentran en discusión parlamentaria dos Proyectos de Ley presentados el año 2001 que pretenden salvar la

falta de legislación al respecto.

2. Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional

La Constitución mexicana de 1917 [396] no dispone de normas especiales que se ocupen de la protección a los datos personales. Tampoco existe de manera explícita un reconocimiento de los derechos a la intimidad y a la vida privada, más bien éstos deben deducirse de algunas de sus disposiciones. Al respecto, se ha dicho que "en el caso de México, no contamos con una norma jurídica que expresa y de manera directa reconozca los mencionados derechos a la intimidad, o bien, de la vida privada" [397] . Sin embargo, cabe anotar que este país es parte de la Convención Americana de Derechos Humanos, con lo cual estimamos se supliría en definitiva esa falta de previsión por el Constituyente [398] . A continuación, se señalarán las disposiciones relacionadas con la protección de la vida privada e intimidad pertinentes, las que han servido de base para la regulación a nivel legal de ciertos ámbitos específicos en materia de protección de datos personales.

El artículo 7 del texto constitucional se refiere al derecho a la vida privada como uno de los límites al derecho a la libertad de expresión, prescribiendo que es inviolable la libertad de escribir y publicar escritos sobre cualquier materia. Se añade que ninguna ley ni autoridad puede establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta, la cual *"(…) no tiene más límites que el respeto a la vida privada, a la moral y a la paz pública. En ningún caso podrá secuestrarse la imprenta como instrumento del delito".*

Más adelante, el artículo 16 reconoce la inviolabilidad de la persona, su domicilio y comunicaciones, disponiendo al respecto en su inciso 1º que: *"n adie puede ser molestado en persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal de procedimiento (…). En toda orden de cateo, que sólo la autoridad judicial podrá expedir, y que será escrita, se expresará el lugar que ha de inspeccionarse, la persona o personas que hayan de aprehenderse y los objetos que se buscan, a lo que únicamente debe limitarse la diligencia (…). La autoridad administrativa podrá practicar visitas domiciliarias únicamente para cerciorarse de que se han cumplido los reglamentos sanitarios y de policía; y exigir la exhibición de los libros y papeles indispensables para comprobar que se han acatado las disposiciones fiscales, sujetándose, en estos casos, a las leyes respectivas y a las formalidades prescritas para los cateos".* El inciso 2º de este artículo agrega que: *"la correspondencia que bajo cubierta circule por las estafetas estará libre de*

396 [En línea]< http://www.georgetown.edu/pdba/Constitutions/Mexico/mexico1917.html > [consulta: 17 de Octubre 2002].

397 Ríos Estavillo, Juan José: *"El Hábeas Data: ¿Algún día en México?".* [En línea] < http://legal.terra.com.mx/Legal/EnLinea/Columnas/articulo/31default.asp > [consulta: 15 de Noviembre 2002].

398 [En línea] < http://www.oas.org/juridico/spanish/firmas/b-32.html > [consulta: 20 de Marzo 2003].

todo registro, y su violación será penada por la ley".

En otro ámbito, el artículo 6 de la Constitución señala que: *"l a manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; el derecho a la información será garantizado por el Estado".*

Para algunos autores, la disposición anterior serviría de fundamento constitucional tanto al derecho a ser informado y a rectificar la información, como al derecho de acción de hábeas data [399] . En nuestra opinión, una interpretación como la anterior sin mayores explicaciones nos parece un tanto aventurada. La consagración del derecho a la información se engarza principalmente con el derecho a la libertad de expresión, el cual, salvo el derecho de réplica, no confiere ningún poder de control sobre la integridad, exactitud, oportunidad y legalidad con que se usa por terceros la propia información.

Por otro lado, el artículo 8 que reconoce el derecho de petición señala que: *"los funcionarios y empleados públicos respetarán el ejercicio del derecho de petición, siempre que ésta se formule por escrito, de manera pacífica y respetuosa; pero en materia política sólo podrán hacer uso de ese derecho los ciudadanos de la República. A toda petición deberá recaer un acuerdo escrito de la autoridad a quien se haya dirigido, la cual tiene obligación de hacerlo conocer en breve término al peticionario".* En esta disposición eventualmente podría fundarse una acción de hábeas data con el fin de acceder a los registros o bancos de datos en poder de organismos del Estado.

Finalmente en materia constitucional, debemos mencionar la disposición que consagra la acción de amparo en el ordenamiento jurídico mexicano. Al respecto, el artículo 103 dispone que los Tribunales de la Federación resolverán toda controversia que se suscite; *"I. Por leyes o actos de la autoridad que violen las garantías individuales (…)".* Más adelante, el artículo 107 señala que la acción de amparo se sujetará a los procedimientos y formas del orden jurídico que determine la ley, según las bases que se indican. Éstas se reseñarán más adelante al analizar esta acción en el punto Nº 6.

En suma, podemos afirmar que la Constitución mexicana no prevé normas encaminadas a la protección de los datos personales. Tampoco reconoce directamente el derecho a la intimidad y el derecho a la vida privada como derechos fundamentales, lo cual, sin embargo, puede deducirse de otras disposiciones, en especial de la Convención Americana de Derechos Humanos, la cual ha sido ratificada por México. En tanto no exista una consagración constitucional del derecho a la protección de datos y su respectiva garantía, sea que aquél se funde en el derecho a la autodeterminación informativa, sea que se haga en la intimidad o en la vida privada, la protección de los datos personales en definitiva queda entregada -como en otras legislaciones- a la acción de amparo de los derechos y garantías constitucionales.

2.2 Protección Legal de los Datos Personales

En el ámbito legal, el ordenamiento jurídico mexicano no cuenta con una ley de

[399] Del villar "et al", *op. cit.*, [en línea] pág. 121. Esto se desprende del cuadro comparativo señalado por los autores al tratar los fundamentos constitucionales.

protección de datos personales. Sólo se han dictado por el legislador normas sectoriales, algunas más desarrolladas que otras en cuanto a la protección de los datos. Cabe destacar dentro de éstas a la Ley Federal de Protección a los Consumidores y a la Ley que regula las Sociedades de Información Crediticia. Esta última, la hemos considerado como un estatuto sectorial complejo, es decir, un cuerpo legal que regula un área muy específica, como lo es el mercado de la información crediticia, a través de normas que evidenciarían una eventual influencia de principios y reglas internacionales en materia de protección de datos personales, lo que la diferencia de un simple estatuto sectorial en materia de protección de datos, como lo sería la ley de bancos que establece sin más normas de secreto bancario.

Finalmente, debemos señalar que la falta de legislación en la materia ya ha sido asumida por los congresistas mexicanos, los cuales han impulsado la discusión de este tema en el seno legislativo. En este sentido se enmarcan dos Proyectos de Ley presentados el año 2001, los cuales pretenden regular todo el instituto de manera sistemática y acorde a los estándares internacionales en la materia [400] A continuación, se revisarán las normas legales que regulan ciertos aspectos en materia de protección de datos personales.

2.2.1) Ley de Imprenta [401]

Esta ley del año 1917, en general tiene como finalidad la protección de la vida privada y honra de las personas. En el artículo 9, pueden encontrarse las primeras aproximaciones a la protección del bien jurídico vida privada al señalar que queda prohibido, entre otras acciones [402] : *(…)*:*II.-Publicar en cualquier tiempo sin consentimiento de todos los interesados, los escritos, actas de acusación y demás piezas de los procesos que se sigan por los delitos de adulterio, atentados al pudor, estupro, violación y ataques a la*

400 La primera iniciativa fue presentada por el Senador Antonio García Torres el 14 de Febrero de 2001 y puede ser consultada [en línea] < http://telematica.cicese.mx/propuestaley/Leydatos/ > [consulta: 15 de Diciembre 2002]. La segunda iniciativa es de Septiembre del mismo año y fue presentada por el Diputado Miguel Barbosa Huerta. Esta iniciativa puede ser consultada [en línea] < http://www.cddhcu.gob.mx/servicios/datorele/cmprtvs/1po2/set/2.htm > [consulta: 22 de Noviembre 2002].

401 **[En línea] < http://www.cddhcu.gob.mx/leyinfo/pdf/40.pdf > [consulta: 22 de Noviembre 2002].**

402 Otros numerales del artículo señalan que también queda prohibido: VI.-Publicar los nombres de las personas que formen un jurado, el sentido en que aquéllas hayan dado su voto y las discusiones privadas que tuvieren para formular su veredicto; VII.-Publicar los nombres de los soldados o gendarmes que intervengan en las ejecuciones capitales; VIII.-Publicar los nombres de los Jefes u Oficiales del Ejército o de la Armada y Cuerpos Auxiliares de Policía Rural, a quienes se encomiende una comisión secreta del servicio; IX.-Publicar los nombres de las víctimas de atentados al pudor, estupro o violación; X.-Censurar a un miembro de un jurado popular por su voto en el ejercicio de sus funciones; XI.-Publicar planos, informes o documentos secretos de la Secretaría de Guerra y los acuerdos de ésta relativos a movilización de tropas, envíos de pertrechos de guerra y demás operaciones militares, así como los documentos, acuerdos o instrucciones de la Secretaría de Estado, entre tanto no se publiquen en el Periódico Oficial de la Federación o en Boletines especiales de las mismas Secretarías; XII.-Publicar las palabras o expresiones injuriosas u ofensivas que se viertan en los Juzgados o Tribunales, o en las sesiones de los cuerpos públicos colegiados.

vida privada; III.-Publicar sin consentimiento de todos los interesados las demandas, contestaciones y demás piezas de autos en los juicios de divorcio, reclamación de paternidad, maternidad o nulidad de matrimonio, o diligencia de reconocimiento de hijos y en los juicios que en esta materia puedan suscitarse; IV.-Publicar lo que pase en diligencias o actos que deban ser secretos por mandato de la ley o por disposición(…)". Puede decirse que, en general, esta normativa busca tutelar la honra y vida privada de las personas, salvo en aquellas disposiciones en que el deber de secreto se ha establecido en atención a intereses generales de la nación.

2.2.2) Ley de Instituciones de Crédito [403]

Según esta Ley, su objeto es: regular el servicio de banca y crédito; la organización y funcionamiento de las instituciones de crédito; las actividades y operaciones que las mismas pueden realizar; su sano y equilibrado desarrollo; la protección de los intereses del público; y los términos en que el Estado ejercerá la rectoría financiera del Sistema Bancario Mexicano(Art. 1º).

En lo que a nuestro estudio compete, debemos decir que dentro del Título Sexto denominado "De la Protección de los Intereses del Público", la ley establece ciertas normas que imponen deberes de secreto y responsabilidades en caso de violarse éstos. Así, se señala por el artículo 17 que: *"Las instituciones de crédito en ningún caso podrán dar noticias o información de los depósitos, servicios o cualquier tipo de operaciones, sino al depositante, deudor, titular o beneficiario que corresponda, a sus representantes legales o a quienes tenga otorgado poder para disponer de la cuenta o para intervenir en la operación o servicio, salvo cuando las pidieren, la autoridad judicial en virtud de providencia dictada en juicio en el que el titular sea parte o acusado y las autoridades hacendarias federales, por conducto de la Comisión Nacional Bancaria, para fines fiscales. Los empleados y funcionarios de las instituciones de crédito serán responsables, en los términos de las disposiciones aplicables, por violación del secreto que se establece y las instituciones estarán obligadas en caso de revelación del secreto, a reparar los daños y perjuicios que se causen".* El inciso 2º de este artículo agrega que el deber de secreto *"en forma alguna afecta la obligación que tienen las instituciones de crédito de proporcionar a la Comisión Nacional Bancaria, toda clase de información y documentos que, en ejercicio de sus funciones de inspección y vigilancia, les solicite en relación con las operaciones que celebren y los servicios que presten".*

De las normas anteriores queda claro que el legislador mexicano le otorga máxima importancia para el buen funcionamiento del sistema financiero el que se respete la confidencialidad de "cualquier tipo de operación", es decir, tanto activas como pasivas, que se realicen a través de ese mercado, vislumbrándose tras estas disposiciones tanto el orden público económico como la protección de la vida privada de las personas.

2.2.3) Código Fiscal de la Federación [404]

La ley tributaria mexicana consagra la reserva fiscal o tributaria en los artículos 63 y 69.

[403] **[En línea] < http://www.shcp.gob.mx/servs/normativ/leyes/l_ic.html > [consulta: 22 de Noviembre 2002].**

El primero de éstos, dispone entre otras cosas que las autoridades fiscales estarán obligadas a mantener la confidencialidad de la información proporcionada por terceros independientes que afecte su posición competitiva. A su turno, el artículo 69 señala que: *"el personal oficial que intervenga en los diversos tramites relativos a la aplicación de las disposiciones tributarias estará obligado a guardar absoluta reserva en lo concerniente a las declaraciones y datos suministrados por los contribuyentes o por terceros con ellos relacionados, así como los obtenidos en el ejercicio de las facultades de comprobación".* La segunda parte de este párrafo establece las excepciones al deber de reserva mencionado, disponiendo que: "*dicha reserva no comprenderá los casos que señalen las leyes fiscales y aquéllos en que deban suministrarse datos a los funcionarios encargados de la administración y de la defensa de los intereses fiscales federales, a las autoridades judiciales en procesos del orden penal o a los tribunales competentes que conozcan de pensiones alimenticias, o en el supuesto previsto en el articulo 63 de este Código. Dicha reserva tampoco comprenderá la información relativa a los créditos fiscales exigibles de los contribuyentes, que las autoridades fiscales proporcionen a las sociedades de información crediticia que obtengan autorización de la secretaria de hacienda y crédito público de conformidad con la ley de agrupaciones financieras".* Más adelante, el inciso 3º del artículo 69 señala que: *"solo por acuerdo expreso del secretario de hacienda y crédito publico se podrán publicar los siguientes datos por grupos de contribuyentes: nombre, domicilio, actividad, ingreso total, utilidad fiscal o valor de sus actos o actividades y contribuciones acreditables o pagadas".* Esta última parte no es clara, pues no se señalan las condiciones en que puede ejercerse la facultad de publicar los datos del los contribuyentes, ni la finalidad de ello.

En suma, la legislación tributaria mexicana establece como regla general el deber de reserva que pesa sobre el personal fiscal de la Administración Tributaria, respecto de las informaciones suministradas por los contribuyentes u obtenidas a través de la fiscalización de ese organismo. Con todo el margen de excepciones es también bastante amplio.

2.2.4) Ley Federal de Protección al Consumidor [405]

La ley mexicana de protección al consumidor, dentro del Capitulo I intitulado "Disposiciones Generales", dedica algunos artículos a la regulación de la recolección, tratamiento e información de los datos personales con fines de mercadeo, por parte de empresas de investigación de crédito o de mercado. En el marco de las obligaciones establecidas para estas empresas se prescribe lo siguiente: *"las empresas dedicadas a la investigación de crédito o a la recopilación de información sobre consumidores con fines mercadotécnicos están obligadas a informar gratuitamente a cualquier persona que lo solicite si mantienen información acerca de ella. De existir dicha información, deberán ponerla a su disposición si ella misma o su representante lo solicita, e informar acerca de*

[404] **[En línea] < http://www.ciat.org/doc/docu/leg/cod/lmx_02_codigo_fiscal_mexico.doc > [consulta: 26 de Diciembre 2002].**

[405] **[En línea] < http://www.cddhcu.gob.mx/leyinfo/113/ > [consulta: 26 de Diciembre 2002].**

que información han compartido con terceros y la identidad de esos terceros, así como las recomendaciones que hayan efectuado. La respuesta a cada solicitud deberá darse dentro de los 30 días siguientes a su presentación. En caso de existir alguna ambigüedad o inexactitud en la información, la empresa deberá efectuar de inmediato las correcciones que fundadamente indique la persona afectada, e informar las correcciones a los terceros que hayan recibido dicha información" (Art. 16).

La disposición anterior claramente consagra un derecho de acceso y rectificación de la información sobre los consumidores contenida en las bases de datos o archivos de las empresas de investigación de mercado o de crédito. El ejercicio de este derecho es de carácter informal o extrajudicial, pues se realiza directamente ante la empresa respectiva sin intervención de juez alguno. La respuesta a la solicitud de información debe entregarse dentro de 30 días contados desde la presentación de ésta por el consumidor, y debe ser exacta, sin ambigüedades, y señalar si se tiene información respecto del solicitante; en caso afirmativo ponerla a disposición de él. Conjuntamente, debe señalarse qué tipo de información se ha compartido con terceros, sus identidades y las recomendaciones efectuadas a esos terceros.

A su turno, el artículo 18 establece una regla muy importante, limitativa de la actividad de recolección de datos personales. Esta disposición señala que: *"queda prohibido a las empresas dedicadas a la investigación de crédito o de mercadotecnia y a sus clientes, utilizar la información con fines diferentes a los crediticios o mercadotécnicos".* Esta regla se enmarca claramente dentro del principio de la finalidad en el tratamiento de los datos personales.

Finalmente, debemos hacer presente que la Ley prevé sanciones pecuniarias (multas) para aquellos proveedores que no respeten sus disposiciones. Éstas serán analizadas más adelante en el punto Nº 9.1, relativo a las sanciones administrativas.

En suma, podemos afirmar que la Ley Federal de Protección al Consumidor ha previsto reglas que se ocupan de la protección a los datos personales de los consumidores circunscrita a situaciones específicas, como lo es la defensa de éstos frente a las actividades de las empresas de mercadotecnia y de investigación de crédito, las que realizan tratamiento de datos personales hasta ahora sin más regulación que la anterior. Si bien estas normas no son suficientes para lograr una protección más general a los datos personales, creemos que pueden servir de base interpretativa para solucionar casos no regulados por la ley en otros ámbitos. Por otra parte, queda en la duda el escenario jurídico que se presentaría en el caso de no prosperar el ejercicio del derecho de acceso y corrección de los datos personales ante las empresas señaladas, pues si bien pueden ser sancionadas pecuniariamente si se niegan a entregar o a corregir la información, al parecer no podría coaccionarse administrativamente a esas empresas a realizar esas acciones. Creemos que de darse la situación anterior, a falta de regla expresa, abriría la posibilidad de recurrir de amparo ante la instancia respectiva. Sin embargo, nos toparíamos en principio con un impedimento legal, pues la Ley de Amparo no contempla como sujetos pasivos de la acción a los particulares. Con todo, pensamos que igualmente sería posible solicitar la tutela judicial basada en el artículo 25.1 del Pacto de San José de Costa Rica.

Ley de Protección y Defensa al Usuario de Servicios Financieros [406]

Esta ley tiene por objeto *"la protección y defensa de los derechos e intereses del público usuario de los servicios financieros, que prestan las instituciones públicas, privadas y del sector social debidamente autorizadas, así como regular la organización, procedimientos y funcionamiento de la entidad pública encargada de dichas funciones"* (Artículo1º). Para tales efectos, se dispuso la creación de una institución pública denominada Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, la cual tiene facultad para sancionar administrativamente a las instituciones financieras que violen las disposiciones de esta ley. En este sentido, dicha Comisión operaría como un órgano de control en ese específico ámbito de regulación.

Dentro de los ámbitos regulados que interesan a nuestro estudio, cabe mencionar ciertos deberes de secreto impuestos a la propia Comisión y a sus funcionarios respecto de las informaciones sobre operaciones financieras realizadas por terceros, y que lleguen a conocimiento de éstos en razón de su oficio. Al efecto, el artículo 13 dispone que: *"la Comisión Nacional deberá guardar estricta reserva sobre la información y documentos que conozca con motivo de su objeto, relacionada con los depósitos, servicios o cualquier tipo de operaciones llevadas a cabo por las Instituciones Financieras. Solamente en el caso de que dicha información o documentos sean solicitados por la autoridad judicial, en virtud de providencia dictada en juicio en el que el titular sea parte, la Comisión Nacional estará legalmente facultada para proporcionarlos"*

Luego, el artículo 14 prescribe que: *"los servidores públicos de la Comisión Nacional serán responsables, en los términos de las disposiciones aplicables, por violación de la reserva o secreto a que se refiere el artículo anterior"*. Por último, el artículo 15 establece una regla de responsabilidad para el caso de violarse las disposiciones anteriores. Ésta se analizará en el punto Nº 9.2 relativo a las sanciones civiles.

En suma, de lo recién señalado se entiende que la ley sólo ha extendido la regla del secreto financiero o bancario tanto a la entidad administrativa (Comisión) como a sus funcionarios, los cuales velan por los derechos de los usuarios de los servicios financieros. Con ello se logra una regulación concordante en la materia.

2.2.6) Ley para regular las Sociedades de Información Crediticia [407]

Esta reciente ley (en adelante LSIC) tiene por objeto regular la constitución y operación de las Sociedades de Información Crediticia (en adelante SIC) [408] . Según el artículo 5º, estas SIC son las únicas autorizadas legalmente para la prestación de servicios consistentes en la recopilación, manejo y entrega o envío de información relativa al historial crediticio de personas físicas y morales, así como también a operaciones

406 [En línea] < http://www.condusef.gob.mx/marco_juridico/ley_proteccion_defensa.htm > [consulta: 22 de Noviembre 2002].

407 Esta ley fue publicada en el Diario Oficial de la Federación el 15 de Enero de 2002 Su texto puede ser consultado [en línea] < http://www.shcp.gob.mx/servs/normativ/leyes/l_rsic.html > [consulta: 22 de Noviembre 2002].

408 El objeto de la ley está definido de esta forma en el artículo 1º, el cual además agrega que *"(…) sus disposiciones son de orden público y de observancia general en todo el territorio mexicano".*

crediticias y otras de naturaleza análoga que éstas realicen con Entidades Financieras y Empresas Comerciales [409] . Por lo tanto, estas sociedades son empresas privadas que recopilan y tratan información relativa al comportamiento comercial de las personas. Los datos con que se nutren estas SIC son proporcionados por los agentes del sistema financiero y las empresas comerciales, los que una vez procesados y consolidados son entregados a su vez como información a quienes facilitaron esos datos (bancos y empresas comerciales) y, a los propios titulares de éstos materializados en los denominados reportes de crédito. Ahora bien, para analizar las disposiciones de esta extensa ley, en lo atingente a la protección de los datos personales, dividiremos la exposición por materias.

a) Las Sociedades de Información Crediticia (SIC)

La LSIC, luego de señalar el objeto de ésta, dispone en el inciso 2º del artículo 5º que para los efectos de esta ley, "*no se considerará que existe violación al Secreto Financiero cuando los Usuarios proporcionen información sobre operaciones crediticias u otras de naturaleza análoga a las Sociedades, así como cuando éstas compartan entre sí información contenida en sus bases de datos o proporcionen dicha información a la Comisión. Tampoco se considerará que existe violación al Secreto Financiero cuando las Sociedades proporcionen dicha información a sus Usuarios, en términos del Capítulo III de este Título Segundo, o cuando sea solicitada por autoridad competente, en el marco de sus atribuciones"*.

Lo señalado anteriormente es una regla básica para que pueda legalmente funcionar el mercado de la información crediticia, cual es, la libertad de información o libertad de circulación de datos personales referidos a *"operaciones crediticias u otras de naturaleza análoga"* entre las SIC y los Usuarios (bancos e instituciones financieras y empresas comerciales), quienes por regla general están sujetos al deber de secreto. La importancia de la libertad de información, radica en que ésta permite el funcionamiento de las SIC, las cuales para elaborar los informes de crédito deben contar con datos que deben ser entregados directamente por los Usuarios del sistema. Es decir, se establece una

[409] Para la comprensión de esta ley se señalaran algunos de los términos usados por el legislador y su significado legal que para nuestro análisis interesan. Al respecto, el artículo 2º dispone que para los efectos de esta ley, se entenderá por: *"(…) II.* ***Cliente*** *, en singular o plural, cualquier persona física o moral que solicite o sobre la cual se solicite información a una Sociedad; III.* ***Comisión*** *, la Comisión Nacional Bancaria y de Valores; (…) VI* ***. Reporte de Crédito*** *, en singular o plural, la información formulada documental o electrónicamente por una Sociedad para ser proporcionada al Usuario que lo haya solicitado en términos de esta ley, que contiene el historial crediticio de un Cliente, sin hacer mención de la denominación de las Entidades Financieras o Empresas Comerciales acreedoras; VII.* ***Reporte de Crédito Especial*** *, en singular o plural, la información formulada documental o electrónicamente por una Sociedad que contiene el historial crediticio de un Cliente que lo solicita, en términos de esta ley y que incluye la denominación de las Entidades Financieras o Empresas Comerciales acreedoras; VIII.* ***Secretaría,*** *la Secretaría de Hacienda y Crédito Público; IX* ***. Secreto Financiero*** *, al que se refieren los artículos 117 y 118 de la Ley de Instituciones de Crédito, 25 de la Ley del Mercado de Valores, 55 de la Ley de Sociedades de Inversión y 34 de la Ley de Ahorro y Crédito Popular, así como los análogos contenidos en las demás disposiciones legales aplicables; X* ***. Sociedad*** *, en singular o plural, la sociedad de información crediticia; XI.* ***UDIS*** *, las unidades de inversión, y XII.* ***Usuario*** *, en singular o plural, las Entidades Financieras o las Empresas Comerciales que proporcionen información o realicen consultas a la Sociedad"* (negrita nuestra).

cooperación mutua entre Usuarios y SIC. Sin embargo, esa cooperación basada en la libertad de flujo de información crediticia, ciertamente crea un riesgo para los clientes del sistema financiero, los cuales se verán expuestos a que sus datos personales circulen libremente entre los bancos y las SIC. Ante ese riesgo y, con la finalidad de evitar la fuga y mal uso de esos datos personales, la ley ha establecido consecuentemente deberes positivos que se traducen en la adopción de medidas de seguridad y control de parte de las SIC para evitar el uso indebido de la información. Conjuntamente con éstos, ha prescrito deberes de estricta reserva de la información, los cuales obligan tanto a las SIC como a sus funcionarios que en ejercicio de sus cargos tomen conocimiento datos que por regla general están afectos al secreto financiero.

b) Requisitos para el funcionamiento de las Sociedades de Información Crediticia

Dada la particularidad del mercado de la información crediticia, el legislador se ha encargado de reglamentar el desempeño de las SIC exigiendo ciertos planes de organización y funcionamiento para quienes quieran entrar en ese mercado A este respecto, el artículo 7 de la LSIC señala que la solicitud para constituirse y operar como Sociedad deberá contener lo siguiente: *"(…) V. Programa general de funcionamiento, que comprenda por lo menos: 1. La descripción de los sistemas de cómputo y procesos de recopilación y manejo de información; 2. Las características de los productos y servicios que prestarán a los Usuarios y a los Clientes; 3. Las políticas de prestación de servicios con que pretenden operar; 4. Las medidas de seguridad y control a fin de evitar el manejo indebido de la información; 5. Las bases de organización (…)"*. De lo dispuesto por la LSIC, se desprende un interés por circunscribir precisamente la actividad de estas Sociedades, así como también hacer públicos los métodos que se utilizarán para llevar a cabo esa actividad y las medidas de seguridad y de control que se emplearán para evitar la fuga de información confidencial o su mal uso.

En el mismo sentido anterior, se enmarcan las disposiciones contenidas en el Capitulo II, titulado "De la Base de Datos". Dentro de éste, el artículo 21 señala que: *"las Sociedades establecerán manuales operativos estandarizados que deberán ser observados por los diferentes tipos de Usuarios, para llevar a cabo el registro de información en su base de datos, así como para la emisión, rectificación e interpretación de los Reportes de Crédito y Reportes de Crédito Especiales que la Sociedad emita. (…) Los manuales operativos citados en el párrafo anterior, deberán ser aprobados por el consejo de administración de la Sociedad".*

Con la regla anterior, se busca homogeneizar el funcionamiento del sistema, lo que apareja la ventaja de reducir los costos de transacción y hacer más expedito el funcionamiento del mercado de la información crediticia. Lo dicho, nos muestra también la intención del legislador de fomentar la autorregulación en esta materia.

c) Medidas de seguridad

El artículo 22 por su parte, se refiere tanto a las medidas de seguridad que deben adoptar las SIC para poder desempeñarse en el mercado, como al uso indebido de la

información. En relación a lo primero, se prescribe en el inciso 1º que: *"la Sociedad deberá adoptar las medidas de seguridad y control que resulten necesarias para evitar el manejo indebido de la información".* En este mismo sentido se enmarca el artículo 37, el cual dispone que: *"las Sociedades deberán presentar a la Comisión manuales que establezcan las medidas mínimas de seguridad, mismas que incluirán el transporte de la información, así como la seguridad física, logística y en las comunicaciones. Dichos manuales deberán contener, en su caso, las medidas necesarias para la seguridad del procesamiento externo de datos"*. Asimismo, el inciso 2º de este artículo 37 agrega que: *"los Usuarios podrán verificar, con el consentimiento de las Sociedades, que existan las medidas de seguridad necesarias para salvaguardar la información que los Usuarios les proporcionen".*

Sin duda, las disposiciones anteriores son de gran importancia pues permiten controlar los niveles de seguridad implementados por las SIC. En nuestra opinión, el hecho de facultarse a estas empresas para establecer sus propios manuales de seguridad, en general, no significa que en caso de responsabilidad por daños pueda aducirse que esos manuales constituyan el estándar de conducta debido, y que una conducta ajustada a esos manuales excluye la culpa. Por el contrario, las prácticas o usos existentes en cierta actividad no son vinculantes para el juez a la hora de determinar deberes de cuidado, pues el que "en una actividad algo se haya hecho siempre no expresa *per se* que su uso sea correcto" [410] . Con todo, la afirmación anterior resulta de difícil aplicación en el caso mexicano, pues la LSIC establece expresamente que la responsabilidad tanto de las SIC como de los Usuarios solamente se circunscribe a la "culpa grave o dolo o mala fe" (Art. 51), por lo que un actuar descuidado de éstas, en principio no tiene reparación por la vía civil, lo que nos parece inaceptable.

d) Uso indebido de la información

Otra temática abordada por la LSIC es la utilización indebida de la información. A este respecto, el artículo 22 inciso 2º se pronuncia y señala que: *"para efectos de esta ley, se entenderá por uso o manejo indebido de la información cualquier acto u omisión que cause daño en su patrimonio, al sujeto del que se posea información, así como cualquier acción que se traduzca en un beneficio patrimonial a favor de los funcionarios y empleados de la Sociedad o de esta última, siempre y cuando no se derive de la realización propia de su objeto".*

La disposición anterior tiende a confundir, pues parece que circunscribiera la calificación del uso indebido al sólo daño patrimonial. Si así fuera, creemos que sería un error, pues las consecuencias del uso indebido de la información pueden afectar tanto el patrimonio como la esfera moral de las personas, por lo que sería una arbitrariedad excluir el potencial daño moral a las personas [411] . Con todo, no creemos que en definitiva sea ese el sentido de la norma, sino más bien que la disposición trata de facilitar dentro del ámbito probatorio la configuración de un abuso de información, lo cual no quiere decir

[410] Barros Bourie, Enrique: *"Curso de Derecho de Obligaciones. Responsabilidad civil Extracontractual",* Apuntes preparados con la participación de los ayudantes Eduardo Ugarte D. y Alejandro Vícari V., Universidad de Chile, Facultad de derecho, 2001, pág. 55.

que sólo constituyan abuso esas circunstancias. Con la segunda interpretación, se evita el riesgo de pensar que se estaría frente a un error legislativo, en el cual se trataría de definir una acción (uso indebido de información) a través de las consecuencias que se deriven de ella, independiente del resultado efectivo. No creemos que sea este el caso.

El uso indebido de los datos, a su vez está íntimamente relacionado con los deberes de confidencialidad. El artículo 38 se refiere a ello, y hace aplicables las disposiciones legales relativas al Secreto Financiero, *"(…) a las Sociedades, a sus funcionarios y a sus empleados (…)".* Por lo tanto, *"(…) los Usuarios de los servicios proporcionados por las Sociedades, sus funcionarios, empleados y prestadores de servicios, deberán guardar confidencialidad sobre la información contenida en los Reportes de Crédito a los que tengan acceso"*. Este deber de secreto subsiste incluso cuando los mencionados funcionarios o empleados dejen de prestar sus servicios en dichas Sociedades (Art. 38 inciso 1º).

d) Caducidad de la información

La ley en comento, también establece plazos durante los cuales puede lícitamente tratarse la información crediticia. Al efecto, señala el artículo 23 que las Sociedades están obligadas a conservar la información que les sea proporcionada por los Usuarios, relativa a personas físicas, durante un plazo de ochenta y cuatro meses, contados a partir de la fecha en que*: "I. El Usuario cobre el crédito otorgado; II. Se ejecute la sentencia ejecutoriada que haya condenado al Cliente al pago de las obligaciones derivadas del crédito correspondiente; III. Se extinga el derecho del actor para pedir la ejecución de dicha sentencia, o IV. Prescriba la acción del Usuario para cobrar el crédito a cargo del Cliente".* Agrega el inciso 2º que:*"tratándose de personas físicas, las Sociedades deberán eliminar de su base de datos la información relativa a las operaciones respecto de las cuales el plazo antes mencionado haya transcurrido, una vez que el Usuario correspondiente le haya notificado dicha circunstancia, así como en aquellos casos en que el Banco de México, mediante disposiciones de carácter general determine sobre la eliminación de créditos menores a mil UDIS"* (Art. 23 inciso 2º). Finalmente, cabe consignar que el inciso 3º dispone que: *"Las Sociedades no podrán eliminar de su base de datos, información que les haya sido proporcionada por los Usuarios, relativa a personas morales".*

De lo prescrito por las normas recién vistas, debemos concluir que el límite temporal de utilización de los datos de personas naturales relativos a operaciones crediticias, es de siete años -lo que nos parece excesivo- contados desde la ocurrencia de los hechos señalados en la LSIC. En el caso de los datos de personas morales la regla anterior no se aplica, por lo que las SIC no pueden eliminar de su base de datos la información que les

411 El daño moral está expresamente definido por el Código Civil mexicano en el inciso 1º del artículo 1.916, el cual señala que*: "Por daño moral se entiende la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físicos, o bien en la consideración que de sí misma tienen los demás. Se presumirá que hubo daño moral cuando se vulnere o menoscabe ilegítimamente la libertad o la integridad física o psíquica de las personas".* De la configuración anterior aparece más o menos claro que este tipo de daño es concebido por el legislador mexicano como "el precio del dolor".

haya sido proporcionada por los Usuarios relativas a ellas. Esta situación que no es explicada en la Ley nos parece carente de sustento, por lo que estimamos que igualmente debería contemplarse el plazo de caducidad de la información.

e) Reglas generales de la prestación de servicios de información crediticia

En el Capítulo referido a la prestación de servicios de información crediticia, se establecen diversas reglas al respecto. En lo relativo a quienes tienen la calidad de "Usuarios" del sistema, el artículo 25 señala que: *"Sólo las Entidades Financieras y las Empresas Comerciales podrán ser Usuarios de la información que proporcionen las Sociedades".* A continuación, el artículo 26 dispone que las SIC deberán proporcionar información: *"a los Usuarios, a las autoridades judiciales en virtud de providencia dictada en juicio en el que el Cliente sea parte o acusado, así como a las autoridades hacendarias federales, a través de la Comisión, para efectos fiscales, de combate al blanqueo de capitales o de acciones tendientes a prevenir y castigar el financiamiento del terrorismo"* [412] .

f) Reportes de crédito

Como ya se señaló, en definitiva la información que entregan las SIC a los Usuarios y Clientes se materializa en los denominados 'reportes de crédito'. El contenido de éstos está regulado en el artículo 27, el cual dispone que las SIC al entregar reportes de crédito, deberán guardar secreto respecto de la identidad de los acreedores, salvo en el caso de que se ejerza el derecho de acceso a la información por parte de un Cliente de una institución financiera o empresa comercial directamente ante éste. En este caso, la SIC informará directamente al Cliente el nombre de los acreedores que correspondan [413] .

Se agrega a renglón seguido que las SIC sólo podrán proporcionar información a un Usuario (bancos o empresas comerciales en general), cuando éste cuente con *"la autorización expresa del Cliente mediante su firma autógrafa, en donde conste de manera fehaciente que tiene pleno conocimiento de la naturaleza y alcance de la información que la Sociedad proporcionará al Usuario que así la solicite, del uso que dicho Usuario hará de tal información y del hecho de que éste podrá realizar consultas periódicas de su historial crediticio, durante el tiempo que mantenga relación jurídica con el Cliente"* (Art. 28).

La disposición anterior tiene relevancia en materia de protección de datos personales, pues establece el principio del consentimiento previo e informado del titular

[412] El inciso 2º por su parte establece el principio de reciprocidad en la actividad de la prestación de la información, disponiendo que: *"Las Sociedades podrán negar la prestación de sus servicios a aquellas personas que no les proporcionen información para la realización de su objeto. Para esos efectos, se considerará que una persona no proporciona información, cuando realice en forma habitual y profesional operaciones de crédito u otras de naturaleza análoga y no proporcione información sobre las mismas".*

[413] Artículo 27.-*"Las Sociedades, al proporcionar información sobre operaciones crediticias y otras de naturaleza análoga, deberán guardar secreto respecto de la identidad de los acreedores, salvo en el supuesto a que se refiere el artículo 39 de la presente ley, en cuyo caso, informarán directamente a los Clientes el nombre de los acreedores que correspondan".*

de los datos como condición de licitud del tratamiento de éstos.

En el inciso 4º del artículo 28, se contemplan excepciones a la regla ya señalada disponiéndose que la obligación de obtener las autorizaciones a que se refiere este artículo, no se aplicará a la *"información solicitada por la Comisión, por las autoridades judiciales en virtud de providencia dictada en juicio en que el Cliente sea parte o acusado y por las autoridades hacendarias federales, cuando la soliciten a través de la Comisión, para fines fiscales, de combate al blanqueo de capitales o de acciones tendientes a prevenir y castigar el financiamiento del terrorismo".* En cuanto a la vigencia de la autorización para tratar la información crediticia, el inciso 5º del dispone que*"será de un año contado a partir de su otorgamiento, o hasta dos años adicionales a ese año si el Cliente así lo autoriza expresamente. En todo caso, la vigencia permanecerá mientras exista relación jurídica entre el Usuario y el Cliente"*.De esta forma, la LSIC establece un límite temporal al consentimiento para el tratamiento de los datos financieros, la cual no podrá exceder la vigencia de las relaciones contractuales.

Por otra parte, este mismo artículo señala que los reportes de créditos otorgados a los clientes o deudores, "*deberán contener la identidad de los Usuarios que hayan consultado su información en los veinticuatro meses anteriores"* (Art. 28 inciso 6º).Por consiguiente, en estos casos se debe identificar a todos los usuarios del sistema financiero que hayan solicitado reportes de crédito.

Finalmente, diremos que el artículo 34 establece una regla de carácter probatoria que nos parece muy razonable y que señala: *"los Reportes de Crédito y los Reportes de Crédito Especiales no tendrán valor probatorio en juicio, y deberán contener una leyenda que así lo indique".* Creemos que es adecuada esta consideración en atención a que esos reportes sólo muestran una realidad creada con información que no refleja necesariamente obligaciones indubitadas.

g) Derecho de acceso y rectificación

La LSIC se ocupa de proteger los derechos de los Clientes (deudores) de los usuarios del sistema de información crediticia (instituciones financieras o empresas comerciales). Para tal efecto, la LSIC establece el derecho de acceso a la información a través de los *"reportes de crédito especiales"* y, en caso de no conformarse el Cliente con este reporte de crédito, está facultado para interponer una *"reclamación"* con el fin de que se rectifique o cancele la información errónea. Las disposiciones pertinentes se señalan a continuación.

El artículo 39 señala que: *"los Clientes que gestionen algún servicio ante algún Usuario, podrán solicitar a éste los datos que hubiere obtenido de la Sociedad, a efecto de aclarar cualquier situación respecto de la información contenida en el Reporte de Crédito".*

Luego, el artículo 40 en su inciso 1º dispone que: *"los Clientes tendrán el derecho de solicitar a la Sociedad su Reporte de Crédito Especial, a través de las unidades especializadas de la Sociedad, de las Entidades Financieras o, en el caso de Empresas Comerciales, de quienes designen como responsables para esos efectos. Dichas unidades estarán obligadas a tramitar las solicitudes presentadas por los Clientes".* Se

agrega por la Ley que: *"la Sociedad deberá formular el Reporte de Crédito Especial solicitado en forma clara, completa y accesible, de tal manera que se explique por sí mismo o con la ayuda de un instructivo anexo, y enviarlo o ponerlo a disposición del Cliente en un plazo de cinco días hábiles contado a partir de la fecha en que la Sociedad hubiera recibido la solicitud correspondiente. (…) el Reporte de Crédito Especial deberá permitir al Cliente conocer de manera clara y precisa la condición en que se encuentra su historial crediticio"* (Art. 40 incs. 2º y 3º) [414] . De lo preceptuado hasta ahora por el artículo 40, se desprende una clara intención legislativa de que los reportes sean autosuficientes y puedan ser entendidos por cualquier persona, sin mayores explicaciones. Lo dicho por el legislador mexicano guarda concordancia con lo preceptuado en el artículo 12 de la Directiva 95/46 CE y principalmente, con el artículo 15.1 de la Ley 25.326 de la República Argentina. La similitud de de sus disposiciones es evidente.

El artículo 40 finaliza señalando que: *"las Sociedades estarán obligadas a enviar o a poner a disposición de los Clientes, junto con cada Reporte de Crédito Especial, un resumen de sus derechos y de los procedimientos para acceder y, en su caso, rectificar los errores de la información contenida en dicho documento. Adicionalmente, estarán obligadas a mantener a disposición del público en general el contenido del resumen mencionado".* Esta disposición parece de gran utilidad para la difusión de los derechos de los deudores o clientes, pues permite además el control por parte de éstos de que se respete la ley y, en caso de no ser así, saber donde acudir para denunciar estos hechos, en este caso ante la Comisión Nacional Bancaria y de Valores.

En lo relativo al derecho de rectificación, podemos señalar que el legislador ha dispuesto que cuando los Clientes no estén conformes con la información contenida en su Reporte de Crédito o Reporte de Crédito Especial *"podrán presentar una reclamación. (…) Dicha reclamación deberá presentarse por escrito o por medios electrónicos ante la unidad especializada de la Sociedad, adjuntando copia del Reporte de Crédito o Reporte de Crédito Especial en el que se señale con claridad los registros en que conste la información impugnada, así como copias de la documentación en que funden su inconformidad. En caso de no contar con la documentación correspondiente, deberán explicar esta situación en el escrito o medio electrónico que utilicen para presentar su reclamación"* (Art. 42). Los plazos o términos que tendrán las SIC para resolver la reclamación *"(…) serán determinados por el Banco de México, mediante las disposiciones de carácter general a que se refiere el artículo 12 de la presente ley"* (Art. 42 inciso 2º).

El artículo 43 por su parte, dispone que: *"la Sociedad deberá entregar a la unidad especializada de las Entidades Financieras o, en el caso de Empresas Comerciales, a quienes designen como responsables para esos efectos, la reclamación presentada por el Cliente, dentro de un plazo de cinco días hábiles contado a partir de la fecha en que la Sociedad la hubiere recibido. Los Usuarios de que se trate deberán responder por escrito a la reclamación presentada por el Cliente, dentro del plazo previsto en el artículo 44 de esta ley".* Como medida de publicidad, se establece que una vez que la Sociedad

[414] Por su parte, el artículo 41 agrega que: "los Clientes tendrán derecho a solicitar a las Sociedades el envío gratuito de su Reporte de Crédito Especial cada vez que transcurran doce meses".

notifique por escrito la reclamación al Usuario respectivo, deberá incluir en el registro de que se trate la leyenda *"registro impugnado*" la cual no se eliminará sino hasta que concluya el trámite de los artículos 44, 45 y 46 (Art. 43 inciso 2º).

El artículo 44 a su vez prescribe que: *"si las unidades especializadas de las Entidades Financieras, o en el caso de Empresas Comerciales, de quienes designen como responsables para esos efectos, no hacen llegar a la Sociedad su respuesta a la reclamación presentada por el Cliente dentro de un plazo de treinta días naturales contado a partir de que hayan recibido la notificación de la reclamación, la Sociedad deberá modificar o eliminar de su base de datos la información que conste en el registro de que se trate, según lo haya solicitado el Cliente, así como la leyenda registro impugnado"*. Por lo tanto, en caso de no recibirse respuesta por parte de los usuarios, se hace fe de lo planteado en su reclamación por el cliente, con lo que se debe necesariamente acoger su petición.

El mencionado artículo 45, señala por su parte que si el usuario acepta total o parcialmente lo señalado en la reclamación presentada por el cliente, *"deberá realizar de inmediato las modificaciones conducentes en su base de datos y notificar de lo anterior a la Sociedad que le haya enviado la reclamación, remitiéndole la corrección efectuada a su base de datos*". En caso que el Usuario aceptara parcialmente la reclamación o señalare la improcedencia de ésta, *"deberá expresar en su respuesta los elementos que consideró respecto de la reclamación, misma que la Sociedad deberá remitir al Cliente que haya presentado la reclamación, dentro de los cinco días hábiles siguientes a que reciba la respuesta del Usuario".* En el caso anterior se le otorga el derecho al cliente de manifestar en un texto de no más de cien palabras los argumentos por los que a su juicio la información proporcionada por el usuario es incorrecta y solicitar a la sociedad que incluya dicho texto en sus futuros Reportes de Crédito (Art. 45 inciso 2º). En el caso que los errores objeto de la reclamación presentada por el cliente sean imputables a la sociedad*, "ésta deberá corregirlos de manera inmediata".*

Finalmente, el artículo 46 dispone que las sociedades sólo podrán incluir nuevamente dentro de su base de datos *"la información previamente contenida en los registros que haya modificado o eliminado de conformidad con lo dispuesto en los artículos 44 y 45 de esta ley, cuando el Usuario le envíe los elementos que sustenten, a juicio de éste, la inclusión, nuevamente, de la información impugnada. En tal supuesto, la Sociedad eliminará la leyenda "registro impugnado" e informará de dicha situación al Cliente, remitiéndole la respuesta del Usuario junto con un nuevo Reporte de Crédito Especial, en un plazo de cinco días hábiles, contado a partir de que la Sociedad haya incluido nuevamente la información impugnada por el Cliente. El costo del Reporte de Crédito Especial referido y el de su envío será con cargo al Usuario".*

En lo relativo a la responsabilidad de las SIC con motivo de las modificaciones, inclusiones o eliminaciones de información o de registros que realicen como parte del procedimiento de reclamación previsto en el Capítulo que analizamos, se señala en el artículo 46 inciso 2º que: *"las Sociedades no tendrán responsabilidad alguna"* y *"en el desahogo de dicho procedimiento las Sociedades se limitarán a entregar a los Usuarios y a los Clientes la documentación que a cada uno corresponda en términos de los artículos anteriores, y no tendrán a su cargo resolver, dirimir o actuar como amigable componedor*

de las diferencias que surjan entre unos y otros".

En los casos en que de la reclamación por el Cliente resulte una modificación a la información de éste contenida en la base de datos de la Sociedad, *"ésta deberá poner a disposición del cliente un nuevo Reporte de Crédito Especial en la dirección establecida al efecto. Adicionalmente, deberá enviar un Reporte de Crédito actualizado a los Usuarios que hubieran recibido información sobre el Cliente en los últimos seis meses y a las demás Sociedades. El costo de los Reportes anteriores y su envío será cubierto por el Usuario o la Sociedad, dependiendo de a quien sea imputable el error en la información contenida en la referida base de datos"* (Art. 47). Adicionalmente, el artículo 49 establece que una vez que la SIC haya actualizado la información contenida en su base de datos, "*deberá poner a disposición de la Comisión un listado de los registros que por cualquier causa hubiesen sido eliminados, incluidos o modificados como resultado de la reclamación presentada por el Cliente"* [415] .

h) Resolución de conflictos

La LSIC dispone en el artículo 48 que las SIC podrán establecer en los contratos de prestación de servicios que celebren con los Usuarios, que ambos se comprometen a dirimir los conflictos que tengan con los Clientes con motivo de la disconformidad sobre la información contenida en los registros que aparecen en la base de datos, a través del proceso arbitral. Éstos son conocidos y resueltos por la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros o por la instancia de información, protección y defensa de las personas, según sea el caso, siempre y cuando el Cliente solicite suscribir el modelo de compromiso arbitral en amigable composición que se anexe a dichos contratos, el cual deberá prever plazos máximos [416] . De lo anterior, se deduce que la LSIC estimula que el conocimiento de los conflictos suscitados entre los clientes y los usuarios o sociedades no llegue a los tribunales ordinarios de justicia, sino que sea resuelto por instancias de carácter administrativas a través de un procedimiento arbitral, las cuales para estas materias específicas no tendrían facultades sancionatorias en caso de la violación de las normas de esta ley. La afirmación anterior la basamos en que la única entidad administrativa autorizada para aplicar sanciones por las infracciones a la LSIC es la Comisión Nacional Bancaria y de Valores (Arts. 52-55).

En suma, de las disposiciones de la LSIC que hemos señalado, se desprende a nuestro juicio que la protección a los datos personales de carácter crediticio y comercial, ha sido regulada de manera consecuencial a la legalización e implementación del mercado de la información crediticia, por lo que creemos su configuración no ha sido

[415] Cabe agregar que, la Sociedad trimestralmente deberá poner a disposición de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros y de la instancia de información, protección y defensa de las personas, según corresponda, "el número de reclamaciones y errores respecto de la información contenida en su base de datos, relacionando dicha información con los Usuarios o Sociedad de que se trate, y los modelos de convenios arbitrales que, en su caso, se comprometan a adoptar junto con los Usuarios (…). Lo anterior podrá ser dado a conocer al público por la autoridad correspondiente" (Art. 50).

[416] Además se agrega que: *"Las unidades especializadas de las Entidades Financieras o, en el caso de Empresas Comerciales, quienes designen como responsables para esos efectos, deberán informar a la Sociedad el laudo respectivo"*(Artículo 48 inciso 2º).

pensada de manera independiente, sino que tratando de compatibilizarla con la actividad que se está regulando.

Lo recién aseverado explicaría en parte las diversas deficiencias que presenta la regulación legal de la LSIC. Entre éstas podemos mencionar las siguientes: a) La configuración poco clara del uso o manejo indebido de la información; b) La debilidad con que se consagra el derecho de acceso a los datos personales de carácter financiero o comercial al señalarse que*"(…) podrán solicitar a éste los datos (…) a efectos de aclarar cualquier situación"*. Expresiones como éstas, nos parecen casi graciosas concesiones para los deudores o clientes, las cuales tienden a rebajar el carácter de derecho fundamental que generalmente se le atribuye al derecho a la autodeterminación informativa, con lo cual visualizamos que en definitiva éste no estaría tras la Ley; c) El excesivo plazo que se otorga a las SIC para la entrega del reporte de crédito (5 días hábiles). Dados los avances tecnológicos, éstos deberían estar inmediatamente a disposición de quien los solicita; d) Dejar entregada a la autoridad administrativa (Banco de México) la determinación del plazo en que deberán resolverse las "reclamaciones" de los reportes de crédito por las Sociedades; e) El excesivo plazo otorgado (indirectamente) a las instituciones financieras o empresas comerciales para que respondan la "reclamación" hecha por el cliente a la Sociedad (30 días naturales); f) La burocratización del ejercicio del derecho de rectificación o "reclamación", pues ésta se presenta a la sociedad, la cual a su vez se la transmite a la institución financiera correspondiente o a la empresa comercial de la cual recibió la información. Creemos que el derecho de rectificación debe realizarse ante quien es responsable de la base de datos primaria, es decir, directamente ante el banco o empresas comercial. Tal como está la ley se trianguliza y encarece absurdamente el proceso; g) El excesivo plazo de caducidad de la información el cual llega a los siete años y, h) Finalmente, estimamos que el punto más débil de la Ley, estaría dado por la limitación de responsabilidad que se establece tanto para los Usuarios del sistema (instituciones financieras en general y las empresas comerciales) como para las SIC, pues el señalar que sólo se responderá de los daños que se causen con *"culpa grave, dolo o mala fe"*, altera las reglas generales de la responsabilidad civil extracontractual en la cual se responde de todo daño causado por culpa o negligencia,a menos que se demuestre que el daño se produjo como consecuencia de culpa o negligencia inexcusable de la víctima [417] . La deficiente norma, pone de cargo de los deudores o clientes el riesgo que implica el funcionamiento del mercado de la información, con lo cual se beneficia injustamente a quienes lucran con este mercado, pues al sancionarse sólo las conductas dolosas de aquellos que están en la mejor posición para evitar los riesgos, se desconoce toda la fundamentación de justicia que se erige tras la atribución de responsabilidad por negligencia.

Para finalizar, queremos destacar -a pesar de las críticas recién expuestas- la previsión legislativa de incluir dentro de la información relativa a los reportes de crédito, las sentencias ejecutoriadas que hayan condenado al cliente al pago de las obligaciones derivadas del crédito correspondiente (artículo 23 II). Pensamos que es una buena medida, pues aportaría información más específica a tener en cuenta en la toma de decisiones por parte de los acreedores, dado que se consolida en un solo informe la

[417] Artículo 1.910 inciso 1º del Código Civil mexicano.

situación crediticia, comercial y judicial de una persona, evitando tener que investigar los acreedores si es que un deudor ha sido demandado judicialmente o no por incumplimiento de sus obligaciones. Favorecería incluso indirectamente a la *par condictio creditorum* ante una eventual apertura de concurso de bienes, pues permitiría rápidamente saber cuántos acreedores han solicitado la ejecución de un determinado deudor, con lo que indudablemente se evitan ejecuciones particulares que sólo benefician al acreedor más diligente y constante. Por otra parte, consideramos que también es una buena medida legal el que los reportes de crédito especiales sean entregados a los Clientes indicando *"la identidad de los Usuarios que hayan consultado su información en los veinticuatro meses anteriores"* (Art. 28 inciso 6º). Esta regla permite saber exactamente quienes han sido los destinatarios de los datos personales durante ese período.

3. Bienes Jurídicos Protegidos por la Legislación de Datos Personales

En esta materia, y dada la inexistencia de una ley de protección de datos personales no podremos hacer referencia a los bienes jurídicos que ésta protegería. Sin embargo, se puede decir que de las normas legales especiales señaladas, particularmente de la Ley para regular las Sociedades de Información Crediticia, no podría afirmarse que se vislumbrara el derecho a la autodeterminación informativa como bien jurídico protegido, pues no aparecen claramente configurados los elementos esenciales de este derecho, aunque se contemplen algunas facultades que comprende éste (derecho de acceso, rectificación y corrección). Más bien atisbamos en esas normas jurídicas una confluencia de bienes jurídicos, como la vida privada e intimidad.

4. Principios Informativos de la Legislación de Protección de Datos Personales

A falta de legislación de protección de datos personales, sólo nos referiremos someramente a los principios que pueden observarse en la Ley de Protección al Consumidor y en la Ley para regular las Sociedades de Información Crediticia; esta última es el cuerpo legal que mejor desarrolla una protección sectorial de algunos datos personales.

1º. Principio de licitud y lealtad de los archivos de datos

Este principio se desprende del artículo 5 de la LSIC, al señalar que las sociedades de información crediticia son las únicas autorizadas legalmente para la prestación de esos servicios. Por otra parte, el artículo 18 dispone que: *"a las Sociedades les estará prohibido: I. Solicitar y otorgar información distinta a la autorizada conforme a esta ley y a las demás disposiciones aplicables (…)".* También puede apreciarse este principio en el artículo 20 de la LSIC, el cual señala que: *"la base de datos de las Sociedades se integrará con la información sobre operaciones crediticias y otras de naturaleza análoga*

que le sea proporcionada por los Usuarios".

2º. Principio de la calidad de los datos

Respecto de este principio, puede señalarse que el legislador lo contempla en diversas normas de la LSIC. Así, el artículo 36 inciso 2º dispone que con el fin de mantener actualizada la información *"las Sociedades deberán proporcionar la información capturada cada mes en su Base Primaria de Datos a todas aquellas Sociedades que así lo hubieren solicitado".* Además, se agrega por el inciso 4º que cada Sociedad, al proporcionar información a otras Sociedades, deberá evitar distorsiones en la información transmitida respecto de la que originalmente fue recibida de los Usuarios.Más adelante, el artículo 45 inciso final prescribe que en caso de que los errores objeto de la reclamación presentada por el Cliente sean imputables a la Sociedad, ésta deberá corregirlos de manera inmediata. El artículo 47 a su turno, agrega en la materia que en los casos en que la reclamación resulte en una modificación a la información del Cliente contenida en la base de datos de la Sociedad, ésta deberá poner a disposición del Cliente un nuevo Reporte de Crédito Especial en la dirección establecida al efecto.

La Ley de Protección al Consumidor por su lado, contempla este principio en el artículo 16 ya visto, el cual señala que en caso de existir alguna ambigüedad o inexactitud en la información *"la empresa deberá efectuar de inmediato las correcciones que fundadamente indique la persona afectada, e informar las correcciones a los terceros que hayan recibido dicha información"* (Art. 16).

3º. Principio del consentimiento informado del titular de los datos

Este principio sólo se encuentra contenido en el artículo 28 de la LSIC, el cual dispone que: *"las Sociedades sólo podrán proporcionar información a un Usuario, cuando éste cuente con la autorización expresa del Cliente, mediante su firma autógrafa, en donde conste de manera fehaciente que tiene pleno conocimiento de la naturaleza y alcance de la información que la Sociedad proporcionará al Usuario que así la solicite, del uso que dicho Usuario hará de tal información y del hecho de que éste podrá realizar consultas periódicas de su historial crediticio, durante el tiempo que mantenga relación jurídica con el Cliente".*

4º. Principio de seguridad de los datos

A este principio se refieren diversos artículos ya vistos de la LSIC, como el 7º Nº 5.4, el cual dispone que la solicitud para constituirse y operar como Sociedad deberá contener entre otros, el programa general de funcionamiento, que comprenda por lo menos: *"(…) 4. Las medidas de seguridad y control a fin de evitar el manejo indebido de la información (…)"*. También está presente el principio de seguridad de los datos en el artículo 22 de la misma Ley el cual señala que: *"la Sociedad deberá adoptar las medidas de seguridad y control que resulten necesarias para evitar el manejo indebido de la información".*

5º. Principio de confidencialidad de los datos

Podemos afirmar que este principio se encuentra contenido en el artículo 29 inciso 4º de la LSIC al señalar que: *"los Usuarios que sean Empresas Comerciales deberán guardar absoluta confidencialidad respecto al contenido de los Reportes de Crédito que les sean proporcionados por las Sociedades".* También podemos visualizarlo en el artículo 38 de esta misma Ley, que como ya se dijo prescribe que: *"con excepción de la información que las Sociedades proporcionen en los términos de esta ley y de las disposiciones generales que se deriven de ella, serán aplicables a las Sociedades, a sus funcionarios y a sus empleados las disposiciones legales relativas al Secreto Financiero, aun cuando los mencionados funcionarios o empleados dejen de prestar sus servicios en dichas Sociedades"*. Se añade a ello que los Usuarios de los servicios proporcionados por las Sociedades, sus funcionarios, empleados y prestadores de servicios*, "deberán guardar confidencialidad sobre la información contenida en los Reportes de Crédito a los que tengan acceso".*

6º Principio del consentimiento para la cesión de los datos

Este principio se encuentra contenido implícitamente en el ya señalado artículo 28 de la LSIC, al cual nos remitimos.

7º. Principio de la finalidad

Por último, debemos decir que el principio de la finalidad se encuentra contenido en el artículo 28 de la LSIC, al disponer que sólo podrán entregarse reportes de crédito si el Cliente ha dado expresa autorización al Usuario, en la cual además debe constar de manera fehacienteque el Clientetiene pleno conocimiento de la naturaleza y alcance de la información que la Sociedad proporcionará al Usuario que así la solicite y del uso que dicho Usuario hará de tal información. Se vislumbra también este principio de manera indirecta en el artículo 22, el cual prescribe que la Sociedad deberá adoptar las medidas de seguridad y control que resulten necesarias para *"evitar el manejo indebido de la información".* Si se habla de uso indebido de ésta, es porque la utilización de información debe obedecer a una determinada finalidad.

Por otra parte, cabe recordar que en la Ley de protección al Consumidor también se inserta este principio. El artículo 18 no deja dudas de ello al señalar que: *"queda prohibido a las empresas dedicadas a la investigación de crédito o de mercadotecnia y a sus clientes, utilizar la información con fines diferentes a los crediticios o mercadotécnicos".*

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

En atención a la inexistencia de una ley general de protección de datos personales en el ordenamiento jurídico mexicano, no desarrollaremos este punto.

6. Modelos de Tutela

Como ya se ha señalado, el ordenamiento jurídico mexicano, no prevé una ley de protección de datos personales que establezca mecanismos de tutela a los derechos de los titulares de los datos. Por lo mismo, tampoco puede hablarse de modelos de tutela propios de éstos. A falta de ley general, cabe analizar la legislación especial. Dentro de ésta, encontramos al menos dos que establecen derechos de acceso y rectificación de carácter informal o extrajudicial. Éstas son: la Ley de Protección al Consumidor, cuyo procedimiento ya se señaló en el punto Nº 2.2.4 de este análisis y, laLey para regular las Sociedades de Información Crediticia. Su procedimiento especial ya lo hemos señalado en la letra g del punto Nº 2.2.6. Respecto de ambos cuerpos legales nos remitiremos a lo ya dicho en los respectivos numerales.

En cuanto al ámbito de tutela constitucional de los derechos fundamentales, debemos señalar que ante la falta de una acción específica de protección a los datos personales, cabría recurrir a la acción constitucional de amparo.

6.1 La acción de Amparo [418]

El artículo 103 de la Constitución mexicana dispone que los Tribunales de la Federación resolverán toda controversia que se suscite: *"I. Por leyes o actos de la autoridad que violen las garantías individuales (…)".* Más adelante, el artículo 107 señala que la acción de amparo de sujetará a los procedimientos y formas del orden jurídico que determine la ley, según las bases que indica. La ley respectiva es la Ley de Amparo (en adelante la Ley) y data del año 1936.

Cabe hacer presente que la regulación legal del amparo mexicano es compleja. Con este término se engloban diversos objetos que en definitiva buscan tutelar los derechos consagrados en la Constitución. El propio artículo 1º de la Ley señala que *"el juicio de amparo tiene por objeto resolver toda controversia que se suscite: I.- por leyes o actos de la autoridad que violen las garantías individuales; Ii.- por leyes o actos de la autoridad federal, que vulneren o restrinjan la soberanía de los estados; Iii.- por leyes o actos de las autoridades de estos, que invadan la esfera de la autoridad federal".*

En lo que sigue, nos referiremos sucintamente a la acción de amparo en lo pertinente para la tutela de los bienes jurídicos vida privada e intimidad. Debemos aclarar, que la configuración de la acción de amparo no contempla su interposición ante actos de particulares, lo que le quita sin duda alcance de tutela. A pesar de esta deficiencia, estimamos que recurriendo a las normas de derecho internacional sobre Derechos Humanos, en especial al Pacto de San José de Costa Rica, es posible fundamentar una protección que incluya a los actos de particulares de atenten en contra de la intimidad y la vida privada.

6.1.1) Procedencia de la Acción

Del texto del artículo 103. I de la Constitución mexicana se deduce que procederá el amparo *"por leyes o actos de la autoridad que violen las garantías individuales"*. Por otra

[418] La acción se amparo está regulada en la Ley de Amparo de 1936. Esta puede ser consultada [en línea] < http://info4.juridicas.unam.mx/const/frames/ley.htm > [consulta: 6 de Febrero 2003].

parte, el artículo 1º de la Ley señala que el juicio de amparo tiene por objeto resolver toda controversia que se suscite: I.- Por leyes o actos de la autoridad que violen las garantías individuales; Ii.- Por leyes o actos de la autoridad federal, que vulneren o restrinjan la soberanía de los Estados; Iii.- Por leyes o actos de las autoridades de estos, que invadan la esfera de la autoridad federal. Por su lado, el artículo 73 dispone que el juicio de amparo es improcedente: *"(…) Ix.- contra actos consumados de un modo irreparable (…) Xi.- contra actos consentidos expresamente o por manifestaciones de voluntad que entrañen ese consentimiento"*. De lo anterior, se deduce que se restringe la procedencia de la acción sólo a los casos en que exista amenaza o perturbación del derecho o, que el derecho se encuentre afectado de manera no irreversible.

6.1.2) Legitimación Activa

El artículo 4 de la Ley dispone que: *"el juicio de amparo únicamente puede promoverse por la parte a quien perjudique (…)"*, pudiendo hacerlo por sí, o por su representante, por medio de algún pariente o persona extraña en los casos en que la ley lo permita expresamente; y solo podrá seguirse por el agraviado, por su representante legal o por su defensor.

En relación a las personas jurídicas, se señala que: *"las personas morales privadas podrán pedir amparo por medio de sus legítimos representantes"* (Articulo 8 Ley).

6.1.3) Legitimación Pasiva

En el caso de vulnerarse los derechos constitucionales, sólo se prevé como sujetos pasivos de la acción, a los entes públicos representados sus respectivas autoridades. Al efecto señala el articulo 5 que: *"son partes en el juicio de amparo: (…) Ii.- la autoridad o autoridades responsables (…)".* Luego, el artículo 11 aclara el término autoridad responsable señalando que es la que dicta, promulga, publica, ordena, ejecuta o trata de ejecutar la ley o el acto reclamado.

6.1.4) Competencia

El artículo 36 de la Ley señala que *"cuando conforme a las prescripciones de esta ley sean competentes los jueces de distrito para conocer de un juicio de amparo, lo será aquel en cuya jurisdicción deba tener ejecución, trate de ejecutarse, se ejecute o se haya ejecutado el acto reclamado"*. Más adelante, el articulo 38 agrega que: *"en los lugares en que no resida juez de distrito, los jueces de primera instancia dentro de cuya jurisdicción radique la autoridad que ejecuta o trate de ejecutar el acto reclamado tendrán facultad para recibir la demanda de amparo, pudiendo ordenar que se mantengan las cosas en el estado en que se encuentren por el termino de setenta y dos horas, que deberá ampliarse en lo que sea necesario, atenta la distancia que haya a la residencia del juez de distrito; ordenara que se rindan a este los informes respectivos (…)"*. Terminado el trámite anterior este juez debe remitir sin demora alguna, la demanda original con sus anexos al juez de distrito.

6.1.5) Procedimiento Aplicable

El procedimiento establecido para la tramitación del amparo puede sintetizarse de la siguiente forma:

1) *Demanda:* el artículo 21 de la Ley nos dice que el término para la interposición de la demanda de amparo será de quince días. Dicho termino se cuenta *"desde el día siguiente al en que haya surtido efectos, conforme a la ley del acto, la notificación al quejoso de la resolución o acuerdo que reclame; al en que haya tenido conocimiento de ellos o de su ejecución, o al en que se hubiese ostentado sabedor de los mismos"* (sic). Todas las actuaciones deberán hacerse por escrito, salvo las que se hagan en las audiencias y notificaciones (Articulo 3).

2) *Suspensión del acto*: en los casos de la competencia de los jueces de distrito, la suspensión del acto reclamado se decretara de oficio o a petición de la parte agraviada (Articulo 122). En los casos en que proceda la suspensión de oficio, si hubiere peligro inminente de que se ejecute el acto reclamado con notorios perjuicios para el quejoso, el juez de distrito, con la sola presentación de la demanda de amparo, *"podrá ordenar que las cosas se mantengan en el estado que guarden hasta que se notifique a la autoridad responsable la resolución que se dicte sobre la suspensión definitiva, tomando las medidas que estime convenientes para que no se defrauden derechos de tercero y se eviten perjuicios a los interesados, hasta donde sea posible, o bien las que fueren procedentes para el aseguramiento del quejoso, si se tratare de la garantía de la libertad personal"* (Articulo 130). Asimismo, en los casos en que la suspensión sea procedente, *"se concederá en forma tal que no impida la continuación del procedimiento en el asunto que haya motivado el acto reclamado, hasta dictarse resolución firme en el; a no ser que la continuación de dicho procedimiento deje irreparablemente consumado el daño o perjuicio que pueda ocasionarse al quejoso"* (Articulo 138). El juez de distrito examinara el escrito de demanda y si encontrare motivo manifiesto e indudable de improcedencia, la desechara de plano, sin suspender el acto reclamado (Articulo 145).

3) *Informe*: si el juez de distrito no encontrare motivos de improcedencia, o se hubiesen llenado los requisitos omitidos, *"admitirá la demanda y, en el mismo auto, pedirá informe con justificación a las autoridades responsables y hará saber dicha demanda al tercer perjudicado, si lo hubiere; señalara día y hora para la celebración de la audiencia, a mas tardar dentro del termino de treinta días, y dictara las demás providencias que procedan con arreglo a esta ley"* (Articulo 147). Finalmente, cabe señalar que los jueces de distrito o las autoridades judiciales que conozcan de los juicios de amparo, con arreglo a esta ley, *"deberán resolver si admiten o desechan las demandas de amparo dentro del termino de veinticuatro horas, contadas desde la en que fueron presentadas"* (Articulo 148).

6.1.6) La Sentencia

En cuanto a la sentencia, se dispone que éstas *"sólo se ocuparan de los individuos particulares o de las personas morales, privadas u oficiales que lo hubiesen solicitado, limitándose a ampararlos y protegerlos, si procediere, en el caso especial sobre el que verse la demanda, sin hacer una declaración general respecto de la ley o acto que la motivare"* (sic)(Articulo 76 Ley).

En lo relativo a los requisitos de las sentencias de amparo, el artículo 77 de la Ley nos dice que éstas deberán contener: *"I.- La fijación clara y precisa del acto o actos reclamados, y la apreciación de las pruebas conducentes para tenerlos o no por demostrados; Ii.- Los fundamentos legales en que se apoyen para sobreseer en el juicio, o bien para declarar la constitucionalidad o inconstitucionalidad del acto reclamado; Iii.- Los puntos resolutivos con que deben terminar, concretándose en ellos, con claridad y precisión, el acto o actos por los que sobresea, conceda o niegue el amparo"*.

En cuanto a los efectos de la sentencia de amparo, se señala que: "*la sentencia que conceda el amparo tendrá por objeto restituir al agraviado en el pleno goce de la garantía individual violada, restableciendo las cosas al estado que guardaban antes de la violación, cuando el acto reclamado sea de carácter positivo; y cuando sea de carácter negativo, el efecto del amparo será obligar a la autoridad responsable a que obre en el sentido de respetar la garantía de que se trate y a cumplir, por su parte, lo que la misma garantía exija"* (Articulo 80 Ley).

6.2 Otras Acciones

No tenemos noticia de otras acciones que pudiesen tutelar los bienes jurídicos en los cuales fundamentar una protección de los datos personales.

7. Mecanismos de Control

En este punto sólo podemos señalar que tanto la Ley de Protección al Consumidor como la Ley de Servicios de Información Financiera prevén órganos encargados de velar por del cumplimiento de los respectivos estatutos jurídicos, facultándoles en algunos casos para aplicar sanciones administrativas y actuar como árbitros en la resolución de conflictos. En el caso de la Ley de Protección al Consumidor el órgano de control es la Procuraduría Federal del Consumidor [419] . En el ámbito de la Ley para Regular Las Sociedades De Información Crediticia, se establece como órgano de control a la Comisión Nacional Bancaria y de Valores, la cual está facultada para aplicar sanciones administrativas tanto a los funcionarios de las Sociedades o de las Entidades Financieras como también a los Usuarios [420] .

En suma, a pesar de la falta de texto legal en materia de protección de datos, las

[419] El artículo 20 de esta Ley señala que: *"La Procuraduría Federal del Consumidor es un organismo descentralizado de servicio social con personalidad jurídica y patrimonio propio. Tiene funciones de autoridad administrativa y esta encargada de promover y proteger los derechos e intereses del consumidor y procurar la equidad y seguridad jurídica en las relaciones entre proveedores y consumidores. Su funcionamiento se regirá por lo dispuesto en esta ley, los reglamentos de esta y su estatuto"*. Por otra parte, el artículo 24 establece como atribuciones de la Procuraduría: *"(…) II. Procurar y representar los intereses de los consumidores, mediante el ejercicio de las acciones, recursos, trámites o gestiones que procedan; III. Representar individualmente o en grupo a los consumidores ante autoridades jurisdiccionales y administrativas, y ante los proveedores; XVII. Denunciar ante el Ministerio Público los hechos que puedan ser constitutivos de delitos y que sean de su conocimiento y, ante las autoridades competentes, los actos que constituyan violaciones administrativas que afecten los intereses de los consumidores; XIX. Aplicar las sanciones establecidas en esta ley"*.

disposiciones sectoriales ya mencionadas contemplan órganos de control cuya función esencial es velar a nivel administrativo, por el cumplimiento de cada estatuto jurídico, dentro de los cuales -como se vio- se establecen algunas normas de protección a los datos personales.

8. Transmisión Internacional de Datos

En materia de transmisión internacional de datos personales, no existen reglas generales al respecto. A pesar de lo anterior, se constata la existencia de algunas normas sectoriales que hacen referencia a la materia. Las disposiciones pertinentes son las siguientes:

8.1 Artículo 117 Bis de la Ley de Instituciones de Crédito

Este artículo dispone que *"la Comisión Nacional Bancaria y de Valores estará facultada para proporcionar a autoridades financieras del exterior, información sobre las operaciones y servicios previstos en el artículo 117(…)"*, así como las relativas operaciones de fideicomiso. Cabe recordar, que el artículo 117 de esa ley establece el secreto financiero o bancario, el cual cubre cualquier tipo de operaciones o servicios realizados ante las instituciones financieras, por lo que la facultad señalada haría excepción a este deber de secreto. Esta misma disposición autoriza a la Comisión Nacional Bancaria y de Valores a llevar a cabo mandatos y comisiones, que reciba de las instituciones de crédito. El requisito para que puedan operar tales transmisiones de datos personales es señalado por el propio artículo 117 Bis, el cual dispone que operará la facultad *"siempre que tenga suscritos con dichas autoridades acuerdos de intercambio de información en los que se contemple el principio de reciprocidad, debiendo en todo caso abstenerse de proporcionar la información cuando a su juicio ésta pueda ser usada para fines distintos a los de la supervisión financiera, o bien, por causas de orden público, seguridad nacional o por cualquier otra causa prevista en los acuerdos respectivos".*

Por lo tanto, en materia financiera la ley autoriza la transmisión internacional de datos siempre que existan acuerdos basados en el principio de la reciprocidad, dejando a juicio del órgano administrativo la determinación de cuándo no debería realizarse la transferencia. Creemos que la forma como se encuentra configurada la posibilidad de realizar una transmisión internacional de datos no es adecuada, pues del principio de reciprocidad no se sigue obviamente que el país receptor o el emisor tengan niveles adecuados de protección de datos. Por otra parte, estimamos que las situaciones que harían inoperativa una transmisión de datos personales al exterior son demasiado amplias, por lo que la regla general pierde fuerza ante los casos de excepción.

8.2 Artículo 69 del Código Fiscal de la Federación

El Código Fiscal o tributario mexicano contempla dentro de sus artículos una disposición

420 Las sanciones aplicables por esta Comisión se analizan más abajo en el punto Nº 6.1 relativo a la responsabilidad administrativa.

que permite la transmisión internacional de datos personales relativos a las declaraciones y datos suministrados por los contribuyentes o por terceros con ellos relacionados. Al efecto se dispone que: *"mediante acuerdo de intercambio reciproco de información, suscrito por el Secretario de Hacienda y Crédito Público, se podrá suministrar la información a las autoridades fiscales de países extranjeros, siempre que se pacte que la misma solo se utilizara para efectos fiscales y se guardara el secreto fiscal correspondiente por el país de que se trate".*

Esta disposición, similar a la del artículo 6º A 6º del Código Tributario chileno, autoriza expresamente a un funcionario estatal para convenir con países extranjeros el intercambio de información confidencial en materia tributaria. Si bien la ley exige que se cumplan ciertos requisitos, no se contemplan entre éstos que el país receptor de esos datos posea una legislación de protección de datos de un nivel adecuado. En este punto creemos que se hace necesaria una legislación acorde a los estándares internacionales de protección de datos personales, pues de la forma cómo se regula la materia, no se asegura que los datos personales serán tratados de manera adecuada.

9. Régimen de Responsabilidad

El ordenamiento jurídico mexicano no contempla un régimen especial de responsabilidad en materia de protección de datos personales. Por lo tanto, ante esta carencia estimamos que deberían aplicarse las reglas contenidas en los estatutos jurídicos sectoriales, y a falta de éstos, aplicarse las reglas generales de la responsabilidad. A continuación revisaremos las disposiciones pertinentes en las tres áreas del derecho a las cuales nos hemos referido en cada análisis.

9.1 Responsabilidad Administrativa

Dentro de los estatutos sectoriales mexicanos que hemos analizado, se contemplan sanciones administrativas para aquellos funcionarios de la administración del Estado que violen los preceptos legales. A falta de esos estatutos, cabría hacer aplicación de las reglas generales en materia de responsabilidad funcionaria. Las disposiciones particulares se señalan a continuación.

9.1.1) Código Fiscal de la Federación

El artículo 87 de este Código señala que constituyen infracciones a las disposiciones fiscales en que pueden incurrir los funcionarios o empleados públicos en el ejercicio de sus funciones: *"(…) IV. Divulgar, hacer uso personal o indebido de la información confidencial proporcionada por terceros independientes que afecte su posición competitiva a que se refieren los artículos 46, fracción IV y 48, fracción VII de este Código".* El artículo 88 contempla la sanción respectiva diciendo que: *"Se sancionará con una multa de $ 45,000.00 a $ 60,000.00, a quien cometa las infracciones a las disposiciones fiscales a que se refiere el artículo 87".*

9.1.2) Ley Federal de Protección al Consumidor

Dentro de la Ley de Protección al Consumidor existe una disposición que opera como regla general en materia de sanciones, ella es la contenida en el articulo 126 y señala que: *"Las infracciones a lo dispuesto por los artículos (…) 16, 18, (…) serán sancionadas con multa por el equivalente por una y hasta ochocientas veces el salario mínimo general vigente en el distrito federal".* A continuación, el articulo 127 prescribe que: "*las infracciones a lo dispuesto por los artículos (…), 17 (…) serán sancionadas con multa hasta por el equivalente de una a mil quinientas veces el salario mínimo general vigente para el distrito federal".* Debemos recordar, que las sanciones indicadas se aplican, en general, a aquellas empresas de investigación de mercado o de mercadotecnia directa, en caso que no respondan a las solicitudes de los consumidores sobre la existencia de datos personales en sus bases de datos, la finalidad para la cual se utilizan y a quiénes se ha entregado tal información. Las normas aludidas ya fueron tratadas más arriba en el punto Nº 2.2.4.

Ley para regular las Sociedades de Información Crediticia

Esta extensa ley prevé diversas sanciones tanto para los usuarios como sociedades de información que violen las disposiciones legales que los obligan en materia de datos personales crediticios y comerciales. Las normas pertinentes se indican a continuación.

El artículo 53 de la Ley dispone que: *"La Comisión, oyendo previamente al interesado, podrá inhabilitar para desempeñar un empleo, cargo o comisión dentro del sistema financiero mexicano, por un periodo de seis meses a diez años, a aquellos funcionarios o empleados de las Sociedades o de las Entidades Financieras que, de cualquier forma, cometan alguna violación a las disposiciones relativas al Secreto Financiero. Dichas personas estarán obligadas, además, a reparar los daños que se hubieran causado. Lo anterior, sin perjuicio de las sanciones a que los Usuarios se hagan acreedores conforme a esta ley u otros ordenamientos legales".* De esta norma, se desprende que las sanciones podrían ser aplicables tanto a los funcionarios del Estado como a los empleados particulares de las instituciones financieras y sociedades de información de crédito.

Por su parte, el artículo 54 señala que: *"La Comisión sancionará a las Sociedades con multa de 20 a 100 veces el salario mínimo general diario vigente en el Distrito Federal, cuando: I. No se envíe el Reporte de Crédito Especial al Cliente dentro de los plazos previstos en esta ley; II. No se envíen los informes y los Reportes de Crédito en los plazos previstos en el Capítulo IV del Título Segundo de la presente ley; III. Alteren, eliminen o modifiquen algún registro de la base de datos de las Sociedades, sin algún motivo que así lo justifique. Sin perjuicio de lo anterior, la Sociedad deberá proceder a efectuar la corrección respectiva".* Como se ha visto, las reglas recién enunciadas sancionan los incumplimientos de deberes funcionarios, los cuales sólo son aplicables a las sociedades de información crediticia.

A renglón seguido, el artículo 55 prescribe que: "*La Comisión sancionará a las Sociedades con multa de 100 a 500 veces el salario mínimo general diario vigente en el Distrito Federal, cuando: I. Proporcionen el nombre, domicilio y cualquier otro dato del Cliente contenido en su base de datos a un Usuario o a un tercero, sin contar con la autorización del Cliente, sin perjuicio de las demás sanciones a que se hagan*

acreedores, incluso de naturaleza penal, conforme a esta ley u otros ordenamientos legales, y II. Hagan uso o manejo indebido de la información, en los términos del artículo 22 de esta ley". Sin duda, lo recién señalado es de máxima importancia, pues se establece claramente que las infracciones a los deberes de secreto y uso de los datos personales son estimadas como graves por el legislador.

A continuación, el artículo 56 agrega a lista de sanciones que: *"Las comisiones encargadas de la inspección y vigilancia de las Entidades Financieras de que se trate, podrán sancionar a las mismas con una multa de 100 a 500 veces el salario mínimo general diario vigente en el Distrito Federal, cuando soliciten información sin contar con la autorización prevista en el artículo 28, sin perjuicio de las demás sanciones a que se hagan acreedoras incluso de naturaleza penal, conforme a esta ley u otros ordenamientos legales".* El inciso 2º añade que: *"En caso de que alguna Sociedad proporcione información sin que se haya recabado la autorización a que se refiere este artículo, en los términos de los artículos 29 y 30 siguientes, se entenderá como violación de dicha Sociedad a las disposiciones".* Lo recién dicho es concordante con el principio del consentimiento e información del titular de los datos para el tratamiento de éstos, pues la referencia al artículo 28 alude directamente a la autorización previa e informada que debe prestar el cliente para que la entidad financiera pueda entregar sus datos personales a las sociedades de información crediticia.

9.2 Responsabilidad Civil

En cuanto al régimen de responsabilidad civil, debemos señalar que comúnmente las disposiciones estatutarias sectoriales se refieren a ella en términos generales, por lo que se entiende que deben aplicarse las reglas generales de esta clase de responsabilidad (Arts. 1910 y ss. Código Civil). Sólo hace excepción a lo dicho las reglas de la Ley para regular las Sociedades de Información Crediticia. A continuación señalaremos las normas aplicables según las leyes ya analizadas.

9.2.1) Ley de Instituciones de Crédito

El artículo 118 de esta Ley dispone que salvo toda clase de información que sea solicitada por la Comisión Nacional Bancaria, la violación del secreto propio de las operaciones bancarias en general generará *"(…) responsabilidad civil por los daños y perjuicios ocasionados, sin perjuicio de las responsabilidades penales procedentes".*

Ley de Protección y Defensa al Usuario de Servicios Financieros

Esta Ley dispone en el artículo 15 en materia de responsabilidad que: *"La Comisión Nacional y sus servidores públicos, según sea el caso, estarán obligados a reparar los daños y perjuicios que se causen en caso de revelación del secreto bancario, fiduciario o bursátil, en términos de la legislación aplicable".*

9.2.3) Ley para regular las Sociedades de Información Crediticia

Sin duda, son las disposiciones de esta ley las que hacen excepción a las reglas generales de la responsabilidad civil, pues prescribe el artículo 51 que: "*Las Sociedades*

responderán por los daños que causen a los Clientes al proporcionar información cuando exista culpa grave, dolo o mala fe en el manejo de la base de datos. (…) Los Usuarios que proporcionen información a las Sociedades igualmente responderán por los daños que causen al proporcionar dicha información, cuando exista culpa grave, dolo o mala fe".

A renglón seguido, el artículo 52 señala que: *"Aquellos Usuarios que obtengan información de una Sociedad sin contar con la autorización a que se refiere el artículo 28 de esta ley, o que de cualquier otra forma cometan alguna violación al Secreto Financiero, estarán obligados a reparar los daños que se causen, sin menoscabo de las demás sanciones, incluyendo las penales, que procedan".*

En esta materia ya hemos señalado que creemos que el régimen de responsabilidad establecido por esta Ley es inadecuado, pues conlleva a una limitación de la responsabilidad tanto de los usuarios del sistema (instituciones financieras en general y las empresas comerciales) como de las sociedades de información crediticia. Al disponerse que sólo se responderá de los daños que se causen con *"culpa grave, dolo o mala fe"*, no sólo se alteran las reglas generales de la responsabilidad civil extracontractual, en la cual se responde de todo daño causado por culpa o negligencia, sino que pone de cargo de los deudores o clientes el riesgo que implica el funcionamiento del mercado de la información crediticia. Reafirmamos nuevamente lo dicho más arriba (punto Nº 2.2.6. de este análisis), en cuanto a que en este caso la ley ha beneficiado injustamente a quienes lucran con este mercado, pues al hacer procedente la responsabilidad civil sólo ante conductas dolosas de quienes que están en la mejor posición para evitar los riesgos (Sociedades de Información Crediticia), se desconoce toda la fundamentación de justicia que se erige tras la atribución de responsabilidad por negligencia.

Finalmente, tenemos que señalar que en los demás casos en que se cause daño injustamente como consecuencia de la vulneración de los bienes jurídicos que están tras la protección de los datos personales en el ordenamiento jurídico mexicano, cabría aplicar las reglas generales de responsabilidad civil, a falta de normas especiales. A este respecto, el artículo 1910 del Código Civil dispone que: *"El que obrando ilícitamente o contra las buenas costumbres cause daño a otro, esta obligado a repararlo, a menos que demuestre que el daño se produjo como consecuencia de culpa o negligencia inexcusable de la victima"*. Esta responsabilidad se extiende también al daño moral, el cual está expresamente contemplado tanto en materia contractual como extracontractual [421].

9.3 Responsabilidad Penal

Algunas de los estatutos sectoriales que hemos analizado, tipifican ciertas conductas como delitos. Respecto de éstos, resulta difícil predicar que el objeto de protección sea la libertad informática o el derecho a la protección de datos. A lo más, podría afirmarse que la protección alcanza a bienes jurídicos como la intimidad o la vida privada. Las disposiciones especiales se señalan a continuación.

[421] Las reglas generales de la responsabilidad por daño se encuentran establecidas en el artículo 1910 y ss. Éstas pueden consultarse [en línea] < http://www.solon.org/Statutes/Mexico/Spanish/codigo_civil.pdf > [consulta: 25 de Marzo 2003].

9.3.1) Ley de Instituciones de Crédito

El artículo112 bis de esta ley señala que se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que: *"(…) IV. Obtenga o use indebidamente la información sobre clientes u operaciones del sistema bancario, y sin contar con la autorización correspondiente".* El inciso 2º agrega por su parte que: *"La pena que corresponda podrá aumentarse hasta en una mitad más, si quien realice cualquiera de las conductas señaladas en las fracciones anteriores tiene el carácter de consejero, funcionario o empleado de cualquier institución de crédito".*

9.3.2) Código Penal [422]

El Código Penal mexicano por su parte, contempla los delitos contra la vida privada o la intimidad que, en general, están presentes en todas las legislaciones latinoamericanas. A continuación se señalaran las disposiciones pertinentes.

a) Violación de comunicación escrita

El artículo173, sanciona con la pena de tres a ciento ochenta jornadas de trabajo en favor de la comunidad: *"I - Al que abra indebidamente una comunicación escrita que no esté dirigida a él, y II - Al que indebidamente intercepte una comunicación escrita que no esté dirigida a él, aunque la conserve cerrada y no se imponga de su contenido".*

b) Violación de comunicaciones privadas

Por otra parte, el artículo 177 castiga a quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, sancionándolo *"de seis a doce años de prisión y de trescientos a seiscientos días multa".*

c) Violación de secretos

En cuanto al delito de revelación de secreto, el artículo 210 sanciona con treinta a doscientas jornadas de trabajo en favor de la comunidad, *"al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto".*

d) Revelación de información privada obtenida ilícitamente

El artículo 211 bis castiga a quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, la sanción puede ir *"de seis a doce años de prisión y de trescientos a seiscientos días multa".*

[422] **[En línea] < http://www.unifr.ch/derechopenal/legislacion/mx/cp_mexico.htm > [consulta: 25 de Marzo 2003].**

e) Violación de domicilio

Por último, en materia de violación de domicilio, el artículo 285 señala que: *"Se impondrán de un mes a dos años de prisión y multa de diez a cien pesos, al que, sin motivo justificado, sin orden de autoridad competente y fuera de los casos en que la ley lo permita, se introduzca, furtivamente o con engaño o violencia, o sin permiso de la persona autorizada para darlo, a un departamento, vivienda, aposento o dependencias de una casa habitada".*

9.3.3) Ley de Imprenta

El artículo 10 de esta Ley sanciona la infracción de cualquiera de las prohibiciones que contenidas en el artículo 9 (ver punto Nº 2.2.1), se castigará con multa de cincuenta a quinientos pesos y arresto que no bajará de un mes ni excederá de once. El artículo 12 por su parte dispone que: *"Los funcionarios y empleados que ministren datos para hacer una publicación prohibida, sufrirán la misma pena que señala el artículo 10 y serán destituidos de su empleo, a no ser que en la ley esté señalada una pena mayor por la revelación de secretos, pues en tal caso se aplicará ésta".*

10. Conclusiones

El ordenamiento jurídico mexicano no cuenta con una ley de protección de datos personales, así como tampoco dispone a nivel constitucional de reglas que reconozcan el derecho a la protección de datos o hábeas data. En este ámbito sólo encontramos indirectamente consagrados los derechos a la intimidad y a la vida privada, los cuales, sin embargo, se encuentran garantizados por la vigencia de la Convención Americana de Derechos Humanos, texto ratificado por el Estado mexicano.

A pesar de la falta de legislación en la materia de estudio, cabe destacar a lo menos dos estatutos legales que se ocupan de regular la protección a los datos personales desde distintos ámbitos. Ellos son, la Ley de Protección al Consumidor y la Ley para Regular las Sociedades de Información Crediticia. Las demás normas legales especiales sólo se ocupan del secreto financiero y tributario. Con todo, en la actualidad se encuentra en discusión parlamentaria dos Proyectos de Ley sobre protección de datos personales, los cuales esperamos puedan llenar el vacío legislativo en la materia.

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN NICARAGUA

1. Generalidades

El sistema jurídico nicaragüense reconoce a nivel constitucional el derecho de acceso a los datos personales que se encuentren en poder de los organismos del Estado. Sin embargo, este derecho de acceso a los datos no aparece tutelado por un mecanismo constitucional específico, por lo cual sería necesario recurrir al mecanismo procesal del amparo para que éste no quede sin protección efectiva.

En el ámbito infraconstitucional, Nicaragua no dispone de una legislación de protección a los datos personales. Ante ello, sólo nos referiremos a una disposición de la Legislación Común Tributaria, dado que es el único estatuto relacionado con la materia de estudio al cual hemos accedido.

2. Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional

A nivel constitucional, el ordenamiento jurídico nicaragüense contempla expresamente un derecho de acceso a la información registrada por las autoridades estatales. Este derecho es reconocido en una misma disposición junto a la vida privada de la persona y de su familia, la inviolabilidad de domicilio, correspondencia y de las comunicaciones, así como también junto al derecho a la honra y la reputación. Al efecto, se señala en el artículo 26 que toda persona tiene derecho:

"*1. A su vida privada y la de su familia.*

2. A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo.

3. Al respeto de su honra y reputación.

4. A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información". [423]

Cabe comentar que el numeral 4 del artículo 26 reconoce un derecho de acceso a los datos personales muy particular, pues si bien implica tanto el derecho a conocer el porqué el Estado registra esos datos, como la finalidad de su utilización, llama la atención la opción del Constituyente de omitir los derechos de rectificación, actualización y supresión respecto de los archivos o bancos de datos pertenecientes a organismos del Estado. Por otra parte, también extraña la exclusión de los archivos y bancos de datos de carácter privado. La razones de esta particular configuración no la sabemos, por lo que en este punto nuestro estudio queda limitado al sólo análisis exegético del texto.

Debemos agregar a lo ya dicho, que el Constituyente si bien reconoce un derecho de acceso limitado, tampoco señala el procedimiento aplicable para hacerlo efectivo ante los entes públicos responsables de los archivos o bancos de datos. En razón de lo anterior, creemos que a falta de disposición específica deberá utilizarse el procedimiento de amparo constitucional.

[423] [En línea] < http://www.georgetown.edu/pdba/Constitutions/Nica/nica95.html > [consulta: 3 de Noviembre 2002]

En lo relativo a los otros derechos reconocidos por la Constitución nicaragüense, cabe decir que el inciso 2º del artículo 26 reconoce la inviolabilidad del domicilio de la siguiente forma: *"el domicilio sólo puede ser allanado por orden escrita de juez competente"*, excepto: a) Si los que habitaren en una casa manifestaren que allí se está cometiendo un delito o de ella se pidiera auxilio; b) Si por incendio, inundación u otra causa semejante, se hallare amenazada la vida de los habitantes o de la propiedad; c) Cuando se denunciare que personas extrañas han sido vistas en una morada, con indicios manifiestos de ir a cometer un delito; d) En caso de persecución actual e inmediata de un delincuente y e) Para rescatar a la persona que sufra secuestro. A continuación, se dispone que: *"la ley fija los casos y procedimientos para el examen de documentos privados, libros contables y sus anexos, cuando sea indispensable para esclarecer asuntos sometidos al conocimiento de los tribunales de justicia o por motivos fiscales"*. Se añade que las cartas, documentos y demás papeles privados substraídos ilegalmente no producen efecto alguno en juicio o fuera de él (Art. 26 inciso final).

Más adelante, y en otro ámbito, el artículo 29 prescribe que toda persona tiene derecho a la libertad de conciencia, de pensamiento y de profesar o no una religión, prescribiendo que: *"nadie puede ser objeto de medidas coercitivas que puedan menoscabar estos derechos ni a ser obligado a declarar su credo, ideología o creencia".*

De la disposición anterior deducimos que nadie está obligado a suministrar datos personales de carácter sensible relativos a los pensamientos, ideologías y creencias religiosas. Consecuencialmente, creemos que existiría al menos un principio de prohibición de la recolección y tratamiento de este tipo de datos sin la autorización de su titular. Asimismo, consideramos que la disposición señalada estaría tutelando el derecho a la intimidad aunque el Constituyente no lo señale de manera directa, pues tanto el credo, la ideología o las creencias, en general pueden estimarse como pertenecientes a un ámbito más particular y reservado del derecho a la vida privada, como lo es la intimidad personal.

Siguiendo el análisis de la protección constitucional a los datos personales, debemos agregar que el artículo 182 señala que: *"la Constitución Política es la carta fundamental de la República; las demás leyes están subordinadas a ella. No tendrán valor alguno las leyes, tratados, órdenes o disposiciones que se le opongan o alteren sus disposiciones"*. En relación con esta disposición tenemos dudas en cuanto al nivel jerárquico que se le otorgaría por el Estado de Nicaragua a los tratados internacionales sobre Derechos Humanos ratificados por éste, pues no existe disposición expresa al respecto. Sin embargo, pensamos que si el Estado nicaragüense ratificó el tratado y además reconoció competencia a la Corte Interamericana de Derechos Humanos [424], puede deducirse, a lo menos, que los derechos consagrados en la Convención se integrarían en un nivel no inferior a las normas de carácter constitucional y, que en caso de conflicto normativo con las disposiciones constitucionales nacionales deberían primar por sobre éstas. Si se interpretara de otra forma, no tendría sentido el hacerse parte y someterse jurídicamente a lo previsto en un tratado internacional de protección a los Derechos Humanos.

Finalmente, y en lo referente a la tutela de los derechos consagrados por la Constitución, cabe hacer presente que el artículo 45 prescribe que: *"las personas cuyos derechos constitucionales hayan sido violados o estén en peligro de serlo, pueden*

interponer el recurso de exhibición personal o de amparo, según el caso y de acuerdo con la Ley de Amparo". Por lo tanto, entendemos que los derechos consagrados por la Ley Fundamental, están tutelados en general por la acción de amparo que regula la propia Ley de Amparo. Esta normativa, en virtud del artículo 184 de la Constitución, tiene el rango de Ley Constitucional.

En suma, en el ordenamiento jurídico constitucional de Nicaragua sólo se contempla un derecho de acceso a los datos personales, ejercitable a través de la acción de amparo únicamente respecto de los archivos, registros o bancos de datos pertenecientes al Estado y sus organismos. Pensamos que esta configuración no se ajusta al principio de igualdad y no vemos la razón de excluir el acceso a los archivos o bancos de datos particulares, pues los peligros que entraña el tratamiento automatizado de datos están presentes con independencia del carácter de quién sea el que los recolecte y efectúe su tratamiento. Por otra parte, la limitación del derecho sólo a su variante informativa, deja trunca la efectiva protección de los derechos de los particulares, sean éstos la vida privada o la intimidad. Por lo mismo, nos inclinamos a pensar que la autodeterminación informativa no estaría detrás de la disposición del Nº 4 del artículo 26, sino más bien la vida privada e intimidad.

2.2 Protección Legal de los Datos Personales

A nivel infraconstitucional, el ordenamiento jurídico nicaragüense no dispone de una ley de protección de datos personales. A pesar de lo anterior, podemos señalar que existen, al menos, dos estatutos jurídicos que establecen deberes de reserva respecto de ciertos datos personales. Estos son, la Ley de Bancos y la Legislación Tributaria Común las cuales que se reseñan a continuación.

2.2.1) Ley General de Bancos, Instituciones Financieras no Bancarias y Grupos Financieros [425]

Esta Ley contempla el denominado "Sigilo bancario" en el artículo 109, el cual dispone que: *"Los bancos no podrán dar informes de las operaciones activas y pasivas que*

[424] El 12 de febrero de 1991 se presentó en la Secretaría General de la OEA, un instrumento de fecha 15 de enero de 1991, mediante el cual el Gobierno de Nicaragua declara: I. El Gobierno de Nicaragua reconoce como obligatoria de pleno y sin convención especial, la competencia de la Corte Interamericana de Derechos Humanos, sobre todo los casos relativos a la interpretación o aplicación a la Convención Interamericana sobre Derechos Humanos, "Pacto de San José de Costa Rica", de conformidad con lo dispuesto en el artículo 62, inciso 1 de la misma. II. El Gobierno de Nicaragua, al consignar lo referido en el punto I de esta Declaración, deja constancia que la aceptación de la competencia de la Corte Interamericana de Derechos Humanos se hace por plazo indefinido, con carácter general, bajo condiciones de reciprocidad y con la reserva de que los casos en que se reconoce la competencia, comprenden solamente hechos posteriores o hechos cuyo principio de ejecución sean posteriores a la fecha de depósito de esta declaración ante el Secretario General de la Organización de Estados Americanos. [En línea] < http://www.oas.org/juridico/spanish/firmas/b-32.html > [consulta: 20 de Marzo 2003].

[425] Esta Ley de Octubre de 1999 (Nº 314) se encuentra disponible [en línea] < http://www.siboif.gob.ni/DOCS/leyes/grales/LEY314.htm > [consulta: 26 de Marzo 2003].

celebren con sus clientes, sino al depositante, ahorrador, suscriptor, deudor o beneficiario, según fuere el caso, a sus representantes legales, o a quienes tengan poder para retirar los fondos o para intervenir en la operación de que se trate, salvo cuando lo autorice expresamente el cliente o cuando lo pidiese la autoridad judicial en virtud de providencia dictada conforme a la ley".

Si bien lo recién anotado es la regla general, la misma disposición señala que quedan exceptuados de estas normas: 1) Los requerimientos que en esa materia demande el Superintendente de Bancos. Asimismo, el Superintendente está facultado para procesar información en materia de legitimación de capitales conforme lo dispongan las leyes y los tratados internacionales; 2) La información crediticia que soliciten otras empresas bancarias como parte del proceso administrativo normal para la aprobación de operaciones de crédito, así como la que solicite el Superintendente para la formación de una central de riesgo. Esto último conforme al reglamento que dicte el Consejo Directivo de la Superintendencia de Bancos; 3) Las publicaciones que, por cualquier medio, realicen los bancos de los nombres de clientes en mora o en cobro judicial, así como de aquellos clientes que emitan cheques sin fondo; 4) La información que se canalice a través de convenios de intercambio y de cooperación suscritos por el Superintendente con autoridades supervisoras financieras de otros países y, 5) Las otras excepciones que contemple la ley. Con todo, se agrega que ninguna autoridad administrativa, exceptuándose a la Superintendencia, podrá solicitar directamente a los bancos, información particular o individual de sus clientes bancarios (Art. 109 inciso 3º).

Las disposiciones recién señaladas establecen claramente el deber de sigilo de las operaciones bancarias tanto activas como pasivas. Ahora bien, dentro del campo de las excepciones a ese deber, cabe comentar la amplitud de éstas, las cuales permiten la transmisión de la información tanto entre las entidades de carácter financiero dentro de Nicaragua como fuera de este país, en base a convenios de intercambio y de cooperación suscritos por el Superintendente con autoridades supervisoras financieras de otros países. Esto último, sin duda que milita en contra de los derechos de las personas, dado que se faculta a una autoridad administrativa para acordar la transmisión internacional de datos personales sin tomar en cuenta las reglas internacionales generalmente reconocidas en la materia. Todo lo anterior, da cuenta de serias falencias normativas en la materia, lo cual sumado a la estrechez del derecho constitucional de acceso a los archivos y bancos de datos del Estado, configuran un panorama no muy alentador en cuanto a la protección a los datos personales, teniendo en cuenta además la gran cantidad de información de la que dispone la Superintendencia, órgano que a su vez es el encargado del registro denominado central de riesgo, el cual cuenta con información consolidada y clasificada sobre los deudores de los bancos [426].

[426] Al respecto se señala por la Ley en el artículo 111 que*: "La Superintendencia de Bancos establecerá un sistema de registro, denominado central de riesgo que contará con información consolidada y clasificada sobre los deudores de los bancos. La información correspondiente estará a disposición de las instituciones financieras autorizadas por la Superintendencia de Bancos. (…) En los casos de centrales de riesgo privadas, éstas estarán sometidas a la aprobación y reglamentación de la Superintendencia, y estarán sujetas al sigilo bancario"*. A su vez, el artículo 112 agrega que *"los bancos están obligados a suministrar mensualmente a la Superintendencia, dentro de los quince días del mes siguiente y en la forma que ella determine, la información que se requiera para mantener al día el registro de que trata el artículo anterior".*

2.2.2) Legislación Tributaria Común [427]

El Decreto Legislativo Nº 713 de 22 de Junio de 1962, establece las normas de la Legislación Tributaria Común. Curiosamente, dentro de este estatuto sólo hemos encontrado una disposición que indirectamente se referiría al secreto bancario. El artículo 12 denominado "Depósitos bancarios" señala que: "*las instituciones bancarias no estarán obligadas a suministrar a las Oficinas Fiscales ningún informe en relación con las cuentas de depósitos de sus clientes".*

De la disposición anterior, se desprende que si bien los bancos no están obligados legalmente a entregar información relativa a las cuentas de depósitos de sus clientes, podrían eventualmente suministrar información a las Oficinas Fiscales, pues no se establece una prohibición al respecto. Por lo tanto, es la institución bancaria la que en definitiva decidirá, teniendo en cuenta las disposiciones legales pertinentes, cuándo podría sin incurrir en responsabilidad, informar a ése órgano del Estado. Lo anterior reforzaría en teoría lo prescrito en el artículo 109 de la Ley de Bancos, lo cual sin embargo, no elimina el peligro del cruce de información, pues si bien la administración tributaria está vedada de exigir de los bancos la información relativa las operaciones pasivas de los clientes, podría enterarse de ésta a través de otros órganos del Estado respecto de los cuales eventualmente no operara la regla de sigilo. Finalmente, cabe agregar que en materia de secreto fiscal o tributario, curiosamente no encontramos disposiciones en este sentido en la Ley señalada.

En suma, a nivel infraconstitucional Nicaragua no cuenta con una ley de protección de datos personales. En materia legal sectorial, sólo podemos afirmar que se establecería el deber de sigilo bancario de las operaciones tanto activas como pasivas, así como también que no existe una obligación de información a las Oficinas Fiscales por parte de los bancos respecto de las operaciones activas de sus clientes.

3. Bienes Jurídicos Protegidos por la Legislación de Datos Personales

En esta materia, sólo vamos a referirnos a las disposiciones constitucionales respectivas. Como ya se señaló, el artículo 26 reconoce un derecho de acceso relativo a la información personal que conste en los archivos o bases de datos de carácter estatal. Si bien pudiera pensarse en calificar este derecho como de protección de datos, cabría precisar que éste aparece tan limitado *ab initio* que no creemos en esta alternativa, pues no se refiere a los derechos de rectificación, cancelación o supresión de datos. Por otro lado, nada dice respecto de los archivos o bancos de datos de carácter particular o privados. En razón de lo anterior, consideramos que no se estaría frente al bien jurídico libertad informática o derecho a la autodeterminación informativa, sino que más bien la protección dispensada tendría una configuración más cercana al derecho a la vida

[427] **[En línea] < http://www.ciat.org/doc/docu/leg/cod/lni_02_legislacion_tributaria_comun_ nicaragua.doc > [consulta: 26 de Marzo 2003].**

privada -reconocido en el artículo 26- y al derecho a la intimidad. Este último, estimamos se encontraría consagrado de manera indirecta en la Constitución a través del propio derecho a la vida privada, como asimismo en el reconocimiento a que nadie puede ser objeto de medidas coercitivas que puedan menoscabar estos derechos ni a ser obligado a declarar su credo, ideología o creencia (Art. 29 C. Pol.).

4. Principios Informativos de la Legislación de Protección de Datos Personales

Ante la falta de legislación general de protección datos personales en el ordenamiento jurídico de Nicaragua, no nos podremos detener en este punto.

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

Al respecto cabe hacer igual prevención a la señalada en el punto anterior. Por lo tanto, no desarrollaremos esta materia.

6. Modelos de Tutela

En el ordenamiento jurídico nicaragüense, si bien se reconoce constitucionalmente el derechoa conocer toda información que sobre las personashayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información(Art. 26 Nº 4 C. Política), no se contempla un mecanismo específico para hacer valer esos derechos. A pesar de lo anterior, estimamos que ante la falta de normas legales para hacer efectivo el derecho constitucional de acceso a la información, sería procedente aplicar las normas constitucionales que regulan la acción de amparo, la cual pasamos a reseñar.

6.1 La Acción de Amparo

Por mandato constitucional el legislador nicaragüense se ha encargado de regular la acción de amparo. La respectiva normativa es la Ley de Amparo, la cual según el artículo 184 de la Constitución tiene rango de ley constitucional [428] .

6.1.1) Procedencia de la Acción

Se prescribe por la Ley que es procedente la acción de amparo: *"(…) por toda disposición, acto o resolución, y en general, toda acción u omisión de cualquier funcionario, autoridad o agente de los mismos, que viole o trate de violar los derechos y garantías consagrados en la Constitución Política"* (Art. 23).

[428] Esta ley lleva el Nº 49 y es de fecha 16 de noviembre de 1988. Fue publicada en La Gaceta Nº 241 de 20 de diciembre de 1988. [En línea] < http://www.uc3m.es/uc3m/inst/MGP/JCI/02-nicaragua-leydeamparo.htm > [consulta: 19 de Enero 2003].

El artículo 51 por su parte, señala entre los casos en que no será procedente la acción de Amparo los siguientes: Cuando hayan cesado los efectos del acto, reclamado o este se haya consumado de modo irreparable y cuando se trate de actos que hubieren sido consentidos por el agraviado de modo expreso o tácito. Se añade por este mismo artículo, que se presumen consentidos aquellos actos por los cuales no se hubiere recurrido de Amparo dentro del término legal, sin perjuicio de la suspensión del término de conformidad al derecho común.

6.1.2) Legitimación Activa

En relación a la legitimación activa del amparo, el artículo 23 señala que: *"el Recurso de Amparo sólo puede interponerse por parte agraviada. Se entiende por tal toda persona natural o jurídica a quien perjudique o esté en inminente peligro de ser perjudicada (…)".*

6.1.3) Legitimación Pasiva

La ley dispone en esta materia que: *"el Recurso de Amparo se interpondrá en contra del funcionario o autoridad que ordene el acto que se presume violatorio de la Constitución Política contra el agente ejecutor o contra ambos"* (Art. 24).

6.1.4) Competencia

En lo tocante a la competencia para conocer del amparo, el artículo 25 prescribe que esta acción se interpondrá ante "*el Tribunal de Apelaciones respectivo o ante la Sala para lo Civil de los mismos, en donde estuviera divididos en Salas, el que conocerá de las primeras actuaciones hasta la suspensión del acto inclusive, correspondiéndole a la Corte Suprema de Justicia el conocimiento ulterior hasta la resolución definitiva. Si el Tribunal de Apelación se negare a tramitar el recurso, podrá el perjudicado recurrir de Amparo por la vía de hecho ante la Corte Suprema de Justicia"* (sic).

6.1.5 Procedimiento Aplicable

El procedimiento de la acción de amparo puede sintetizarse de la siguiente forma:

1) *Demanda*: la acción de amparo debe se interponerse dentro del término de treinta días, contados *"desde que se haya notificado o comunicado legalmente al agraviado, la disposición, acto o resolución. En todo caso este término se aumentará en razón de la distancia. También podrá interponerse el Recurso desde que la acción u omisión haya llegado a su conocimiento"* (Art. 26 Ley Amparo). Dentro de los requisitos formales, se señala que la acción de amparo se interpondrá por escrito en papel común con copias suficientes para las autoridades señaladas como responsables y para la Procuraduría General de Justicia (Art. 27). El escrito deberá contener:1) Nombres y apellidos del agraviado y de la persona que lo promueva en su nombre; 2) Nombre, apellidos y cargos del funcionario, autoridades o agentes de los mismos contra quien se interpone la acción; 3) Disposición, acto, resolución, acción u omisión contra los cuales se reclama, incluyendo si la Ley, Decreto Ley, Decreto o Reglamento, que a juicio del recurrente fuere inconstitucional; 4) Las disposiciones constitucionales que el reclamante estime violadas;

5) La acción podrá interponerse personalmente o por apoderado especialmente facultado para ello; 6) El haber agotado los recursos ordinarios establecidos por la ley, o no haberse dictado resolución en la última instancia dentro del término que la ley respectiva señala y, 7) Señalamiento de casa conocida en la ciudad sede del Tribunal para subsiguientes notificaciones. En relación al requisito del Nº 6 recién expuesto, cabe hacer presente que no tenemos conocimiento de procedimiento especial mediante el cual hacer valer el derecho de acceso a la información consagrado en el artículo 26 de la Constitución. De lo dispuesto en el número 6 del artículo 27, consideramos que la facultad de ejercitar el derecho de acceso a los datos personales a través de la acción de amparo, tendría el carácter de subsidiaria al ejercicio directo del derecho ante las autoridades estatales respectivas. Cabe agregar que en estos casos la Procuraduría General de Justicia será parte en la sustanciación de la presente acción (Art. 30).

2) *Traslado y suspensión del acto*: interpuesto en forma la acción ante el tribunal, se deberá poner en conocimiento de la Procuraduría General de Justicia acompañándole copia del Recurso. El Tribunal dentro del término de tres días, de oficio o a solicitud de parte, debe decretar la suspensión del acto contra el cual se reclama o denegarla en su caso (Art. 31). Procederá la suspensión de oficio, "*cuando se trate de algún acto que de llegar a consumarse, haría físicamente imposible restituir al quejoso en el goce del derecho reclamado, o cuando se notoria la falta de jurisdicción o competencia de la autoridad, funcionario o agente contra quien se interpusiera el Recurso, o cuando el acto sea de aquellos que ninguna autoridad puede ejecutar legalmente"* (Art. 32). Al decretarse la suspensión, el Tribunal debe fijar la situación en que habrán de quedar las cosas y tomará las medidas pertinentes para conservar la materia objeto del amparo, hasta la terminación del respectivo procedimiento (Art. 34). Una vez resuelta la suspensión del acto reclamado, *"se remitirán los autos en el término de tres días a la Corte Suprema de Justicia para la tramitación correspondiente previniéndoles a las partes que deberán personarse dentro del término de tres días hábiles, más el de la distancia, para hacer uso de sus derechos. Si el recurrente no se persona dentro del término señalado anteriormente, se declarará desierto el Recurso"* (Art. 38).

3) *Informe*: el Tribunal respectivo pedirá a los señalados como responsables, envíen informe a la Corte Suprema de Justicia dirigiéndoles oficio por correo en pieza certificada, con aviso de recibo, o por cualquier otra vía que a juicio del Tribunal resulte mas expedito. El informe deberá rendirse dentro del término de diez días, contados desde la fecha en que reciban el correspondiente oficio. Con él se remitirán en su caso, las diligencias de todo lo actuado (Art. 37). Recibidos los autos por la Corte Suprema de Justicia, con o sin el informe, dará al Amparo el curso que corresponda. La falta de informe establece la presunción de ser cierto el acto reclamado (Art. 39).

4) *Ampliación de hechos*: la Corte Suprema de Justicia podrá pedir al recurrente, ampliación sobre los hechos reclamados y resolver sobre todo lo relativo a la suspensión del acto (Art. 40).

5) *Plazos*: en el amparo *"no habrá lugar a caducidad ni cabrán alegatos orales (…)"* (Art. 41).

6) *Prueba*: si el Tribunal Supremo no encontrara datos suficientes para resolver el Amparo, lo abrirá a prueba por el término de diez días, siendo admisible toda clase de

pruebas y podrá recabar de oficio otras que considere convenientes (Art. 43).

6.1.6) La Sentencia

En cuanto a la sentencia de amparo se señala que: *"sólo se referirá a las personas naturales o jurídicas que hubieren interpuesto el Recurso, limitándose si procediese a ampararlo y protegerlos en el caso especial controvertido"* (Art. 44). Ésta deberá ser razonada, con fijación clara del acto o actos reclamados, indicación de los fundamentos legales en que se apoya para declarar la legalidad o ilegalidad del acto reclamado y de los puntos resolutivos del mismo, señalándose en ellos con claridad y precisión el acto o actos por los que se concede o deniegue el amparo (Art. 45).

Respecto de los efectos de la sentencia, se indica por la Ley que cuando el acto o actos reclamados sean de carácter positivo, *"la sentencia que concede el Amparo tendrá por objeto restituir al agraviado en el pleno goce de los derechos transgredidos, restableciendo las cosas al estado que tenían antes de la transgresión".* En el caso que sea de carácter negativo el efecto del Amparo éste consistirá en *"obligar a las autoridades o funcionarios responsables a que actúen en el sentido de respetar la ley o garantía de que se trate y a cumplir por su parte lo que la misma exija"* (Art. 46). Finalmente, debemos agregar que la Corte Suprema de Justicia, *"en todo caso deberá dictar la sentencia definitiva dentro de los cuarenta y cinco días posteriores a la recepción de las diligencias"* (Art. 47).

6.2 Otras Acciones

No tenemos conocimiento de otras acciones que sean procedentes para la protección de los datos personales en el ordenamiento jurídico nicaragüense.

7. Mecanismos de Control

Al respecto, no podremos referirnos dada la inexistencia de una ley general de protección de datos que los prevea.

8. Transmisión Internacional de Datos

En materia de transmisión internacional de datos personales, sólo cabe recordar lo señalado en el artículo 109 de la Ley General de Bancos, el cual establece como excepción al sigilo bancario, el suministro de información que se canalice a través de convenios de intercambio y de cooperación suscritos por el Superintendente con autoridades supervisoras financieras de otros países. Esta facultad, sin más explicaciones ni requisitos, en nuestro concepto sería un ámbito de riesgo para los derechos de las personas, dado que nada asegura que el uso de esos datos se corresponda con la finalidad para la cual ha sido cedida.

9. Régimen de Responsabilidad

Ante la falta de una legislación en materia de protección de datos personales que prevea un régimen especial en Nicaragua, sólo nos referiremos a las normas que ya hemos señalado en el punto Nº 2.2 de este análisis, y para cuyos casos de inobservancia se establecen sanciones. Junto con ellas revisaremos las normas penales que tutelan la vida privada e intimidad.

9.1 Responsabilidad Administrativa

En este campo, podemos señalar que la Ley General de Bancos prevé reglas de responsabilidad por violación al sigilo bancario. Al efecto, el artículo 110 señala que: "*Los funcionarios y empleados de los bancos serán responsables, de conformidad con la Ley, por la violación del sigilo que se establece en el artículo anterior. En el caso de violación, los bancos y empleados o funcionarios responsables estarán obligados solidariamente a reparar los daños y perjuicios que se causen".*

Por otra parte, el artículo 80 de la Ley de Amparo dispone que: *"Siempre que al declararse con lugar cualquiera de los recursos que establece esta Ley, apareciera que la violación cometida constituye delito se dará parte a quien corresponda deducir la responsabilidad por la infracción cometida"*. De lo anterior, se deduce que ante una violación a los preceptos constitucionales por los funcionarios públicos, en especial, a las disposiciones del artículo 26, será procedente la responsabilidad administrativa de éstos según las reglas particulares o generales que los rijan en la materia.

9.2 Responsabilidad Civil

En materia civil no estamos al tanto de la normativa general sobre la responsabilidad por daño, por lo que no nos referiremos a ésta. Aún sin conocerla, se puede afirmar que es de toda justicia que ante un daño antijurídico sea procedente la reparación de éstos y la compensación de los daños morales. En el evento de violación del deber de sigilo bancario -como ya se anotó- el artículo 110 de la Ley General de Bancos dispone que: *"En el caso de violación, los bancos y empleados o funcionarios responsables estarán obligados solidariamente a reparar los daños y perjuicios que se causen".*

9.3 Responsabilidad Penal

En materia penal sólo nos referiremos a los tipos establecidos por la legislación general del Código Penal nicaragüense que tutelan ordinariamente, los bienes jurídicos vida privada e intimidad [429] .

a) Violación de secretos:

El artículo 238 del Código Penal prescribe en la materia que: *"Será castigado con arresto inconmutable de seis meses a dos años y multa de cincuenta a veinte mil córdobas el empleado de correos o telégrafos que abusando de su empleo se apodere de carta, de un pliego, de un sobre cerrado, de un telegrama, o de otras piezas de correspondencia*

[429] [En línea] < http://www.unifr.ch/derechopenal/legislacion/ni/cp_nicaragua.htm > [consulta: 26 de Marzo 2003].

siempre que se impusiere de su contenido, la entregare a otro que no fuere el destinatario o ya sea rompiendo u ocultando, o cambiando su texto, agravándose la pena si lo propalare a otras personas sin la debida autorización, máxime cuando tenga un carácter de intimidad".

Por su parte, el artículo 239 agrega que: *"Será castigado con arresto inconmutable de seis meses a dos años y con multa de cincuenta a veinte mil córdobas, el que teniendo noticias por razón de su estado, oficio, empleo, profesión o arte, de un secreto cuya divulgación puede cuasar daño, lo revelare sin causa justa".*

A continuación de lo anterior, el artículo 240 sanciona al que: *"Sin facultad del que pueda otorgarla publicare o hiciere circular el contenido de una carta"*, con la pena de prisión de 3 meses a 1 año. Si la publicación del contenido de la carta, pliego o mensaje se hiciere por medio de la prensa, radio o televisión, la pena será de arresto inconmutable de seis meses a dos años y multa de cincuenta a veinte mil córdobas, y en este caso se considerará coautor del delito al dueño o empleado de la empresa publicitaria que hubiere ordenado o autorizado la publicación.

El artículo 242, prescribe por otra parte que: *"El administrador, empleado o dependiente que en tal concepto conociere los secretos de su principal y los divulgare, será castigado con la pena de arresto inconmutable de seis meses a dos años y multa de cincuenta a veinte mil córdobas".*

b) Violación de domicilio y allanamiento de morada:

En relación con estos delitos, el artículo 244 señala que: *"El particular que entrare en domicilio ajeno contra la voluntad expresa de su morador, comete el delito de violación de domicilio y será castigado con arresto de 1 a 2 meses y multa de diez a cien córdobas. Si la violación del domicilio se verificare con violencia o intimidación, se aumentará la pena de 2 a 4 meses de arresto y multa de veinte a doscientos córdobas".*

Finalmente, el artículo 248 dispone en lo que nos interesa que: *"El funcionario público, agente de la autoridad, fotógrafo o periodista que penetrare en un domicilio ajeno sin permiso de moradores o sin las formalidades prescritas por las leyes, comete el delito de allanamiento de morada y sufrirá la pena de seis meses a dos años de arresto inconmutable y multa de cincuenta a veinticinco mil córdobas".*

10. Conclusiones

El ordenamiento jurídico nicaragüense sólo cuenta a nivel constitucional con una disposición que reconoce el derecho de acceso a los datos personales que se encuentren en poder de los organismos del Estado. Este derecho de acceso a la información, es restringido pues nada se dice respecto de los derechos de rectificación supresión o cancelación. Por otro lado, el texto restringe el derecho de acceso sólo a los datos contenidos en archivos o bancos de datos públicos, por lo cual el ejercicio de la acción de de tutela, en principio, no podría dirigirse en contra de particulares. Ante esta omisión, opinamos que es factible alegar una eventual violación del derecho de igualdad, fundado ya no en la Constitución sino en la Convención Americana de Derechos Humanos, la cual

ha sido ratificada por Nicaragua. Dada la inexistencia de un mecanismo de tutela específico y omnicomprensivo de las violaciones a los derechos de las personas a consecuencia del tratamiento de sus datos personales, creemos que el medio idóneo para tal efecto en la actualidad sería la acción de amparo constitucional la cual, sin embargo, no satisface completamente las exigencias de una acción específica de hábeas data, pues sólo puede dirigirse en contra de funcionarios del Estado que violen los derechos constitucionales. La falencia anotada, podría eventualmente ser suplida haciendo un llamado al artículo 25.1 del Pacto de San José de Costa Rica a falta de la previsión por la Ley de Amparo.

En el plano sustantivo legal, Nicaragua no cuenta con una ley de protección de datos personales. En cuanto a leyes sectoriales que se ocupen de la materia, sólo en el ámbito bancario encontramos normas relativas al sigilo bancario, las que tampoco otorgan una protección adecuado a los titulares de la información, dada la amplia configuración de las excepciones a esos deberes, especialmente en cuanto a la transmisión internacional de datos.

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN PANAMÁ

1. Generalidades

El ordenamiento jurídico panameño no dispone de normas constitucionales que reconozcan un derecho a la autodeterminación informativa ni que establezcan una acción de hábeas data. En materia legal, tampoco posee una ley de protección de datos personales. Sin embargo, a nivel infraconstitucional cuenta con dos leyes que se ocupan de materias relacionadas con la protección de datos personales pero de forma diversa; la primera, regula el mercado de la información crediticia y, a propósito de esa regulación desarrolla una normativa eventualmente influida por los principios y normas contempladas en la Directiva 95/46 CE, estableciendo un derecho de acceso, rectificación y supresión de ciertos datos. La otra ley, consagra la acción de hábeas data respecto de los datos personales que obran en los registros y archivos pertenecientes a los organismos del Estado, así como también a los contenidos en registros y archivos privados pero que contienen información de carácter público. Además de las normas legales ya señaladas, se prevén ciertas disposiciones sectoriales que comúnmente establecen deberes de confidencialidad de los datos de carácter bancario y tributario.

2. Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional

La Constitución Política panameña [430] no contiene disposiciones que reconozcan el derecho a la protección de datos personales o derecho a la autodeterminación informativa, ni que establezcan la garantía del hábeas data. Tampoco existe en la Carta Fundamental un directo reconocimiento al derecho a la vida privada y a la intimidad. En esta materia, sólo se prevén algunas disposiciones referidas a la inviolabilidad del domicilio, de la correspondencia y de toda clase de comunicaciones. Sin embargo, debemos señalar que el Estado panameño ha suscrito y ratificado la Convención Americana de Derechos Humanos, con lo cual los vacíos normativos podrían ser suplidos por las normas del derecho internacional de los Derechos Humanos [431] . A continuación se señalarán las disposiciones constitucionales relacionadas con la protección de los bienes jurídicos vida privada e intimidad.

Dentro del Capítulo III, relativo a los Derechos y Deberes Fundamentales, el artículo 17 establece un deber general de protección de los derechos constitucionales por parte de las autoridades de la República, señalando que éstas se encuentran *"(…) instituidas para proteger en su vida, honra y bienes a los nacionales donde quiera se encuentren y a los extranjeros que estén bajo su jurisdicción; asegurar la efectividad de los derechos y deberes individuales y sociales, y cumplir y hacer cumplir la Constitución y la Ley".*

En materia de derechos específicos, el artículo 26 dispone que: *"el domicilio o residencia son inviolables. Nadie puede entrar en ellos sin el consentimiento de su dueño, a no ser por mandato escrito de autoridad competente y para fines específicos, o para socorrer a víctimas de crímenes o desastres".* Luego, se añade en el inciso 2º que: *"los servidores públicos de trabajo, de seguridad social y de sanidad pueden practicar, previa identificación, visitas domiciliarias o de cumplimiento de las leyes sociales y de salud pública".*

Por otra parte, el artículo 29 prescribe que: *"la correspondencia y demás documentos privados son inviolables y no pueden ser ocupados o examinados sino por disposición de autoridad competente, para fines específicos y mediante formalidades legales".* Se añade que en todo caso, se guardará reserva sobre los asuntos ajenos al objeto de la ocupación o del examen. El inciso 2º a su vez agrega que: *"igualmente, las comunicaciones telefónicas privadas son inviolables y no podrán ser interceptadas. El registro de papeles se practicará siempre en presencia del interesado o de una persona de su familia, o en su defecto, de dos vecinos honorables del mismo lugar".*

Más adelante, el Constituyente reconoce el derecho de petición, señalándole plazo a la autoridad pública para que ésta se pronuncie sobre las peticiones que se la hagan. Al efecto, dispone el artículo 41 que: *"toda persona tiene derecho a presentar peticiones y quejas respetuosas a los servidores públicos por motivos de interés social o particular, y el de obtener pronta resolución".* A continuación, el inciso 2º agrega que: *"el servidor público ante quien se presente una petición, consulta o queja deberá resolver dentro del término de treinta días".* Finalmente, se agrega que la Ley señalará las sanciones que

[430] [En línea] < http://www.georgetown.edu/pdba/Constitutions/Panama/panama1994.html > [consulta: 3 de Noviembre 2003].

[431] La ratificación del Pacto San José Costa Rica por el Estado panameño data del 5 de Agosto de 1978. [En línea] < http://www.oas.org/juridico/spanish/firmas/b-32.html > [consulta: 20 de Marzo 2003].

corresponden a la violación de esta norma.

Las disposiciones del artículo 41 recién anotado tienen gran importancia, pues sirven de base a la Ley Nº 6 del año 2002 la cual establece normas para la transparencia en la gestión pública, consagrando la acción de hábeas data. Esta ley, regula el ejercicio del hábeas data en un cuerpo legal en que se confunde tanto la versión del hábeas data impropio como la del hábeas data propio, pues a través del procedimiento previsto se puede solicitar el acceso, actualización, confidencialidad o supresión de los datos personales que consten en los registros o archivos públicos, como también el acceso a información pública sobre la gestión de los entes administrativos del Estado.

Finalmente, cabe añadir en materia constitucional, que el artículo 50 consagra la acción de amparo en los siguiente términos: "*toda persona contra la cual se expida o se ejecute, por cualquier servidor público, una orden de hacer o no hacer, que viole los derechos y garantías que está constitución consagra, tendrá derecho a que la orden sea revocada a petición suya o de cualquiera persona".* El inciso 2º agrega que: *"el recurso de amparo de garantías constitucionales a que este artículo se refiere, se tramitará mediante procedimiento sumario y será de competencia de los tribunales judiciales".*

En suma, el Constituyente panameño no dispone de norma alguna que reconozca el derecho a la protección de datos personales ni su garantía específica, la acción de hábeas data. Por otra parte, tampoco prevé un reconocimiento explícito del derecho a la vida privada e intimidad. No obstante lo anterior, creemos que esos vacíos normativos se suplirían por la aplicación de las normas contenidas en el Pacto de San José de Costa Rica, el cual obliga en esta materia al Estado panameño desde el año 1978.

2.2 Protección Legal de los Datos Personales

Dentro del ordenamiento jurídico panameño, a nivel legal, no se prevé un estatuto de protección a los datos personales. A pesar de ello, destacan dos cuerpos legales que se ocupan parcialmente del tema; uno en materia de información sobre el historial crediticio de los consumidores y el otro en materia de acceso a los datos personales en poder del Estado. Además, se observan ciertas disposiciones legales sectoriales que establecen un deber de confidencialidad respecto de determinados datos.A continuación se analizarán tales normas legales.

Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores o Clientes [432]

La Ley N° 24 del 22 de mayo de 2002, que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores o Clientes (en adelante LSIHCC) tiene dos objetivos principales: 1º) Proteger y garantizar la confiabilidad, la veracidad, la actualización y el buen manejo de los datos personales de consumidores o clientes, relativos a su historial de crédito, incorporados o susceptibles de ser incorporados a una agencia de información de datos administrada por una persona natural o jurídica, debidamente autorizada conforme a la presente Ley y, 2º) Regular la actividad de las personas naturales y jurídicas, públicas o privadas, que se dediquen a administrar las

[432] [En línea] < http://www.legalinfo-panama.com/legislacion/00297.pdf > [consulta: 18 de Noviembre 2002].

agencias de información de datos y a los agentes económicos que mantengan o manejen datos sobre el historial de crédito de los consumidores o clientes (Art. 1).

El ámbito de aplicación de esta normativa está circunscrito a los agentes económicos, personas naturales o jurídicas, públicas o privadas, que se dediquen a realizar cualquier actividad económica, financiera, bancaria, comercial o industrial, que mantengan o manejen datos sobre el historial de crédito de los consumidores o clientes. También será aplicable esta ley a las agencias de información de datos, personas naturales o jurídicas, públicas o privadas, que se dediquen a prestar servicios de almacenamiento, transmisión e información, por cualquier medio tecnológico o manual, de los datos sobre el historial de crédito de los consumidores o clientes (Art. 2) [433] .

De las disposiciones anteriores, se deduce el acotado ámbito de aplicación de la Ley. Pese a ello, creemos que los principios que se desprenden de esta regulación, pueden servir de base para solucionar conflictos en otras materias relacionadas con la protección a los datos personales y que no estén reglamentadas por la ley [434] . A continuación se reseñaran los principales temas desarrollados por la ley en comento.

a) Derechos del consumidor o cliente

La LSIHCC ha señalado expresamente en el artículo 23 los derechos de los titulares de los datos personales tratados por las Agencias de Información de Datos sobre el historial de crédito, éstos son los siguientes:

1)*Acceso a la información*: los consumidores o clientes tienen derecho a conocer

[433] Cabe señalar al respecto, que el artículo 45 de esta Ley dispone que ella es *"de orden público y de interés social, y tiene efecto retroactivo en lo relativo al derecho de rectificación y eliminación de la información de los consumidores o clientes, establecido en el numeral 5 del artículo 23"*. Por otra parte, en materia de vigencia de la ley, el artículo 46 señala que ésta entrará a regir desde su promulgación y deroga cualquier disposición que le sea contraria.

[434] Asimismo, estimamos que algunas de las definiciones utilizadas por el legislador, a pesar de estar contempladas para los efectos de esta Ley, podrían utilizarse en otros ámbitos para solucionar conflictos jurídicos en la materia. Al respecto, el legislador señala en el artículo 3 que para los efectos de esta Ley, los siguientes términos se definirán así: 1) Agencia de información de datos: *"Persona natural o jurídica que se dedica a recopilar, almacenar, conservar, organizar, comunicar, transferir o transmitir los datos sobre el historial de crédito de los consumidores o clientes, a través de procedimientos técnicos, automatizados o no"*. 2) Agentes económicos: *"Personas naturales o jurídicas, proveedoras de bienes y servicios, que registran, suministran y obtienen información de una base o banco de datos"*. 3) Base o banco de datos: *"Conjunto organizado de datos sobre el historial de crédito de los consumidores o clientes, cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso"*. 4) Consumidor: *"Persona natural o jurídica que adquiere de un agente económico bienes o servicios finales de cualquier naturaleza"*. 5) Cliente: *"Persona natural o jurídica, que mantiene una relación de carácter económico, financiero, bancario, comercial o industrial con un agente económico, el cual mantiene o maneja datos o referencias de crédito"*. 6) Dato: *"Información sobre el historial de crédito de los consumidores o clientes que conste en una base o banco de datos"*. 7) Historial de crédito: *"Datos de los consumidores o clientes, debidamente incorporados en una base o banco de datos, que reflejan las transacciones económicas, mercantiles, financieras o bancarias pagaderas a plazos"*. 8) Tratamiento de datos: *"Cualquier operación o conjunto de operaciones o procedimientos técnicos automatizados o no que, dentro de una base o banco de datos, permiten recopilar, almacenar, organizar, elaborar, seleccionar, extraer, confrontar, compartir, comunicar, transmitir o cancelar datos de consumidores o clientes"*.

toda la información que de ellos mantengan o manejen los agentes económicos y las agencias de información de datos. La agencia de información de datos correspondiente deberá proveer la información al consumidor o cliente, según sea requerida de forma verbal, así como darle a conocer qué entidades acreedoras tuvieron acceso a su historial de crédito. Esta información no causará costo alguno a los consumidores o clientes (Art. 23 Nº 1) [435] .

2)*Fidelidad de la información*: los datos de carácter personal serán exactos y actualizados, de forma que respondan con veracidad a la situación actual del consumidor o cliente (Art. 23 Nº 2).

3)*Buen manejo de la información*: los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recopilados. No se considerará incompatible el tratamiento de datos para fines históricos, estadísticos o científicos (Art. 23 Nº 4)*Consentir la recopilación y transmisión de la información*: los datos sobre historial de crédito brindados por los consumidores o clientes a los agentes económicos, sólo podrán ser recopilados y/o transmitidos a las agencias de información de datos y suministrados por éstas a los agentes económicos, con el consentimiento expreso de los consumidores o clientes, con excepción de las obligaciones de carácter económico, financiero, bancario, comercial o industrial, siempre que éstas consten en cheques protestados por falta de fondos o por haber sido girados contra cuenta corriente cerrada o por orden de suspensión de pago (Art. 23 Nº 4).

5)*Rectificación y eliminación de la información*: tan pronto un consumidor o cliente tenga conocimiento del hecho de haberse registrado o suministrado un dato sobre su historial de crédito erróneo, inexacto, equívoco, incompleto, atrasado o falso acerca de cualquier información de crédito o transacción económica, financiera, bancaria, comercial o industrial que le afecte, podrá exigir su rectificación o cancelación, de acuerdo con el procedimiento establecido por esta Ley (Art. 23 Nº 5).

6) *Indemnización*: los consumidores o clientes que, sufran algún tipo de daño como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el agente económico o la agencia de información de datos sobre historial de crédito, tendrán derecho a ser indemnizados. Este derecho se ejercerá ante la jurisdicción ordinaria correspondiente (Art. 23 Nº 6).

7) *Actualización*: todo consumidor o cliente tiene derecho a que se actualice la información sobre su historial de crédito (Art. 23 Nº 7).

Sin duda, puede afirmarse que de los diversos derechos señalados por la LSIHCC, se desprenden varios principios en materia de protección de datos personales. Éstos serán tratados más adelante en el punto Nº 4.

b) Caducidad de los datos

Ley panameña habla erróneamente de prescripción de los datos personales de carácter

[435] Se agrega por el artículo 25 que: *"si los datos sobre historial de crédito están en una base o banco de datos al que tienen acceso diversos organismos, el consumidor o cliente puede requerir copia de dicha información a cualquiera de ellos".*

crediticio para referirse al plazo de caducidad de éstos, señalando en el artículo 26 que: *"el tiempo para la prescripción de los datos sobre historial de crédito de los consumidores y clientes que reposen en un banco o base de datos de una agencia de información de datos, que no hayan cumplido con su obligación, es de siete años, contado a partir del último pago realizado por el consumidor o cliente o del incumplimiento en caso de que no hubiera efectuado ningún pago".* Se agrega por este artículo que transcurrido el plazo señalado, el dato debe ser excluido del sistema, base o banco de datos sobre historial de crédito que tenga la agencia de información de datos. Finalmente se añade que en el caso de mediar sentencia judicial, el término de la prescripción será de diez años, computado a partir de su ejecutoria (Art. 26 incisos 2º y 3º).

En relación con lo anterior, estimamos que los plazos de caducidad son excesivos, además de no parecer razonable la forma de cómputo de éste en el caso que se hubieren realizado pagos parciales por el cliente, pues se daría la absurda situación en la cual quien nada paga, goza en definitiva de un menor plazo de caducidad (7 años a partir del incumplimiento) que alguien que pagó parcialmente, pues el plazo de caducidad para este último se cuenta desde que efectuó el último pago el cual obviamente será mayor a 7 años contados desde que incumplió originalmente.

c) Deber de los consumidores o clientes

La Ley sólo establece un deber respecto de los consumidores o clientes. Éste consiste en que deberán suministrar información veraz a los agentes económicos sobre sus datos personales (Art. 27).

d) Deberes de las agencias de información de datos

En cuanto a los deberes de las agencias de información de datos, éstos obviamente son correlativos a los derechos de los consumidores o clientes. A ellos se refiere explícitamente el artículo 28. Esos deberes son: 1) Informar, verbalmente sobre el historial de crédito al consumidor o cliente que lo solicite; 2) Suministrar al consumidor o cliente que lo solicite copia de su historial de crédito [436] . El consumidor o cliente recibirá sin costo alguno las dos primeras certificaciones sobre su historial de crédito, solicitadas en el término de un año y pagará, según los usos del comercio, las certificaciones siguientes ; 3) Mantener actualizada la información sobre el historial de crédito que reciba de los agentes económicos; 4) Procesar en un periodo de tres días hábiles, los datos relativos al historial de crédito que le suministren los agentes económicos; 5) Cumplir lo establecido en la LSIHCC, en especial, lo relativo a los derechos de información, acceso, rectificación y cancelación de los datos del historial de crédito y, 6) Proporcionar gratuitamente, por solicitud del consumidor o cliente, copia del registro en la parte pertinente, en caso de solicitud de modificación o eliminación de datos. En el caso de que se hayan efectuado nuevas modificaciones o eliminaciones de datos, el consumidor o cliente podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que

[436] Tanto para cumplir con los deberes señalados en el Nº 1 anterior y en este Nº 2, la Ley señala que: *"para obtener esta información, el consumidor o cliente deberá presentarse personalmente a las oficinas de la agencia de información de datos y mostrar su cédula de identidad personal"* (Artículo 28 Nº 1 y 2).

hayan transcurrido al menos seis meses desde la precedente oportunidad en que hizo uso de este derecho. El derecho consignado en este artículo solo podrá ejercerse personalmente.

Las normas anteriores, en general nos parecen adecuadas a las disposiciones internacionales (europeas) en materia de condiciones para el tratamiento de los datos personales.

e) Deberes y obligaciones de los agentes económicos

Por otra parte, el artículo 291 de la LSIHCC se ocupa de señalar los deberes y las obligaciones a las que deberán sujetarse los agentes económicos. Éstos son los siguientes: 1) Proporcionar información actualizada, verdadera y confiable a las agencias de información de datos, a las cuales están afiliados. Se agrega en esta materia que los agentes económicos tienen la obligación de comunicar a los consumidores y clientes cómo se ingresa la información en la base o banco de datos de la agencia de información de datos y cuál es el criterio utilizado por ellos para la mora o retraso en el cumplimiento de la obligación crediticia; 2) Remitir la orden de rectificación de la información suministrada a las respectivas agencias de información de datos según corresponda, dentro de tres días hábiles después de solicitada la corrección del dato por el consumidor o cliente; 3) Enviar dentro de tres días hábiles a las agencias de información de datos correspondientes, la actualización de los datos referentes a las obligaciones de los clientes o consumidores; 4) Brindar la información que les soliciten las autoridades competentes, tanto administrativas como jurisdiccionales y, 5) Atender las quejas que, por escrito, les presenten los consumidores o clientes.

Finalmente, debemos agregar que en materia de acceso para consultar la información crediticia de un cliente o consumidor, el agente económico sólo podrá tener acceso a la información que proporcione una agencia de información de datos, cuando cuente *"con la autorización escrita del consumidor o cliente"* (Art. 24). Por lo tanto, en esta materia se le impone un deber de abstención al agente económico en caso de no contar con la autorización respectiva del cliente.

f) Prohibiciones

La LSIHCC establece diversas normas prohibitivas en la materia que regula, las cuales deben entenderse sin perjuicio de otras prohibiciones contenidas en la misma Ley. Así, se señala por el artículo 30 que queda expresamente prohibido: 1) Incluir en las bases o bancos de datos de las agencias de información de datos, el historial de pago de los usuarios de los servicios públicos residenciales básicos, tales como telefonía, electricidad, agua, alcantarillado y recolección de basura; 2) Incluir en las bases o bancos de datos de las agencias de información de datos el nombre de las personas naturales que representen a las personas jurídicas, salvo el caso de que dichas personas naturales estén vinculadas con la transacción de crédito correspondiente; 3) Incluir en las bases o bancos de datos de las agencias de información de datos el nombre de las personas que tienen condición de fiadores o codeudores. En este caso, sólo se podrá incluir al fiador o codeudor si previamente se le ha comunicado el incumplimiento de la obligación por el

deudor principal y se le ha requerido el pago de forma escrita con una advertencia en el sistema de información de crédito de que se trata de un fiador o codeudor; 4) Incluir en las bases o bancos de datos sobre historial de crédito cualquier tipo de calificativo del consumidor o cliente sobre la experiencia, comportamiento o manejo en el cumplimiento de sus obligaciones crediticias; 5) Publicar, por cualquier medio de comunicación, el nombre de una persona natural o jurídica acompañado de epítetos o calificativos, por incumplimiento de sus obligaciones crediticias; 6) Incluir en los bancos o bases de datos de las agencias de información de datos los números telefónicos y la dirección del domicilio o residencia y, 7) Ejercer la actividad de agencia de información de datos sin haber obtenido previamente la autorización correspondiente por parte del Ministerio de Comercio e Industrias.

De las prohibiciones anteriores, creemos que la señalada en el número 3 es, en general, una medida razonable que transparenta el mercado crediticio y permite tomar decisiones con una mayor calidad de la información. Sin embargo, tenemos dudas en cuanto a la oportunidad en que los terceros obligados solidaria o subsidiariamente al pago de una obligación debieran aparecer en un historial de crédito.

g **) Procedimiento para la rectificación y cancelación de datos**

En lo relativo al procedimiento para hacer efectivos los derechos de los clientes, el artículo 31 de la Ley señala que *"los derechos de acceso, rectificación y cancelación de los datos almacenados para prestar los servicios de información de datos sobre historial de crédito, serán ejercidos por el consumidor o cliente ante el agente económico o la CLICAC"*. Se agrega que, el consumidor o cliente afectado podrá actuar personalmente o a través de un mandatario, en cuyo caso será necesario que éste acredite tal condición. Como lo señala la Ley, el consumidor puede optar por ejercer sus derechos directamente ante el agente económico o ante la CLICAC. Los procedimientos respectivos, de carácter administrativo se reseñan a continuación.

1) Ejercicio de los derechos ante el agente económico:

En caso que el consumidor o cliente decida actuar primero ante al agente económico, la solicitud será presentada por escrito al encargado, quien deberá recibirla, expresando el día y la hora en que lo haga. El agente económico deberá contestar por escrito la solicitud que le dirija el interesado, en un plazo no mayor de tres días hábiles (Art. 33). El ejercicio de los derechos ante el agente económico o la CLICAC deberá efectuarse mediante solicitud escrita (Art. 32).

2) Ejercicio de los derechos ante la CLICAC:

El artículo 34 de la Ley establece un derecho de opción para el cliente de acudir directamente ante la CICLAC. Al efecto, se señala que: *"transcurrido el plazo de tres días hábiles de presentada la solicitud de rectificación, modificación o cancelación de los datos o referencias de crédito, sin que el agente económico haya dado respuesta al consumidor o cliente o, habiéndola dado, ésta no lo satisfaga, éste podrá acudir ante la CLICAC, para entregar copia de la solicitud presentada y la respuesta si la hubiere, con el objeto de que*

dicho ente estatal ordene la investigación correspondiente y verifique si procede lo solicitado. Esto, en ningún caso, impedirá que el consumidor o cliente actúe primeramente ante la CLICAC". El artículo 35 dispone a su turno que, la CLICAC, con fundamento en la solicitud que le presente el consumidor o cliente requerirá del agente económico y de la agencia de información de datos un informe de lo acontecido en donde sustente las razones que motivaron el suministro de los datos reflejados, o bien las razones por las cuales no accedió a la solicitud de rectificación, modificación o cancelación solicitada, en caso de que se hubiere dado. Luego, se agrega que la CLICAC presentará este requerimiento al encargado del agente económico y a la agencia de información de datos, quienes tendrán un término de tres días hábiles, contado a partir de la fecha en que reciban el requerimiento, para responder y presentar las pruebas que estimen pertinentes. Si el agente económico y/o la agencia de información de datos no remite la información solicitada, la CLICAC podrá realizar las investigaciones administrativas necesarias en los locales de los agentes económicos proveedores de datos o en las agencias de información de datos, con el objeto de obtener la documentación necesaria para resolver la queja presentada (Art. 35 inciso 2º).

En cuanto a la resolución del requerimiento ante la CLICAC, se dispone que ésta, con fundamento en la solicitud que le presente el consumidor o cliente, en la documentación recabada, así como en la respuesta que haya recibido del agente económico y de la agencia de información de datos, dictará una resolución motivada dentro de los cinco días hábiles siguientes. Dicha resolución *"contendrá una relación sucinta de los hechos, con fundamento en las pruebas que consten en el expediente y en la información brindada, en la que decidirá si procede o no la rectificación, modificación o cancelación de datos, así como las sanciones que correspondan, de acuerdo con esta ley, y ordenará, si ello es lo que procede, al agente económico o a la agencia de información de datos que rectifique o cancele la referencia correspondiente"* (Art. 36 inciso 1º). La orden emanada de la CLICAC debe ejecutarse en el término de tres días hábiles, contado a partir de fecha de la notificación de la resolución respectiva, so pena de desacato (Art. 36.inciso 2º). En contra de las resoluciones dictadas por la CLICAC, podrá apelarse ante el Pleno de los Comisionados. Este recurso se concederá en el efecto devolutivo y deberá presentarse dentro de los cinco días hábiles siguientes a la respectiva notificación (Art. 37).

En suma, la Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores o Clientes legaliza el mercado de la información crediticia, teniendo en vista eventualmente las condiciones generales para la licitud del tratamiento de los datos personales señaladas por la Directiva 95/46 CE. Llama la atención de la normativa panameña, que en definitiva la resolución de los conflictos entre los clientes y los agentes se resuelva ante la autoridad administrativa (CLICAC), y no ante los tribunales de justicia a través de una acción de hábeas data, agotada la vía previa extrajudicial.

2.2.2) Ley de Transparencia en la Gestión Pública, establece la acción de Hábeas Data y dicta otras disposiciones (Ley Nº 6-2002) [437]

[437] [En línea] < http://www.legalinfo-panama.com/legislacion/administrativo/00195.pdf > [consulta: 17 de Enero 2003].

Esta reciente ley tiene por objeto principal regular la libertad de acceso a la información pública que conste en los registros, archivos o expedientes de la administración del Estado. Ese objeto a su vez puede dividirse, y apuntar por una parte, al acceso a la información de interés público o a las actuaciones de organismos del Estado, y por otro lado, referirse al acceso, rectificación y cancelación de los datos personales en poder del Estado. En este sentido, puede señalarse que la normativa en estudio regula respectivamente el ejercicio del hábeas data impropio y del hábeas data propio.

Concordante con lo anterior, el artículo 2 de la Ley señala que: *"toda persona tiene derecho a solicitar, sin necesidad de sustentar justificación o motivación alguna, la información de acceso público en poder o en conocimiento de las instituciones indicadas en la presente Ley".* Agrega el inciso 2º que: "*las empresas privadas que suministren servicios públicos con carácter de exclusividad, están obligadas a proporcionar la información que les sea solicitada por los usuarios del servicio, respecto a éste".* Por lo tanto, el derecho de acceso a la información de carácter pública, aunque esté en manos de privados, se rige por las normas señaladas por esta ley. Con todo, la propia Ley señala los límites al ejercicio de los derechos consagrados, disponiendo en el artículo 8 que las instituciones del Estado están obligadas a brindar, a cualquier persona que lo requiera, información sobre el funcionamiento y las actividades que desarrollan, *"exceptuando únicamente las informaciones de carácter confidencial y de acceso restringido".*

Conteste con una de las finalidades de la Ley que se analiza -como ya se señaló- se consagra el derecho de acceso, rectificación y cancelación de datos personales contenidos en archivos, registros o bancos de datos pertenecientes a los organismos del Estado. Al efecto, el artículo 3 de esta Ley señala: *"toda persona tiene derecho a obtener su información personal contenida en archivos, registros o expedientes que mantengan las instituciones del Estado, y a corregir o eliminar información que sea incorrecta, irrelevante, incompleta o desfasada, a través de los mecanismos pertinentes"* [438] . En relación al ejercicio de los derechos señalados, cabe hacer la siguiente prevención: la Ley si bien consagra la acción de hábeas data, también establece un procedimiento administrativo previo al ejercicio de ésta el cual debe agotarse necesariamente para que sea procedente dicha acción.

El procedimiento administrativo para el ejercicio de los derechos de acceso, rectificación y cancelación de datos personales es el siguiente:

1) Solicitud de acceso, rectificación y cancelación de datos personales: la petición

[438] Complementa lo recién señalado el artículo 4, el cual dispone que: *"el acceso público la información será gratuito en tanto no se requiera la reproducción de esta. Los costos de reproducción de la información estarán a cargo del solicitante. En todo caso, las tarifas cobradas por la institución deberán incluir únicamente los costos de reproducción. (…) La información será suministrada en copia simple, o en su reproducción digital, sonora, fotográfica, cinematográfica o videográfica, según se peticione y sea técnicamente factible. (…) Para los efectos de prestar el servicio de acceso por medio de Internet, las instituciones deberán prever una oficina de consulta que tenga los medios electrónicos indispensables para ofrecer un servicio de acceso de calidad. Esto se podrá lograr también por medio de kioscos de información que hayan previsto las distintas instituciones". (…) Parágrafo. En caso de que la información solicitada sea requerida de manera certificada, el peticionario deberá cumplir, para los efectos de las formalidades y de los costos, con las disposiciones legales que rigen la materia".*

debe hacerse por escrito en papel simple o por medio de correo electrónico, cuando la institución correspondiente disponga del mismo mecanismo para responderlo, sin formalidad alguna, ni necesidad de apoderado legal, detallando en la medida de lo posible la información que se requiere, y se presentará en la oficina asignada por cada institución para el recibo de correspondencia. Recibida la petición, deberá llevarse de inmediato al conocimiento del funcionario a quien se dirige (Art. 5).

2) Plazo para contestar la solicitud: el funcionario receptor tendrá treinta días calendario desde la fecha de la presentación de la solicitud para contestarla por escrito y, en caso que éste no posea el o los documentos o registros solicitados, así lo informará. Si el funcionario está en conocimiento que otra institución tiene o pueda tener en su poder dichos documentos o documentos similares, estará obligado a indicárselo al solicitante. De tratarse de una solicitud compleja o extensa, el funcionario informará por escrito, dentro de los treinta días calendario antes señalados, la necesidad de extender el término para recopilar la información solicitada. En ningún caso, dicho término podrá exceder de treinta días calendarios adicionales (Art. 7) [439] .

Los pasos recién señalados, configuran el ejercicio de los derechos de los titulares de los datos personales en sede administrativa, lo cual -como se dijo- es requisito previo para el ejercicio de la acción de hábeas data contemplado por la Ley, la cual se analizará en el punto Nº 6 relativo a los modelos de tutela.

En suma, la Ley Nº 6 del año 2002, consagra expresamente la acción de hábeas data respecto de los datos personales que se encuentren en poder de los organismos de la Administración del Estado, y abarca los derechos de acceso, rectificación y supresión de la información que sea incorrecta, irrelevante, incompleta o desfasada.

2.2.3) Código Fiscal [440]

El Código Tributario o Fiscal panameño establece en el artículo 722 el secreto tributario o fiscal de la siguiente forma: *"no se podrá divulgar en forma alguna la cuantía o fuentes de entradas o beneficios, ni las pérdidas, gastos o algún otro dato relativo a ello que figuren en las declaraciones del contribuyente, ni permitirá que éstas o sus copias y los documentos que con ella se acompañen sean examinados por personas distintas al contribuyente o de su representante o apoderado".* Se agrega en el inciso 2º que, no obstante lo dispuesto en el inciso anterior, *"podrá permitirse la inspección de la declaración y de los documentos que con ella se acompañen que verifiquen las autoridades judiciales y fiscales, cuando tal inspección sea necesaria para la persecución de juicios o investigaciones en los cuales el Estado tenga interés".* Añade este artículo,

[439] Se agrega por la Ley en el artículo 7 que: *"se deberá prever un mecanismo claro y simple de constancia de la entrega efectiva de la información al solicitante, que puede hacerse también a través de correo electrónico cuando se disponga de tal facilidad y, en todo caso, cuando la solicitud hubiere sido presentada por esa vía"* (Artículo 7 inciso 2º). En el caso que la información solicitada por la persona ya esté disponible al público en medios impresos tales como libros, compendios, trípticos, archivos públicos de la administración, así como también en formatos electrónicos disponibles en Internet o en cualquier otro medio, se le hará saber la fuente, el lugar y la forma en que puede tener acceso a dicha información previamente publicada (Artículo 7 inciso 3º).

[440] **[En línea] < http://www.legalinfo-panama.com/legislacion/fiscal/isr_06.htm > [consulta: 17 de Enero 2003].**

que será permitida la publicación de datos estadísticos en forma que no puedan identificarse los informes, declaraciones o partidas en cada caso (Art. 722 inciso 3º). Es decir, la ley estaría señalando indirectamente que para el tratamiento de estos datos, se requeriría la utilización de procedimientos de disociación de datos. Finalmente, se dispone que en las causas civiles en que un contribuyente sea parte, *"podrán llevarse a cabo inspecciones oculares en los mismos casos y con los mismos requisitos y formalidades permitidos para la inspección de los libros y documentos de los comerciantes"* (Art. 722 inciso final).

En suma, se garantiza el secreto de toda la información proporcionada por los contribuyentes a la Administración Tributaria, salvo los casos en que se siga un juicio en que el Estado tenga interés, con lo cual la excepción más bien se relativiza en favor del propio Estado, con el subsecuente riesgo que implica el cruce de informaciones.

2.2.4) Ley Bancaria (Decreto-Ley Nº 9) [441]

Esta ley del año 1998, dispone en materia de reserva bancaria tanto normas aplicables a los funcionarios de la Superintendencia de Bancos, como normas aplicables a los funcionarios bancarios. Respecto de los primeros, la ley prescribe que: *"la información obtenida por la Superintendencia en el ejercicio de sus funciones relativa a clientes individuales de un Banco, sólo podrá ser revelada a la autoridad competente conforme a las disposiciones legales vigentes, dentro del curso de un proceso penal"* (Art. 84). El inciso 2º agrega en esta materia que, la Superintendencia, incluyendo a todo su personal y a los auditores externos, asesores e interventores designados por ella, *"deberá guardar la debida reserva sobre toda información que le haya sido suministrada o que haya obtenido conforme a este Decreto-Ley, y en consecuencia no podrán revelarla a terceras personas, salvo que se trate de autoridad competente conforme a lo dispuesto en este artículo. Se exceptúan de esta disposición aquellos informes o documentos que de conformidad con este Decreto-Ley deban hacerse de conocimiento público".* Finalmente, se hace extensible el deber de secreto a todo funcionario público en los siguientes términos: *"los funcionarios públicos que con motivo de los cargos que desempeñen tengan acceso a la información de que trata este artículo, quedarán obligados a guardar la debida reserva aún cuando cesen en sus funciones"* (Art. 84 inciso final). Ahora bien, respecto de los bancos y sus funcionarios, el artículo 85 dispone que los Bancos sólo divulgarán información acerca de sus clientes, salvo cuando medie solicitud formal de autoridad competente de conformidad con la Ley. El inciso 2º de esta disposición agrega que los Bancos *"podrán divulgar información de sus clientes a las instituciones que actúen como centrales de crédito, a discreción del Banco".*

Tenemos dudas acerca de la efectiva vigencia de esta última disposición, por cuanto no se aclara por el legislador qué entiende por central de crédito. Si ésta pudiera asimilarse conceptualmente a una agencia de información de crédito, nos inclinaríamos a pensar que la disposición señalada habría sido derogada tácitamente en virtud de la Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores o Clientes (Art. 46). En el caso negativo, y que se entienda lo señalado por el legislador

[441] **[En línea] < http://www.shirleylaw.com/documents/Ley.Bancaria_1998_sp.htm,fecha > [consulta: 14 de Abril 2003].**

como centrales de riesgos, nos parecería en definitiva, que la ley otorga una excesiva libertad a las instituciones financieras, dejando a la sola consideración de éstas cuando se hace excepción a l secreto bancario y cuando no.

En suma, si bien la Ley establece la reserva de información de los clientes de las bancos, no específica a qué tipo de información se refiere ni la extensión de ella, con lo cual en definitiva la norma se vacía de contenido, salvo que se opte por una interpretación amplia en que se incluya todo tipo de información relativa a los clientes bancarios, lo cual pareciera ser un exceso.

3. Bienes Jurídicos Protegidos Por la Legislación de Datos Personales

En materia de bien jurídico protegido, a nivel Constitucional, sólo pueden apreciarse indirectamente los derechos a la vida privada e intimidad, los cuales a su vez se encuentran complementados por las normas pertinentes en materia de derechos humanos, en especial por la Convención Americana de Derechos Humanos.

A nivel infraconstitucional, Panamá cuenta con dos leyes que consagran acciones de hábeas data; una respecto de los datos personales contenidos en los registros o archivos públicos en manos de la administración del Estado o de privados que tratan información pública y, la segunda ley, que consagra un hábeas data administrativo respecto de los datos personales tratados por las agencias investigadoras de crédito. Si bien esta última contiene una reglamentación que pudiera fundamentarse en un derecho a la autodeterminación informativa, creemos que se torna difícil derivar directamente ese bien jurídico del texto constitucional, dado el total silencio al respecto y, en razón de la inexistencia de una disposición que contenga un *numerus apertus* en materia de derechos fundamentales, por lo que nos inclinamos a pensar que a nivel legal, los bienes jurídicos presentes son la protección de la vida privada e intimidad.

4. Principios Informativos de la Legislación de Protección de Datos Personales

A pesar de la inexistencia de una ley de protección de datos personales en el ordenamiento jurídico panameño, éste contempla una legislación sectorial que en general se enmarca dentro de las condiciones generales para el tratamiento de datos personales establecidos en la Directiva 95/46 CE. En razón de lo anterior, nos referiremos a los principios informativos de la Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores o Clientes (LSIHCC).

1º. Principio de la licitud y lealtad de los archivos de datos

Este principio se contiene en el artículo 1º de la Ley, al definir su objeto, cuando señala que éste comprende proteger y garantizar la confiabilidad, la veracidad, la actualización y el buen manejo de los datos personales de consumidores o clientes, relativos a su

historial de crédito, incorporados o susceptibles de ser incorporados a una agencia de información de datos administrada por una persona natural o jurídica, *"debidamente autorizada conforme a la presente Ley".* También se vislumbra el principio, en la exigencia de autorización y registro para la prestación de los servicios de crédito por parte de las agencias de información de crédito (Art. 11 LSIHCC) [442] .

2º. Principio de la calidad de los datos

En el artículo 1º de la LSIHCC se aprecia este principio al describir el objeto de ella: *"proteger y garantizar la confiabilidad, la veracidad, la actualización y el buen manejo de los datos personales de consumidores o clientes, relativos a su historial de crédito (…)".*

Luego en el artículo 4, la LSIHCC incluso define este principio de la siguiente forma: "*los datos sobre historial de crédito, brindados por los consumidores o clientes o por los agentes económicos, los manejados por las agencias de información de datos y los generados por transacciones de carácter económico, financiero, bancario, comercial o industrial, deberán ser exactos y actualizados de forma que respondan con veracidad a la situación real del consumidor o cliente".*

Por otra parte, se reafirma lo señalado anteriormente en el artículo 23 Nº 2, el cual al definir el derecho del consumidor a la fidelidad de la información dispone que: *"los datos de carácter personal serán exactos y actualizados, de forma que respondan con veracidad a la situación actual del consumidor o cliente"*.

Asimismo, el artículo 28 Nº 3 señala como deber de las agencias de información de crédito el *"mantener actualizada la información sobre el historial de crédito que reciba de los agentes económicos".*

Finalmente, cabe anotar que el artículo 29 Nº 1 también se refiere a este principio a propósito de los deberes y obligaciones de los agentes económicos, entre los cuales se encuentra: *"Proporcionar información actualizada, verdadera y confiable a las agencias de información de datos, a las cuales están afiliados".*

3º. Principio del consentimiento del titular de los datos

Este principio puede constatarse, al señalar la ley que los datos sobre historial de crédito brindados por los consumidores o clientes a los agentes económicos, sólo podrán ser recopilados y/o transmitidos a las agencias de información de datos y suministrados por éstas a los agentes económicos, *"con el consentimiento expreso de los consumidores o*

[442] El artículo 11 de la Ley dispone que: *"Toda persona natural o jurídica que desee operar una agencia de información de datos sobre historial de crédito, deberá solicitar autorización al Ministerio de Comercio e Industrias para ejercer dicha actividad. Este Ministerio está facultado para realizar las investigaciones que sean necesarias, con el objeto de verificar la información suministrada en la solicitud"*. Por otra parte, el artículo 19 intitulado "Registro de la autorización" dispone que la autorización expedida por el Ministerio de Comercio e Industrias, se inscribirá en un registro especial denominado Registro de Agencias de Información de Datos sobre Historial de Crédito. La inscripción en este Registro deberá contener la siguiente información: 1) Número de la resolución y su fecha de expedición; 2) Nombre, domicilio y números telefónicos de la persona natural o jurídica a quien se dio la autorización y, además, el de su representante legal; 3) Nombre comercial y dirección exacta del establecimiento donde operará la empresa y, 4) Fecha de inicio de operaciones.

clientes, con excepción de las obligaciones de carácter económico, financiero, bancario, comercial o industrial, siempre que éstas consten en cheques protestados por falta de fondos o por haber sido girados contra cuenta corriente cerrada o por orden de suspensión de pago"(Art. 23 Nº 4 LSIHCC).

Por otro lado, se divisa el principio del consentimiento previo, al prescribir la Ley que el agente económico *"solo podrá tener acceso para consultar la información existente en una base o banco de datos de una agencia de información de datos, con la autorización escrita del consumidor o cliente"* (Art. 24 LSIHCC).

4º. Principio de la seguridad de los datos

La seguridad de los datos está prevista expresamente por el legislador panameño, al disponer que: *"los agentes económicos y las agencias de información de datos sobre historial de crédito, deberán adoptar las medidas o controles técnicos necesarios para evitar la alteración, pérdida, tratamiento o acceso no autorizado de los datos sobre historial de crédito que manejen o mantengan en sus respectivas bases o bancos de datos"* (Art. 5 LSIHCC).

5º. Principio de la confidencialidad de los datos

Se puede apreciar este principio en la Ley de un modo expreso. En efecto, el artículo 6 inciso 1º de la LSIHCC, define la "reserva" señalando que: *"todas las personas naturales o jurídicas, públicas o privadas, que tengan acceso a cualquier información relacionada con el historial de crédito de conformidad con esta Ley, deberán guardar la debida reserva sobre dicha información y, en consecuencia, no podrán revelarla a terceras personas, salvo que se trate de autoridad competente"*. Luego, el inciso 2º de esta disposición agrega: *"los funcionarios públicos o privados que, con motivo de los cargos que desempeñen, tengan acceso a la información de que trata esta Ley, quedarán obligados a guardar la debida reserva, aun cuando cesen en sus funciones"* (Art. 6 inciso 2º).

6º. Principio del consentimiento para la cesión de los datos

La LSIHCC consagra este principio en los artículos 23 Nº 1 y 24 ya vistos, a propósito del principio del consentimiento previo del titular de los datos. El primero de ellos, establece como derecho de los consumidores o clientes el *"consentir la recopilación y transmisión de la información"*. El artículo 24 por su parte señala que: *"El agente económico solo podrá tener acceso para consultar la información existente en una base o banco de datos de una agencia de información de datos, con la autorización escrita del consumidor o cliente".* En relación a esto último, estimamos que el término "consultar" utilizado por el legislador, es lo suficientemente amplio como para incluir dentro de él la cesión de datos.

7º. Principio de la finalidad

Finalmente, en materia de principios, puede afirmarse que el de la finalidad se encuentra contenido en la disposición que establece el derecho del consumidor o cliente al "Buen

manejo de la información", lo cual implica que: *"Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recopilados. No se considerará incompatible el tratamiento de datos para fines históricos, estadísticos o científicos"* (Art. 23 Nº 3 LSIHCC). Este tema ya había sido tratado por el legislador al señalar los objetivos de la Ley, uno de los cuales es proteger y garantizar la confiabilidad, la veracidad, la actualización y *"el buen manejo de los datos personales de consumidores o clientes (…)"*.

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

Dada la inexistencia de una ley general de protección de datos personales en el ordenamiento jurídico panameño, no nos detendremos en este punto.

6. Modelos de Tutela

Las dos legislaciones especiales que prevén una protección parcial a los datos personales, disponen de procedimientos administrativos para el ejercicio de los derechos señalados por sus respectivas normas. En el caso de la Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores, sólo se dispone de un procedimiento administrativo para resolver los conflictos que se susciten como consecuencia del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los consumidores o clientes. En cambio, la Ley de Transparencia y Derecho a la Información, no sólo contempla un procedimiento administrativo para la tutela de los derechos de acceso, corrección y supresión de la información incorrecta, irrelevante, incompleta o desfasada (Art. 3 Ley Nº 6-2002), sino que prevé una acción de hábeas data ejercitable ante los tribunales de justicia una vez que se haya agotado la vía administrativa. A continuación se tratará solamente la acción de habeas data señalada por la Ley de Transparencia y Derecho a la Información, ya que los procedimientos administrativos fueron tratados al analizar las respectivas leyes en los puntos Nº 2.2.1 y 2.2.2 de este análisis.

6.1 La Acción de Hábeas Data

Como ya se ha señalado, el artículo 3 de la Ley Nº 6 del año 2002 establece una acción de hábeas data ejercitable ante los tribunales de justicia una vez agotada la vía administrativa en el ejercicio de los derechos de acceso, corrección y supresión de los datos personales en poder del Estado.

6.1.1) Procedencia de la Acción

Según el artículo 17 de la Ley, es procedente la acción de hábeas data, cuando el funcionario público titular o responsable del registro, archivo o banco de datos en el que se encuentra la información o dato personal reclamado, no le haya suministrado lo solicitado o si suministrado lo requerido, se haya hecho de manera insuficiente o en forma

inexacta.

6.1.2) Legitimación Activa

El artículo 17 señala al respecto que toda persona estará legitimada para promover acción de hábeas data, con miras a garantizar el derecho de acceso a la información previsto en esta Ley.

6.1.3) Legitimación Pasiva

De lo dispuesto en el artículo 17, se desprende que el sujeto pasivo del hábeas data será *"el funcionario público titular o responsable del registro, archivo o banco de datos en el que se encuentra la información o dato personal reclamado"*. A ello hay que agregar, sólo en lo relativo al derecho de acceso, que podría ejercitarse el hábeas data en contra de los privados o particulares que suministren servicios públicos con carácter de exclusividad y que sean responsables de archivos o registros de datos personales. La limitación anterior estaría dada por el tenor de los artículos 2 y 3 de la Ley Nº 6-2002.

6.1.4) Competencia

El artículo 18 dispone en esta materia, que la acción de hábeas data *"será de competencia de los Tribunales Superiores que conocen de la acción de Amparo de Garantías Constitucionales, cuando el funcionario titular o responsable del registro, archivo o banco de datos, tenga mando y jurisdicción a nivel municipal o provincial".* En el caso que el titular o responsable del registro, archivo o banco de datos tenga mando o jurisdicción en dos o más provincias o en toda la República, *"será de competencia del Pleno de la Corte Suprema de Justicia".*

Sin duda alguna, el legislador ha dado al hábeas data la importancia que se merece, a pesar de no estar consagrada constitucionalmente la acción. En este sentido estimamos correcta la disposición legal.

6.1.5) Procedimiento Aplicable

En materia de procedimiento, en general, puede afirmarse que la Ley Nº 6 del 2002 se remite a la tramitación de la acción de amparo. Al efecto, el artículo 19 dispone que la acción de hábeas data se tramitará mediante procedimiento sumario sin formalidades, sin necesidad de abogado, y en lo que respecta a la sustanciación, impedimentos, notificaciones y apelaciones, se aplicarán las normas que para estas materias se regulan en el ejercicio de la acción de Amparo de Garantías Constitucionales.

Nos parece acertado que se disponga por el legislador de un procedimiento sumario para la tramitación del hábeas data. Por el contrario, estimamos que hubiera sido preferible no remitirse a las normas del amparo y haber señalado reglas propias de procedimiento, pues entre las desventajas que presenta el amparo, por regla general, cabe mencionar el establecimiento de plazos de caducidad para la interposición de la acción, lo cual en la práctica redunda en que la vida del derecho se limite al plazo de caducidad señalado por la ley, lo cual no nos parece razonable. En lo que respecta a la

ley de Amparo, cabe señalar que lamentablemente no hemos accedido a ésta por lo que no podremos referirnos a su tramitación.

6.1.6) La Sentencia

A este respecto no se pronuncia la Ley Nº 6 del 2002, por lo que se entiende que se remite a las reglas de la acción de amparo, a la cual no nos referiremos.

6.2 Otras Acciones

En los ámbitos no abarcados por la Ley Nº 6, consideramos que sería procedente el ejercicio directo de la acción de amparo contemplada en el artículo 50 de la Constitución y que señala: "*toda persona contra la cual se expida o se ejecute, por cualquier servidor público, una orden de hacer o no hacer, que viole los derechos y garantías que está constitución consagra, tendrá derecho a que la orden sea revocada a petición suya o de cualquiera persona".* El inciso 2º agrega que: *"el recurso de amparo de garantías constitucionales a que este artículo se refiere, se tramitará mediante procedimiento sumario y será de competencia de los tribunales judiciales".*

7. Mecanismos de Control

A pesar de la inexistencia de una ley de protección de datos personales en Panamá, la Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores otorga competencia a dos órganos administrativos que de manera conjunta cumplen un rol de órganos de control de la aplicación de la LSIHCC.

Respecto de la competencia del Ministerio de Comercio e Industrias, se dispone que a éste le compete expedir y revocar la resolución que autoriza a las personas naturales o jurídicas para ejercer la actividad de agencia de información de datos sobre historial de crédito, y de mantener un registro de éstas. Asimismo, dicho Ministerio tiene la facultad de inspeccionar y verificar que las agencias de información de datos cumplan con los requisitos de seguridad, confiabilidad y actualización de los datos de los consumidores y clientes, así como cualquier otra que le establezca la Ley. Por último, cabe agregar que el Ministerio de Comercio e Industrias, tiene la facultad de sancionar a las agencias de información de datos que infrinjan lo establecido en la LSIHCC (Art. 7).

En cuanto a la competencia de la Comisión de Libre Competencia y Asuntos del Consumidor (CLICAC), cabe anotar que ésta conoce y atiende las quejas de los consumidores o clientes, y supervisa e investiga las prácticas de los agentes económicos y las agencias de información de datos, de acuerdo con el ámbito de aplicación de la Ley. Asimismo, la CLICAC también está facultada para sancionar a los agentes económicos y a las agencias de información de datos que, por razón de la investigación de las quejas que se le presenten, se les compruebe que han infringido los derechos del consumidor o cliente en los supuestos señalados en esta Ley (Art. 8 incisos 1º y 2º). Cabe añadir que la CLICAC está facultada además para solicitar la información necesaria y efectuar verificaciones, a fin de realizar las investigaciones administrativas relacionadas exclusivamente, y en cada caso, con la queja presentada (Art. 8 inciso 3º).

Finalmente, debemos mencionar que la CLICAC está obligada a remitir mensualmente al Ministerio de Comercio e Industrias copia de todas las resoluciones debidamente ejecutoriadas, que se impongan a las agencias de información de datos, originadas por las infracciones a la Ley en perjuicio de un consumidor o cliente en particular (Art. 8 inciso 4º) [443] .

En suma, estimamos que dada la regulación legal que atribuye amplias facultades fiscalizadoras y sancionadoras a los organismos administrativos mencionados, estaríamos frente a verdaderas autoridades de control de la aplicación de la Ley que regulan el Servicio de Información sobre el Historial de Crédito de los Consumidores.

8. Transmisión Internacional de Datos

A esta materia no se refieren las disposiciones legales analizadas, por lo que no nos detendremos en este punto.

9. Régimen de Responsabilidad

En materia de responsabilidad, nos referiremos a las reglas contenidas en las leyes más arriba indicadas, salvo en materia penal, donde nos detendremos en los delitos contemplados en el Código Penal panameño que se relacionan con la protección de la vida privada e intimidad.

9.1 Responsabilidad Administrativa

En este punto, revisaremos las sanciones administrativas previstas en la Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores, la cual hemos estimado de carácter sectorial compleja. También nos referiremos a las sanciones establecidas en la Ley de Transparencia en la Gestión Pública, de carácter especial en materia de protección de datos y finalmente revisaremos las disposiciones respectivas de Ley Bancaria, ley sectorial por excelencia.

9.1.1) Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores

En materia de responsabilidad administrativa esta Ley contempla diversas infracciones y sanciones. Al efecto, el artículo 38 señala que: *"Las infracciones de los agentes económicos y de las agencias de información de datos serán leves, graves y muy graves"* [444] . En cuanto a los tipos de sanciones que pueden aplicarse, el artículo 42 indica lo siguiente:

[443] A modo de disposición que cierra el ámbito de competencia de las instituciones administrativas ya señaladas, el parágrafo del artículo 8 dispone que: *"se entiende que la CLICAC impondrá las sanciones correspondientes a los agentes económicos y a las agencias de información de datos, en atención a las quejas presentadas por los consumidores o clientes. Por su parte, el Ministerio de Comercio e Industrias impondrá sanciones a las agencias de información de datos como resultado de sus funciones de monitoreo e inspección a éstas".*

"1. Las infracciones leves serán sancionadas con amonestación escrita la primera vez. De existir reincidencia en estas infracciones, las subsiguientes se considerarán graves.

2. Las infracciones graves serán sancionadas con multa de mil balboas (B/.1,000.00) a cinco mil balboas (B/.5,000.00) la primera vez. De existir reincidencia en estas infracciones, las subsiguientes se considerarán muy graves.

3. Las infracciones muy graves serán sancionadas con multa de cinco mil balboas con un centésimo (B/.5,000.01) a diez mil balboas (B/.10,000.00)" [445] .

Ley de Transparencia en la Gestión Pública (Ley Nº 6-2002)

Esta normativa dispone en el artículo 20 que: *"El funcionario requerido por el Tribunal que conoce del Recurso de Hábeas Data, que incumpla con la obligación de suministrar la información, incurrirá en desacato y será sancionado con multa mínima equivalente al doble del salario mensual que devenga"*. El inciso 2º por su parte agrega que: *"en caso de reincidencia, el funcionario será sancionado con la destitución del cargo".* Como se recordará, en el análisis de la protección a los datos personales en Chile, al comentar la

[444] A su vez el legislador establece un catálogo de conductas constitutivas de infracción a la ley, según la gravedad de éstas. Al respecto dispone lo siguiente: Artículo 39. *"Infracciones leves. Se consideran infracciones leves desatender las solicitudes del interesado de revisión, rectificación o cancelación de los datos personales".* Artículo 40. *"Infracciones graves. Son infracciones graves las siguientes:* 1. Confeccionar bases o bancos de datos de usuarios del crédito o recopilar datos personales, con finalidad diferente a la que se establece en la Ley. 2. Mantener los archivos de los usuarios del crédito con información desactualizada. 3. No entregar la información que solicite la CLICAC con respecto a los casos que ingresen a esta institución y que, por razón de su competencia, deban conocer. 4. Manejar la información personal de los consumidores o clientes, para otros fines que no estén relacionados con el objeto para el cual se recopilaron. 5. Mantener la información de los consumidores o clientes en lugares inseguros. 6. Obstruir el ejercicio de la función inspectora de parte de la autoridad competente. 7. No depurar la base o banco de datos con relación a la prescripción. 8. Infringir las normas de reserva. 9. Acceder a la base o banco de datos de una agencia de información de datos sobre referencias de crédito sin la autorización previa, expresa y escrita, del consumidor para obtener información sobre su historial crediticio. 10. Proporcionar, mantener y transmitir datos que no sean exactos o veraces. 11. No adoptar las medidas o controles técnicos para evitar la alteración, pérdida, tratamiento o acceso del dato. 12. Modificar los datos suministrados en la documentación de autorización sin comunicarlo a la autoridad competente en el tiempo establecido por esta Ley. *13. No remitir a la agencia de información de datos la actualización de los datos dentro del término establecido en la presente Le"y.* Artículo 41. *Infracciones muy graves. Son infracciones muy graves las siguientes:* 1. Incumplir las disposiciones de la presente Ley en materia de prescripción de los datos de consumidores o clientes. 2. Obtener datos en forma fraudulenta o engañosa. 3. Incumplir las órdenes que determine la CLICAC, en cuanto al manejo de las referencias o historial de crédito. 4. Incumplir las instrucciones impartidas por el Ministerio de Comercio e Industrias, en el cumplimiento de las funciones que le señala esta Ley. 5. Publicar y difundir información sobre incumplimiento de obligaciones crediticias. *6. Realizar algunas de las actividades prohibidas por esta Ley".*

[445] Se agrega por el artículo 42, que la cuantía de las sanciones se graduará atendiendo al grado de intencionalidad, a la reincidencia y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora (Artículo 42 penúltimo inciso). Además se señala que la CLICAC sancionará el desacato o desobediencia a las órdenes de hacer o no hacer, emitidas a través de resoluciones, con multa de quinientos balboas (B/.500.00) a mil balboas (B/.1,000.00). Esta multa será reiterativa y se causará por día, hasta que se cumpla con lo ordenado (Artículo 42 inciso final).

naturaleza de la sanción contemplada en el inciso final del artículo 16, sostuvimos que ella era una figura especial de desacato. La disposición recién señalada apunta expresamente en esa dirección, lo cual nos hace reafirmar lo dicho más atrás a propósito de la Ley 19.628.

Finalmente, el artículo 22 de esta Ley prescribe que: "*El funcionario que obstaculice el acceso a la información, destruya o altere un documento o registro, sin perjuicio de las responsabilidades administrativas y penales derivadas del hecho, será sancionado con multa equivalente a dos veces el salario mensual que devenga".*

9.1.3) Ley Bancaria (Decreto-Ley Nº 9)

En materia bancaria, la ley respectiva no señala una sanción específica para la violación del deber de secreto que pesa tanto sobre la Superintendencia de Bancos como sobre los propios bancos, sino que se dispone en el artículo 86 que: *"Las violaciones a lo dispuesto en este capítulo serán sancionadas con multa de hasta cien mil balboas (B/.100,000.00), sin perjuicio de las sanciones civiles o penales que puedan corresponder".*

9.2 Responsabilidad Civil

En materia de responsabilidad civil, tanto la Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores como la Ley de Transparencia en la gestión pública establecen reglas especiales. La primera de ellas señala que: *"Los consumidores o clientes que, sufran algún tipo de daño como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el agente económico o la agencia de información de datos sobre historial de crédito, tendrán derecho a ser indemnizados. Este derecho se ejercerá ante la jurisdicción ordinaria correspondiente"* (Art. 2 Nº 1). Más adelante, agrega que los juzgados civiles creados mediante la Ley 29 de 1996, conocerán de las demandas que se presenten en contra de los agentes económicos y/o agencias de información de datos, así como las reclamaciones por daños y perjuicios causados. (Art. 9 inciso 1º). Se añade por el legislador que para los efectos de esta Ley, el término de prescripción para recurrir ante los tribunales de justicia correspondientes y solicitar indemnización por daños y perjuicios es de un año, contado a partir del momento en que el consumidor o cliente tuvo conocimiento de la afectación (Art. 9 inciso 2º). Añade el artículo 10, que el término de prescripción de la acción por daños y perjuicios se interrumpe por la presentación de reclamo formal ante la CLICAC.

Por su parte, la Ley de Transparencia en la Gestión Pública establece en el artículo 21 una curiosa regla que exime de responsabilidad al Estado por el hecho de sus funcionarios, disponiendo que: *"La persona afectada por habérsele negado el acceso a la información, una vez cumplidos con los requisitos y trámites expuestos en la presente Ley, tendrá derecho a demandar civilmente al servidor público responsable por los daños y perjuicios que se le hayan ocasionado".*

No nos parece razonable la regla anterior, pues desconoce toda la construcción dogmática que está detrás de la consideración del Estado como sujeto pasivo de responsabilidad por la falta o deficiencia del servicio. Sin duda, la norma anterior sólo

perjudica al afectado, pues en definitiva la víctima sólo tendrá el patrimonio del funcionario público para resarcirse y compensar los daños provocados.

Finalmente, estimamos que en las situaciones no cubiertas por las normas señaladas deberían aplicarse las reglas generales en materia de responsabilidad civil, respecto de las cuales no tenemos mayor información.

9.3 Responsabilidad Penal

En materia penal, no se establecen reglas especiales en la Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores ni tampoco en la Ley Nº 6 de 2002. Por su parte, el Código Penal contempla delitos contra la inviolabilidad del domicilio y delitos contra la inviolabilidad del secreto, los cuales protegen los bienes jurídicos vida privada e intimidad [446] . Éstos se transcriben a continuación.

a) Delitos contra la inviolabilidad del domicilio:

Artículo 163.-*"El que entre en morada o casa ajena o en sus dependencias, sea contra la voluntad expresa o presunta de quien tenga derecho a excluirlo, sea clandestinamente o con engaño, será sancionado con prisión de 6 a 20 meses y hasta 30 días-multa.*

La misma sanción se impondrá al que permanezca en tales lugares contra la voluntad expresa de quien tenga derecho a excluirlo o al que se establezca en los mismos clandestinamente o con engaño.

La sanción será de 1 a 3 años y de 30 a 100 días-multa si el hecho fuere cometido con fuerza en las cosas, violencia en las personas, con armas o por dos o más personas".

Artículo 164.-*"El que se introduzca en oficina privada o en el lugar reservado de trabajo de una persona, sin la voluntad de quien ejerza en él sus funciones o actividad profesional o laboral, será sancionado con prisión de 6 meses a un año y hasta 25 días-multa".*

Artículo 165.-*"El servidor público que allane la morada, casa o lugar de trabajo, sin las formalidades prescritas por la ley o fuera de los casos que ésta determina, será sancionado con prisión de 6 meses a 1 año y hasta 30 días-multa".*

b) Delitos contra la inviolabilidad de secretos:

Artículo 166.- "*El que abra indebidamente una carta, un pliego cerrado o un despacho cablegráfico o de otra naturaleza, que no le esté dirigido, o el que sin abrir la correspondencia, por medios técnicos se impusiere de su contenido, será sancionado con 30 a 60 días-multa.*

Si la persona que ha cometido el hecho punible divulga el contenido de la correspondencia mencionada en el párrafo anterior, con perjuicio ajeno, la pena será de 10 meses a 2 años de prisión, pero si es empleado de Correos y Telecomunicaciones o de alguna empresa privada de comunicaciones nacionales o internacionales, la sanción

[446] [En línea] < http://www.unifr.ch/derechopenal/legislacion/pa/cp_panama6.pdf > [consulta: 17 de Enero 2003].

se aumentará de una sexta parte a la mitad".

Artículo 167.-*"El que sustraiga, destruya, sustituya, oculte, extravíe o intercepte correspondencia dirigida a otro, será sancionado con prisión de 1 a 2 años y si es empleado de Correos y Telecomunicaciones o de alguna empresa privada de comunicaciones nacionales o internacionales, la sanción se aumentará de una sexta parte a la mitad.*

Si la persona que ha cometido el hecho punible divulga el contenido de la correspondencia, con perjuicio ajeno, la pena será de 15 a 30 meses de prisión y si es empleado de Correos y Telecomunicaciones o de una empresa privada de comunicaciones nacionales o internacionales, la sanción se aumentará de una sexta parte a la mitad".

Artículo 168.-"*El que posee legítimamente una correspondencia, grabaciones o papeles no destinados a la publicidad y los haga públicos sin la debida autorización, aunque le hubiesen sido dirigidos, será sancionado con 15 a 60 días-multa cuando el hecho pudiere causar perjuicio.*

No se considerará delito la divulgación de documentos indispensables para la comprensión de la historia y los hechos políticos".

Artículo 169.-*"El que grabe las palabras de otro no destinadas al público, sin su consentimiento, o el que mediante procedimientos técnicos escuche conversaciones privadas que no le estén dirigidas, será sancionado con 15 a 50 días-multa".*

Artículo 170.-*"El que por razón de su oficio, empleo, profesión o arte, tenga noticia de secretos cuya publicación pueda causar daño y los revele sin consentimiento del interesado o sin que la revelación fuere necesaria para salvaguardar un interés superior, será sancionado con prisión de 10 meses a 2 años o de 30 a 150 días-multa, e inhabilitación para ejercer tal oficio, empleo, profesión o arte hasta por 2 años".*

10. Conclusiones

El ordenamiento jurídico de la República panameña no contiene a nivel constitucional previsión alguna en materia de protección a los datos personales. En aquél, apenas se reconocen indirectamente el derecho a la vida privada y a la intimidad. A pesar de lo anterior, estimamos que la Convención Americana de Derechos Humanos supliría los vacíos normativos constitucionales respecto de aquellos derechos.

En materia legal, Panamá no dispone de una ley de protección de datos personales. Sin embargo, puede señalarse que existen dos estatutos legales que se ocupan de la protección de los datos personales de forma parcial; la primera de carácter procedimental, contempla la acción de hábeas data con el fin de acceder, rectificar y cancelar los datos personales en poder de los órganos del Estado, y acceder a los datos en poder de particulares que tienen a su cargo servicios públicos en carácter de exclusividad. La segunda ley, regula el mercado de la información crediticia de los reportes o informaciones de crédito y reconoce los derechos de acceso, rectificación y supresión de los datos personales en los casos que señala. Por otra parte, existen en

materia legal disposiciones sectoriales simples que, en general, establecen deberes de confidencialidad de ciertas informaciones, de las cuales por lo cierto, no se deduce principio alguno en materia de tratamiento y transmisión de datos personales. Finalmente, cabe anotar que no tenemos conocimiento de Proyectos de Ley en materia de protección de datos personales que se hayan presentado en Panamá.

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN PARAGUAY

1. Generalidades

El ordenamiento jurídico paraguayo contempla una disposición constitucional en la cual se reconoce expresamente la garantía del hábeas data, lo que se traduce en una acción que sólo puede tener como sujetos pasivos a los responsables de los registros, archivos o bancos de datos de carácter oficial, o los privados de carácter público.

En materia legal, Paraguay cuenta desde el año 2000 con la Ley Nº 1.682 de regulación de la información privada, la cual fue modificada a sólo dos años de su vigencia. Esta ley, pretende normar el tratamiento de los datos personales realizado tanto por el sector público como por el privado, sin embargo, sus disposiciones son demasiado estrechas como para pretender regular de manera completa y sistemática la protección a los datos personales; existen serios vacíos tanto sustantivos como procesales, éstos últimos graficados en la inexistencia de reglas de competencia ni de procedimiento para hacer efectiva la acción constitucional de hábeas data.

En otros ámbitos legales sólo se aprecian normas sectoriales que, en general, establecen deberes de secreto respecto de las informaciones que tratan en razón de sus actividades. Este es el caso de la legislación tributaria y bancaria.

2. Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional

La Constitución Política paraguaya de 1992 [447] reconoce en el artículo 135, insertado dentro del Capítulo XII, intitulado “De las Garantías Constitucionales”, la garantía del hábeas data. Al efecto señala:

Artículo 135. Del Hábeas Data.

“Toda persona puede acceder a la información y a los datos que sobre si misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como

[447] [En línea] < http://www.georgetown.edu/pdba/Constitutions/Paraguay/para1992.html > [consulta: 11 de Diciembre 2002].

conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos".

En cuanto a la naturaleza del hábeas data paraguayo, se ha señalado por Benítez que "es una garantía específica dirigida a asegurar un poder jurídico para que su titular o sujeto activo pueda controlar el flujo de información o datos que se plasmen en archivos públicos o privados de carácter público y que puedan trascender a terceros (…)" [448] . En este mismo sentido se ha pronunciado la Corte Suprema de Justicia, señalando que "(…) esta es una garantía constitucional tendiente a tornar efectivas algunas previsiones constitucionales, tales como el derecho a la intimidad (art. 33 C.N), la inviolabilidad del patrimonio documental y la comunicación privada (art. 36 C.N) o la protección de la dignidad imagen privada de las personas (…)" (sic) [449] .

Se ha dicho que los antecedentes de la garantía del hábeas data paraguayo se encontrarían en el artículo 35 de la Constitución Portuguesa, así como también en el artículo 105 letra b) de la Constitución Española de 1978 [450] . Es posible afirmar, que la historia de la inclusión de la norma del artículo 135 en la Constitución paraguaya va de la mano con los acontecimientos políticos y sociales ocurridos en ese país tras largos años de dictadura militar, pues emerge en gran medida como respuesta ante la falta de una herramienta jurídica que les permitiera saber a los ciudadanos, qué clase de datos personales estaban aún en poder de algunos organismos del Estado, como las policías y otros entes de seguridad. La operatividad del instituto una vez plasmado en la Constitución, se pone a prueba en uno de los casos más importantes de hábeas data que haya conocido la jurisprudencia paraguaya; un pedido en contra de la Policía Nacional para que ésta le exhibiera a un ciudadano las constancias que sobre él obraban en su poder [451] .

Siguiendo con la historia del establecimiento del institutito en comento, cabe hacer presente que, en el debate del texto base que luego pasaría a ser el artículo 135, se discutió particularmente lo referido al sujeto pasivo de la acción, en particular, respecto a la diferencia conceptual entre los registros oficiales y los privados de carácter público. Finalmente, se aclaró que los registros privados de carácter público son los que pertenecen a las fundaciones, centros culturales, centros de investigación, etc., y que el acceso a los registros privados no sería factible pues se vulneraría la disposición constitucional que garantiza la inviolabilidad de los papeles privados [452] . Lo anterior, se ve reflejado en la redacción del texto actual ya transcrito, por lo que para la solución de conflictos interpretativos en la materia, servirá de guía lo señalado en el seno de la Convención Constituyente de la Carta Fundamental de 1992.

448 Benítez, Luis María: *"La Acción de Hábeas Data en el Derecho Paraguayo"*, Revista Ius et Praxis, Universidad de Talca, Año 3 Nº 1, 1997, Talca, pág. 111.

449 Citado por Puccinelli, Óscar R., *op. cit*., pág. 554.

450 Benítez, Luis María, *op. cit*., pág. 111.

452 Puccinelli, Óscar, *op. cit*., pág. 551.

Por otra parte, debemos señalar que al menos tres disposiciones complementan la configuración constitucional de la garantía del hábeas data, otorgándole a ésta una amplitud que lamentablemente a nivel legal no se ve reflejada. La primera disposición, es la del artículo 45 titulado "De los Derechos y Garantías no enunciados", la que señala: *"La enunciación de los derechos y garantías contenidos en esta Constitución no debe entenderse como negación de otros que, siendo inherentes a la personalidad humana, no figuren expresamente en ella. La falta de ley reglamentaria no podrá ser invocada para negar ni para menoscabar algún derecho o garantía".* De lo recién anotado, queda claro que la falta de reglamentación en ningún caso perjudica a los titulares de los derechos y garantías, por lo que se entiende que todos los órganos del Estado deben actuar siempre en defensa de ellos.

El artículo 131, a su turno dispone que: *"Para hacer efectivos los derechos consagrados en esta Constitución, se establecen las garantías contenidas en este capítulo, las cuales serán reglamentadas por la ley".* Como ya se ha adelantado, si bien la Ley 1.682 sólo reglamenta parcialmente la disposición del artículo 135, ello no es obstáculo para la actuación de los jueces, los cuales están obligados a tramitar las acciones que tutelan las garantías constitucionales. Esto se reafirma por la disposición contenida en el artículo 136 intitulado "De la Competencia y de la Responsabilidad de los Magistrados", la cual prescribe que: *"Ningún magistrado judicial que tenga competencia podrá negarse a entender en las acciones o recursos previstos en los artículos anteriores; si lo hiciese injustificadamente, será enjuiciado y, en su caso, removido (…) En las decisiones que dicte, el magistrado judicial deberá pronunciarse también sobre las responsabilidades en que hubieran incurrido las autoridades por obra del proceder ilegítimo y, de mediar circunstancias que prima facie evidencien la perpetración de delito, ordenará la detención o suspensión de los responsables, así como toda medida cautelar*

[451] Benítez (a la sazón juez de la República del Paraguay que participó en ese caso), reafirmando la importancia del hábeas data en Paraguay en el campo de los derechos humanos, relata lo sucedido: "La policía nacional ante la requisitoria de la magistratura contesta y dice "no obra nada en nuestro registro". Pasan diez, quince días y ocurre que el magistrado competente ante el cual se presentó el recurso de Hábeas data recibe una información de que las informaciones sobre tal persona estarían en tal lugar, en una dependencia policial X. (…) Este magistrado dicta una orden de allanamiento a dicha dependencia policial, y acompañado también por el juez del crimen de turno que tenía procesos por violaciones de derechos humanos, amplía a través de una resolución la constitución y allanamiento en dicho lugar con el objeto de obtener conocimiento de los elementos probatorios que existirían en ese lugar sobre las desapariciones, (…) se procede al allanamiento, se entra en dicho lugar, se pide la apertura de una puerta, se abre y se encuentran documentaciones, (…) que se referían a la Operación Cóndor: intercambio de prisioneros entre Paraguay, Uruguay, Argentina, y otros países. (…) Al día siguiente, los mismos jueces disponen el allanamiento del Ministerio del Interior en lo que sería la Sección Técnica, Sección Política, en la cual también cae abundante documentación sobre informaciones a partir del año 1920 en adelante. O sea, toda la vida e historia de la represión de un país" (Benítez, Luis M., *op, cit*, págs. 115 y 116). Cabría preguntarse si este camino podría tener el mismo éxito en nuestro país, y eventualmente, solucionar en parte una duda de no pocos ciudadanos, como lo es saber qué información existe aún en los registros, archivos o bancos de datos de las Fuerzas Armadas acerca de su persona y que están caratulados o clasificados como secretos en razón de la seguridad de la nación u otra causa legal. La respuesta a ello no es fácil, pues la propia Ley 19.628 niega el derecho de información, modificación, cancelación o bloqueo de datos, cuando se afecte *"la reserva o secreto establecido en disposiciones legales o reglamentarias, la seguridad de la nación o el interés nacional".* Con todo, sería la Corte Suprema la llamada a resolver estos casos, si se denegara el ejercicio de los derechos de los titulares fundado en la causal seguridad de la nación o interés nacional (Art. 16 inc. 3º Ley 19.628).

que sea procedente para la mayor efectividad de dichas responsabilidades. Asimismo, si tuviese competencia, instruirá el sumario, pertinente y dará intervención al Ministerio Público; si no la tuviese, pasará los antecedentes al magistrado competente par su prosecución". De lo anterior, se sigue la obligación que tienen los jueces de conocer y fallar las acciones entabladas en resguardo de los derechos y garantías fundamentales, entre las cuales se cuenta el hábeas data.

Sin duda, las disposiciones recién señaladas son de máxima importancia, pues vienen a complementar la protección constitucional a los derechos humanos, y a establecer la supremacía en todo caso de los derechos fundamentales y sus garantías. En esta materia, cabe hacer presente que Paraguay es parte de la Convención Americana de Derechos Humanos, con lo cual el precepto del artículo 45 toma mayor fuerza a falta de norma expresa del Constituyente [453] .

Siguiendo dentro del ámbito constitucional de protección a los datos personales, debemos anotar por otra parte, que el inciso 4º del artículo 24 titulado "De la Libertad Religiosa y la Ideológica" dispone lo siguiente: *"nadie puede ser molestado, indagado u obligado a declarar por causa de sus creencias o de su ideología".* De esta norma, podríamos deducir un principio de prohibición de recolección y tratamiento de esa clase de datos sensibles. En nuestra opinión, la actividad encaminada a recolectar y tratar datos sensibles sería una actividad que se relacionaría directamente con el objeto que pretende cautelar la norma, cual es, evitar la discriminación de las personas o clasificarlas según sus credos e ideologías.

Por su lado, el artículo 28 intitulado "Del Derecho a Informarse" señala en el inciso 2º que: *"las fuentes públicas de información son libres para todos. La ley regulará las modalidades, plazos y sanciones correspondientes a las mismas, a fin de que este derecho sea efectivo".* Respecto de esta regla, se ha dicho por Puccinelli que sería otra versión del hábeas data, la destinada a acceder a la información pública, la cual se relaciona con la libertad de expresión y la libertad de prensa [454] .

Más adelante, el artículo 33 denominado "Del Derecho a la Intimidad", reconoce la inviolabilidad de la intimidad en los siguientes términos: *"la intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública".* Agrega el inciso 2º que: "s*e garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas".* Llama la atención de esta norma, que por una parte reconozca una serie de derechos y que por otra, sólo se refiera a algunos de éstos al establecer las garantías a esos derechos. En este caso por ejemplo, por un lado se reconoce el respeto a la vida privada -entre otros derechos-, pero no se menciona la garantía específica de éste. Una interpretación consistente con lo preceptuado por la Constitución debería considerar incluida la garantía del respeto a la vida privada en la garantía del derecho a la intimidad pues, en general, se

[453] La ratificación paraguaya al texto de la Convención se realizó el 18 de Agosto año 1989. [En línea] < http://www.oas.org/juridico/spanish/firmas/b-32.html > [consulta: 20 de Marzo 2003].

[454] Puccinelli, Óscar, *op. cit.*, pág., 553.

estima que la intimidad estaría incluida dentro del derecho a la vida privada como una parcela específica de éste.

Finalmente, el artículo 34 denominado "Del Derecho a la Inviolabilidad de los Recintos Privados", señala que: *"todo recinto privado es inviolable. Sólo podrá ser allanado o clausurado por orden judicial y con sujeción a la ley. Excepcionalmente podrá serlo, además, en caso de flagrante delito o para impedir su inminente perpetración, o para evitar daños a la persona o a la propiedad".*

En suma, podemos afirmar que en el ordenamiento jurídico constitucional paraguayo se contempla una protección directa a los datos personales a través de la garantía del hábeas data, la cual se traduce en una acción no regulada por el Constituyente, y que no opera respecto de los registros o archivos de carácter privado. Esta acción ha sido concebida por la jurisprudencia como una garantía constitucional tendiente a hacer efectivos derechos constitucionales como la intimidad, la inviolabilidad de las comunicaciones privadas e incluso la dignidad e imagen privada de las personas. De lo anterior, puede deducirse que en sede judicial, no existiría referencia a la autodeterminación informativa o libertad informática como bien jurídico protegido, lo que no significa que la doctrina haya hecho suya esa opinión. Por el contrario, como se vio, al menos un autor (Benítez) habla de la facultad de control de la propia información, con lo cual se aleja de la postura tradicional acerca del bien jurídico protegido y se acerca a la concepción del hábeas data como garantía del derecho a la protección de datos o autodeterminación informativa, según el enfoque terminológico que se adopte.

2.2 Protección Legal de los Datos Personales

En materia legal, Paraguay sólo cuenta con la Ley Nº 1.682 del año 2000 que reglamenta la información de carácter privado [455] . El objeto de esta ley es *"regular la recolección y el tratamiento de datos personales contenidos en archivos, registros, bancos de datos o cualquier otro medio técnico de tratamiento de datos públicos o privados destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares"*. Esta normativa no se aplica a las bases de datos ni a las fuentes de informaciones periodísticas ni a las libertades de emitir opinión y de informar (Art. 1º Ley Nº 1.682). De lo recién expuesto, podría entenderse a primera vista que el legislador habría ampliado los sujetos pasivos de la acción de hábeas data constitucional, cuales son: los responsables de los *"registros oficiales o privados de carácter público"* (Art. 135 C. Pol.). La afirmación anterior es sólo parcial, pues esa ampliación del sujeto pasivo sólo alcanzaría a los responsables de registros o bancos de datos de carácter privados que suministren información sobre solvencia económica y situación patrimonial. Nuestra afirmación, se basa en lo prescrito por el artículo 8º de la Ley, el cual dispone que: *"Toda persona podrá acceder a la información y a los datos que sobre sí misma, sobre su cónyuge, sobre personas que acredite se hallen bajo su tutela o curatela, o sobre sus bienes, obren en registros oficiales o privados de carácter público* ***o en entidades que suministren información sobre solvencia económica y situación patrimonial*** *, así*

[455] [En línea] < http://www.ulpiano.com/DataProtection-LA-links.htm > [consulta: 18 de Noviembre 2002]. Cabe hacer presente que esta Ley fue modificada en Agosto de 2002 por la Ley Nº 1.969.

como conocer el uso que se haga de los mismos o su finalidad" (negrita nuestra).

Por otra parte, llama la atención que el legislador sólo se refiera a los derechos de acceso, actualización, modificación o eliminación, a propósito de los datos personales sobre la situación patrimonial, solvencia económica y el cumplimiento de obligaciones comerciales (Art. 7º Ley 1.682) y omita referirse a esos derechos en el señalado artículo 8º, el cual sólo trata del derecho de acceso. Todo lo anterior se desprende de lo señalado en el artículo 7º, del cual se deduce además que el ejercicio de los derechos de actualización, modificación o eliminación en contra de los responsables de archivos o bancos de datos personales sobre la situación patrimonial, solvencia económica y el cumplimiento de obligaciones comerciales, debe realizarse directamente ante éstos [456] .

En otro ámbito, también nos llama la atención el artículo 2º de la Ley, el cual consagra el derecho a recolectar y procesar datos de forma privada, cuestión que en nuestro concepto, a lo más, podría establecerse como excepción a una regla general, pero no transformar legalmente en regla general a la excepción. Al respecto se señala: *"Toda persona tiene derecho a recolectar, almacenar y procesar datos personales para uso estrictamente privado".* Luego agrega en el inciso 2º que: *"Las fuentes públicas de información son libres para todos. Toda persona tiene derecho al acceso a los datos que se encuentren asentados en los registros públicos, incluso los creados por la Ley Nº 879 del 2 de diciembre de 1981, la Ley Nº 608 del 18 de julio de 1995, y sus modificaciones".*

Cabe hacer presente por otra parte, que la Ley Nº 1.682 fue objeto de una modificación legal el año 2002, la cual si bien amplió el objeto de ésta -en el sentido ya anotado-, por otro lado rebajó el *quantum* de las multas aplicables a las empresas que emiten reportes de crédito y a las usuarias del servicio que violen las disposiciones legales [457] .

timamos que la inconsistente configuración legal anterior, podría ser consecuencia de una finalidad no explicitada por la Ley, cual sería la legalización del mercado de la información de carácter económico, financiero y comercial, pues aunque esta legislación trate de presentarse con carácter de general, de un somero análisis a ella se desprende todo lo contrario, es decir, estaría más cercana a una regulación carácter sectorial

[456] Artículo 7º.-"*Serán actualizados permanentemente los datos personales sobre la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales que de acuerdo con esta ley pueden difundirse. (…) La obligación de actualizar los datos mencionados en el párrafo anterior pesan sobre las empresas, personas o entidades que almacenan, procesan y difunden esa información. Esta actualización deberá realizarse dentro de los cuatro días siguientes del momento en que llegaren a su conocimiento. Las empresas, personas o entidades que utilizan sus servicios tienen la obligación de suministrar la información pertinente a fin de que los datos que aquellas almacenen, procesen y divulguen, se hallen permanentemente actualizados, para cuyo efecto deberán comunicar dentro de los dos días, la actualización del crédito atrasado que ha generado la inclusión del deudor. (…) Los plazos citados precedentemente empezarán a correr a partir del reclamo realizado par parte del afectado. (…) En caso de que los datos personales fuesen erróneos, inexactos, equívocos o incompletos, y así se acredite, el afectado tendrá derecho a que se modifiquen.(…) La actualización, modificación o eliminación de los datos será absolutamente gratuita, debiendo proporcionarse además, a solicitud del afectado y sin costo alguno, copia auténtica del registro alterado en la parte pertinente".*

[457] Esta Ley es la Nº 1.969 de Agosto de 2002, la cual está disponible [en línea] < http://www.informconf.com.py/informconf/site/downloads/Ley_1682.pdf > [consulta: 3 de Febrero 2003].

compleja.

En suma, creemos que la garantía constitucional del hábeas data del artículo 135, sólo ha sido parcialmente regulada y sectorialmente ampliada por el legislador; lo primero en razón a que sólo se refiere a los derechos de acceso, actualización, modificación o eliminación de datos a propósito del tratamiento de datos sobre la situación patrimonial, la solvencia económica y el cumplimiento de las obligaciones comerciales. Lo segundo, dado que esa ampliación está circunscrita al sujeto pasivo de la acción de hábeas data, la cual alcanza exclusivamente a los responsables de los archivos, registros o bancos de datos que traten y difundan datos personales sobre la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales.

2.2.1) Otras Normas Legales de Protección a los Datos Personales

En otros cuerpos legales, se constatan normas sectoriales que establecen deberes de secreto. En materia tributaria, éste cubre los datos suministrados a la administración tributaria por los contribuyentes. Por su parte, la legislación bancaria establece normas que velan por la confidencialidad de las operaciones realizadas por los clientes y los usuarios del sistema. A continuación se señalarán las respectivas disposiciones en la materia.

2.2.1.1) Ley que establece el Nuevo Régimen Tributario (Ley Nº 125/91) [458]

La Ley 125 de 1991, establece el nuevo régimen tributario paraguayo. Dentro de sus disposiciones encontramos el artículo 190 titulado "Secreto de las actuaciones", el cual dispone que: *"las declaraciones, documentos, informaciones, o denuncias que la Administración reciba y obtenga tendrán carácter reservado y sólo podrán ser utilizados, para los fines propios de la Administración".* Luego, el inciso 2º señala que: *"los funcionarios de ésta no podrán, bajo pena de destitución y sin perjuicio de su responsabilidad personal, civil y o penal, divulgar a terceros en forma alguna datos contenidos en aquéllas. El mismo deber de reserva pesará sobre quienes no perteneciendo a la Administración Tributaria, realicen para ésta trabajos o procesamientos automáticos de datos u otras labores que importan el manejo de material reservado de la administración tributaria".* A continuación el inciso 3º y final establece las excepciones al deber de secreto, señalando que: *"las informaciones comprendidas en este artículo, sólo podrán ser proporcionadas a los órganos jurisdiccionales que conocen los procedimientos sobre tributos y su cobro, infracciones fiscales, débitos comunes, pensiones alimenticias y causas de familia o matrimoniales, cuando entendieran que resulta imprescindible para el cumplimiento de sus fines y lo soliciten por resolución fundada. Sobre la información así proporcionada regirá el mismo secreto y sanciones establecidas en el párrafo segundo".*

En suma, de las reglas anteriores, se desprende que el deber de secreto no sólo pesa sobre los funcionarios de la administración tributaria, sino que también sobre los particulares que presten servicios a ese organismo estatal y manejen las informaciones

[458] **[En línea] < http://www.paraguaygobierno.gov.py/ley125.doc > [consulta: 18 de Noviembre 2002].**

tributarias de carácter reservadas. Destaca además la explícita referencia a la finalidad del uso de esa clase de información, cual es la propia de la Administración Tributaria.

2.2.1.2) Ley General de Bancos, Financieras y Otras Entidades de Crédito [459]

En materia bancaria, el artículo 84 denominado "Secreto sobre operaciones" dispone que: *"Prohíbese a las Entidades del Sistema Financiero, así como a sus directores, órganos de administración y fiscalización y trabajadores, suministrar cualquier información sobre las operaciones con sus clientes, a menos que medie autorización escrita de éstos o se trate de los supuestos consignados en los artículos siguientes. La prohibición no alcanzará a los casos en que la divulgación de las sumas recibidas de los distintos clientes resulte obligada para los fines de liquidación de las entidades bancarias o financieras".* De lo recién señalado, se entiende que el deber de secreto cubriría tanto las operaciones activas como pasivas, pues el legislador habla de *"las operaciones"* sin circunscribirlas determinadamente.

A renglón seguido, el artículo 85 cuyo encabezado reza "Deber de secreto", dispone que la prohibición mencionada en el artículo anterior recaerá también sobre: *a) Los directivos y funcionarios de la Superintendencia de Bancos, salvo que se trate de información respecto de los titulares de las cuentas corrientes cerradas por el libramiento de cheques sin provisión de fondos; b) Los directores y trabajadores del Banco Central del Paraguay; y, c) Los socios, representantes, empleados y trabajadores de las sociedades de auditoría que examinen los balances de las Entidades del Sistema Financiero".*

La norma anterior da cuenta de la visión sistémica que tiene el legislador en materia de secreto bancario lo cual parece bastante razonable y recomendable, pues ahorra esfuerzos de búsqueda de normas sectoriales que apunten a una misma finalidad [460].

En otro ámbito de la legislación bancaria, cabe agregar que existen algunas disposiciones relacionadas con la actividad que realiza la Central de Riesgo del sistema bancario paraguayo cuyo objeto es *"(…) facilitar a las Entidades del Sistema Financiero y al Banco Central del Paraguay información sobre la situación global de endeudamiento de los diferentes clientes del Sistema Financiero"* (Art. 89). En concordancia con el objeto de la Central de Riesgo, el artículo 90 establece un deber de información por parte de los bancos para con la Superintendencia de Bancos. Al respecto, se dispone en el inciso 1º que: *"las Entidades del Sistema Financiero estarán obligadas a suministrar a la Superintendencia de Bancos, en la forma que ella determine, la información que se requiera para mantener al día la Central de Riesgos.* Por otra parte, el artículo 91 limita el uso de la información, disponiendo que: *"las Entidades del Sistema Financiero tendrán acceso a toda la información de la Central de Riesgos, la cual será utilizada por ésta exclusivamente para adoptar decisiones sobre riesgo crediticio. La Superintendencia de Bancos podrá exigir el pago de un canon por este servicio".* De lo anterior puede afirmarse que se consagraría al menos parcialmente, el principio de la finalidad en el uso de los datos por parte de las entidades del sistema financiero. Luego, el inciso 2º de este

[459] [En línea] < http://www2.paraguaygobierno.gov.py/ley_861.html > [consulta: 5 de Febrero 2003].

artículo señala que:*"los informes de la Central de Riesgos tendrán carácter reservado; no podrán publicarse, comunicarse ni exhibirse a terceros, y en ningún caso harán constar el nombre de las entidades de crédito acreedoras".* Por último, se prescribe que: *"el Banco Central del Paraguay podrá utilizar para el ejercicio de sus funciones la información obtenida por la Central de Riesgos, y no será responsable de los perjuicios que pudieran derivarse del suministro por las entidades financieras declarantes de datos inexactos"* (Art. 91 inc. Final).

En suma, el legislador ha establecido el secreto bancario de una forma amplia, el cual abarcaría todas las operaciones de los clientes. Por otra parte, también se establecen deberes de información necesarios para que la Central de Riesgo pueda cumplir su cometido, así como deberes de secreto respecto de los informes transmitidos por ese organismo. Cabe destacar en esta materia, la disposición en la cual se vislumbra en parte el principio de la finalidad, al señalarse que el uso de los datos obtenidos a través de la Central de Riesgo por parte de las Instituciones Financieras, se circunscribe exclusivamente a la adopción de decisiones sobre riesgo crediticio.

3. Bienes Jurídicos Protegidos por la Legislación de Datos Personales

En materia de bien jurídico tutelado por las normas de protección de datos personales, debemos señalar en primer lugar, que a nivel constitucional, la configuración del hábeas data -que podría ser entendida como un reconocimiento al derecho a la protección de datos- no señala cuáles serían los bienes jurídicos tutelados por esa garantía. Al respecto, se ha dicho por Puccinelli que a pesar de lo anterior, la formulación amplia que

460 Por su lado, el artículo 86 también establece otras excepciones al deber de secreto señalando que la reserva bancaria no regirá cuando la información sea requerida por: a) El Banco Central del Paraguay y la Superintendencia de Bancos en ejercicio de sus facultades legales; b) La autoridad judicial competente en virtud de resolución dictada en juicio, en el que el afectado sea parte. En tal caso, deberán adoptarse las medidas pertinentes que garanticen la reserva; c) La Contraloría General de la República y las autoridades impositivas en el marco de sus atribuciones sobre la base de las siguientes condiciones: I) Debe referirse a un responsable determinado; II) Debe encontrarse en curso una verificación impositiva con respecto a ese responsable; y, III) Debe haber sido requerido formal y previamente; d) Las entidades de crédito que intercambian entre sí, de acuerdo a reciprocidad y prácticas bancarias, conservando el secreto bancario. Por último, el inciso final del artículo 86 dispone que: *"el deber de secreto se transmite a las instituciones y personas exceptuadas en los incisos anteriores. En todos los casos, cuando en procesos judiciales o administrativos para cuya tramitación se haya utilizado información sobre operaciones resguardadas por el secreto bancario, éste cesará a todos los efectos en forma automática si de tales actuaciones se derivara culpabilidad de los beneficiados con el secreto. Los involucrados en la causa que resultaran sobreseídos en las actuaciones judiciales conservarán la protección de secreto para sus operaciones".* La disposición anterior aclara un punto importante relativo a la publicidad de lo obrado en los procesos judiciales. En los casos de excepción al secreto bancario señalados por la ley, se establece expresamente que en caso de existir culpabilidad de quien se beneficia con el secreto, éste cesará para todos los efectos. Por otro lado, el artículo 87 referente a las "Informaciones consolidadas" dispone que: "*el deber de secreto no alcanzará a informaciones de carácter agregado y calificaciones que suministren el Banco Central del Paraguay y la Superintendencia de Bancos inclusive por tipos de depósito, sin identificar a clientes en particular"*. En este caso se desprende que sería requisito indispensable para tal cometido, la utilización de mecanismos de disociación de datos para evitar la identificación de los titulares de éstos.

realiza el Constituyente "permite alojar la más amplia gama de bienes" [461] . La Corte Suprema por su parte, ha señalado algunos de los bienes jurídicos tutelados por la norma del artículo 135 de la Constitución, a saber: el derecho a la intimidad, la inviolabilidad del patrimonio documental y la comunicación privada, la protección de la dignidad y la imagen privada de las personas, así como también la libertad y la seguridad de éstas. También se ha mencionado el derecho a la libre expresión de la personalidad [462] . Con todo, Puccinelli concluye en relación a la garantía del hábeas data constitucional que "si bien ni en las normas ni en la jurisprudencia se observa mención expresa a la autodeterminación informativa o a la libertad informática, es perfectamente factible crear este derecho, vía legal o pretoria, y darle una tutela mediante esta garantía" [463] .

En nuestra opinión, la configuración constitucional del hábeas data está más cerca de considerarse un derecho a la protección de datos personales, pues se reconoce como garantía que puede proteger diversos bienes jurídicos como la intimidad o la vida privada, e incluso el honor, lo cual no significa excluir a la libertad informática. El problema con esta última se plantea en razón de la limitación constitucional del instituto, el cual deja fuera a los bancos de datos de carácter privado. Por otra parte, la Ley 1.682 tampoco aporta mucho en este ámbito, pues más bien se ocupa de regular el mercado de la información crediticia, lo que ha traído como consecuencia que si bien potencialmente han aumentado los sujetos pasivos de una acción de hábeas data, éstos se limitan a aquellos que tratan datos de carácter comercial, por lo que la eventual mayor protección respecto de los bancos de datos particulares es sólo parcial pues deja fuera a otros bancos de datos dedicados a tratar otro tipo de informaciones.

Por tanto, estimamos que podría afirmarse la existencia de un derecho a la protección de datos o hábeas data limitado en el ordenamiento jurídico paraguayo, el cual es necesario desarrollarlo sistemáticamente en una ley general de protección de datos. Opinamos que sería un derecho limitado *ab initio*, porque excluye del ámbito de control de la información personal a los bancos de datos de carácter privado, lo cual le quita fuerza. Lo anterior no es de extrañar, pues tal limitación más bien es una situación característica de los ordenamientos jurídicos latinoamericanos que reconocen de alguna forma el derecho a la protección de datos o hábeas data según se le designe.

4. Principios Informativos de la Legislación de Protección de Datos Personales

En materia de principios informativos de la legislación de protección de datos personales, sólo nos referiremos a aquéllos que se desprenden de la Ley Nº 1.682 que reglamenta la información de carácter privado, pues es el único cuerpo normativo referido especialmente a la protección de los datos personales.

461 Puccinelli, *op cit*, pág. 556.

462 Citado por Puccinelli, *op cit*., pág. 557.

463 *Ibídem*.

1º. Principio de la licitud y lealtad de los archivos de datos

Como ya se ha visto, el artículo 1º de la Ley Nº 1.682 señala el objeto de ésta, cual es, regular la recolección, almacenamiento, distribución, publicación, y en general, el tratamiento de datos personales contenidos en archivos, registros, bancos de datos públicos o privados destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares. De lo señalado por el legislador, se sigue que los bancos de datos o registros o archivos de datos personales, para que sean lícitos, deben adecuarse a las mínimas prescripciones de esta ley. Entre éstas podemos mencionar aquella contenida en el artículo 2º inciso 1º que dispone: *"toda persona tiene derecho a recolectar, almacenar y procesar datos personales para uso estrictamente privado".* De lo anterior se deduce que el legislador tuvo presente las discusiones llevadas a cabo en el seno de la Comisión Constituyente a la hora de discutirse el alcance del hábeas data del artículo 135 de la Constitución, la cual llegó a la conclusión de que los archivos privados estaban fuera del alcance de la ley por contraponerse al derecho a la inviolabilidad documental (ver punto Nº 2.1). Por lo tanto, todo particular está habilitado para recolectar y tratar datos personales siempre que sea para el uso estrictamente privado.

El artículo 3º por su parte señala que:*"es lícita la recolección, almacenamiento, procesamiento y publicación de datos o características personales, que se realicen con fines científicos, estadísticos, de encuestas y sondeos de la opinión pública o de estudio de mercados, siempre que en las publicaciones no se individualicen las personas o entidades investigadas"*. De lo anterior se sigue la licitud de los bancos de datos o registros que traten datos personales mediante procesos de disociación de éstos.

A renglón seguido, el artículo 4º inciso 1º prescribe que: *"se prohíbe dar a publicidad o difundir datos sensibles de personas que sean explícitamente individualizadas o individualizables".* Esta regla implícitamente establece la licitud de los archivos, registros o bancos de datos sensibles siempre y cuando no se difundan o publiciten. En esta materia creemos que el legislador no ha tenido el debido cuidado con el tratamiento de este tipo de datos, pues sólo se limita a señalar la regla anterior sin más. Creemos que habría sido conveniente señalar una prohibición general de tratamiento de los datos sensibles y, sólo por la vía excepcional permitirse el tratamiento de éstos.

El artículo 5º a su vez, dispone que los datos de las personas físicas o jurídicas individualizadas que revelen, describan o estimen su situación patrimonial, su solvencia económica o el cumplimiento de sus obligaciones comerciales, podrán ser publicados o difundidos solamente: "*a) Cuando esas personas hubiesen otorgado autorización expresa y por escrito para que se obtengan datos sobre el cumplimiento de sus obligaciones no reclamadas judicialmente; b) Cuando se trate de informaciones o calificaciones que entidades estatales o privadas deban publicar o dar a conocer en cumplimiento de disposiciones legales específicas y, c) Cuando consten en las fuentes públicas de información".* En esta disposición no sólo está presente el principio de la licitud de los archivos sino también el del consentimiento del titular tanto para el tratamiento como para la transmisión de los datos.

Finalmente, el artículo 6º señala en una norma poco clara, que podrán ser publicados

y difundidos: *"a) Los datos que consistan únicamente en nombre y apellido, documento de identidad, domicilio, edad, fecha y lugar de nacimiento, estado civil, ocupación o profesión, lugar de trabajo y teléfono ocupacional; b) Cuando se trate de datos solicitados por el propio afectado; y, c) Cuando la información sea recabada en el ejercicio de sus funciones, por magistrados judiciales, fiscales, comisiones parlamentarias o por otras autoridades legalmente facultadas para ese efecto".*

2º. Principio de la calidad de los datos

Encontramos este principio, aunque restringido a los datos de carácter crediticio, en el artículo 7º de la Ley Nº 1.682 que señala: *"serán actualizados permanentemente los datos personales sobre la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales que de acuerdo con esta ley pueden difundirse"* [464] . Luego agrega el inciso 2º que:*"la obligación de actualizar los datos mencionados en el párrafo anterior pesan sobre las empresas, personas o entidades que almacenan, procesan y difunden esa información".*

En el mismo sentido anterior se enmarca el artículo 9º, el cual establece la caducidad de la información registrada en los archivos y bancos de datos. Al efecto, se dispone por el legislador que las empresas, personas o entidades que suministran información sobre la situación patrimonial, la solvencia económica o sobre el cumplimiento de obligaciones comerciales no transmitirán ni divulgarán datos: a) Sobre deudas vencidas no reclamadas judicialmente cuando la mora no sea superior a los noventa días; b) Pasados tres años de la inscripción de deudas vencidas no reclamadas judicialmente; c) Pasados tres años del momento en que las obligaciones reclamadas judicialmente hayan sido canceladas por el deudor o extinguidas de modo legal; d) Sobre deudas reclamadas en juicios en los que se haya producido la caducidad de la instancia o las demandas que fuesen rechazadas por los juzgados por sentencias firmes y ejecutorias, siempre que esos hechos hubieran llegado a su conocimiento por informaciones públicas o por los propios afectados; e) Pasados cinco años del momento en que fueran suscritas las inhibiciones generales de vender o gravar bienes, y, en el caso en que fueran reinscriptas, después de los cinco años subsiguientes a esa reinscripción; f) Pasados siete años de la fecha en que se haya dictado sentencia definitiva que determine obligaciones patrimoniales, en los que no conste su cumplimiento por el condenado; g) Sobre sentencias declaratorias de quiebras después de siete años de su dictado, o, si se hubiese producido la rehabilitación del fallido, después de tres años de ese hecho; y, h) Sobre juicios de convocatoria de

464 Se agrega que: *"Esta actualización deberá realizarse dentro de los cuatro días siguientes del momento en que llegaren a su conocimiento. Las empresas, personas o entidades que utilizan sus servicios tienen la obligación de suministrar la información pertinente a fin de que los datos que aquellas almacenen, procesen y divulguen, se hallen permanentemente actualizados, para cuyo efecto deberán comunicar dentro de los dos días, la actualización del crédito atrasado que ha generado la inclusión del deudor.* Los plazos citados precedentemente empezarán a correr a partir del reclamo realizado por parte del afectado. En caso de que los datos personales fuesen erróneos, inexactos, equívocos o incompletos, y así se acredite, el afectado tendrá derecho a que se modifiquen. *La actualización, modificación o eliminación de los datos será absolutamente gratuita, debiendo proporcionarse además, a solicitud del afectado y sin costo alguno, copia auténtica del registro alterado en la parte pertinente".* (Artículo 7 incisos 2º, 3º 4º y 5º).

acreedores después de cinco años de la resolución judicial que la admita (Art. 9º).

El inciso final del artículo 9 dispone en relación a lo ya señalado que: *"las empresas o entidades que suministran información, sobre la situación patrimonial, la solvencia económica y el cumplimiento de compromisos comerciales deberán implementar mecanismos informáticos que de manera automática elimine de su sistema de información los datos no publicables, conforme se cumplan los plazos establecidos en este Artículo".*Sin duda, esta última disposición implícitamente apunta al respeto del principio de la calidad de los datos, a la vez que obliga a implementar sistemas informáticos que cumplan con la finalidad de eliminación de datos. Con ello, se endosa a los particulares la determinación en concreto de cuáles sistemas cumplirán con la finalidad, lo que en definitiva se traduce en una regla de conducta. Finalmente, serán los jueces los que determinen en abstracto el deber de diligencia que ha debido emplearse en la implementación de los sistemas informáticos llamados a resguardar el principio de la calidad de los datos, en lo relativo a la exactitud y actualización de éstos.

3º. Principio del consentimiento informado del titular de los datos

En lo relativo al principio del consentimiento informado del titular de los datos para el tratamiento de éstos, sólo una norma en la Ley paraguaya se refiere indirectamente a éste, el cual además está circunscrito al tratamiento de datos de carácter comercial. Al respecto, el artículo 5º de la Ley 1.682 dispone -como ya se vio- que los datos de personas físicas o jurídicas individualizadas que revelen, describan o estimen su situación patrimonial, su solvencia económica o el cumplimiento de sus obligaciones comerciales, podrán ser publicados o difundidos solamente: *a) Cuando esas personas hubiesen otorgado autorización expresa y por escrito para que se obtengan datos sobre el cumplimiento de sus obligaciones no reclamadas judicialmente (…)".* Por lo tanto, la regla exclusivamente está referida a la publicación y difusión de esa clase especial de datos. Consideramos que en materia de tratamiento de datos referidos al cumplimiento de obligaciones económicas, debería entenderse implícito el consentimiento del titular para aquél objetivo, pues ello antecede a la publicación o transmisión de éstos. Por otra parte, cabe comentar que si bien se reconocería implícitamente el principio del consentimiento previo del titular para el tratamiento de datos, la presencia de excepciones a éste -que no están determinadas exhaustivamente-, en definitiva, tiende a reducir el ámbito de aplicación de dicho principio, el cual se ve desplazado en materia de datos comerciales o de solvencia patrimonial por la disposición de la letra a) del artículo 5º, es decir, a través del empleo por parte de los acreedores de contratos de adhesión con cláusulas de estilo que autoricen a éstos para recabar información sobre el cumplimiento e incumplimiento de las obligaciones. Lo anterior, sin duda va en beneficio del sistema crediticio y constituye un poderoso incentivo al cumplimiento de las obligaciones, aunque por otra parte se limite en alguna forma la autonomía de la voluntad de los consumidores o deudores.

Otras excepciones al eventual principio del consentimiento para el tratamiento de los datos se señalan en el artículo 3º de la Ley 1.682, el cual dispone que: *"es lícita la recolección, almacenamiento, procesamiento y publicación de datos o características personales, que se realicen con fines científicos, estadísticos, de encuestas y sondeos de*

la opinión pública o de estudio de mercados, siempre que en las publicaciones no se individualicen las personas o entidades investigadas".

4º. Principio de la seguridad de los datos

En relación a este principio, debemos señalar que la Ley Nº 1.682 no dispone de reglas explícitas en la materia. De un modo implícito se visualizarían en el artículo 9 inciso final, al establecer el deber de los bancos de datos de información comercial de implementar mecanismos informáticos que de manera automática eliminen de su sistema de información los datos no publicables. Lo anterior, dado que la implementación de sistemas informáticos que velen por la exactitud de los datos, implicaría también que se tomen los resguardos necesarios para que esa información no pueda ser alterada, modificada o utilizada para otros fines por terceros.

Por otra parte, del artículo 3º también indirectamente se deduciría el principio de seguridad de los datos al señalarse que es lícita la recolección, almacenamiento, procesamiento y publicación de datos o características personales, que se realicen con fines científicos, estadísticos, de encuestas y sondeos de la opinión pública o de estudio de mercados, *"siempre que en las publicaciones no se individualicen las personas o entidades investigadas".* De lo señalado podría entenderse que, para evitar la individualización de los titulares de los datos es necesario tomar las medidas de seguridad pertinentes para cumplir con ese mandato de anonimato que establece el legislador.

5º. Principio de confidencialidad de los datos

Respecto de este principio, la Ley Nº 1.682 paraguaya no se pronuncia.

6º. Principio del consentimiento para la cesión de los datos

Este principio se encuentra débilmente presente en el artículo 5º ya visto, al señalar que los datos personales que revelen, describan o estimen la situación patrimonial, solvencia económica o el cumplimiento las obligaciones comerciales *"podrán ser publicados o difundidos solamente: a) Cuando esas personas hubiesen otorgado autorización expresa y por escrito para que se obtengan datos sobre el cumplimiento de sus obligaciones no reclamadas judicialmente".* Entre las excepciones a lo recién señalado podemos mencionar el hecho de no requerirse el consentimiento del titular, cuando esas obligaciones consten en las fuentes públicas de información (Art. 5º letra c). Respecto de los demás datos personales, se dispone en el artículo 6º de la Ley que podrán ser publicados y difundidos: *"a) Los datos que consistan únicamente en nombre y apellido, documento de identidad, domicilio, edad, fecha y lugar de nacimiento, estado civil, ocupación o profesión, lugar de trabajo y teléfono ocupacional; b) Cuando se trate de datos solicitados por el propio afectado; y, c) Cuando la información sea recabada en el ejercicio de sus funciones, por magistrados judiciales, fiscales, comisiones parlamentarias o por otras autoridades legalmente facultadas para ese efecto".* Finalmente, cabe mencionar que el artículo 3º no exige el consentimiento del titular de los datos para publicación de datos o características personales, que se realicen con fines científicos,

estadísticos, de encuestas y sondeos de la opinión pública o de estudio de mercados, siempre que en las publicaciones no se individualicen las personas o entidades investigadas.

7º. Principio de la finalidad

En lo relativo al principio de la finalidad, debemos decir que el artículo 8 de la Ley 1.682 lo reconocería al momento de señalar que toda persona podrá *"conocer el uso que se haga de los mismos o su finalidad"*,refiriéndose a los datos que obren en registros oficiales o privados de carácter público o en entidades que suministren información sobre solvencia económica y situación patrimonial. Es decir, restringido al ámbito específico que en definitiva regula la Ley 1.682, aunque se diga por ésta que su objeto es más amplio.

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

La ley paraguaya Nº 1.682, que según ella misma "reglamenta la información de carácter privado", es una normativa poco consecuente con sí misma, pues si bien pretende regular de manera general el tratamiento de los datos personales, mayoritariamente se ocupa de los datos de carácter económico o de solvencia patrimonial.

A continuación se señalarán aquellos ámbitos regulados por la ley paraguaya en los cuales se observa un tratamiento diferenciado del sector público y del sector privado en materia de protección de datos, en base a las áreas temáticas que ya hemos desarrollados en los análisis de la leyes generales argentina y chilena en la materia.

5.1 Consentimiento para el Tratamiento de los Datos

En lo relativo al consentimiento para el tratamiento de datos, como regla general, éste no aparece reconocido dentro de la ley 1.682. Así, el artículo 2º- ya visto- señala que: *"toda persona tiene derecho a recolectar, almacenar y procesar datos personales para uso estrictamente privado".* De lo recién anotado, aparece claro que el consentimiento del titular para nada importa en estos casos. Por otra parte, el ya señalado artículo 3º dispone que: *"Es lícita la recolección, almacenamiento, procesamiento y publicación de datos o características personales, que se realicen con fines científicos, estadísticos, de encuestas y sondeos de la opinión pública o de estudio de mercados, siempre que en las publicaciones no se individualicen las personas o entidades investigadas".* Nuevamente nada se dice respecto del consentimiento del titular de datos.

Podemos afirmar que en materia de consentimiento del titular de los datos para el tratamiento de éstos, nada se señala expresamente, sino que la única referencia implícita a éste es aquella en que se exige el consentimiento del titular para efectos de la "publicación" de sus datos. Al efecto, el artículo 5º letra a) de la Ley prescribe que los datos de personas físicas o jurídicas individualizadas que revelen, describan o estimen su situación patrimonial, su solvencia económica o el cumplimiento de sus obligaciones comerciales, podrán ser publicados o difundidos solamente: *"a) Cuando esas personas hubiesen otorgado autorización expresa y por escrito para que se obtengan datos sobre*

el cumplimiento de sus obligaciones no reclamadas judicialmente (…)". La regla del consentimiento para el tratamiento de esta clase de datos podría estimarse implícita en el requisito del mismo para la publicación o difusión de los datos, si se entendiera que el proceso de tratamiento y difusión de datos como una actividad integrada.

En suma, no se aprecia con claridad el requisito del consentimiento para el tratamiento de los datos personales y, en el único caso en que se avista, éste eventualmente sería aplicable sólo a los particulares, salvo que el Estado en sus relaciones patrimoniales con los particulares esté facultado para utilizar tal medio, cuestión que desconocemos.

5.2 Consentimiento para la Cesión de Datos Personales

En lo relativo al requisito del consentimiento del titular para la cesión o transmisión de sus datos personales, la única disposición que lo exige es la letra a) del artículo 5º ya visto en el punto anterior. En esta materia cabe repetir nuevamente lo señalado en aquél punto, en atención a que podría eventualmente avistarse un trato diferenciado sólo aplicable al sector privado, salvo que el Estado esté facultado para regirse en sus relaciones patrimoniales con los particulares por tal norma, lo cual desconocemos.

5.3 Tratamiento de los Datos Sensibles

En materia de datos sensibles la Ley paraguaya solamente se refiere a ellos en el artículo 4º el cual dispone que: *"Se prohíbe dar a publicidad o difundir datos sensibles de personas que sean explícitamente individualizadas o individualizables".* El inciso 2º de la norma agrega que: *"Se consideran datos sensibles los referentes a pertenencias raciales o étnicas, preferencias políticas, estado individual de salud, convicciones religiosas, filosóficas o morales; intimidad sexual y, en general, los que fomenten prejuicios y discriminaciones, o afecten la dignidad, la privacidad, la intimidad doméstica y la imagen privada de personas o familias".*

De la disposición anterior se desprende que la prohibición de difusión de tales datos es general y, por lo tanto, afectaría al Estado y a los particulares. Sin embargo, debe recordarse lo dispuesto en el conocido artículo 2º: *"Toda persona tiene derecho a recolectar, almacenar y procesar datos personales para uso estrictamente privado".* Dado que no existe prohibición de almacenar y procesar datos sensibles, entendemos que la regla anterior operaría en este caso, favoreciendo sólo a los particulares o privados más no al Estado, salvo que alguien pudiera predicar de éste un ámbito de derecho a la vida privada, lo cual nos parecería absurdo.

5.4 Derechos de los Titulares de los Datos Personales

En esta materia, podemos señalar que en cuanto al derecho de acceso e información, el artículo 8º dispone que: *"Toda persona podrá acceder a la información y a los datos que sobre sí misma, sobre su cónyuge, sobre personas que acredite se hallen bajo su tutela o curatela, o sobre sus bienes, obren en registros oficiales o privados de carácter público o en entidades que suministren información sobre solvencia económica y situación patrimonial , así como conocer el uso que se haga de los mismos o su finalidad"*. De lo

expuesto, se aprecia que existe una clara omisión de cierta clase de registros, a saber, los privados que no que sean de carácter público y los que no pertenezcan a entidades que suministren información sobre solvencia económica y situación patrimonial de las personas. Lo anterior es concordante con la regla del artículo 2º, que reconoce la libertad de recolección y procesamiento de datos para el uso estrictamente privado. Por lo tanto, en lo relativo al derecho de acceso e información existiría un trato diferenciado, dado que respecto del sector público -representado por los registros o archivos estatales- aquel derecho operaría ampliamente, a diferencia del sector privado o particulares los cuales no podrían ser sujetos pasivos de una acción de hábeas data informativo si la recolección y procesamiento de datos es de uso estrictamente privado.

En lo relativo a los derechos de actualización, modificación o eliminación de datos, cabe señalar que éstos solamente se tratan por la Ley a propósito de los datos sobre la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales, omitiéndose toda referencia respecto de los demás datos personales. En efecto, el artículo 7º de la Ley 1.682 dispone que: *"Serán actualizados permanentemente los datos personales sobre la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales que de acuerdo con esta ley pueden difundirse".* Luego, se agrega que la obligación de actualizar los datos recién mencionados pesa sobre las empresas, personas o entidades que almacenan, procesen y difunden esa información [465] . El inciso 4º por su parte señala que: *"En caso de que los datos personales fuesen erróneos, inexactos, equívocos o incompletos, y así se acredite, el afectado tendrá derecho a que se modifiquen".* Por último, se dispone que: *"La actualización, modificación o eliminación de los datos será absolutamente gratuita, debiendo proporcionarse además, a solicitud del afectado y sin costo alguno, copia auténtica del registro alterado en la parte pertinente".* De todo lo dicho, se desprende que el ejercicio de los derechos constitucionales de actualización, rectificación y destrucción de datos personales (Art. 135 C. Pol.) sólo aparecería regulado legalmente respecto de los datos sobre la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales. Con ello se aprecia claramente una diferenciación injustificada que podría ser atacada de inconstitucional. Sin perjuicio de la diferenciación anterior, estimamos que la operatividad de las garantías constitucionales no puede quedar entregada a la conveniente o inconveniente regulación legislativa, por lo que en ningún caso ellas quedarían sin tutela, en estos casos entendemos que la vía para hacer efectivos esos derechos sería la acción de amparo constitucional.

5.5 Excepciones al Ejercicio de los Derechos de los Titulares de Datos

A lo largo de la normativa de la Ley 1.682, no se aprecian excepciones al ejercicio de los

[465] Se agrega por la Ley que: *"Esta actualización deberá realizarse dentro de los cuatro días siguientes del momento en que llegaren a su conocimiento. Las empresas, personas o entidades que utilizan sus servicios tienen la obligación de suministrar la información pertinente a fin de que los datos que aquellas almacenen, procesen y divulguen, se hallen permanentemente actualizados, para cuyo efecto deberán comunicar dentro de los dos días, la actualización del crédito atrasado que ha generado la inclusión del deudor. (…) Los plazos citados precedentemente empezarán a correr a partir del reclamo realizado par parte del afectado"* (Art. 7 inciso 2º y 3º).

derechos de los titulares, sino más bien un deficiente regulación de la materia, razón por lo cual concluimos que en este punto no existiría un tratamiento diferenciado entre el sector público y el privado.

5.6 Creación y Registro de los Archivos, o Bancos de Datos Personales

En esta materia, nada podemos decir, pues la ley paraguaya no se ha pronunciado al respecto.

5.7 Archivos, Registros o Bancos de Datos Relativos a Encuestas

La única disposición de la Ley 1.682 que hace alusión a la materia es el artículo 3º el cual señala que es lícita la recolección, almacenamiento, procesamiento y publicación de datos o características personales, que se realicen *"con fines científicos, estadísticos, de encuestas y sondeos de la opinión pública o de estudio de mercados, siempre que en las publicaciones no se individualicen las personas o entidades investigadas".* Entendemos que dicha norma es aplicable tanto al sector público como a los particulares.

5.8 Tratamiento Manual o Automatizado de Datos

La ley paraguaya no se refiere expresamente a uno u otro tipo de tratamiento de datos. Sin embargo, de lo señalado por el artículo 1º se desprende que el ámbito de aplicación de la ley alcanzaría tanto al tratamiento manual como automatizado de datos, dado el objeto de la ley: regular en general, el tratamiento de datos personales contenidos en archivos, registros, bancos de datos *"o cualquier otro medio técnico de tratamiento de datos"* públicos o privados destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares. Por lo tanto, de la referencia al tratamiento de datos contenidos en cualquier otro medio técnico, deducimos la amplitud con que el legislador ha querido señalar el ámbito objetivo de aplicación de la ley, el que en nuestro concepto abarcaría a los archivos manuales y con mayor razón a los automatizados.

En definitiva, creemos que el legislador ha incluido tanto al tratamiento de datos manual como automatizado como objeto de regulación a través de la Ley 1.682 y que operaría tanto respecto del sector público como privado sin diferencias de tratamiento.

5.9 Personas Jurídicas como Titulares de Datos

Al respecto la ley paraguaya no se pronuncia, sino que sólo habla de "toda persona" (Art. 8), en lo relativo al derecho de acceso e información. Dado el silencio del legislador, y el ámbito normativo más bien reducido que en verdad presenta la Ley, podría pensarse en principio que sólo serían sujetos de derecho de tal normativa las personas naturales o físicas. Sin embargo, la disposición del artículo 5º nos hace dudar de tal interpretación, pues señala que los datos de "*personas físicas o jurídicas individualizadas"* que revelen, describan o estimen su situación patrimonial, su solvencia económica o el cumplimiento de sus obligaciones comerciales, podrán ser publicados o difundidos solamente: *"a) Cuando esas personas hubiesen otorgado autorización expresa y por escrito para que se obtengan datos sobre el cumplimiento de sus obligaciones no reclamadas judicialmente*

(…)". Obviamente dentro de "esas personas" están las jurídicas, con lo cual parecería absurdo que la Ley por una parte, diera valor al consentimiento de las personas ideales para efectos de aceptar el tratamiento y difusión de sus datos, y al mismo tiempo negarles la calidad de sujetos de derecho. En definitiva, nos inclinamos a pensar que la ley 1.682, a lo menos en lo que se refiere a los datos de carácter comercial o de solvencia patrimonial, habría reconocido como sujetos de los derechos señalados en ésta a las personas jurídicas cuyos datos son objeto de tratamiento manual o automatizado.

En lo que respecta a la determinación de la existencia o no de trato diferenciado en la regulación al sector público y del sector privado en la materia, ella depende en parte de la respuesta a la interrogante acerca de si efectivamente han sido consideradas las personas jurídicas como titulares de datos personales y por ende de los derechos respectivos, cuestión que no está resuelta. En razón de lo anterior, y para efectos de este análisis estimaremos que la materia no está regulada y en consecuencia no cabría hablar de trato diferenciado entre el sector público y el sector privado.

5.10 Transmisión Internacional de Datos Personales

Esta materia no aparece regulada por la Ley 1.682 que reglamenta la información de carácter privado.

6. Modelos de Tutela

El ordenamiento jurídico paraguayo contempla a nivel constitucional la garantía del hábeas data en el artículo 135 pero no la regula. Por su parte, el legislador no ha aportado mayormente a lo prescrito por el Constituyente, pues de las disposiciones de la Ley 1.682 mal podría afirmarse que reglamentan la acción de hábeas data Más bien nada aportan, pues no señala el órgano competente para conocer de la acción, el procedimiento, los plazos ni los recursos. Sólo deducimos de lo señalado por la de la Ley, que el ejercicio de los derechos de los titulares de datos tratados por las empresas de información de crédito, deben ejercerse ante éstas informalmente según lo señalado por el artículo 7º.

Aparte de las reglas recién mencionadas, no tenemos conocimiento de otras normas legales que se ocupen de la tutela de los datos personales, por lo que la protección de éstos queda entregada en principio a la Ley Nº 1.682 la cual presenta serios vacíos, tanto en materia sustantiva como de procedimiento. Con todo, debemos recordar la importante regla del artículo 136 de la Constitución que dispone: *"Ningún magistrado judicial que tenga competencia podrá negarse a entender en las acciones o recursos previstos en los artículos anteriores; si lo hiciese injustificadamente, será enjuiciado y, en su caso, removido".* Entre esos artículos se encuentra el 135 que reconoce la garantía del hábeas data.

6.1 La Acción de Hábeas Data

La acción de hábeas data constitucional se encuentra incompletamente regulada en la Ley Nº 1.682, la cual como se dijo, adolece de un sinnúmero de vacíos tanto en materia

de derecho sustantivo, como en materia procesal. Respecto de los primeros, puede señalarse que la ley sólo se refiere al hábeas data informativo, aditivo y al rectificador relativo a los datos personales sobre la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales, pero nada dice respecto de las demás clases de datos. En cuanto a los vacíos procesales, puede señalarse que la ley no señala el tribunal competente para conocer de las acciones, ni tampoco se remite a algún procedimiento especial u ordinario para su tramitación, no hay plazos ni recursos. Tampoco se señalan aspectos básicos como los efectos de las sentencias de hábeas data. A continuación analizaremos la acción de hábeas data teniendo presentes las limitaciones que a esta tarea se plantean.

6.1.1) Procedencia de la Acción

El artículo 135 de la Constitución consagra el hábeas data como una acción encaminada a: 1) Acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad y, 2) Solicitar la actualización, la rectificación o la destrucción de los datos personales que fueren erróneos o afectaran ilegítimamente los derechos de las personas.

Por su parte la Ley Nº 1.682 en su artículo 8º, se refiere al hábeas data informativo de la siguiente manera: *"toda persona podrá acceder a la información y a los datos que sobre sí misma, sobre su cónyuge, sobre personas que acredite se hallen bajo su tutela o curatela, o sobre sus bienes, obren en registros oficiales o privados de carácter público o en entidades que suministren información sobre solvencia económica y situación patrimonial, así como conocer el uso que se haga de los mismos o su finalidad".*

En cuanto al hábeas data rectificador, aditivo y cancelatorio, el artículo 7º (refiriéndose a los datos personales sobre la situación patrimonial, solvencia económica y el cumplimiento de obligaciones comerciales), señala que, *"en caso de que los datos personales fuesen erróneos, inexactos, equívocos o incompletos, y así se acredite, el afectado tendrá derecho a que se modifiquen.* Agrega que la actualización, modificación o eliminación de los datos será absolutamente gratuita, debiendo proporcionarse además, a solicitud del afectado y sin costo alguno, copia auténtica del registro alterado en la parte pertinente.

De lo recién señalado se concluye que el legislador, extrañamente ha omitido el hábeas data aditivo, el rectificador y el cancelatorio o exclutorio respecto de los datos personales que no se refieran a la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales. Estimamos que tal omisión es jurídicamente intolerable en una ley que pretende regular generalmente el instituto del hábeas data, más aún si desconoce lo preceptuado por el propio Constituyente. Sin embargo, de la falta de ley al respecto no podría seguirse la indefensión del titular de los datos, en atención a que la propia Constitución señala que: *"la falta de ley reglamentaria no podrá ser invocada para negar ni para menoscabar algún derecho o garantía"* (Art. 45 C. Pol.). Por otra parte, el artículo 136 obliga a los jueces a resolver las acciones de hábeas data so pena de enjuiciarlos y removerlos. En suma, estimamos que aunque el legislador haya

regulado defectuosamente el hábeas data, los tribunales competentes tienen el deber de resolver las esas acciones, pues están obligados constitucionalmente por los preceptos de los artículos 45 y 136.

6.1.2) Legitimación Activa

En base a lo dispuesto en el artículo 135 de la Constitución, que habla de *"toda persona"*, se ha entendido en el Paraguay que estarían legitimados activamente para ejercer la acción de hábeas data, tanto las personas físicas o naturales como las personas jurídicas. En este sentido se pronuncia tanto la jurisprudencia como la doctrina [466] . La Corte ha señalado que "está legitimada para promover la acción cualquier persona física o jurídica, afectada por la existencia de datos que pudieran ser erróneos o falsos o indebidamente difundidos" [467] .

En el ámbito legal, se señala por el artículo 7º que respecto de los datos personales sobre la situación patrimonial, solvencia económica y el cumplimiento de obligaciones comerciales *"en caso de que los datos personales fuesen erróneos, inexactos, equívocos o incompletos, y así se acredite, el afectado tendrá derecho a que se modifiquen".* En este caso sólo se refiere al sujeto activo como el *"afectado".* En cuanto al hábeas data informativo, el artículo 8º habla de *"toda persona"*.

6.1.3) Legitimación Pasiva

Respecto del sujeto pasivo del hábeas data, la Constitución señala que se ejercerá en contra de los *"registros oficiales o privados de carácter público"* que contengan información y datos sobre el sujeto activo, o sobre sus bienes (Art. 145). Lo anterior debe matizarse, y entenderse que la acción se dirige en contra de los responsables de esas clases de archivos o registros.

La ley por su parte, respecto del hábeas data informativo señala en el artículo 8º que ésta procederá en contra de los *"registros oficiales o privados de carácter público o en entidades que suministren información sobre solvencia económica y situación patrimonial".* En cuanto al hábeas data aditivo y rectificador de los datos personales sobre la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales, la ley no se pronuncia en la materia, por lo que estimamos debería aplicarse por analogía la regla legal del artículo 8º o bien directamente la Constitución.

6.1.4) Competencia

En materia de competencia, ni la Constitución ni la ley se refieren a ella.

6.1.5) Procedimiento Aplicable

Tampoco se han pronunciado respecto del procedimiento al que se somete la acción de

466 Puccinelli, *op cit*., pág. 557.

467 *Ibídem*.

hábeas data, la Constitución y la Ley. A pesar de ello, ha sido la doctrina y jurisprudencia las que han dado ciertas pautas en la materia. Por la doctrina, Benítez ha señalado que "el procedimiento que corresponde utilizar debe ser simplificado, y dividirse en dos etapas: en la primera se debe acreditar la existencia y carácter del registro y compulsar los datos, y en la segunda se deben contrastar tales datos con lo manifestado por el sujeto activo, y disponer sobre la procedencia o no de las operaciones solicitadas por éste" [468] . Agrega este autor que "necesariamente, a los efectos de la observancia de las reglas del debido proceso legal, en esta etapa debe observarse el Principio de Bilateralidad, dado que en caso contrario se libraría al arbitrio de cualquiera, asentar en registros públicos cualquier dato que pudiera resultar inexacto y con ello originar perjuicio a terceros". Luego, en función de las etapas ya señaladas el juez debe "(…) adoptar una decisión que solamente puede tener como contenido: a) no hacer lugar a la petición porque los datos son correctos; b) disponer, en su caso, la corrección de los datos asentados en el registro, ante la constatación del error existente; y c) disponer la destrucción de lo que estuviere indebidamente asentado en el registro, supuesto que tales datos, aparte de erróneos, afecten ilegítimamente los derechos del recurrente" [469] .

La opinión de la jurisprudencia,-citada por Puccinelli- es igual a la sostenida por Benítez, por lo que no repetiremos el mismo proceso [470] .

De las opiniones anotadas, se desprende la idea relativa a que debe existir una excesiva cautela en cuanto al estudio por los jueces de los antecedentes que fundamentan el hábeas data. Entendemos por nuestra parte, que tal cautela no se justifica si de las peticiones puede deducirse que la información requerida no está afecta a régimen especial de reserva o secreto, pues quien acciona de hábeas data es el titular de los datos, a quien le asiste constitucionalmente todo el derecho de saber quién posee sus datos, para qué fines, a quién se los transmite, etc. No vemos la aprehensión por cautelar tanto los derechos de los responsables de los archivos, registros o bancos de datos. Estimamos que en la tramitación de las acciones, basta que se presente un pedido de hábeas data para que sin más se solicite informe al demandado y, con esos antecedentes en mano se tomen decisiones al respecto. Seguir la postura de la doctrina y de la jurisprudencia paraguaya implica entrabar el ejercicio del hábeas data injustificadamente, pues son los derechos de los titulares de los datos los que especialmente se tutelan por la normativa constitucional.

6.1.6) La Sentencia

Nada dice la Ley respecto de los requisitos y efectos de las sentencias de hábeas data.

6.2 Otras Acciones

468 Citado por Puccinelli, *op cit.,* pág. 559.

469 Benítez, Luis María, *op cit.*, pág. 114.

470 Puccinelli, *op. cit.*, págs. 559 y 560.

En lo relativo a otras acciones que puedan tutelar los derechos que están tras la protección de los datos personales, creemos que dado el carácter de garantía que le otorga la Constitución al hábeas data, sólo sería procedente aplicar el procedimiento de amparo constitucional de manera excepcional [471] . Lo anterior, debe entenderse sin perjuicio de la obligación de los jueces de conocer y fallar siempre estas acciones, tal como lo manda el artículo 136 constitucional

7. Mecanismos de Control

La legislación paraguaya que regula la información privada, no prevé la creación de un organismo de control que vele por el respeto y cumplimiento de la legislación de protección de los datos personales.

8. Transmisión Internacional de Datos

Respecto de la transmisión internacional de datos personales, la Ley Nº 1.682 no se pronuncia.

9. Régimen de Responsabilidad

La ley paraguaya que regula la información privada si bien establece algunas sanciones, el carácter de ellas es dudoso, entre otras razones porque no se señala el tribunal ante el cual debe interponerse la acción de hábeas data, ni el procedimiento aplicable. Con todo, creemos que la sanción tendría naturaleza administrativa y no civil (ni menos penal), en razón de la configuración de éstas por la ley, las cuales sólo consisten en multas. Consecuente con lo que hemos venido afirmando en relación al carácter de la Ley, debemos señalar que, en general, las sanciones están pensadas para ser aplicadas a los responsables de los bancos de datos o registros de datos personales de carácter comercial. Por último, existen algunas reglas establecidas en otros cuerpos normativos de carácter sectorial que, comúnmente, prevén sanciones administrativas, sin perjuicio de la responsabilidad civil y criminal correspondiente.

[471] Respecto al procedimiento de amparo, cabe señalar que no lo analizaremos dada la configuración de garantía constitucional que tiene el hábeas data, el cual debería ser amparado por cualquier tribunal de la República con competencia constitucional. Con todo, se reproducirá el texto constitucional que lo consagra: Artículo 134 - Del Amparo. “Toda persona que por un acto u omisión, manifiestamente ilegítimo, de una autoridad o de un particular, se considere lesionada gravemente, o en peligro inminente de serlo en derechos o garantías consagradas en esta Constitución o en la ley, y que debido a la urgencia del caso no pudiera remediarse por la vía ordinaria, puede promover amparo ante el magistrado competente. el procedimiento será breve, sumario, gratuito, y de acción popular para los casos previstos en la ley. El magistrado tendrá facultad para salvaguardar el derecho o garantía, o para restablecer inmediatamente la situación jurídica infringida. Si se tratara de una cuestión electoral, o relativa a organizaciones políticas, será competente la justicia electoral. El Amparo no podrá promoverse en la tramitación de causas judiciales, ni contra actos de órganos judiciales, ni en el proceso de formación, sanción y promulgación de las leyes. La ley reglamentará el respectivo procedimiento. Las sentencias recaídas en el Amparo no causarán estado”.

9.1 Responsabilidad Administrativa

Dentro de éste ámbito nos referiremos a las sanciones establecidas por las leyes analizadas en el punto Nº 2.2 de este estudio particular.

9.1.1) Ley que Regula la Información Privada (Ley Nº 1.682)

El artículo 10 de esta Ley señala que se sancionarán las siguientes conductas:

a) La publicación o distribución de información, sea por personas físicas o jurídicas, sobre la situación patrimonial, solvencia económica o cumplimiento de obligaciones comerciales y financieras, que viole las disposiciones de la Ley 1.682. En estos casos, *"serán sancionadas con multas que oscilarán, de acuerdo con las circunstancias del caso, entre cincuenta y cien jornales mínimos para actividades laborales diversas no especificadas, multas que se duplicarán, triplicarán, cuadruplicarán y así sucesivamente por cada reincidencia del mismo afectado"* [472] .

b) Cuando las personas físicas o jurídicas que, pese a estar obligadas a rectificar o a suministrar información sobre la situación patrimonial, solvencia económica o cumplimiento de obligaciones comerciales y financieras, no lo hagan o lo hagan fuera de los plazos señalados en el artículo 7º. En estos eventos, *"serán sancionadas con multas que, de acuerdo con las circunstancias del caso, oscilarán entre cincuenta y cien jornales mínimos para actividades laborales diversas no especificadas, multas que, cada caso de reincidencia, serán aumentadas de acuerdo con la pauta establecida en el apartado a)"* [473] .

c) Cuando los reclamos extrajudiciales a los que se refiere el artículo 8º (derecho de acceso e información) no fueran atendidos sin razón o sin base legal. En estos casos, *"se aplicará a la entidad reacia al cumplimiento de sus obligaciones, una multa que, de acuerdo con las circunstancias del caso, oscilará entre cien y doscientos jornales mínimos para actividades laborales diversas no especificadas".*

9.1.2) Ley que establece el Nuevo Régimen Tributario (Ley Nº 125/91)

La Ley 125 de 1991, dispone en el inciso 2º del artículo 190, titulado "Secreto de las actuaciones", que los funcionarios de la administración tributaria *"(…) no podrán, bajo pena de destitución y sin perjuicio de su responsabilidad personal, civil y o penal, divulgar a terceros en forma alguna datos contenidos (…)"* en las declaraciones impositivas.Luego agrega que: "*el mismo deber de reserva pesará sobre quienes no perteneciendo a la Administración Tributaria, realicen para ésta trabajos o procesamientos automáticos de*

[472] Se agrega luego que: *"para que se produzca la multa, la duplicación, triplicación, cuadruplicación, etc. Se requerirá que la entidad reacia al cumplimento de la actualización dentro del plazo establecido en el Artíc. 7 de esta Ley, haya recibido el previo reclamo por escrito del particular afectado"* (Artículo 10 letra a).

[473] Se agrega por la ley que: *"para que se produzca la multa, duplicación, triplicación, cuadruplicación, etc, se requerirá que la entidad reacia al cumplimiento de la actualización dentro del plazo establecido en el Art. 7 de esta Ley, haya recibido el previo reclamo por escrito del particular afectado*"(Artículo 10 letra b).

datos u otras labores que importan el manejo de material reservado de la administración tributaria".

9.1.3) Ley General de Bancos, Financieras y Otras Entidades de Crédito

El artículo 88 de esta ley intitulado "Sanciones por incumplimiento" dispone que: *"La infracción a las disposiciones de este capítulo por parte de las personas comprendidas en el deber de secreto se considerará falta grave a los efectos laborales y disciplinarios sin perjuicio de las responsabilidades penales establecidas por las leyes".*

9.2 Responsabilidad Civil

En materia de responsabilidad civil, la Ley 1.682 no prevé reglas especiales. Tampoco se refiere genéricamente a una eventual acción indemnizatoria por los perjuicios causados a consecuencia de la violación de las normas legales. En razón de lo anterior, entendemos que a falta de normativa especial deberían aplicarse las reglas generales que establecen la responsabilidad civil por daños. Al efecto, el artículo 1.833 del Código Civil paraguayo prescribe: *"El que comete un acto ilícito queda obligado a resarcir el daño. Si no mediare culpa, se debe igualmente indemnización en los casos previstos por la ley, directa o indirectamente"* [474] .

En lo relativo a la responsabilidad civil del Estado, cabe señalar la regla del artículo 39 de la Constitución, la cual dispone que: *"Toda persona tiene derecho a ser indemnizada justa y adecuadamente por los daños o perjuicios de que fuere objeto por parte del Estado. La ley reglamentará este derecho".*

9.3 Responsabilidad Penal

La Ley 1.682 no contempla sanciones penales para el caso de violaciones a las reglas que ésta establece. En razón de lo anterior, sólo revisaremos las disposiciones penales que guardan relación con algunos de los bienes jurídicos generalmente reconocidos como tutelados por el derecho a la protección de datos o hábeas data, es decir, aquéllos delitos que atentan en contra de la intimidad y la vida privada. Al respecto, el Código Penal paraguayo contempla en el Libro II, Título I un Capítulo VII intitulado "Hechos punibles contra el ámbito de vida y la intimidad de la persona". Dentro de éste, se contemplan diversos delitos que pasamos a señalar [475] .

a) Violación de domicilio:

Artículo 141.- *"1º El que: 1. entrara en una morada, local comercial, despacho oficial u otro ámbito cerrado, sin que el consentimiento del que tiene derecho de admisión haya sido declarado expresamente o sea deducible de las circunstancias; o 2. no se alejara de*

[474] Esta materia se encuentra regulada en los artículos 1.833 y siguientes del Código Civil. [En línea] < http://comunidad.derecho.org/desvars/cc.html > [consulta: 31 de Marzo 2003].

[475] [En línea] < http://www.itacom.com.py/ministerio_publico/codigo_penal/index.html > [consulta: 1 de Abril 2003].

dichos lugares a pesar del requerimiento del que tiene derecho a excluirlo, será castigado con pena privativa de libertad de hasta dos años o con multa.

2º Cuando el autor actuara conjuntamente con otra persona, abusando gravemente de su función pública o con empleo de armas o violencia, la pena será privativa de libertad de hasta cinco años o multa.

3º La persecución penal dependerá de la instancia de la víctima".

b) Invasión de inmueble ajeno:

Artículo 142.- *"El que individualmente o en concierto con otras personas y sin consentimiento del titular ingresara con violencia o clandestinidad a un inmueble ajeno y se instalara en él, será castigado con pena privativa de libertad de hasta dos años o con multa".*

c) Lesión de la intimidad de la persona:

Artículo 143.-*"1º El que, ante una multitud o mediante publicación en los términos del artículo 14, inciso 3º, expusiera la intimidad de otro, entendiéndose como tal la esfera personal íntima de su vida y especialmente su vida familiar o sexual o su estado de salud, será castigado con pena de multa* [476] *.*

2º Cuando por su forma o contenido, la declaración no exceda los límites de una crítica racional, ella quedará exenta de pena.

3º Cuando la declaración, sopesando los intereses involucrados y el deber de comprobación que según las circunstancias incumba al autor, sea un medio adecuado para la persecución de legítimos intereses públicos o privados, ella quedará exenta de pena.

4º La prueba de la verdad de la declaración será admitida sólo cuando de ella dependiera la aplicación de los incisos 2º y 3º".

Este artículo establece una disposición muy importante en el numeral 1º, el cual tutela directamente la intimidad de las personas cuando de éstas se ha predicado públicamente, entre otras, su vida sexual o salud. Lo anterior, queda reafirmado en el numeral 4º al señalar la ley que no opera la *exceptio veritatis*, por lo que la lesión al bien jurídico es independiente a la veracidad de la publicación o divulgación. En suma, vemos en esta disposición una tutela directa a la intimidad, cuya esfera se entiende que abarcaría entre otras, la vida sexual y los estados de salud, es decir, los datos sensibles, con lo que eventualmente podría aplicarse este artículo ante un tratamiento o transmisión que haga público datos sensibles, siempre y cuando se reúnan todos los elementos del tipo. Con ello se reafirma lo dispuesto en el artículo 4º de la Ley 1.682 que dispone: *"Se prohíbe dar a publicidad o difundir datos sensibles de personas que sean explícitamente individualizadas o individualizables".*

[476] El artículo 14 inciso 3º señala que: *"Como publicación se entenderán, en las disposiciones que se remitan a este concepto, los escritos, cintas portadoras de sonido o imágenes, reproducciones y demás medios de registro".*

d) Lesión del derecho a la comunicación y a la imagen:

Artículo 144.- *"1º El que sin consentimiento del afectado: 1. Escuchara mediante instrumentos técnicos; 2. Grabara o almacenara técnicamente; o 3. Hiciera, mediante instalaciones técnicas, inmediatamente accesible a un tercero, la palabra de otro, no destinada al conocimiento del autor y no públicamente dicha, será castigado con pena privativa de libertad de hasta dos años o con multa.*

2º La misma pena se aplicará a quien, sin consentimiento del afectado, produjera o transmitiera imágenes: 1. De otra persona dentro de su recinto privado; 2. Del recinto privado ajeno; 3. De otra persona fuera de su recinto, violando su derecho al respeto del ámbito de su vida íntima.

3º La misma pena se aplicará a quien hiciera accesible a un tercero una grabación o reproducción realizada conforme a los incisos 1º y 2º.

4º En los casos señalados en los incisos 1º y 2º será castigada también la tentativa.

5º La persecución penal del hecho dependerá de la instancia de la víctima, salvo que el interés público requiera una persecución de oficio. Si la víctima muriera antes del vencimiento del plazo para la instancia sin haber renunciado a su derecho de interponerla, éste pasará a sus parientes".

e) Violación de la confidencialidad de la palabra:

Artículo 145.- *"1º El que sin consentimiento del afectado: 1. Grabara o almacenara técnicamente; o 2. Hiciera inmediatamente accesibles a un tercero, mediante instalaciones técnicas, la palabra de otro destinada a su conocimiento confidencial, será castigado con multa.*

2º La misma pena se aplicará a quien hiciera accesible a un tercero una grabación o reproducción realizada conforme al inciso anterior".

f) Violación del secreto de la comunicación:

Artículo 146.- "*1º El que, sin consentimiento del titular: 1. Abriera una carta cerrada no destinada a su conocimiento; 2. Abriera una publicación, en los términos del artículo 14, inciso 3º, que se encontrara cerrada o depositada en un recipiente cerrado destinado especialmente a guardar de su conocimiento dicha publicación, o que procurara, para sí o para un tercero, el conocimiento del contenido de la publicación; 3. Lograra mediante medios técnicos, sin apertura del cierre, conocimiento del contenido de tal publicación para sí o para un tercero, será castigado con pena privativa de libertad de hasta un año o con multa.*

2º La persecución penal dependerá de la instancia de la víctima. Se aplicará lo dispuesto en el artículo 144, inciso 5º, última parte".

g) Revelación de un secreto de carácter privado:

Artículo 147.- *"1º El que revelara un secreto ajeno: 1. Llegado a su conocimiento en su*

actuación como, a) Médico, dentista o farmacéutico; b) Abogado, notario o escribano público, defensor en causas penales, auditor o asesor de Hacienda; c) Ayudante profesional de los mencionados anteriormente o persona formándose con ellos en la profesión; o 2. Respecto del cual le incumbe por ley o en base a una ley una obligación de guardar silencio, será castigado con pena privativa de libertad de hasta un año o con multa.

2º La misma pena se aplicará a quien divulgue un secreto que haya logrado por herencia de una persona obligada conforme al inciso anterior.

3º Cuando el secreto sea de carácter industrial o empresarial, la pena privativa de libertad podrá ser aumentada hasta tres años. Será castigada también la tentativa.

4º La persecución penal del hecho dependerá de la instancia de la víctima. Se aplicará lo dispuesto en el artículo 145, inciso 5º, última parte.

5º Como secreto se entenderá cualquier hecho, dato o conocimiento: 1. De acceso restringido cuya divulgación a terceros lesionaría, por sus consecuencias nocivas, intereses legítimos del interesado; o 2. Respecto de los cuales por ley o en base a una ley, debe guardarse silencio".

h) Revelación de secretos privados por funcionarios o personas con obligación especial:

Artículo 148.-*"1º El que revelara un secreto ajeno llegado a su conocimiento en su actuación como: 1. Funcionario conforme al artículo 14, inciso 1º, numeral 2; o 2. Perito formalmente designado, será castigado con pena privativa de libertad de hasta tres años o con multa.*

2º La persecución penal del hecho dependerá de la instancia de la víctima. Se aplicará lo dispuesto en el artículo 144, inciso 5º, última parte".

10. Conclusiones

El ordenamiento jurídico paraguayo contempla expresamente en la Constitución la garantía del hábeas data, la cual se traduce en una acción que sólo puede tener como sujetos pasivos a los responsables de los registros, archivos o bancos de datos de carácter oficiales o de los privados de carácter público. De lo anterior, se sigue que se excluyen como sujetos pasivos de la acción a los responsables de registros o bancos de datos personales de carácter privado que no tengan el carácter de públicos. Dada esa configuración del hábeas data, hemos estimado que el Constituyente paraguayo ha reconocido un derecho a la protección de datos limitado.

En el ámbito infraconstitucional, puede señalarse que desde el año 2000 Paraguay cuenta con la Ley Nº 1682, la cual fue modificada en el año 2002. Este cuerpo normativo, si bien pareciera en principio regular el tratamiento de los datos personales tanto para el sector público como para el privado, del análisis de sus disposiciones se desprende otra cosa; más bien la ley paraguaya estaría pensada y dirigida a regular el mercado de la información crediticia. Esta ley presenta graves vacíos tanto en materia sustantiva como

procedimental, los que ni siquiera permiten saber ante quién interponer la acción de hábeas data, ni qué procedimiento debe seguirse. En suma, puede señalarse que aún queda bastante por hacer en materia de protección de los datos personales en Paraguay a pesar de contar con una garantía constitucional denominada expresamente "Hábeas Data".

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN PERÚ

1. Generalidades

El ordenamiento jurídico peruano dispone a nivel constitucional de normas que reconocen el derecho de toda persona al acceso a la información pública, así como el derecho a que los servicios informatizados no suministren informaciones que afecten la intimidad personal y familiar. Para la tutela de tales derechos, el Constituyente peruano ha consagrado la garantía del hábeas data, circunscrito específicamente a los derechos recién señalados. De lo anterior, resulta un hábeas data o derecho a la protección de datos limitado, el cual no incluye todos los derechos que generalmente se le reconocen a éste. A pesar de la estrechez de la configuración constitucional ya señalada, el legislador ha desarrollado y ampliado el hábeas data en un ámbito específico y delimitado, cual es, el mercado de la información crediticia, avance que no ha logrado concretarse en una ley general de protección de datos personales. Por otra parte, la regulación de la tramitación del hábeas data constitucional ha quedado en manos de una ley del año 1994 que regula transitoria y escuetamente la garantía constitucional del artículo 200 Nº 3 de la Constitución.

2. Niveles de protección Jurídica a los Datos Personales

2.1 Protección Constitucional

La Constitución peruana de 1993 [477] , dentro del Título V denominado "De las Garantías Constitucionales", señala en el artículo 200 que son garantías constitucionales: *"(…) 3. La Acción de Hábeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el Artículo 2º, incisos 5 y 6 de la Constitución".* Añadiendo que: *"una ley orgánica regulará el ejercicio de estas garantías y los efectos de la declaración de inconstitucionalidad o ilegalidad de las normas".*

Por su parte, el artículo 2º, insertado dentro del Capítulo "De los derechos

[477] [En línea] < http://www.georgetown.edu/pdba/Constitutions/Peru/per93.html > [consulta: 11 de Diciembre 2002].

fundamentales" dispone que toda persona tiene derecho: *"(…) 5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. (…) El secreto bancario y la reserva tributaria pueden levantarse a pedido del Juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado. (…) 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar".*

Las disposiciones anteriores configuran el actual sistema constitucional del hábeas data peruano. Se dice actual, dado que hasta el año 1995 el artículo 200 no sólo hacía referencia a los derechos señalados en los numerales 5 y 6 del artículo 2º, sino que también se remitía al numeral 7, el cual dispone que toda persona tiene derecho: *"(…) 7. Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias. (…) Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley".*

La modificación constitucional que eliminó la referencia del hábeas data a los derechos señalados en el número 7 del artículo 2º de la Constitución, tiene como antecedente la incesante crítica hecha a la disposición por los gremios periodísticos. En síntesis, éstos señalaban que al incluirse el numeral 7 en la garantía del hábeas data, el Constituyente estaba dando pie a que los jueces y Tribunales admitieran la acción de hábeas datapara ejercer el derecho de rectificación, institución del todo diversa, con lo cual se afectaría la libertad de prensa, estableciéndose un medio solapado de censura [478] .

La doctrina por su parte, también se pronunció en contra de la disposición constitucional que incluía el numeral 7 del artículo 2º. García Belaúnde, sostuvo que además de innecesaria la inclusión del hábeas data a nivel constitucional (pues bastaba con una adecuada reglamentación del amparo), aparecía como inconveniente el haber incluido dentro del campo de acción del hábeas data el derecho al honor, a la buena reputación, a la intimidad personal y familiar, y a la voz e imagen propia, con lo cual podría producirse un peligroso conflicto que redundaría en una censura previa. Por otro lado, la referencia al derecho a rectificación en cualquier medio de comunicación social, por informaciones inexactas que afecten a las personas, nada tenía que ver con la etimología ni con el contenido teórico de la acción de hábeas data [479] . Por lo tanto, la actual configuración constitucional del hábeas data o derecho a la protección de datos, está dada por el texto del artículo 200 reformado por la Ley Nº 26.470, la cual suprimió la remisión hecha al artículo 2º número 7 de la Constitución.

Se ha señalado por la doctrina, en relación a la versión actual del hábeas data, que la norma del artículo 200 incluye dos variantes diferenciadas de esta acción; la primera,

[478] Puccinelli, Óscar, *op. cit.*,págs. 573 y 574.

[479] Citado por Puccinelli, *op, cit.*, págs. 574 y 575.

destinada a brindar protección frente al tratamiento de datos personales y, la segunda, establecida para recabar información pública [480] . Al respecto, Eguiguren ha dicho que si bien ha sido positiva la consagración constitucional de los derechos ya enunciados, la regulación ha incurrido en serias deficiencias que limitan el alcance de los derechos que se otorgan frente a la actividad de los servicios informáticos, en particular los derechos de conocer, actualizar, o rectificar los datos almacenados en éstos, así como también para suprimir del registro los datos personales sensibles [481] . Agrega este autor, que respecto del derecho a solicitar información de las entidades públicas (Art. 2º inciso 5º C. Pol.), la Constitución introduce una novedad peculiar en este campo, pues según la experiencia comparada predominante, el hábeas data es un remedio procesal pensado para proteger la intimidad personal y ciertos datos sensibles que pueden verse afectados por su registro o difusión a través de servicios informáticos o bancos de datos de acceso o consulta pública. La novedad radica entonces, en que "se trata de información en general a cargo de entidades públicas, sin establecer ninguna conexión o condición que la refiera a información existente en bancos de datos o servicios informáticos; también en que el interés principal protegido no es el resguardo de la intimidad personal o de la privacidad". Luego, el derecho cautelado en verdad por esa norma corresponde a la "libertad de acceso y conocimiento de la información, pública, destinado a favorecer la mayor y mejor participación e información general de los ciudadanos, así como la transparencia de la actuación y gestión de las entidades gubernamentales" [482] .

En relación a lo señalado por Eguiguren, concordamos plenamente en su apreciación, ya que el acceso a la información pública se aleja del fin propio del hábeas data, cual es el ejercer un control sobre el uso y disposición de la propia información personal, lo que se diferencia conceptualmente de un instituto cuya finalidad está encaminada a controlar la transparencia de las actuaciones y gestiones públicas.

Respecto de la segunda variante del hábeas data peruano, es decir, el derecho de toda persona aque "*los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar"*, Eguiguren afirma que éste sería el ámbito más propio y aceptado de aplicación del hábeas data, pero critica a la vez que el precepto constitucional se limite únicamente a "prohibir que los servicios informáticos suministren informaciones o datos que puedan afectar la intimidad personal o familiar", con lo cual se dejan fuera de la norma todos los otros aspectos típicos del derecho a la autodeterminación informativa y a la protección del hábeas data. Lo anterior, revelaría una lamentable ignorancia y ligereza, "pues si el constituyente recogió el Hábeas data de otras experiencias, cuando menos debió hacerlo en forma

480 Puccinelli, *op cit*., pág. 578.

481 Citado por Puccinelli, *op cit*, pág. 579.

482 Agrega este autor que: "en todo caso, si bien esta extensión del Hábeas data a la protección del derecho referido se aparta de los cánones más ortodoxos y difundidos del instituto (por lo que podría ser objetado por cierta falta de coherencia o 'pureza' conceptual) es verdad también que ello no ofrece mayores problemas o perjuicios que ameriten un severo cuestionamiento". Todo lo anterior en Eguiguren Praeli, Francisco J.: *"El Hábeas Data y su Desarrollo en el Perú"*, Revista Ius et Praxis, Universidad de Talca, año 3 Nº 1, Talca, 1997, págs. 125 y 126.

completa e integral. Nótese que al momento de elaborarse la Constitución Peruana ya se encontraban vigentes, para no ir más lejos, las constituciones de Brasil y Paraguay, que regulan este instituto con notoria superioridad en calidad con respecto a nuestra Carta" [483] .

Luego de haber reseñado la configuración actual del hábeas data constitucional, revisaremos otras normas constitucionales que tutelan bienes jurídicos relacionados con la protección de los datos personales. Dentro de éstas podemos mencionar al ya señalado artículo 2º, el cual consagra en otros numerales, la inviolabilidad del domicilio, inviolabilidad de las comunicaciones privadas y, la inviolabilidad de las creencias y del secreto profesional señalando que, toda persona tiene derecho:

"(…) 9. A la *inviolabilidad del domicilio. Nadie puede ingresar en él ni efectuar investigaciones o registros sin autorización de la persona que lo habita o sin mandato judicial, salvo flagrante delito o muy grave peligro de su perpetración. Las excepciones por motivos de sanidad o de grave riesgo son reguladas por la ley".*

"10. Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados. (…) Las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del Juez, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen". A continuación, se agrega que: *"los documentos privados obtenidos con violación de este precepto no tienen efecto legal"*. Por último, se añade que: *"los libros, comprobantes y documentos contables y administrativos están sujetos a inspección o fiscalización de la autoridad competente, de conformidad con la ley. Las acciones que al respecto se tomen no pueden incluir su sustracción o incautación, salvo por orden judicial".*

Más adelante el numeral 18 del artículo 2º señala que toda persona tiene derecho: *"a mantener reserva sobre sus convicciones políticas, filosóficas, religiosas o de cualquiera otra índole, así como a guardar el secreto profesional".*

Finalmente, existe una norma que viene a completar el sistema de protección a los derechos humanos y que, sin duda, debe tenerse siempre presente al interpretar tanto las normas constitucionales como las infraconstitucionales. Al efecto, el artículo 3º dispone que: *"la enumeración de los derechos establecidos en este capítulo no excluye los demás que la Constitución garantiza, ni otros de naturaleza análoga o que se fundan en la dignidad del hombre, o en los principios de soberanía del pueblo, del Estado democrático de derecho y de la forma republicana de gobierno".*

En relación con la disposición anterior, es pertinente señalar que el Estado peruano ha suscrito y ratificado la Convención Americana sobre Derechos Humanos por lo cual las normas de ésta deben tenerse particularmente presentes no sólo a la hora de resolver conflictos entre partes, sino también a la hora de legislar [484] .

[483] *Ídem*, pág. 127.

[484] La ratificación del Pacto de San José de Costa Rica se efectuó el 28 de Julio de 1978. [En línea] < http://www.oas.org/juridico/spanish/firmas/b-32.html > [consulta: 20 de Marzo 2003].

En suma, puede afirmarse que el ordenamiento jurídico constitucional peruano si bien dispone de una norma que consagra la garantía del hábeas data, ésta aparece como insuficiente para proteger de manera adecuada los derechos que comúnmente está llamada a tutelar, pues concibe de manera muy limitada el derecho a la protección de datos. A pesar de lo anterior, puede intentarse una interpretación extensiva de los derechos que protege basado no sólo en el instituto en comento, sino haciendo referencia a las normas sobre derechos humanos que tutelan la libertad y dignidad de la persona.

2.2 Protección Legal de los Datos Personales

Perú no cuenta con una ley general de protección de datos personales que desarrolle lo preceptuado por el Constituyente en la materia. Sin embargo, debemos señalar que el legislador sí se ha ocupado de manera parcial de regular ciertos aspectos de la protección de datos, tanto de manera procedimental como sustantiva sectorial; procesalmente, a través de la Ley Nº 26.301 sobre Aplicación de la Acción Constitucional de Hábeas Data, la cual tiene carácter transitorio en tanto no se dicte la ley orgánica sobre tramitación del hábeas data, y sustantivamente, a través de la Ley Nº 27.489 que regula las Centrales Privadas de Información de Riesgos y de Protección al Titular de la Información. Debemos añadir finalmente, un tercer cuerpo legal que regula tanto sustantiva como procesalmente el derecho de acceso a la información pública, esta es la Ley de Transparencia y Acceso a la Información Pública Nº 27.806. De todos estos estatutos, sólo la Ley 26.301 se ocupa del procedimiento judicial de hábeas data. Las dos leyes restantes, sólo establecen procedimientos administrativos o informales para hacer valer los derechos de los titulares. A la vez, esos procedimientos han sido establecidos como vías previas que deben necesariamente agotarse, para que sea procedente el ejercicio ante la judicatura de la acción de hábeas data regulada parcialmente por la señalada Ley 26.301, cuyos vacíos deberían ser salvados por las disposiciones pertinentes establecidas en la Ley de Amparo.

Por otra parte, puede señalarse que existen ciertas disposiciones sectoriales que establecen deberes de confidencialidad de cierta información de terceros. Tales normas se encuentran tanto en la legislación tributaria, bancaria, así como en la Ley General de la Persona con Discapacidad. Por ultimo, debemos anotar que existe un estatuto legal que otorga facultades a los Fiscales del Ministerio Público peruano para la intervención y control de comunicaciones y documentos privados en casos excepcionales (Ley Nº 27.697).

En lo relativo a propuestas legislativas de regulación en la materia, cabe señalar que existe, al menos, un Proyecto de Ley sobre la Privacidad de los Datos Informáticos y la Creación del Comisionado para la Protección de la Privacidad el cual se encuentra actualmente en tramitación en el Congreso peruano [485] . A continuación pasaremos a examinar las disposiciones ya reseñadas en materia de protección de datos personales.

2.2.1) Ley que Regula las Centrales Privadas de Información de Riesgos y de

[485] Este Proyecto de Ley es el Nº 5233 y fue presentado el 23 de Septiembre de 1999. Su texto puede consultarse [en línea] < http://200.37.159.7/pley/pley1995_2000.htm > [consulta: 21 de Enero 2003].

Protección al Titular de la Información (Ley Nº 27.489) [486]

La Ley que regula las Centrales Privadas de Información de Riesgos y de Protección al Titular de la Información del año 2001 (en adelante Ley de CEPIRS), tiene por objeto: *"regular el suministro de información de riesgos en el mercado, garantizando el respeto a los derechos de los titulares de la misma, reconocidos por la Constitución Política del Perú y la legislación vigente, promoviendo la veracidad, confidencialidad y uso apropiado de dicha información"* (Art. 1º). Es decir, esta normativa regula el mercado de la información crediticia, la cual se entrega o se transmite a los usuarios, a través de los denominados reportes de crédito [487] y, al mismo tiempo, se ocupa de proteger los derechos de los titulares de los datos personales que conforman esos reportes o informaciones de crédito.

Las Centrales Privadas de Información de Riesgos (CEPIRS), según la ley peruana,

[486] **El texto completo de la original Ley Nº 27.489 del año 2001, puede ser consultado [en línea] < http://www.leyes.congreso.gob.pe/Imagenes/Leyes/27489.pdf >. Cabe tener presente que algunas de las disposiciones de ley anterior fueron modificadas el año 2002 por la Ley Nº 27.863, la cual puede consultarse a texto completo [en línea] < http://www.leyes.congreso.gob.pe/Imagenes/Leyes/27863.pdf > [consulta: 11 de Diciembre 2002].**

[487] Con la finalidad de comprender a cabalidad la Ley, transcribiremos algunas definiciones legales utilizadas por ésta, a fin de evitar conceptuar separadamente cada término a medida que se analiza la Ley. Por lo tanto, y en atención a lo preceptuado por el artículo 2º, para los efectos de la Ley de CEPIRS se entiende por: 1) *Información de riesgos*: información relacionada a obligaciones o antecedentes financieros, comerciales, tributarios, laborales, de seguros de una persona natural o jurídica que permita evaluar su solvencia económica vinculada principalmente a su capacidad y trayectoria de endeudamiento y pago. 2) *Información sensible*: información referida a las características físicas, morales o emocionales de una persona natural, o a hechos o circunstancias de su vida afectiva o familiar, tales como los hábitos personales, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual u otras análogas que afecten su intimidad y todo lo referido en la Constitución Política del Perú en su artículo 2° inciso 6). 3) *Titular de la información*: la persona natural o jurídica a la que se refiere la información de riesgos. 4) *Reporte de crédito*: toda comunicación escrita o contenida en algún medio proporcionada por una CEPIR con información de riesgos referida a una persona natural o jurídica, identificada. 5) *Banco de datos*: conjunto de información de riesgos administrado por las CEPIRS, cualquiera sea la forma o modalidad de su creación, organización, almacenamiento, sistematización y acceso, que permita relacionar la información entre sí, así como procesarla con el propósito de transmitirla a terceros. 6) *Recolección de información*: Toda operación o conjunto de operaciones o procedimiento técnico que permitan a las CEPIRS obtener información. 7) *Fuentes de acceso público*: Información que se encuentra a disposición del público en general o de acceso no restringido, no impedida por cualquier norma limitativa, que está recogida en medios tales como censos, anuarios, bases de datos o registros públicos, repertorios de jurisprudencia, archivos de prensa, guías telefónicas u otros medios análogos; así como las listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo. 8) *Tratamiento de información*: toda operación o conjunto de operaciones o procedimiento técnico, de carácter automatizado o no, que permitan a las CEPIRS acopiar, almacenar, actualizar, grabar, organizar, sistematizar, elaborar, seleccionar, confrontar, interconectar, disociar, cancelar y, en general, utilizar información de riesgos para ser difundida en un reporte de crédito. 9) *Difusión de información*: toda operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan a las CEPIRS comunicar, ceder, transmitir, dar acceso o poner en conocimiento de terceros la información de riesgos contenida en sus bancos de datos. La información de fuente Registros Públicos deberá indicar obligatoriamente la fecha y hora de la obtención de la información y si ésta es sólo informativa.

son empresas que: *"en locales abiertos al público y en forma habitual recolecten y traten información de riesgos relacionada con personas naturales o jurídicas, con el propósito de difundir por cualquier medio mecánico o electrónico, de manera gratuita u onerosa, reportes de crédito acerca de éstas"* (Art. 2º letra a). A su vez, se agrega que *"no se consideran CEPIRS, para efectos de la presente Ley"*, a las entidades de la administración pública que tengan a su cargo registros o bancos de datos que almacenen información con el propósito de darle publicidad con carácter general, sin importar la forma como se haga pública dicha información(Art. 2º letra a).

La ley establece ciertas exigencias para que puedan funcionar estas empresas; deben contar como mínimo con: a) Una infraestructura informática adecuada para el debido tratamiento de la información recolectada; b) Procedimientos internos para una eficiente, efectiva y oportuna atención de consultas, quejas y reclamos, cuando sea el caso; y, c) Controles internos que proporcionen seguridad en el desarrollo de sus actividades, así como procedimientos de validez de la información procesada (Art. 5º).

En cuanto a la recolección, tratamiento, difusión y seguridad de la información de riesgos, la Ley de CEPIRS establece diversas normas que regulan estos procesos, así como también normas mínimas que resguarden la seguridad de esa información. Respecto de las fuentes de recolección de la información por parte de las CEPIRS, éstas pueden dividirse en dos grandes grupos; la información proporcionada por terceros y la información proporcionada por el titular de los datos. Éstas las revisaremos a continuación.

a) Información proporcionada por terceros

Respecto de esta información el artículo 7º señala que: *"7.1 Las CEPIRS podrán recolectar información de riesgos para sus bancos de datos tanto de fuentes públicas como de fuentes privadas, sin necesidad de contar con la autorización del titular de la información, entendiéndose que la Base de Datos se conformará con toda la información de riesgo"*. Además, lasCEPIRS también podrán adquirir información de las fuentes recién señaladas "*mediante la celebración de contratos privados directamente con la persona natural o jurídica que tenga o haya tenido relaciones civiles, comerciales, administrativas, bancarias, laborales o de índole análoga con el titular de la información, siempre y cuando ésta se refiera a los actos, situaciones, hechos, derechos y obligaciones materia de tales relaciones o derivadas de éstas y que no constituyan violación del secreto profesional"* (Art. 7º, 7.2). Por otra parte, el Nº 7.3 del artículo 7º, señala que las CEPIRS *"igualmente podrán celebrar contratos privados directamente con las entidades de la administración pública que recolecten o utilicen información de riesgos en el ejercicio de sus funciones y competencias legalmente establecidas, salvo que tal información haya sido declarada o constituya un secreto comercial o industrial".*

La norma anterior abre un abanico de posibilidades de acceso a la información personal sin el consentimiento del titular de los datos, lo cual en principio y, sin tener a la vista las otras normas de la ley, parecería un exceso. Con todo, cabe señalar que la propia ley dispone qué tipo de información no podrá ser tratada por las CEPIRS, cuestión que veremos más adelante.

b) Información proporcionada por el titular de los datos

El artículo 8º de la Ley, se ocupa de la información suministrada por los propios titulares señalando al respecto que, las CEPIRS podrán recolectar información de riesgos directamente de los titulares,debiendo previamente informarles a éstos de modo expreso, preciso e inequívoco lo siguiente:

1) La existencia del banco de datos, la finalidad de la recolección de la información y los potenciales destinatarios de ésta;

2) La identidad y dirección de la CEPIR que recolecta la información;

3) El carácter facultativo de sus respuestas a las preguntas que le sean planteadas;

4) Las posibles consecuencias de la obtención de la información; y

5) El alcance de los derechos desarrollados en el Título Cuarto de la Ley, así como de los procedimientos para hacerlos valer.

El inciso final del artículo 8º, agrega a su vez, que cuando en la recolección de información se utilicen cuestionarios u otro medio impreso, *"(…) se deberá entregar al titular de la información una copia de éstos en la que deberá figurar en forma claramente legible las indicaciones señaladas en los incisos precedentes. La carga probatoria de haber brindado la información antes detallada corresponde a las CEPIRS".*

Sin duda las disposiciones anteriores son de máxima importancia, y concuerdan plenamente con las condiciones generales para la licitud del tratamiento de datos personales señalados en el artículo 10 de la Directiva 95/46 CE, cuando la información es recabada del propio titular de los datos. Importante también es la disposición que releva de prueba al titular de los datos, para el caso que señala. Con todo, las disposiciones anteriores no parecen ser la regla general, dada la amplia facultad de recolección de datos por las CEPIRS sin necesidad del consentimiento del titular de los datos (Art. 7º), con lo que la consagración legal de estos principios, queda relegado más bien, a los casos de excepción.

En otra materia, cabe destacar que la ley peruana establece directrices generales de recolección y tratamiento de la información. Al respecto, el artículo 9º señala ciertas normas que deberán observar las CEPIRS en los procesos de recolección y tratamiento de la información de riesgos que tengan a su cargo. Estas normas la ley las denomina "lineamientos generales" y son los siguientes:

"a) La recolección de información no podrá efectuarse por medios fraudulentos o ilícitos;

b) La información recolectada sólo podrá ser utilizada para los fines señalados en la presente Ley;

c) La información que deberá constar en los reportes informativos será lícita, exacta y veraz, de forma tal que responda a la situación real del titular de la información en determinado momento. Si la información resulta ser ilícita, inexacta o errónea, en todo o en parte, deberán adoptarse las medidas correctivas, según sea el caso, por parte de las CEPIRS, sin perjuicio de los derechos que corresponden a los titulares de dicha

información. (…) A efectos de determinar el momento se deberá, en cada reporte, señalar la fecha del informe. (…) Cuando las CEPIRS reciban de sus fuentes información conteniendo la fecha de extinción de la obligación, la naturaleza de la misma, la tasa de interés efectiva, los otros conceptos cobrados y la entidad acreedora, deberán incluir expresamente dicha información en sus reportes; y,

d) La información será conservada durante el plazo legal establecido en la presente ley o, en su defecto hasta que se produzca su cancelación conforme a lo prescrito en el inciso b) del artículo 13º de la presente ley".

De las disposiciones anteriores claramente se desprende que se ha seguido en general, los principios relativos a la licitud de los archivos, calidad de los datos y finalidad establecidos en la Directiva 95/46 CE, lo cual aparece como muy positivo a pesar del restringido ámbito dentro del cual está llamada a regir la ley. En este sentido, consideramos que los principios que están detrás de las normas anteriores pueden extenderse jurídicamente a otros casos y servir de base para una interpretación por analogía ante una laguna legal, dada la falta de ley general de protección de datos personales.

Como ya se señaló, la libertad de recolección de información por parte de las CEPIRS tiene límites. La propia ley se encarga señalarlos en el artículo 10º, estableciendo que estas empresas no podrán contener en sus bancos de datos, ni difundir en sus reportes de crédito la siguiente información: a) Información sensible; b) Información que viole el secreto bancario o la reserva tributaria; c) Información inexacta o errónea; d) Información referida al incumplimiento de obligaciones de naturaleza civil, comercial o tributaria, cuando (i) la obligación se haya extinguido y hayan transcurrido dos años desde su extinción o (ii) cinco años desde el vencimiento de la obligación. Estos plazos no rigen si el titular ejerce el derecho de cancelación de acuerdo a lo establecido en el inciso b) del artículo 13º de la presente Ley. En caso de los protestos se regirá por la Ley de Títulos Valores; e) Información referida a sanciones exigibles de naturaleza tributaria, administrativa u otras análogas, de contenido económico, cuando (i) hayan transcurrido dos años desde que se ejecutó la sanción impuesta al infractor o se extinguió por cualquier otro medio legal, y (ii) cinco años desde que se impuso la sanción; f) Informaciones referidas al incumplimiento de otras obligaciones que no sean comerciales, civiles, tributarias, laborales o de seguros. Excepcionalmente las CEPIRS sólo podrán contener en su banco de datos obligaciones referidas a servicios públicos cuando se haya dejado de pagar dichos servicios por el titular de la información durante seis meses continuos; g) Información referida a la insolvencia o quiebra del titular de la información, cuando hayan transcurrido dos años desde que se levantó el estado de insolvencia o desde que se declaró la quiebra; o, h) Cualquier otra información excluida por ley (Art. 10º).

La enumeración hecha por la ley en relación a la información que no puede ser recolectada, tratada ni difundida por las CEPIRS nos parece, en general, acertada, salvo algunas redundancias en la redacción de la norma, como la de señalar que es información excluida *"la información ilegal"* (letra a), así como también "*cualquier otra información excluida por la ley"* (letra h).

Por otra parte, la Ley establece ciertas reglas en materia de transmisión de datos a

terceros. En este sentido se enmarca el artículo 11º de la Ley de CEPIRS, el cual dispone que estas empresas podrán difundir a terceras personas, de manera onerosa o a título gratuito, la información de riesgos que contengan en sus bancos de datos. Para estos efectos, *"las CEPIRS podrán implementar en la forma que estimen conveniente procedimientos automatizados para la transmisión, comunicación o acceso de datos a terceros, así como el registro obligatorio de éstos bajo responsabilidad, debiendo cautelar los derechos de los titulares de la información".* El inciso 2º añade que: *"Las CEPIRS difunden la información de riesgo, luego de identificar con medios apropiados al solicitante de la información".* En suma, en esta materia la ley deja a las propias empresas la determinación de los mecanismos tecnológicos a utilizarse para la transmisión automatizada de los reportes de crédito, imponiéndoles en todo caso un deber de cuidado respecto de la información que es transmitida a terceros y, un deber de identificación del requirente previo a la transmisión.

Respecto de los derechos de los titulares de la información, la ley señala -a nuestro juicio acertadamente- en su artículo 13º que: *"de manera enunciativa, mas no limitativa, los titulares de la información registrada en los bancos de datos administrados por las CEPIRS tienen los siguientes derechos*:

a) El derecho de acceso a la información referida a uno mismo registrada en tales bancos;

b)El derecho de modificación y el derecho de cancelación de la información referida a uno mismo registrada en tales bancos que fuese ilegal, inexacta, errónea o caduca;

c)El derecho de rectificación de la información referida a uno mismo que haya sido difundida por las CEPIRS y que resulte ser ilegal, inexacta, errónea o caduca y,

d)El derecho de actualización de la información referida a uno mismo, registrada en los bancos de datos, que no haya incluido pagos parciales o totales, siempre que hubiesen vencido los plazos establecidos en los incisos 15.7 y 15.8 del artículo 15 de la presente Ley".

Creemos que la norma anterior ha sido establecida de un modo conveniente, pues viene a desarrollar la disposición constitucional que consagra la garantía del hábeas data para tutelar a toda persona su derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar (Art. 200 en relación con el numeral 6 del artículo 2º C. Pol.).

Luego, la ley se encarga de regular el ejercicio de los derechos de los titulares de los datos personales, enumerados de manera enunciativa y no exhaustiva. Debemos recordar que el procedimiento contemplado por la ley que se analiza es de carácter informal y según la Ley 26.301, éste debe agotarse para poder ejercer la acción de hábeas data. A continuación revisaremos lo señalado por la Ley en materia de derechos de los titulares.

i) Derecho de acceso

Al respecto la ley señala en el artículo 14º que: *"los titulares podrán acceder, una vez al año o cuando la información contenida en los bancos de datos haya sido objeto de*

rectificación, a la información crediticia que les concierne que estuviese registrada en los bancos de datos administrados por las CEPIRS". Se agrega que, esta información deberá ser acompañada de una reseña explicativa de los derechos de los titulares, así como de los procedimientos para hacerlos valer. En definitiva, la información podrá ser obtenida por el titular de la información: *"a) De forma gratuita, mediante la visualización en pantalla de los datos o; b) Mediante el pago de una suma de dinero, que no excederá de los costos necesarios para la emisión del documento correspondiente, mediante un escrito, copia o fotocopia, en forma legible e inteligible, sin utilizar claves o códigos que requieran de dispositivos mecánicos para su adecuada comprensión".* Se añade que esta información incluirá, a solicitud del titular, *"la identidad de las fuentes de información registrada en los bancos de datos, con excepción de las fuentes de acceso público y la identidad de todas las personas que obtuvieron un reporte de crédito sobre el titular en los últimos doce meses, así como la fecha en que se emitieron tales reportes"* (Art. 14º inciso final).

La disposición recién anotada nos parece, en general, adecuada salvo por la limitación temporal para ejercer el derecho de acceso a la información. Tal limitación, entraba el control efectivo de la información que manejan las CEPIRS por parte de los titulares de los datos. Creemos que en esa limitación no existiría suficiente justificación jurídica, pues para limitar el ejercicio de un derecho constitucional en favor de una eventual recarga de trabajo para las CEPIRS (gratuito si es un acceso por pantalla y pagado si es a través de un informe), debería sostenerse que esa restricción es socialmente más beneficiosa que la alternativa contraria, lo cual no creemos. En suma, consideramos que la disposición del artículo 14, en la parte limitativa del derecho de acceso podría ser atacada por inconstitucionalidad, en razón de limitar injustificadamente el derecho de acceso a la información, sin que la Carta Fundamental de pie para que el legislador pueda actuar es este sentido [488] .

ii) Derecho de modificación y derecho de cancelación

En lo relativo al derecho de los titulares de los datos de solicitar su modificación y cancelación, a través de la vía informal o extrajudicial ante las CEPIRS, el artículo 15º señala que:

1)En caso de considerar que la información contenida en los bancos de datos es ilegal, inexacta, errónea o caduca, el titular de dicha información podrá solicitar que ésta sea revisada por cuenta y costo de las CEPIRS y, de ser el caso, que se proceda a su

[488] Con todo, cabe reconocer que la misma Directiva 95/46 CE, establece en el artículo 12 (Derecho de acceso) que los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento: *"A) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos: - la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran Y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos"* . Lo anterior, en principio guardaría concordancia la Ley de CEPIRS. El punto está en determinar cuánto tiempo debe transcurrir entre dos pedidos de informe para que pueda estimarse que existe una periodicidad razonable. En materia de datos personales comerciales, creemos que esa periodicidad debe ser menor, en atención a la dinámica de la situación patrimonial de las personas, toda vez que el patrimonio de ellas no es estático.

modificación o cancelación;

2)La solicitud para la revisión de la información deberá ser interpuesta por escrito, acompañando los medios probatorios que acrediten que el solicitante es el titular de la información. En dicha solicitud se precisarán los datos concretos que se desea revisar, acompañando la documentación que justifique el pedido;

3) Las CEPIRS establecerán los procedimientos internos necesarios para brindar una eficiente, efectiva y oportuna atención a las solicitudes de revisión presentadas, así como los mecanismos de comunicación y coordinación adecuados con las fuentes de las que recolecta la información;

4) Dentro del plazo de siete días naturales desde la presentación de la solicitud, las CEPIRS obligatoriamente informarán por escrito al titular de la información si su pedido es procedente o si ha sido denegado. Alternativamente, dentro del mismo plazo, las CEPIRS podrán prorrogar, hasta por cinco días naturales adicionales, el plazo para emitir una decisión definitiva, debiendo para ello, hasta que finalice el plazo, difundir que dicha información es materia de revisión;

5) Vencidos los plazos señalados, el titular de la información deberá recibir la comunicación por escrito que responda de manera definitiva su solicitud;

6) Cuando la información se encuentre desactualizada, producto de la no inclusión de datos sobre pagos parciales o totales, la fuente que generó dicha información, una vez detectado el error o la inexactitud, deberá actualizarla en un plazo de dos días hábiles, sin necesidad de solicitud del titular;

7) El plazo para remitir la información a las CEPIRS referidos a pagos parciales o totales, por parte de las fuentes de la información, no deberá ser mayor al plazo utilizado por éstas para remitir información referida a obligaciones vencidas;

El plazo para actualizar los reportes de crédito, emitidos por las CEPIRS referidos a pagos parciales o totales por parte de las fuentes de información, no deberá ser mayor a dos días hábiles, contados a partir del día siguiente de la recepción de la información proveniente de las fuentes. Se añade que lo dispuesto en los numerales 7 y 8 (Arts. 15.7 y 15.8 respectivamente), no será de aplicación a los casos de protestos, los que se rigen por la Ley de Título Valores.

De lo prescrito por el legislador, se desprende el carácter informal o extrajudicial del procedimiento para el ejercicio de los derechos de modificación y cancelación de los datos personales contenidos en las bases de datos de las CEPIRS. La informalidad o carácter extrajudicial del procedimiento es clara, por cuanto no existe intervención de un Tribunal que conozca del hábeas data. Sólo el agotamiento de este procedimiento hace procedente la interposición de la acción constitucional de hábeas data ante la justicia, como se verá más adelante.

iii) Derecho de rectificación

El ejercicio del derecho de rectificación de los datos está regulado en el artículo 16º, el cual dispone que en caso de verificarse que la información contenida en los bancos de datos es ilegal, inexacta, errónea o caduca: *"la CEPIR, a su cuenta y costo, enviará*

comunicaciones rectificatorias, a quienes les hubiera proporcionado dicha información en los doce meses anteriores a la fecha en que se verifique el problema".

Lo señalado recién, es muy significativo pues se permite una actualización de los datos por parte de quienes hayan obtenido reportes de crédito hasta con un año de anterioridad a la fecha de la verificación del problema de ilegalidad, inexactitud, error o caducidad de los datos personales del titular.

Finalmente, debemos agregar que en materia de defensa de los derechos de los titulares de los datos, el artículo 19º insertado dentro del Título V la Ley de CEPIRS, señala que las disposiciones contenidas en el presente Título, son de aplicación a las disputas que surjan entre las CEPIRS y los titulares de la información, los cuales *"son considerados consumidores por mandato de la presente Ley, para efectos de la aplicación de lo dispuesto por el Decreto Legislativo N° 716, Ley de Protección al Consumidor".* Por lo tanto, esta Ley otorga la calidad de consumidores a los titulares de datos personales, para los efectos de hacerles aplicables las disposiciones del estatuto de protección al consumidor en defensa de sus derechos. Consecuente con lo anterior, el artículo 21º dispone que la Comisión de Protección al Consumidor del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) es el órgano administrativo competente para conocer de las infracciones señaladas en el artículo 20º, e imponer las sanciones administrativas y las medidas correctivas a las que hubiere lugar (Art. 21º, 21.1) [489] .

En suma, puede afirmarse que la Ley de CEPIRS, si bien es una normativa sectorial circunscrita al mercado de la información crediticia llevada a cabo a través de los reportes de crédito, sustantivamente cumple en general con estándares internacionales (europeos) de protección de datos personales. Por ello, la consideraremos para los efectos de esta investigación como una ley sectorial compleja, es decir, eventualmente influida por principios y normas internacionales sobre protección de datos personales. Por otra parte, estimamos que las carencias de esta normativa dicen relación con la ausencia de deberes de registro de los bancos de datos, y de un organismo de control especial encargado de vigilar la legalidad de éstos, como también de velar por el respeto de las normas legales en la materia, aunque esta última carencia podría ser justificable en atención al parcial ámbito de aplicación de la Ley. Con todo, el legislador ha encargado la aplicación de las sanciones administrativas respectivas y la medidas correctivas a la Comisión de Protección al Consumidor del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) con lo cual este organismo pasaría a ser en la realidad jurídica peruana el órgano de control con atribuciones limitadas.

2.2.2) Ley de Transparencia y Acceso a la Información Pública (Ley Nº 27.806) [490]

Esta ley, que fue aprobada por el Congreso peruano el 2 de Agosto de 2002, tiene por

[489] También se señala que: *"para presentar una denuncia administrativa por infracción al artículo 20° inciso b), el consumidor titular de la información deberá previamente obtener un pronunciamiento expreso o tácito, denegando una solicitud de revisión o rectificación, tramitada conforme a lo dispuesto en los artículos 15° y 16° de la presente Ley"* (Artículo 21º Nº 21.2).

objeto promover la transparencia de los actos del Estado y regular el derecho fundamental del acceso a la información consagrado en el numeral 5 del artículo 2° de la Constitución Política del Perú (Art. 1). Si bien este derecho no se vincula directamente con la versión tradicional del hábeas data, la configuración constitucional que se le ha dado al instituto en el Perú, hace necesario que se revise esta normativa que regula el derecho de acceso a la información pública a cargo de organismos públicos, pues tal como está concebida la actual Constitución, el ejercicio del derecho a la información pública puede servir tanto para acceder a datos personales, como a otro tipo de información de interés público, confundiéndose dos acciones distintas dentro de una misma regulación. Cabe añadir, que esta Ley contiene tanto disposiciones sustantivas como procedimentales encaminadas a regular el ejercicio del derecho de acceso a la información pública por vía administrativa, la cual sólo una vez agotada, faculta al titular de los datos para el ejercicio de la acción constitucional de hábeas data regulada -transitoriamente desde 1994- por la Ley Nº 26.301. A continuación se señalarán las disposiciones más relevantes de esta Ley para nuestro estudio, asimismo se reseñará el procedimiento administrativo previo a la acción de hábeas data.

Dentro del Título III, denominado "Acceso a la Información Pública del Estado" se inserta el artículo 7º, el cual dispone que: *"toda persona tiene derecho a solicitar y recibir información de cualquier entidad de la Administración Pública. En ningún caso se exige expresión de causa para el ejercicio de este derecho".*

Lo recién expuesto es plenamente concordante con lo preceptuado en el artículo 2º numeral 5º de la Constitución Política peruana. Como se observará, esta Ley tampoco distingue entre el ejercicio del derecho de acceso a datos personales en poder de la administración pública y la simple solicitud de información, distinta a los datos personales en materia de interés público. Sin embargo, entendemos que la variante que nos interesa (acceso a los datos personales) está contenida y se regula por la Ley 27.806, dado que es el único cuerpo normativo infraconstitucional que se refiere directamente a la materia.

Respecto de los organismos obligados a informar a quienes lo soliciten, el artículo 8º señala que ese deber pesa tanto sobre las entidades de la Administración Pública como las Fuerzas Armadas y la Policía Nacional del Perú [491] . El artículo 9º agrega en esta misma materia, que las personas jurídicas sujetas al régimen privado y que gestionen servicios públicos o ejerzan funciones administrativas del sector público bajo cualquier modalidad, *"sólo están obligadas a facilitar la información referida a la prestación de los mismos a sus respectivos organismos supervisores, a efectos que éstos puedan cumplir con las obligaciones establecidas en esta Ley"*. Por lo tanto, se entiende en este último caso que el derecho de acceso se ejerce ante los organismos supervisores de esos servicios y no directamente ante éstos. Aunque la ley no lo dice, entendemos que para el ejercicio del derecho de acceso a los datos personales, el solicitante debe ser el titular de éstos o su legítimo representante.

490 [En línea] < http://www.leyes.congreso.gob.pe/Imagenes/Leyes/27806.pdf > [consulta: 20 de Abril 2003].

491 Estas últimas instituciones responden las solicitudes de información a través del Ministerio de Defensa y del Ministerio del Interior, respectivamente (Artículo 8º en relación con el artículo 2º inciso 2º Ley Nº 27.806).

En cuanto a la información catalogada como de acceso público, el artículo 10º dispone que: *"las entidades de la Administración Pública tienen la obligación de proveer la información requerida si se refiere a la contenida en documentos escritos, fotografías, grabaciones, soporte magnético o digital, o en cualquier otro formato, siempre que haya sido creada u obtenida por ella o que se encuentre en su posesión o bajo su control"*.Se agrega que: *"(…) para los efectos de esta Ley, se considera como información pública cualquier tipo de documentación financiada por el presupuesto público que sirva de base a una decisión de naturaleza administrativa, así como las actas de reuniones oficiales"* (Art. 10º).

La disposición anterior concibe ampliamente el concepto de información mediante la no limitación del soporte material en el cual se encuentre contenida ésta, con lo cual creemos se permite un efectivo acceso a la información manejada o poseída por el Estado, referida tanto a los datos personales, como a información de público interés.

Por otra parte, el artículo 18º de la Ley, refiriéndose a la conservación de la información que el Estado posea, señala que: *"en ningún caso la entidad de la Administración Pública podrá destruir la información que posea"*. Se agrega por este artículo, que la entidad de la Administración Pública deberá remitir al Archivo Nacional la información que obre en su poder, en los plazos estipulados por la Ley de la materia, el cual a su vez, podrá destruir la información que no tenga utilidad pública cuando haya transcurrido un plazo razonable durante el cual no se haya requerido dicha información y de acuerdo a la normatividad por la que se rige el Archivo Nacional.

A continuación, nos referiremos al procedimiento establecido en la Ley para el ejercicio del derecho de acceso a la información. Éste se contempla en el artículo 11º y es el siguiente:

i) Solicitud de información

Toda solicitud debe dirigirse al funcionario designado por la entidad de la Administración Pública para realizar esta labor. En caso que éste no hubiera sido designado, la solicitud se dirige al funcionario poseedor de la información requerida o al superior inmediato (Art. 11º letra a).

ii) Entrega de la información

La entidad de la Administración Pública a la cual se haya presentado la solicitud de información, deberá otorgarla en un plazo no mayor de siete días útiles, plazo que se podrá prorrogar excepcionalmente por cinco días útiles adicionales en caso de existir dificultad inusual para reunir la información solicitada. En este evento, la entidad deberá comunicar por escrito, antes del vencimiento del primer plazo, las razones por las que hará uso de tal prórroga. En el caso que el receptor de la solicitud no posea la información solicitada pero conozca la ubicación y destino de ésta, deberá informarlo al solicitante (Art. 11º letra b).

ii) Denegatoria al acceso

La Ley señala que la denegatoria de acceso a la información se sujetará a lo dispuesto en el segundo párrafo del artículo 13° (Art. 11º letra c). A su vez, el artículo 13º establece que la entidad de la Administración Pública a la cual se solicite información *"no podrá negarla basando su decisión en la identidad del solicitante".* No entendemos la razón de la disposición anterior. A pesar de ello, puede señalarse que se desprende una intención encaminada a evitar una discriminación respecto de quien solicite la información.

La denegatoria al acceso a la información solicitada debe ser debidamente fundamentada en las excepciones del artículo 15° de la Ley [492] , exigiéndose por ésta el deber de señalar expresamente y por escrito las razones por las que se aplican esas excepciones y el plazo por el que se prolongará dicho impedimento [493] . En caso que un documento contenga, en forma parcial, información que no sea de acceso público, la entidad de la Administración Pública deberá permitir el acceso a la información disponible del documento (Art. 16º) [494] . En definitiva, en caso de no mediar respuesta en los plazos legales, el solicitante puede considerar denegado su pedido (Art. 11º letra d).

iv) Agotamiento de la vía administrativa

En los eventos de denegatoria o no respuesta a la solicitud de información, el solicitante puede considerar denegado su pedido para los efectos de dar por agotada la vía administrativa, salvo que la solicitud haya sido cursada a un órgano sometido a superior jerarquía, en cuyo caso deberá interponer el recurso de apelación para agotarla (Art. 11º letra e). Si la apelación es rechazada, o la entidad correspondiente no se pronuncia dentro de diez días útiles de presentado el recurso, el solicitante podrá dar por agotada la vía administrativa (Art. 11º letra f). Agotada la vía administrativa, el solicitante que no obtuvo la información requerida *"podrá optar por iniciar el proceso contencioso administrativo, de conformidad con lo señalado en la Ley N° 27.584 u optar por el proceso constitucional del Hábeas Data, de acuerdo a lo señalado por la Ley N° 26.301".* (Art. 11º letra g). Sin perjuicio de lo señalado en este artículo, se preceptúa que las entidades de la Administración Pública deberán permitir a los solicitantes, el acceso directo e inmediato a la información pública durante las horas de atención al público (Art. 12).

493 El inciso 3º del artículo 13º señala a su vez que: *"la solicitud de información no implica la obligación de las entidades de la Administración Pública de crear o producir información con la que no cuente o no tenga obligación de contar al momento de efectuarse el pedido. En este caso, la entidad de la Administración Pública deberá comunicar por escrito que la denegatoria de la solicitud se debe a la inexistencia de datos en su poder respecto de la información solicitada. Esta Ley tampoco permite que los solicitantes exijan a las entidades que efectúen evaluaciones o análisis de la información que posean".* Por último, el inciso final de la disposición preceptúa que: "*si el requerimiento de información no hubiere sido satisfecho o si la respuesta hubiere sido ambigua, se considerará que existió negativa tácita en brindarla".*

494 Por otra parte, la Ley dispone que el solicitante que requiera la información, deberá abonar el importe correspondiente a los costos de reproducción de la información requerida, cuyo monto de la tasa deberá figurar en el Texto Único de Procedimientos Administrativos (TUPA) de cada entidad de la Administración Pública (Artículo 17). Añade este artículo que: "*cualquier costo adicional se entenderá como una restricción al ejercicio del derecho regulado por esta Ley, aplicándose las sanciones correspondientes"* (Artículo 17º inciso 2º).

De lo señalado por el artículo 11º, queda claro que para poder ejercitar la acción

[492] El artículo 15 establece una compleja enumeración de las excepciones al ejercicio del derecho de acceso a la información pública. Estas excepciones son las siguientes: *"a) La información expresamente clasificada como secreta y estrictamente secreta a través de un acuerdo adoptado por la mayoría del número legal de los miembros del Consejo de Ministros. El acuerdo deberá sustentarse en razones de seguridad nacional en concordancia con el Artículo 163° de la Constitución Política del Perú y tener como base fundamental garantizar la seguridad de las personas. Asimismo, por razones de seguridad nacional se considera información clasificada en el ámbito militar, tanto en el frente externo como interno, aquella cuya revelación originaría riesgo para la integridad territorio y/o subsistencia del sistema democrático. (…) Mediante Decreto Supremo aprobado por la mayoría del número legal de miembros del Consejo de Ministros, el Poder Ejecutivo reglamentará las excepciones que expresamente se enmarcan en el presente artículo. (…) El acuerdo debe constar por escrito y en él deben explicarse las razones por las cuales se produce la clasificación mencionada. Este acuerdo debe ser revisado cada cinco (5) años a efectos de evaluar su desclasificación. El acuerdo que disponga la continuación del carácter secreto y estrictamente secreto deberá ser debidamente motivado y sujetarse a las mismas reglas que rigen para el acuerdo inicial. (…) No se considerará como información clasificada, la relacionada a la violación de derechos humanos o de las Convenciones de Ginebra de 1949 realizada en cualquier circunstancia, por cualquier persona. (…) El Presidente del Consejo de Ministros deberá dar cuenta a la Comisión de Defensa Nacional, Orden Interno e Inteligencia del Congreso de los criterios que el Consejo ha utilizado en la clasificación de la información como secreta o estrictamente secreta. (…) Una vez que la información clasificada se haga pública, una comisión especial del Congreso de la República evaluará si las razones esgrimidas en el acuerdo del Consejo de Ministros que declaró como clasificada una información se adecuaban a la realidad de los hechos. (…) Esto no impide que una comisión competente del Congreso de la República efectúe dicha evaluación en cualquier momento.* b) Materias cuyo conocimiento público pueden afectar los intereses del país en negociaciones o tratos internacionales. *c)* ***La información protegida por el secreto bancario, tributario, comercial, industrial, tecnológico y bursátil*** (negrita nuestra). *d) La información interna de las entidades de la Administración Pública o de comunicaciones entre éstas que contengan consejos, recomendaciones u opiniones producidas como parte del proceso deliberativo y consultivo previo a la toma de una decisión de gobierno. (…) Una vez tomada la decisión, esta excepción cesa si la entidad de la Administración Pública opta por hacer referencia en forma expresa a esos consejos, recomendaciones u opiniones.* e) La información preparada u obtenida por asesores jurídicos o abogados de las entidades de la Administración Pública cuya publicidad pudiera revelar la estrategia a adoptarse en la tramitación o defensa en un proceso administrativo o judicial, o de cualquier tipo de información protegida por el secreto profesional que debe guardar el abogado respecto de su asesorado. *f) La información vinculada a investigaciones en trámite referidas al ejercicio de la potestad sancionadora de la Administración Pública, en cuyo caso la exclusión del acceso termina cuando la resolución que pone fin al procedimiento queda consentida o cuando transcurren más de 6 (seis) meses desde que se inició el procedimiento administrativo sancionador, sin que se haya dictado resolución final.* g) La información que tiene por finalidad prevenir y reprimir la criminalidad en el país y cuya revelación puede entorpecerla. *h* ***) La información referida a los datos personales cuya publicidad constituya una invasión de la intimidad personal y familiar. La información referida a la salud personal, se considera comprendida dentro de la intimidad personal*** (negrita nuestra). *i) Aquellas materias cuyo acceso esté expresamente exceptuado por la Constitución, o por una Ley aprobada por el Congreso de la República. (…) Los casos establecidos en el presente artículo son los únicos en los que se puede limitar el derecho al acceso a la información pública, por lo que deben ser interpretados de manera restrictiva por tratarse de una limitación a un derecho fundamental. No se puede establecer por una norma de menor jerarquía ninguna excepción a la presente Ley. (…) La información contenida en las excepciones señaladas en este artículo son accesibles para el Congreso de la República, el Poder Judicial y el Ministerio Público, con las limitaciones que señala la Constitución Política del Perú en ambos casos. Para estos efectos, el Congreso de la República se sujeta igualmente a las limitaciones que señala su Reglamento. Tratándose del Poder Judicial de acuerdo a las normas que regulan su funcionamiento, solamente el juez en ejercicio de sus atribuciones jurisdiccionales en un determinado caso y cuya información sea imprescindible para llegar a la verdad, puede solicitar la información a que se refiere cualquiera de las excepciones contenidas en este artículo"* (Artículo 15º Ley Nº 27.806).

constitucional de hábeas data en contra de algún organismo del Estado, debe previamente haberse agotado la vía administrativa. Llama la atención que el legislador haga optar al titular de los datos -agotada la vía administrativa- entre un proceso contencioso administrativo o uno de carácter constitucional. Creemos que en materia de hábeas data, debiera existir competencia privativa de los jueces civiles, tanto en razón de la -supuesta- especialización de éstos, como en razón de simplificar la institución en beneficio de los titulares de los datos.

Por último, en lo que toca a la materia de protección de datos regulado por esta Ley, el artículo 19º señala que la Presidencia del Consejo de Ministros deberá remitir un informe anual al Congreso de la República en el que de cuenta sobre las solicitudes pedidos de información atendidos y no atendidos. Para estos efectos se le encarga a la Presidencia del Consejo de Ministros que reúna de todas las entidades de la Administración Pública la información para efectuar el informa anual.

En síntesis, la Ley peruana de Transparencia y Acceso a la Información Pública regula administrativamente el derecho constitucional de acceso a ese tipo de información, sin distinguir entre información de público interés e información relativa a los datos personales. Lo anterior, sin duda es corolario de la fuente constitucional, la que tampoco hace tal distinción y trata el instituto como uno solo. Sin embargo, creemos que es posible separar esos distintos ámbitos y, a partir de ello, lograr diferenciar conceptualmente la acción de hábeas data propia (referida a los datos personales) de la acción de hábeas data impropia (referida a la información pública sobre actos de la administración). La ventaja de ello, radica en simplificar el instituto y marcar la diferencia a la hora de optar por ejercer la acción constitucional según el procedimiento contencioso administrativo o ante un juez civil (Art. 11º letra g). En este sentido, opinamos que el legislador debió ser más claro en la materia y dejar al juez civil privativamente el conocimiento de la acción de hábeas data propia y relegar el hábeas data impropio al juez de lo contencioso administrativo, en atención a la diversa finalidad perseguida por esas acciones. Por último, debemos señalar que estimamos estrecha la configuración del hábeas data peruano, pues sólo se limita a reconocer el derecho de acceso, más no a rectificar, corregir, actualizar ni cancelar los datos que obren en los archivos o registros estatales.

2.2.3) Ley General de la Persona con Discapacidad [495]

Esta ley tiene por objeto proteger a las personas con discapacidad tanto en lo referente a la atención de salud, trabajo, educación, rehabilitación y seguridad social para que ellas puedan lograr su desarrollo e integración social, económica y cultural, en concordancia con lo preceptuado en el artículo 7 de la Constitución (Art. 1º). En el ámbito que nos interesa, esta Ley señala en el artículo 12 que existirá un Registro Nacional de las personas discapacitadas y cuya información contenida en éste *"es de carácter confidencial"*, por lo que *"(…) Sólo puede ser usada con fines estadísticos, científicos y técnicos*". Se visualiza de lo anterior la finalidad en el uso de la información, el cual podría plantearse como principio general en estos casos.

[495] **[En línea] < http://www.leyes.congreso.gob.pe/Imagenes/Leyes/27050.pdf > [consulta: 11 de Diciembre 2002].**

Finalmente, si bien se establece en esta Ley un deber de confidencialidad respecto de la información contenida en el Registro, así como restricciones al uso de ella, no se señalan las consecuencias jurídicas que se aparejarían de no cumplirse lo preceptuado por el legislador.

2.2.4) Ley que crea la Unidad de Inteligencia Financiera-Perú [496]

Esta ley tiene por finalidad el análisis, el tratamiento y la transmisión de información para prevenir y detectar el lavado de dinero o activos. El organismo encargado de llevar a cabo estos objetivos es la Unidad de Inteligencia Financiera, la cual está concebida como una persona jurídica de Derecho Público, con autonomía funcional, técnica y administrativa (Art. 1º).

Dentro de las funciones que le encomienda la ley a la Unidad de Inteligencia Financiera (en adelante UIF), se prevé la de *"solicitar, recibir y analizar información sobre las transacciones sospechosas que le presenten los sujetos obligados a informar por esta Ley"* (Art. 3 Nº 1). A su vez, los sujetos obligados a informar a la UIF [497] están obligados a guardar reserva, deber que se establece en el artículo 12º de la siguiente manera: *"los sujetos obligados, así como sus empleados, que informen a la UIF sobre las transacciones descritas en los artículos anteriores, no pueden poner en conocimiento de persona alguna, salvo de un órgano jurisdiccional o autoridad competente u otra persona autorizada, de acuerdo con las disposiciones legales, el hecho de que una información ha sido solicitada o proporcionada a la UIF, de acuerdo a la presente Ley, bajo responsabilidad legal"* [498] .

En cuanto a las excepciones al deber de reserva, se señala en el artículo 13º que los sujetos obligados por la ley en comento, sus trabajadores, directores y otros representantes autorizados por la legislación, *"están exentos de responsabilidad penal, legal o administrativa, según corresponda, por el cumplimiento de esta Ley o por la revelación de información cuya restricción está establecida por contrato o emane de cualquier otra disposición legislativa, reglamentaria o administrativa, cualquiera sea el resultado de la comunicación. Esta disposición es extensiva a todos los miembros de la*

496 [En línea] < http://www.leyes.congreso.gob.pe/Imagenes/Leyes/27693.pdf > [consulta: 12 de Diciembre 2002].

497 En esta materia, el legislador ha señalado en el artículo 8º una lista de treinta entidades entre personas naturales y jurídicas, tanto públicas como privadas, que están obligadas a suministrar información sobre transacciones sospechosas. A pesar de la pretensión de exhaustividad legislativa, finalmente se señala en el inciso final de este artículo que: *"mediante decreto supremo, refrendado por el Presidente del Consejo de Ministros y el Ministro de Economía y Finanzas, se ampliará la lista de personas naturales o jurídicas obligadas a proporcionar la información que establece este artículo".* Entre las instituciones o personas que integran la lista se encuentran: las empresas del sistema financiero y del sistema de seguros; las sociedades agentes de bolsa y sociedades intermediarias de valores; las sociedades administradoras de fondos mutuos, fondos de inversión, fondos colectivos, y fondos/ seguros de pensiones; los casinos, sociedades de lotería y casas de juegos, incluyendo bingos, hipódromos y sus agencias, entre otras.

498 Se agrega además por el artículo 12º que esta disposición también es de aplicación para los miembros del Consejo Consultivo, el Director Ejecutivo y demás personal de la UIF.

UIF, que actúen en el cumplimiento de sus funciones".

2.2.5) Código Tributario [499]

El artículo 85 del Código Tributario peruano señala que: *"tendrá carácter de información reservada, y únicamente podrá ser utilizada por la Administración Tributaria, para sus fines propios, la cuantía y la fuente de las rentas, los gastos, la base imponible o, cualesquiera otros datos relativos a ellos, cuando estén contenidos en las declaraciones e informaciones que obtenga por cualquier medio de los contribuyentes, responsables o terceros".*

En materia de excepciones a la reserva tributaria, cabe recordar primeramente lo ya señalado por el Constituyente en el artículo 2 Nº 5 inciso 2º el cual dispone que: *"El secreto bancario y la reserva tributaria pueden levantarse a pedido del Juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado"* [500] .

[499] [En línea] < http://www.congreso.gob.pe/out_of_domain.asp?URL=http%3A//www.leyes.congreso.gob.pe/ > [consulta: 5 de Febrero 2003].

[500] La ley tributaria, a su vez ha dispuesto en el artículo 85 inciso 3º que están exceptuados de la reserva tributaria: a) Las exhibiciones de documentos y declaraciones que ordene el Poder Judicial en los procedimientos sobre tributos, alimentos, disolución de la sociedad conyugal o en los procesos penales; el Fiscal de la Nación en los casos de presunción de delito; y la Comisión de Fiscalización o de las Comisiones Investigadoras del Congreso, con acuerdo de la comisión respectiva, con arreglo a ley y siempre que se refieran al caso investigado; b) Los expedientes de procedimientos tributarios respecto de los cuales hubiera recaído resolución que ha quedado consentida, cuando sea autorizado por la Administración Tributaria; c) La publicación que realice la Administración Tributaria de los datos estadísticos, siempre que por su carácter global no permita la individualización de declaraciones, informaciones, cuentas o personas; d) Las publicaciones sobre Comercio Exterior que efectúe la Superintendencia Nacional de Aduanas, respecto a la información contenida en las declaraciones referidas a los regímenes y operaciones aduaneras consignadas en los formularios correspondientes aprobados por dicha entidad y en los documentos anexos a tales declaraciones. Por decreto supremo se regulará los alcances de este inciso y se precisará la información susceptible de ser publicada. Se señala adicionalmente que: *"a juicio del jefe del órgano administrador de tributos, la Administración Tributaria, mediante Resolución de Superintendencia o norma de rango similar, podrá incluir dentro de la reserva tributaria determinados datos que el contribuyente proporcione a la Administración Tributaria a efecto que se le otorgue el Registro Único de Contribuyentes (RUC), y en general, cualquier otra información que obtenga de los contribuyentes, responsables o terceros. En virtud a dicha facultad no podrá incluirse dentro de la reserva tributaria:* 1) La publicación que realice la Administración Tributaria de los contribuyentes y/o responsables, sus representantes legales, así como los tributos determinados por los citados contribuyentes y/o responsables, los montos pagados, las deudas tributarias materia de fraccionamiento y/o aplazamiento, y su deuda exigible, entendiéndose por esta última, aquélla a la que se refiere el artículo 115. La publicación podrá incluir el nombre comercial del contribuyente y/o responsable, si lo tuviera; 2) La publicación de los datos estadísticos que realice la Administración Tributaria, siempre que por su carácter general no permitan la individualización de declaraciones, informaciones, cuentas o personas; 3) La información que solicite el Gobierno Central respecto de sus propias acreencias, pendientes o canceladas, por tributos cuya recaudación se encuentre a cargo de la Superintendencia Nacional de Administración Tributaria - SUNAT o la Superintendencia Nacional de Administración de Aduanas - ADUANAS, siempre que su necesidad se justifique por norma con rango de Ley o por Decreto Supremo. Finalmente, la Ley dispone que la Administración Tributaria no se encuentra obligada a proporcionar a los contribuyentes, responsables o terceros la información que pueda ser materia de publicación (Artículo 85 inciso 3º).

Debemos anotar además, que la obligación del artículo 85 de mantener la reserva tributaria se extiende: *"a quienes accedan a la información calificada como reservada en virtud a lo establecido en el presente artículo, inclusive a las entidades del sistema bancario y financiero que celebren convenios con la Administración Tributaria de acuerdo al artículo 55, quienes no podrán utilizarla para sus fines propios"* (Art. 85 inciso 5º). Finalmente, se establece una disposición que redunda en todo lo dicho anteriormente y que prescribe: *"no incurren en responsabilidad los funcionarios y empleados de la Administración Tributaria que divulguen información no reservada en virtud a lo establecido en el presente artículo, ni aquéllos que se abstengan de proporcionar información por estar comprendida en la reserva tributaria".*

En suma en el ordenamiento jurídico peruano se reconoce a nivel constitucional y legal la reserva tributaria. La ley especifica que ella está referida a las informaciones sobre la cuantía y la fuente de las rentas, los gastos y cualesquiera otros datos relativos a ellos, proporcionados a través de las declaraciones o informes a la administración tributaria.

2.2.6) Ley de Protección al Consumidor (Decreto Legislativo Nº 716-1991) [501]

La Ley de Protección al Consumidor señala en el artículo 39º que la Comisión de Protección al Consumidor es el único órgano administrativo competente para conocer de las presuntas infracciones a las disposiciones contenidas en la presente Ley, así como para imponer las sanciones administrativas y medidas correctivas establecidas en el presente Título. Si bien hasta acá la disposición sólo nos señala la competencia de la Comisión en materia de protección de consumidores, debemos tener presente lo prescrito en el Título V ("De la Defensa de los Consumidores") de la Ley de CEPIRS ya analizada. Como se dijo, esta Ley dispone expresamente que para el efecto de hacer aplicables a los titulares de los datos personales la Ley de Protección al Consumidor, los considera a éstos como consumidores. Consecuente con ello, la Ley de CEPIRS le otorga competencia a la Comisión de Protección al Consumidor para conocer de las infracciones establecidas en esa ley, aplicar las sanciones administrativas y las medidas correctivas a que hubiere lugar (Art. 21.1 Ley de CEPIRS). Por lo tanto, la importancia de la Ley de Protección al Consumidor radica en que las infracciones a la Ley de CEPIRS serán conocidas la Comisión de Protección al Consumidor según el procedimiento establecido en el Título V del Decreto Legislativo Nº 807, el cual establece las Facultades, Normas y Organización de INDECOPI (Art. 21.1 Ley de CEPIRS).

2.2.7) Ley General del Sistema Financiero y del Sistema de Seguros [502]

La ley peruana que regula el sistema financiero y de seguros señala en su artículo 140º [503] que: *"está prohibido a las empresas del sistema financiero, así como a sus directores y*

[501] **[En línea] < http://www.indecopi.gob.pe/upload/cpc/tuo716.pdf > [consulta: 7 de Abril 2003].**

[502] **[En línea] < http://www.fsd.org.pe/normas/Ley.pdf > [consulta: 16 de Enero 2003].**

[503] Artículo modificado por la Ley 27.693 del año 2002, que crea la UIF-Perú.

trabajadores, suministrar cualquier información sobre las operaciones pasivas con sus clientes, a menos que medie autorización escrita de éstos o se trate de los supuestos consignados en los Artículos 142º y 143º" [504] . Asimismo, se encuentran obligados a observar el secreto bancario: 1) El Superintendente y los trabajadores de la Superintendencia, salvo que se trate de la información respecto a los titulares de cuentas corrientes cerradas por el giro de cheques sin provisión de fondos; 2) Los directores y trabajadores del Banco Central de Reserva del Perú y, 3) Los directores y trabajadores de las sociedades de auditoría y de las empresas clasificadoras de riesgo (Art. 140º).

En materia de excepciones al deber de secreto, debemos recordar la norma constitucional del artículo 2 Nº 5, el cual dispone queel secreto bancario puede levantarse *"a pedido del Juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado"*. A nivel legal, cabe agregar que no rige el secreto tratándose de movimientos sospechosos de lavado de dinero o de activos, en cuyo caso las instituciones sobre las cuales pesa el deber de secreto están obligados a comunicar acerca de tales movimientos a la Unidad de Inteligencia Financiera (Art. 140 inciso final) [505] .

Resumidamente, la legislación financiera peruana establece el secreto bancario como regla general, pero sólo en la variante de las operaciones pasivas. Este deber cede en general ante los requerimientos de la justicia y, desde el año 2002, las excepciones se han abierto de manera exorbitante en favor de la Unidad de Inteligencia Financiera del Perú.

[504] El artículo 142, señala por su parte que el secreto bancario no impide el suministro de información de carácter global, particularmente en los siguientes casos: *"1. Cuando sea proporcionada por la Superintendencia al Banco Central y a las empresas del sistema financiero para: I. Usos estadísticos.* II. La formulación de la política monetaria y su seguimiento. 2. Cuando se suministre a bancos e instituciones financieras del exterior con los que se mantenga corresponsalía o que estén interesados en establecer una relación de esa naturaleza. 3. Cuando la soliciten las sociedades de auditoría a que se refiere el numeral 1 del artículo 134º o firmas especializadas en la clasificación de riesgo. *4. Cuando lo requieran personas interesadas en la adquisición de no menos del treinta por ciento (30%) del capital accionario de la empresa. (…) No constituye violación del secreto bancario, la divulgación de información sobre las sumas recibidas de los distintos clientes para fines de liquidación de la empresa".* A su vez, el artículo 143 dispone que el secreto bancario no rige cuando la información sea requerida por: "1. Los jueces y tribunales en el ejercicio regular de sus funciones y con específica referencia a un proceso determinado, en el que sea parte el cliente de la empresa a quien se contrae la solicitud. 2. El Fiscal de la Nación, en los casos de presunción de enriquecimiento ilícito de funcionarios y servidores públicos o de quienes administren o hayan administrado recursos del Estado o de organismos a los que éste otorga soporte económico. 3. El Fiscal de la Nación o el gobierno de un país con el que se tenga celebrado convenio para combatir, reprimir y sancionar el tráfico ilícito de drogas o el terrorismo, o en general, tratándose de movimientos sospechosos de lavado de dinero o de activos, con referencia a transacciones financieras y operaciones bancarias ejecutadas por personas presuntamente implicadas en esas actividades delictivas o que se encuentren sometidas a investigación bajo sospecha de alcanzarles responsabilidad en ellas. 4. El Presidente de una Comisión Investigadora del Poder Legislativo, con acuerdo de la Comisión de que se trate y en relación con hechos que comprometan el interés público. *5. El Superintendente, en el ejercicio de sus funciones de supervisión. (…) En los casos de los numerales 2, 3 y 4, el pedido de información se canaliza a través de la Superintendencia. (…) Quienes accedan a información secreta en virtud de lo dispuesto en el presente artículo, están obligados a mantenerla con dicho carácter en tanto ésta no resulte incompatible con el interés público".*

3. Bienes Jurídicos Protegidos por la Legislación de Datos Personales

Dada la inexistencia de una ley general de protección de datos personales, sólo nos referiremos a las reglas constitucionales y a las leyes especiales recién vistas.

En materia constitucional, se ha señalado que para analizar los bienes jurídicos tutelados por el hábeas data, es necesario distinguir entre el derecho de acceso a la información pública (regulado por la Ley Nº 27.806) y el derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar (Art. 200 en relación con el Art. 2º Nº 6 C. Pol.). Respecto del primero, Eguiguren ha dicho que "en realidad, el derecho cautelado en esta norma corresponde a la libertad de acceso y conocimiento de la información, pública, destinado a favorecer la mayor y mejor participación e información general de los ciudadanos, así como la transparencia de la actuación y gestión de las entidades gubernamentales" [506] . Puccinelli por su parte, señala que "resulta obvio que se pretende tutelar el derecho a la información, y como consecuencia -al menos- la libertad de prensa y el sistema republicano" [507] . Para Sagüés -citado por Puccinelli- es obvio que también se protege "(…) todo el haz de derechos e intereses que el acceso a esa información permite ejercer (salud, ambiente, marcha de las instituciones, etc.)" [508] .

Respecto del segundo supuesto de hábeas data, el propio -que es el que nos interesa-, se ha dicho por Puccinelli que no aparece tan simple señalar el bien jurídico protegido, en especial por los alcances técnicos de ese derecho en el sistema jurídico peruano, los cuales podrían definir un perfil de hábeas data tanto de carácter amplio como uno de carácter reducido [509] . Por su parte, Morales Godós señala que en Perú "se

[505] Se agrega por la Ley de Inteligencia Financiera, que no incurren en responsabilidad legal: *"la empresa y/o sus trabajadores que, en cumplimento de la obligación contenida en el presente artículo, hagan de conocimiento de la Unidad de Inteligencia Financiera, movimientos o transacciones sospechosas que, por su naturaleza, puedan ocultar operaciones de lavado de dinero o de activos. La autoridad correspondiente inicia las investigaciones necesarias y, en ningún caso, dicha comunicación puede ser fundamento para la interposición de acciones civiles, penales e indemnizatorias contra la empresa y/o sus funcionarios"* (Artículo 140 inciso 4º). Asimismo, tampoco incurren en responsabilidad *"quienes se abstengan de proporcionar información sujeta al secreto bancario a personas distintas a las referidas en el Artículo 143º. Las autoridades que persistan en requerirla quedan incursas en el delito de abuso de autoridad tipificado en el Artículo 376º del Código Penal"* (Artículo 140 inciso 5º).

[506] Agrega que "en todo caso, si bien esta extensión del Hábeas data a la protección del derecho referido se aparta de los cánones más ortodoxos y difundidos del instituto (por lo que podría ser objetado por cierta falta de coherencia o "pureza" conceptual) es verdad también que ello no ofrece mayores problemas o perjuicios que ameriten un severo cuestionamiento". Eguiguren Praeli, Francisco J., *op. cit.*, págs. 126 y 127.

[507] Puccinelli, Óscar, *op. cit*., pág. 586.

[508] *Ibídem.*

[509] *Ibídem*.

ha puesto el acento en la defensa ante la intromisión de terceras personas en los aspectos propios de la vida privada, y en el control de la información o divulgación de algún hecho concerniente a la intimidad; sin embargo, no se han desarrollado ciertos aspectos, como el relativo a la autonomía, que cobra importancia para el hombre contemporáneo, por cuanto implica la posibilidad de adoptar las decisiones más importantes de su existencia, libre de manipulaciones (…)" [510] . Eguiguren, indirectamente se ha referido al tema señalando al respecto que "(…) la norma constitucional se limitaría, si nos atenemos a su tenor literal, a proteger a la persona, evitando que los servicios informáticos suministren datos o informaciones que afectan la intimidad personal, desatendiendo aparentemente todas las otras posibilidades de cobertura de este derecho. Incluso podría pretenderse dejar fuera de la prohibición la difusión de datos que, sin vulnerar la intimidad personal o familiar, pueden conllevar formas de discriminación o contribuir a ésta" [511] . De lo anterior, se puede deducir que del hábeas data constitucional peruano difícilmente puede predicarse que protegería el derecho a la autodeterminación informativa dada su estrechez, el cual a lo más tutelaría otros derechos, como la intimidad de las personas y la vida privada. Con todo, Puccinelli, concluye que a pesar del miopismo del Constituyente al consagrar el hábeas data, los demás derechos no contemplados expresamente deberán tutelarse aún frente a los servicios informatizados, por la vía del amparo, si la judicatura peruana no adopta una posición aperturista. Por nuestra parte, agregamos a lo dicho por este autor en 1999, que esa miopía constitucional, ha sido parcialmente corregida por vía legal, al menos en materia de datos personales de carácter comercial y económico a través de la Ley de CEPIRS del año 2001, la cual consagra los derechos de acceso, modificación, cancelación, rectificación y actualización de la información difundida por las CEPIRS y que resulte ilegal, inexacta, errónea o caduca (Art. 13 Ley de CEPIRS). Por lo tanto, si bien en materia constitucional pareciera ser que se está más cerca de la tutela del derecho a la intimidad, en materia legal, específicamente en la Ley de CEPIRS, se estaría más cerca al bien jurídico autodeterminación informativa, lo cual es un logro en este ámbito normativo. Cabría entonces compatibilizar tanto las disposiciones constitucionales como legales para tener una visión sistémica del ordenamiento jurídico peruano. La tarea en esta materia no es fácil, pues se requiere conocer de más antecedentes del sistema jurídico en estudio, así como estar al tanto de los fundamentos legislativos de la ampliación de la protección a los datos personales, cuestión que excede los límites de nuestra investigación.

4. Principios Informativos de la Legislación de Protección de Datos Personales

Ante la falta de legislación general en materia de protección de datos personales, nos referiremos a los principios informativos de la legislación especial que regula las Centrales Privadas de Información de Riesgos así como también la protección de los titulares de la información (Ley de CEPIRS).

510 *Ídem*, pág. 587.

511 Eguiguren Praeli, Francisco J., *op. cit.*, pág. 128.

1º. Principio de la licitud y lealtad de los archivos de datos

La Ley de CEPIRS contempla una disposición de la cual se desprende claramente este principio. Al efecto, el artículo 9º señala en relación a la información de riesgo que: "*a) La recolección de información no podrá efectuarse por medios fraudulentos o ilícitos;(…)".*

2º. Principio de la calidad de los datos

Este principio ya se visualiza en el artículo 1º de la Ley al hablar sobre su objeto, cuando dice que éste, es regular el suministro de información de riesgos en el mercado, garantizando el respeto a los derechos de los titulares de la misma, reconocidos por la Constitución Política del Perú y la legislación vigente, *"promoviendo la veracidad"*, confidencialidad y uso apropiado de dicha información. Por otra parte, el artículo 9 también lo contempla al señalar los "lineamientos generales" del tratamiento de datos personales cuando señala que: *"(…) c) La información que deberá constar en los reportes informativos será lícita, exacta y veraz, de forma tal que responda a la situación real del titular de la información en determinado momento".*

3º. Principio del consentimiento informado del titular de los datos

El principio del consentimiento informado del titular de los datos no aparece claro en esta ley pues se dispone como regla general en el artículo 7.1que: *"las CEPIRS podrán recolectar información de riesgos para sus bancos de datos tanto de fuentes públicas como de fuentes privadas, sin necesidad de contar con la autorización del titular de la información, entendiéndose que la Base de Datos se conformará con toda la información de riesgo".* Sólo en caso que las CEPIRS recolecten información de riesgos directamente de los titulares, deben cumplir con ciertos deberes de información acerca de: *"(…) a) La existencia del banco de datos, la finalidad de la recolección de la información y los potenciales destinatarios de ésta; b) La identidad y dirección de la CEPIR que recolecta la información; c) El carácter facultativo de sus respuestas a las preguntas que le sean planteadas; d) Las posibles consecuencias de la obtención de la información; y, e) El alcance de los derechos desarrollados en el Título Cuarto de la presente Ley, así como de los procedimientos para hacerlos valer"* (Art. 8º).

Por lo tanto, estimamos que aunque no se reconozca de manera precisa y clara el principio del consentimiento previo del titular de los datos, bien puede deducirse del deber de información señalado por la Ley, pues éste sólo se exige en los casos en que el titular ha prestado su consentimiento para el tratamiento de sus datos, por lo cual el principio estaría implícito en esa regla.

4º. Principio de la seguridad de los datos

Respecto de este principio, podemos decir que se encuentra reconocido en dos disposiciones. La primera, al establecer que las CEPIRS deben contar como mínimo con: *"(…) c) Controles internos que proporcionen seguridad en el desarrollo de sus actividades, así como procedimientos de validez de la información procesada"* (Art. 5º). La segunda, al señalar en el artículo 12º que las CEPIRS *"deberán adoptar las medidas*

de índole técnica y administrativa destinadas a garantizar la seguridad de la información que manejen, a fin de evitar su alteración, pérdida, tratamiento o acceso no autorizado".

5º. Principio de la confidencialidad de los datos

En relación a este principio, debemos decir que se contempla en el artículo 1º aunque no es desarrollado por la Ley. La disposición pertinente señala que el objeto de la Ley es regular el suministro de información de riesgos en el mercado, garantizando el respeto a los derechos de los titulares de la misma, reconocidos por la Constitución Política del Perú y la legislación vigente, promoviendo la veracidad, *"confidencialidad"* y uso apropiado de dicha información.

6º. Principio del consentimiento para la cesión de datos

Este principio estaría reconocido implícitamente en los casos que las CEPIRS recolecten información de riesgos directamente de los titulares, pues necesariamente deben informar, entre otras cosas, la existencia del banco de datos, la finalidad de la recolección de la información y *"los potenciales destinatarios de ésta"* (Art. 8º). Por lo tanto, en esta última frase entendemos incluido el principio en comento.

7º. Principio de la finalidad

En lo relativo a este principio, cabe remitirse a lo recién señalado en el principio del consentimiento para la cesión de datos, pues el mismo artículo 8º contiene al principio de la finalidad para esos casos.

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

En atención a la inexistencia de una ley general de protección de datos en el ordenamiento jurídico peruano, no se abordará este punto.

6. Modelos de Tutela

La configuración constitucional del hábeas data, como se recordará, distingue entre el derecho a solicitar sin expresión de causa información de cualquier entidad pública (Art. 2º Nº 5), y el derecho a quelos servicios informáticos no suministren informaciones que afecten la intimidad personal y familiar (Art. 2º Nº 6). El legislador por su parte, se ha ocupado de regular el ejercicio de los derechos respectivos a nivel administrativo o prejudicial, previo a la interposición de la acción constitucional de hábeas data regulada por la Ley Nº 26.301, estableciendo dos cuerpos legales que se ocupan de ello; uno de carácter general, que regula el ejercicio del derecho de acceso a la información pública (Ley Nº 27.806), y otro de carácter sectorial, que regula el ejercicio de los derechos de acceso, rectificación, cancelación y supresión previstos en la Ley de CEPIRS (Nº 27.489).

De lo recién señalado se desprende que, para ejercer el derecho de acceso a la

información pública (dentro del cual debemos considerar incluido el derecho de acceso a los datos personales en poder de los organismos del Estado), debe seguirse el procedimiento administrativo y agotar esta vía antes de entablar la acción de hábeas data ante el juez competente. A su vez, el ejercicio de los derechos de los titulares de los datos tratados por las CEPIRS debe realizarse según el procedimiento informal o extrajudicial señalado en la ley, también como vía previa al ejercicio de la acción de hábeas data ante el juez competente. Con ello, la acción constitucional de hábeas data pasa a ser la vía subsidiaria ante desfavorables resultados en las instancias informales y administrativas.

Respecto de las materias en que no existe una regulación legal especial que establezca mecanismos informales o prejudiciales para hacer valer los derechos que protege el hábeas data, estimamos que cabría hacer aplicación directa de la Ley 26.301 y, por lo tanto ejercer el hábeas data según el procedimiento señalado por aquélla.

A continuación, sólo se analizará la regulación legal del procedimiento judicial contemplado en la Ley Nº 26.301 de 1994, que regula transitoriamente la aplicación de la acción constitucional de hábeas data. Lo anterior, dado que los procedimientos previos a esta acción establecidas en leyes especiales, ya se reseñaron al analizar cada ley en particular (punto Nº 2 de este análisis).

6.1 La Acción de Hábeas Data

Como ya se ha dicho, esta acción se contempla a nivel constitucional en el artículo 200 Nº 3. En efecto, se dispone por éste que son garantías constitucionales: *"(…) 3. La Acción de Hábeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el Artículo 2º, incisos 5 y 6 de la Constitución".* El artículo 2º N º5 prescribe por su parte, que toda persona tiene derecho a ***"*** *solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional".* A su vez el artículo 21 Nº 6 señala que: *"toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar".* A partir de esta consagración constitucional, la Ley Nº 26.301 de 1994 se ocupa de manera transitoria de regular el hábeas data. Esta escueta ley señala en el artículo 3º que para la tramitación y conocimiento de la Garantía Constitucional de la Acción de Hábeas Data serán de aplicación supletoria, las disposiciones pertinentes de la Ley de Amparo Nº 23.506. Por lo tanto, en lo no regulado por aquélla deberá suplirse con lo dispuesto en la Ley de Amparo.

6.1.1) Procedencia de la Acción

De lo prescrito en la Constitución, se desprende que la acción procedería al menos ante dos situaciones:

1º) Ante el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnere o amenace el derecho asolicitar sin expresión de causa la información que

requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Salvo, en los casos que la información solicitada afecte la intimidad personal y en aquéllos que expresamente se excluyan por la ley o por razones de seguridad nacional (Art. 200 Nº 3, en relación con el artículo 2º Nº 5 C. Pol.).

2º)Ante el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnere o amenace el derecho de toda persona a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar (Art. 200 Nº 3, en relación con el artículo 2º Nº 6 C. Pol.).

Hemos dicho que procederían, al menos, por cuanto el legislador ha desarrollado consecuentemente a nivel sectorial la garantía del hábeas data (Ley de CEPIRS), que reconoce no sólo el derecho de acceso, sino que también los derechos de rectificación, modificación, cancelación y actualización de datos tratados por las CEPIRS, los cuales sin duda, sobrepasan la sola consideración de la vulneración del derecho a la intimidad. En razón de lo anterior, estimamos que a pesar de la aparente restricción a la procedencia del hábeas data respecto de los servicios informatizados, debe interpretarse extensivamente la disposición constitucional, acorde con la entidad de la garantía tutelada. Con ello, se ganaría en el resguardo de los derechos reconocidos por el Constituyente, sea intimidad, sea vida privada. Refuerza esta postura interpretativa extensiva de la garantía, la disposición constitucional del artículo 3º el cual señala: *"la enumeración de los derechos establecidos en este capítulo no excluye los demás que la Constitución garantiza, ni otros de naturaleza análoga o que se fundan en la dignidad del hombre, o en los principios de soberanía del pueblo, del Estado democrático de derecho y de la forma republicana de gobierno".*

Por lo tanto, creemos que a pesar de la estrechez del texto constitucional en materia de hábeas data, una interpretación sistemática de la Constitución en relación con a la legislación especial de las CEPIRS, servirían de base para ampliar la procedencia general de la acción de hábeas data. La tarea queda entregada en definitiva a la jurisprudencia en tanto no se modifique la Carta Fundamental y se dicte la ley definitiva que regule la acción en comento.

6.1.2) Legitimación Activa

En materia de legitimación activa del hábeas data, la Ley 26.301 nada dice, pero se deduce de las disposiciones constitucionales que pueden ejercitarla *"todas las personas"*. Por su parte, la Ley de Amparo señala en el artículo 26° que: *"tienen derecho a ejercer la acción de Amparo el afectado, su representante, o el representante de la entidad afectada".* Cabe agregar, que la Ley 26.520 (Ley Orgánica de la Defensoría del Pueblo, publicada el 8 de agosto de 1995) dispone en su artículo 9º, inciso 2º que el Defensor del Pueblo está facultado en el ejercicio de sus funciones para: *"(...) Interponer la acción de hábeas corpus, acción de amparo, acción de hábeas data, la de acción popular y la acción de cumplimiento, en tutela de los derechos constitucionales y fundamentales de la persona y la comunidad (...)"* [512] .

[512] [En línea] < http://www.cajpe.org.pe/rij/bases/legisla/peru/23506c.htm > [consulta: 7 de Abril 2003].

6.1.3) Legitimación Pasiva

De las disposiciones constitucionales se desprende que los sujetos pasivos de la acción de hábeas data serían:

1) *En el caso del acceso a la información pública*:, la autoridad, funcionario o persona, que vulnera o amenaza el derecho asolicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido.

2) *En el caso del Nº 6 del artículo 2º de la Constitución*:, la autoridad, funcionario o persona, que vulnera o amenaza el derecho de toda persona a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

6.1.4) Competencia

La Ley 26.301 señala en su artículo 1º que la acción se tramitará ante el Juez de Primera Instancia en lo Civil de turno, del lugar en donde tiene su domicilio el demandante, o donde se encuentran ubicados los archivos mecánicos, telemáticos, magnéticos, informáticos o similares, o en el que corresponda al domicilio del demandado, sea esta persona natural o jurídica, pública o privada, a elección del demandante. Agrega esta Ley que si la afectación de derechos se origina en archivos judiciales, sean jurisdiccionales, funcionales o administrativos, cualquiera sea la forma o medio en que estos estén almacenados, guardados o contenidos, conocerá de la demanda la Sala Civil de turno de la Corte Superior de Justicia respectiva, la que encargará a un Juez de Primera Instancia en lo Civil su trámite. El fallo en primera instancia, en este caso, será pronunciado por la Sala Civil que conoce de la demanda. Este mismo precepto regirá para los archivos funcionales o administrativos del Ministerio Público (Art. 2º inciso 2º Ley 26.301).

6.1.5) Procedimiento Aplicable

La ley transitoria señala al respecto en el artículo 3º que: *"para la tramitación y conocimiento de la Garantía Constitucional de la Acción de Hábeas Data serán de aplicación, en forma supletoria, las disposiciones pertinentes de la Ley 23.506, 25.011, 25.315, 25.398 y el Decreto Ley 25.433, en todo cuanto se refiera a la Acción de Amparo; con excepción de lo dispuesto en el artículo 11o. de la Ley 23.506".* Por lo tanto, la ley transitoria se remite a la Ley de Amparo en materia de tramitación del hábeas data. A continuación se señalará brevemente el procedimiento del hábeas data.

1) *Procedencia*: el artículo 27 de la Ley de Amparo Nº 23.506 (en adelante LDA) [513] señala que: *"sólo procede la acción de Amparo cuando se hayan agotado las vías previas".* Al respecto la Ley 26.301 dispone en el artículo 5º que para los efectos de las Garantías Constitucionales de Acción de Hábeas Data y Acción de Cumplimiento, además de lo previsto en el art. 27º de la LDA y su Complementaria, *"constituye vía previa en el caso de la Acción de Hábeas Data basada en los incisos 5 y 6 del Artículo*

[513] [En línea] < http://www.cajpe.org.pe/rij/bases/legisla/peru/23506c.htm > [consulta: 23 de Abril 2003].

2o. de la Constitución Política del Estado el requerimiento por conducto notarial con una antelación no menor a quince días calendarios, con las excepciones previstas en la Constitución Política del Estado y en la Ley". Por su parte, dispone en el artículo 28 que no será exigible el agotamiento de las vías previas si: 1) Una resolución, que no sea la última en la vía administrativa, es ejecutada antes de vencerse el plazo para que quede consentida; 2) Por el agotamiento de la vía previa pudiera convertirse en irreparable la agresión; 3) La vía previa no se encuentra regulada, o si ha sido iniciada, innecesariamente por el reclamante, sin estar obligado a hacerlo y, 4) Si no se resuelve la vía previa en los plazos fijados para su resolución.

2) *Traslado*: el artículo 30 (LDA) señala que interpuesta la demanda de Amparo, el juez correrá traslado por tres días al autor de la infracción.

3) *Medidas cautelares*: el artículo 31 (LDA) dispone que a solicitud de parte, en cualquier etapa del proceso y siempre que sea evidente la inminente amenaza de agravio o violación de un derecho constitucional, por cuenta, costo y riesgo del solicitante, el juez podrá disponer la suspensión del acto que dio origen al reclamo. De la solicitud se corre traslado por el término de un día, tramitando el pedido como incidente en cuerda separada, con intervención del Ministerio Público. Luego, con la contestación expresa o ficta, el juez o la Corte Superior resolverá dentro del plazo de dos días, bajo responsabilidad. La resolución que dicta el juez, o en su caso, la Corte será recurrible en doble efecto ante la instancia superior, la que resolverá en el plazo de tres días de elevados los autos bajo responsabilidad.

6.1.6) La Sentencia

El artículo 32º de la LDA, señala que con la contestación de la demanda o sin ella, el juez resolverá la causa dentro de los tres días de vencido el término para la contestación, bajo responsabilidad.

Por su parte, el artículo 2º de la Ley 26.301 dispone en términos bastante criticables que: *"la sentencia consentida o ejecutoriada, se limitará a ordenar la publicación de la rectificación previamente solicitada por el demandante, y que este deberá acompañar necesariamente a su demanda, sin cuyo requisito no será admitida, guardando la correspondiente proporcionalidad y razonabilidad, en forma gratuita, de modo inmediato al cumplimiento de lo ejecutoriado en el plazo de tres días, bajo apercibimiento de Ley"*. El inciso 2º agrega que, la discrepancia en torno a la rectificación, su proporcionalidad y su contenido, *"será decidida por el Juez, o la Sala Civil correspondiente, previo traslado al demandado por el término de tercero día, debiendo el Juez corregir o restringir la rectificación solicitada cuando la misma implique réplica u opinión excediendo los límites de la mera rectificación".* Finalmente se señala que esta decisión es apelable en un sólo efecto o sin efecto suspensivo.

En relación al limitado alcance de la sentencia de hábeas data, creemos que la estrechez de ésta, si bien obedece a la configuración constitucional del instituto, debe ser superada. Estimamos que los jueces deberían adecuar la extensión del fallo a los derechos contenidos en la Ley de CEPIRS y no limitarse a ordenar la sola publicación de la rectificación de la información, sino que ordenar todo lo que de derecho corresponda al

titular de los datos personales, sea éste un derecho de acceso, rectificación, cancelación o actualización de la información, según se señale por el actor en el petitorio de su demanda.

6.2 Otras Acciones

En cuanto a otras acciones que tutelen los datos personales, debemos hacer presente que la Ley de CEPIRS contempla un procedimiento judicial en el artículo 17º aplicable a los titulares de datos personales que no sean considerados consumidores para los efectos de la Ley de Protección al Consumidor, quienes *"podrán solicitar judicialmente la tutela de los derechos enunciados en este Subtítulo en la vía del proceso sumarísimo".* Al efecto, se señala por el artículo17.2 que para poder interponer una demanda con el fin de que se modifique, cancele o rectifique una información de riesgos que se considere ilegal, inexacta, errónea o caduca, *"el titular de dicha información deberá previamente obtener un pronunciamiento, expreso o tácito, denegando una solicitud de revisión o de rectificación, tramitada conforme a lo dispuesto en los artículos 15º y 16º de la presente Ley".*

Respecto de esta vía judicial, la ley de CEPIRS no otorga más información que la ya señalada. Por último, y en relación a la coexistencia de esa acción y la acción constitucional de hábeas data, nada se dice al respecto, con lo cual eventualmente podrían producirse conflictos a la hora de ejercer esta última. Con todo, pensamos que es más específica la acción de tutela consagrada por el artículo 17 de la Ley de CEPIRS que la propia acción de hábeas data regulada por la Ley 26.301.

7. Mecanismos de Control

En esta materia, no existe un órgano de control que vele por el cumplimiento de una ley general de protección de datos personales, pues no existe tal en el ordenamiento jurídico peruano. A pesar de ello, la Ley de CEPIRS en el artículo 21 otorga competencia a la Comisión de Protección al Consumidor del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), como órgano administrativo, para conocer de las infracciones a la Ley e imponer tanto sanciones administrativas como medidas correctivas a las que hubiere lugar. En este caso, estimamos que la señalada Comisión actuaría en alguna medida como órgano de control, restringido sólo al ámbito de la Ley de CEPIRS.

8. Transmisión Internacional de Datos

El ordenamiento jurídico peruano, no prevé una legislación general que se ocupe de la materia. Sin embargo, existe una norma aislada relativa al tema; el artículo 15 de la Ley 27.693 que crea la Unidad de Inteligencia Financiera del Perú (UIF). Esta disposición, establece que: *"la UIF podrá colaborar o intercambiar información con las autoridades competentes de otros países que ejerzan competencias análogas, en el marco de convenios y acuerdos internacionales suscritos en materia de lavado de dinero o de*

activos". Se añade por ésta que: *"la colaboración e intercambio de información con las autoridades competentes de otros países se condicionará a lo dispuesto en los tratados y convenios internacionales y, en su caso, al principio general de reciprocidad y al sometimiento por las autoridades de dichos países a las mismas obligaciones sobre secreto profesional que rigen para las nacionales"* (Art. 15º).

De lo anterior, se desprende una clara intención de traspasar las fronteras con información personal en aras de la prevención y detección del delito de lavado de activos o lavado de dinero. No queda claro finalmente si en definitiva es requisito *sine qua non* para que opere legalmente una transmisión internacional de datos, el que exista una tratado o convenio internacional que lo autorice o, si bastaría con un acuerdo entre autoridades bajo el principio de la reciprocidad. En esta materia nos inclinamos por restringir tal facultad sólo al legislador y no a la autoridad administrativa.

9. Régimen de Responsabilidad

En materia de responsabilidad, a falta de una ley de carácter general de protección de datos personales que se ocupe de establecer reglas de aplicación específica en la materia, cabe circunscribirse a las normas contempladas en los estatutos legales especiales, sectoriales y en la legislación común. En este sentido, podemos señalar que de las leyes analizadas, tanto la Ley de CEPIRS (ley sectorial compleja) como la Ley de Acceso a la Información Pública (ley especial) establecen reglas específicas en materia de responsabilidad. Por otro lado, los demás estatutos sectoriales ya vistos en el punto Nº 2.2 también establecen algunas sanciones para el evento de ser violadas las normas que señalan deberes de reserva o confidencialidad de cierta información (Código Tributario, Ley de Inst. Financieras, etc.).

9.1 Responsabilidad Administrativa

Como ya se ha dicho, Perú no cuenta con una ley de protección de datos personales de carácter general. Sin embargo, dispone de una ley especial que regula el hábeas data respecto de los registros públicos, y de una ley sectorial compleja, la Ley de CERPIRS. Esos estatutos a su vez contemplan normas de responsabilidad administrativa. Por otra parte, como se vio, también existen algunas normas sectoriales que establecen deberes de secreto o reserva de cierta información respecto de las cuales también se prevén sanciones para el incumplimiento de aquéllos.

9.1.1) Ley que Regula las Centrales Privadas de Información de Riesgos y de Protección al Titular de la Información (Ley de CEPIRS)

El artículo 20 de esta Ley, establece un catálogo de conductas constitutivas de infracciones administrativas en las cuales pueden incurrir las CEPIRS, señalándose al efecto las siguientes:

a) Negarse a facilitar el acceso de un consumidor a la información de riesgos de la que es titular;

b) Denegar una solicitud de revisión o una solicitud de rectificación de la información de riesgos de la que es titular un consumidor;

c) Negarse a modificar o a cancelar la información de un titular luego de que éste haya tenido un pronunciamiento favorable en un procedimiento seguido de conformidad con lo establecido en el artículo 15 de la presente Ley (ver *supra* punto Nº 2.2.1) ;

d) No actualizar la información por la no inclusión de registros de pagos totales o parciales a que se refiere el numeral 15.6 del artículo 15;

e) No haberse remitido la información a las CEPIRS en el plazo estipulado en el numeral 15.7 del artículo 15 y,

f) No actualizar los reportes de crédito en el plazo señalado en el numeral 15.8 del artículo 15.

El inciso 2º del artículo 20, agrega que las CEPIRS *"son objetivamente responsables por incurrir en las infracciones antes tipificadas"*, sin perjuicio de la responsabilidad que pudiera corresponder a las fuentes de las que hubieran recolectado información, de ser el caso, *"conforme a las disposiciones contenidas en el Decreto Legislativo Nº 716, Ley de Protección al Consumidor".* De esta disposición, se desprende una regla muy importante; se prescindirá de cualquier elemento subjetivo para determinar si se cometió infracción o no. Es decir, no se permitirá que las CEPIRS puedan alegar que actuaron con la debida diligencia, pues basta que se acredite alguna de las conductas señaladas por la ley, para que a la empresa se la sancione. Todo lo cual, se entiende sin perjuicio de la eventual responsabilidad de las fuentes que hayan recolectado la información ilegal, inexacta o errónea.

En cuanto a las sanciones propiamente tales, éstas deben ser aplicadas por la Comisión de Protección al Consumidor, pero no se señala en qué consisten, sino que se limita a decir *"a las que hubiere lugar"* (Art. 21.1 Ley de CEPIRS). Sin embargo, del texto de la ley se desprende que las reglas a las que se refiere serían las sanciones generales establecidas por la Ley de Protección al Consumidor, en atención a la remisión expresa hecha en el artículo 20, al decir que las CEPIRS son objetivamente responsables *"(…) conforme a las disposiciones contenidas en el Decreto Legislativo Nº 716, Ley de Protección al Consumidor"* [514] .

Por otra parte la Ley de CEPIRS prevé la aplicación de medidas correctivas en caso de infracción a sus normas. Al efecto, se dispone en el artículo 22 que, sin perjuicio de las

[514] A este respecto, el artículo 40 de la Ley de Protección al Consumidor dispone que los proveedores son objetivamente responsables por infringir las disposiciones contenidas en la presente Ley. *"(…) Los proveedores infractores podrán ser sancionados administrativamente con una Amonestación o con una Multa, hasta por un máximo de 100 (cien) Unidades Impositivas Tributarias, sin perjuicio de las medidas correctivas a que se refiere el artículo siguiente, que se dicten para revertir los efectos que las conductas infractoras hubieran ocasionado o para evitar que éstas se produzcan nuevamente en el futuro.(…) La imposición y la graduación de la sanción administrativa a que se refiere el párrafo precedente serán determinadas atendiendo a la gravedad de la falta, el daño resultante de la infracción, los beneficios obtenidos por el proveedor, la conducta del infractor a lo largo del procedimiento, los efectos que se pudiesen ocasionar en el mercado y otros criterios que, dependiendo del caso particular, considere adecuado adoptar la Comisión. Las multas impuestas constituyen en su integridad recursos propios del INDECOPI, salvo por lo dispuesto en el artículo 45 de la presente Ley".*

sanciones administrativas a que hubiere lugar, la Comisión de Protección al Consumidor impondrá a las CEPIRS que incurran en alguna infracción a la presente Ley, las siguientes medidas correctivas: *"a) La modificación o cancelación de la información de riesgos registrada en sus bancos de datos; y, b) La rectificación de la información comercial de riesgos difundida en el mercado, por cuenta y costo del infractor, en la forma que determine la Comisión".*

Finalmente, se señala en el inciso 2º del artículo 22 que adicionalmente a las sanciones administrativas a que hubiere lugar respecto de las CEPIRS, la Comisión de Protección al Consumidor *"impondrá sanciones a las fuentes proveedoras de la información que incurran en alguna infracción a la presente Ley y en general a terceras personas que han proporcionado información de riesgos a las CEPIRS que resulte ilegal, inexacta, errónea o caduca"* [515] .

9.1.2) Ley de Transparencia y Acceso a la Información Pública

El artículo 4º de esta Ley, que regula la acción de hábeas data respecto de los archivos públicos, prescribe que todas las entidades de la Administración Pública quedan obligadas a cumplir lo estipulado en la presente norma, agregando que: *"Los funcionarios o servidores públicos que incumplieran con las disposiciones a que se refiere esta Ley serán sancionados por la comisión de una falta grave, pudiendo ser incluso denunciados penalmente por la comisión de delito de Abuso de Autoridad a que hace referencia el Artículo 377° del Código Penal".*

Por su lado, el artículo 14 señala que el funcionario público responsable de dar información *"que de modo arbitrario obstruya el acceso del solicitante a la información requerida, o la suministre en forma incompleta u obstaculice de cualquier modo el cumplimiento de esta Ley, se encontrará incurso en los alcances del Artículo 4° de la presente Ley".*

En suma, la Ley de Acceso a la Información Pública establece como faltas graves la violación de los deberes señalados por ese cuerpo normativo. Las sanciones específicas deben buscarse en los respectivos estatutos funcionarios, cuestión que no se abordará, pues excede los ámbitos de nuestro estudio.

9.1.3) Ley General del Sistema Financiero y del Sistema de Seguros

El artículo 141 de esta ley sectorial, señala que sin perjuicio de la responsabilidad penal que prevista en el artículo 165 del Código Penal, *"la infracción a las disposiciones de este capítulo se considera falta grave para efectos laborales y, cuando ello no fuere el caso, se sanciona con multa"*. Es decir, la violación a los deberes de secreto de las operaciones bancarias pasivas, tiene una sanción administrativa sin perjuicio de la responsabilidad penal.

[515] Se agrega que: *"la modificación, actualización, rectificación o cancelación de la información de riesgos antes indicada que se encuentre registrada en sus bases de datos se actualizará dentro del día siguiente de notificada la medida"* (Artículo 22º inciso final).

9.1.4) Código Tributario

En materia de secreto fiscal o tributario el inciso final del artículo 186 dispone que: *"(…) serán sancionados con suspensión o destitución, de acuerdo a la gravedad de la falta, los funcionarios y trabajadores de la Administración Tributaria que infrinjan lo dispuesto en los Artículos 85º y 86º".* Es decir, se sancionará con tales medidas a aquellos funcionarios que violen el deber de secreto que pesa sobre éstos.

9.2 Responsabilidad Civil

En esta materia, sólo nos referiremos a las reglas contenidas en la Ley de CEPIRS, dada la falta de un estatuto de protección general a los datos personales que establezca reglas especiales. Para los supuestos de daño distintos a los contemplados por esta ley, debe estarse a las reglas generales de la responsabilidad. En el caso de la responsabilidad civil extracontractual, ella se rige por los artículos 1.969 y siguientes del Código Civil peruano [516] . La responsabilidad civil contractual por su parte se regula por las disposiciones de la Sección Segunda "Efectos de las obligaciones", Título "Inejecución de obligaciones", en especial por el artículo 1.321 [517] .

La Ley que regula las Centrales Privadas de Información de Riesgos y de Protección al Titular de la Información dispone en el artículo 18.1 que: *"La responsabilidad civil de las CEPIRS por los daños ocasionados al titular por efecto del tratamiento o difusión de información será objetiva. Las CEPIRS podrán repetir contra las fuentes proveedoras de información cuando el daño sea ocasionado como consecuencia del tratamiento de información realizada por éstas".*

Luego, el artículo 18.2 señala que: "*igualmente existe responsabilidad por parte de los usuarios o receptores de información de riesgos proporcionada por las CEPIRS, en caso de utilización indebida, fraudulenta o de modo que cause daños al titular de la información, la misma que se determinará conforme a las normas de responsabilidad civil y penal a que hubiese lugar. Sin perjuicio de lo anterior, las CEPIRS podrán repetir contra los usuarios o receptores de información en caso de haber asumido responsabilidad frente al titular de la información o terceros, en los supuestos antes indicados en que esté*

[516] El artículo 1.969 del Código Civil del Perú dispone que: *"Aquel que por dolo o culpa causa un daño a otro está obligado a indemnizarlo. El descargo por falta de dolo o culpa corresponde a su autor".* Por otra parte el artículo siguiente prescribe que: *"Aquel que mediante un bien riesgoso o peligroso, o por el ejercicio de una actividad riesgosa o peligrosa, causa un daño a otro, está obligado a repararlo"* (Art. 1970). Esta última disposición podría tener una aplicación especial si se estimara que la actividad que realizan las CEPIRS es riesgosa o peligrosa. [En línea] < http://www.leyes.congreso.gob.pe/Imagenes/Codigos/1010807++.pdf > [consulta: 24 de Abril 2003].

[517] El artículo 1.321 del Código Civil señala por su parte que: *"Queda sujeto a la indemnización de daños y perjuicios quien no ejecuta sus obligaciones por dolo, culpa inexcusable o culpa leve. (…) El resarcimiento por la inejecución de la obligación o por su cumplimiento parcial, tardío o defectuoso, comprende tanto el daño emergente como el lucro cesante, en cuanto sean consecuencia inmediata y directa de tal inejecución. (…) Si la inejecución o el cumplimiento parcial, tardío o defectuoso de la obligación, obedecieran a culpa leve, el resarcimiento se limita al daño que podía preverse al tiempo en que ella fue contraída". Ídem.*

involucrada la responsabilidad de los usuarios o receptores de información".

De las reglas anteriores, concluimos que la Ley establece dos regímenes de responsabilidad civil; uno de carácter objetivo o estricto, sólo aplicable a las CEPIRS y, otro de responsabilidad por culpa o negligencia, aplicable tanto a los usuarios como a los receptores de los reportes de crédito que hagan una utilización indebida o fraudulenta de la información transmitida. En el primer caso, la responsabilidad de las CEPIRS es independiente del grado de culpabilidad con el que hayan actuado. Es decir, ante todo evento dañoso que sea consecuencia de una actuación o una omisión por parte de esas empresas, se responderá civilmente por los daños y perjuicios causados. En cambio en el caso de la responsabilidad civil de los usuarios o receptores de los reportes de crédito, el actor deberá acreditar la culpa para que sea procedente la indemnización de los perjuicios causados.

9.3 Responsabilidad Penal

En materia penal, podemos afirmar que no existen disposiciones especiales relacionadas con la protección a los datos personales. En razón de lo anterior, se señalarán los tipos penales previstos por la legislación común (Código Penal) vinculados a la protección de los bienes jurídicos intimidad y vida privada [518] . De las normas contempladas por el Código Penal peruano destaca una disposición que se relaciona directamente con el tratamiento de datos sensibles a través de medios informáticos. Este es el artículo 157 intitulado "Uso indebido de archivos computarizados", el cual prescribe lo siguiente:

Artículo 157.- *"El que, indebidamente, organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida íntima de una o más personas, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años.*

Si el agente es funcionario o servidor público y comete el delito en ejercicio del cargo, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme al artículo 36º, incisos 1, 2 y 4".

La disposición anterior, sin duda establece una prohibición de utilización indebida de archivos de datos personales de carácter sensible, de la cual deducimos en principio, una prohibición de tratamiento de este tipo de datos. Lo anterior guardaría relación con la disposición del artículo 10º letra a) de la Ley de CEPIRS (estatuto sectorial complejo), la cual señala que estas empresas no podrán contener en sus bases de datos ni podrán difundir en sus reportes de crédito información sensible. Con todo, el alcance dogmático de esta disposición no es posible dilucidarlo en esta sede pues se requiere de un detenido estudio no sólo de la disposición particular, sino también de las fuentes y motivos legislativos, cuestión que sobrepasa los márgenes de este estudio.

De las demás disposiciones del Código Penal encaminadas a tutelar los bienes jurídicos intimidad y vida privada, podemos señalar las siguientes:

a) Violación de la intimidad:

[518] [En línea] < http://www.unifr.ch/derechopenal/legislacion/pe/cpperuidx.htm > [consulta: 7 de Abril 2003].

Artículo 154.- *"El que viola la intimidad de la vida personal o familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios, será reprimido con pena privativa de libertad no mayor de dos años.*

La pena será no menor de uno ni mayor de tres años y de treinta a ciento veinte días-multa, cuando el agente revela la intimidad conocida de la manera antes prevista.

Si utiliza algún medio de comunicación social, la pena privativa de libertad será no menor de dos ni mayor de cuatro años y de sesenta a ciento ochenta días-multa".

b) Revelación de la intimidad personal y familiar:

Artículo 156.-*"El que revela aspectos de la intimidad personal o familiar que conociera con motivo del trabajo que prestó al agraviado o a la persona a quien éste se lo confió, será reprimido con pena privativa de libertad no mayor de un año".*

c) Violación de domicilio ***:***

Artículo 159.- *"El que, sin derecho, penetra en morada o casa de negocio ajena, en su dependencia o en el recinto habitado por otro o el que permanece allí rehusando la intimación que le haga quien tenga derecho a formularla, será reprimido con pena privativa de libertad no mayor de dos años y con treinta a noventa días-multa".*

d) Allanamiento ilegal de domicilio:

Artículo 160.- *"El funcionario o servidor público que allana un domicilio, sin las formalidades prescritas por la ley o fuera de los casos que ella determina, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años e inhabilitación de uno a dos años conforme al artículo 36º, incisos 1, 2 y 3".*

e) Violación de correspondencia:

Artículo 161.- *"El que abre, indebidamente, una carta, un pliego, telegrama, radiograma, despacho telefónico u otro documento de naturaleza análoga, que no le esté dirigido, o se apodera indebidamente de alguno de estos documentos, aunque no esté cerrado, será reprimido con pena privativa de libertad no mayor de dos años y con sesenta a noventa días-multa".*

f) Interferencia telefónica:

Artículo 162.- *"El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años.*

Si el agente es funcionario público, la pena privativa de libertad será no menor de tres ni mayor de cinco años e inhabilitación conforme al artículo 36º, incisos 1, 2 y 4".

g) Violación del secreto profesional:

Artículo 165.- *"El que, teniendo información por razón de su estado, oficio, empleo, profesión o ministerio, de secretos cuya publicación pueda causar daño, los revela sin consentimiento del interesado, será reprimido con pena privativa de libertad no mayor de dos años y con sesenta a ciento veinte días-multa".*

10. Conclusiones

El ordenamiento jurídico peruano contempla a nivel constitucional, una disposición que consagra parcialmente la garantía del hábeas data. El alcance de los derechos reconocidos, en principio se limitan al derecho de acceso a la información poseída por el Estado y, a impedir el suministro de informaciones que afecten la intimidad personal y familiar por parte de los servicios informáticos, sean éstos públicos o privados. Para hacer efectivos estos derechos, se ha dictado una escueta ley transitoria que regula deficientemente la acción del hábeas data.

En el ámbito infraconstitucional sustantivo, Perú no dispone de una legislación general de protección de datos personales. Sin embargo, se prevé un estatuto sectorial complejo que regula el mercado de la información crediticia (Ley de CEPIRS) en el cual no sólo se puede observar la ampliación de los derechos tutelados por el hábeas data constitucional, sino que también establece normas sustantivas imbuidas algunas de los principios contenidos en la Directiva 95/46 CE de protección de datos personales. En otros ámbitos sectoriales, en general, se prevén normas que establecen deberes de secreto de informaciones relacionadas con las operaciones financieras pasivas y con las informaciones proporcionadas a la administración tributaria por los contribuyentes. Por último, cabe señalar que la normativa que obliga a un número significativo de personas a informar de operaciones sospechosas a la Unidad de Inteligencia Financiera del Perú, si bien tiene un finalidad que es justificable (evitar el lavado de dinero), entrega al Estado a través de un órgano descentralizado, una gran cantidad y calidad de información, que de no mediar una estricta regulación, puede sin duda llegar a vulnerar los derechos de las personas. El peligro latente es el cruce de información con otros entes públicos, los resultados de ello, sin duda van en desmedro, al menos, del derecho a la intimidad o vida privada de las personas.

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN REPÚBLICA DOMINICANA

1. Generalidades

El sistema jurídico dominicano carece de normativa relativa a la protección de los datos personales. A nivel constitucional, no contempla disposiciones que se refieran al hábeas data así como tampoco a nivel legal. Las pocas disposiciones relacionadas con la materia

de estudio, en general, sólo establecen ciertos deberes de reserva o confidencialidad de informaciones que llegan a conocimiento de ciertos funcionarios públicos en el ejercicio de sus funciones.

2. Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional

La novísima Constitución Política Dominicana del año 2002 [519] , llama la atención por la ausencia de disposiciones básicas en materia de derechos fundamentales. Así, por ejemplo, no existe un reconocimiento directo del derecho a la intimidad ni del derecho a la vida privada. Tampoco se establece una acción de amparo que tutele los derechos consagrados expresamente por el texto constitucional. Con todo, cabe señalar que pese a las falencias constatadas en el texto fundamental dominicano, el año 1978 se ratificó por ese Estado la Convención Americana de Derechos Humanos, la cual obliga a éste a adecuar su normativa a las disposiciones de esa Convención [520] . En razón de lo anterior, estimamos que a pesar de lo exigua que aparece la Constitución en materia de derechos fundamentales y garantías, sus deficiencias deben ser suplidas por aplicación directa de las normas de la Convención Americana de Derechos Humanos [521] .

A continuación, revisaremos las normas constitucionales relacionadas con la protección jurídica del derecho a la vida privada e intimidad, en las cuales poder fundamentar una protección subsecuente de los datos personales.

El artículo 8 constitucional señala que se reconoce como finalidad principal del Estado: *"la protección efectiva de los derechos de la persona humana y el mantenimiento de los medios que le permitan perfeccionarse progresivamente dentro de un orden de libertad individual y de justicia social, compatible con el orden público, el bienestar general y los derechos de todos"*. Luego agrega que, para garantizar la realización de esos fines se fijan las siguientes normas: *"(…) 3. La inviolabilidad de domicilio. Ninguna visita domiciliaria puede verificarse sino en los casos previstos por la ley y con las*

519 [En línea] < http://www.georgetown.edu/pdba/Constitutions/DomRep/domrep02.html > [consulta: 6 de Noviembre 2002].

520 La ratificación del Pacto de san José de Costa Rica por el Estado de la República Dominicana se realizó el 21 de Enero de 1978. Cabe agregar, que se le reconoció competencia a la Corte Interamericana de DD.HH el 19 de febrero de 1999 en los siguientes términos*: "El Gobierno de la República Dominicana por medio del presente Instrumento, declara que reconoce como obligatoria de pleno derecho y sin convención especial, la competencia de la Corte Interamericana de Derechos Humanos sobre todos los casos relativos a la interpretación o aplicación de la Convención Interamericana de Derechos Humanos, del 22 de Noviembre de 1969"*. [En línea] < http://www.oas.org/juridico/spanish/firmas/b-32.html > [consulta 20 de Marzo 2003].

521 Llama la atención el hecho que en materia penal, sí se contemple directamente una protección al derecho a la intimidad de las personas en una disposición que confunde por su redacción. Esta norma es el artículo 337, el cual dispone que se castiga con prisión de seis meses a un año y multa de veinticinco mil a cincuenta mil pesos "*el hecho de atentar voluntariamente contra la intimidad de la vida privada (…)"*. La disposición completa se señala más adelante en el punto Nº 9.3 al analizar el régimen de responsabilidad.

formalidades que ella prescribe; *(…) 9. La inviolabilidad de la correspondencia y demás documentos privados, los cuales no podrán ser ocupados ni registrados sino mediante procedimientos legales en la substanciación de asuntos que se ventilen en la justicia. Es igualmente inviolable el secreto de la comunicación telegráfica, telefónica y cablegráfica. (…) 10. Todos los medios de información tienen libre acceso a las fuentes noticiosas oficiales y privadas, siempre que no vayan en contra del orden público o pongan en peligro la seguridad nacional".*

De las disposiciones recién señaladas, podemos deducir una protección a la vida privada de carácter limitado y un derecho de acceso a la información por parte de los medios de comunicación, cuestión relacionada con el ejercicio de la actividad periodística. Dada esa configuración constitucional, se dificulta la tarea de construir dogmáticamente un derecho de la envergadura que posee la autodeterminación informativa, pues faltan disposiciones normativas expresas que permitan tal tarea, como por ejemplo, la consagración expresa del derecho a la intimidad. Como ya se dijo, ante la falencia normativa constitucional deben aplicarse las disposiciones internacionales de protección a los Derechos Humanos, en especial el artículo 11 del Pacto de San José de Costa Rica titulado "Protección de la Honra y de la Dignidad", en el cual se señala que:

"1.Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad".

2.Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación".

3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

Dicho lo anterior, y teniendo presente los señalados vacíos constitucionales, puede afirmarse que en el ordenamiento jurídico constitucional dominicano, no se contempla una acción de hábeas data que tutele ciertos derechos de las personas en la dimensión de autonomía de control sobre la propia información personal, así como tampoco existe norma expresa que reconozca el derecho fundamental a la intimidad.

2.2 Protección Legal de los Datos Personales

A nivel infraconstitucional, el ordenamiento jurídico dominicano no cuenta con una ley de protección de datos personales. Sólo se observan algunas disposiciones sectoriales que establecen ciertos deberes de confidencialidad respecto de determinada información personal. A continuación se señalarán tales disposiciones.

2.2.1) Ley sobre Expresión y Difusión del Pensamiento (Ley Nº 6.132-1962) [522]

El artículo 43 de esta Ley señala que queda prohibida la publicación por medio del libro, de la prensa, de la radio, del cine o de cualquier medio de: *"todo texto o de toda ilustración concerniente a la identidad y la personalidad de los menores de dieciséis años*

[522] **[En línea] < http://www.iijusticia.edu.ar/privacidad/RD.htm#EDP > [consulta: 3 de Enero 2003].**

que se hubieren separado de sus padres, su tutor, la persona o la institución encargada de su custodia o a la cual se le confiera el cuidado de dichos menores".

La disposición anterior, guarda concordancia con las normas internacionales de protección a los derechos del niño, en especial en lo relativo al ámbito de la tutela de sus identidades cuando respecto de ellos se han adoptado medidas de protección.

2.2.2) Ley General de Bancos [523]

Esta ley no contempla ninguna norma que establezca el deber de secreto bancario respecto las operaciones realizadas por los clientes de estas instituciones. Sólo se señala en el artículo 33 que los bancos tendrán la obligación de dar acceso a su contabilidad a todos los libros y documentos justificativos de sus operaciones al Superintendente de Bancos y a los empleados de su dependencia. Luego, el artículo 34 dispone que los datos recogidos por el Superintendente de Bancos *"serán de carácter estrictamente confidencial"*. Se añade a continuación que: *"la revelación por los funcionarios y empleados de la Superintendencia, de la Secretaria de Estado de Finanzas o del banco central, de cualesquiera informaciones obtenidas en el desempeño de funciones, será sancionada con la destitución, sin perjuicio de las otras penas aplicables".* De lo anterior, podría deducirse que solamente existiría un deber de reserva que afecta a la Superintendencia de bancos y a sus funcionarios, respecto de la información obtenida en ejercicio de la labor de fiscalización. Como dentro de esta labor cabe el revisar operaciones particulares de personas, entendemos que indirectamente se establecería el deber de secreto aplicable a ese organismo público pero no a los bancos.

2.2.3) Código para la Protección de Niños, Niñas y Adolescentes [524]

El artículo 66 de esta ley, a propósito de los procesos de adopción señala que: *"todos los documentos y actuaciones administrativas o jurisdiccionales propios del proceso de adopción serán reservados por el término de treinta (30) años; de ellos solo podrá expedirse copia, por solicitud que los adoptantes hicieren directamente, a través de su apoderado(a), o del o de la Defensor(a) de Niños, Niñas, Adolescentes y Familia, del o de la adoptado (a) que hubiere llegado a la mayoría de edad o de la Procuraduría General de la República, para efecto de las investigaciones a que hubiere lugar".* La finalidad de esta norma es mantener en secreto todos los antecedentes relativos tanto a la familia de origen de un menor dado en adopción, como también aquéllos referidos a las actuaciones propias del proceso mismo.

2.2.4) Código Tributario [525]

Dentro de los deberes de la administración tributaria, se contempla por el artículo 47 el de

[523] **[En línea] < http://cnnc.cancilleria.gov.do/bancos.doc > [consulta: 8 de Abril 2003].**

[524] **[En línea] < http://www.iijusticia.edu.ar/privacidad/RD.htm#EDP > [consulta: 3 de Enero 2003].**

[525] **[En línea] < http://www.ciat.org/doc/docu/leg/cod/lal_domin_02_codigo_tributario.doc > [consulta: 8 de Abril 2003].**

reserva, el cual se traduce en que: *"las declaraciones y las informaciones que la Administración Tributaria obtenga de los contribuyentes, responsables y terceros por cualquier medio, en principio tendrán carácter reservado y podrán ser utilizadas para los fines propios de dicha administración y en los casos que autorice la ley".* Luego, agrega en el párrafo I que no rige dicho deber de reserva "*en los casos en que el mismo se convierta en un obstáculo para promover la transparencia del sistema tributario, así como cuando lo establezcan las leyes, o lo ordenen órganos jurisdiccionales en procedimientos sobre tributos, cobros compulsivos de éstos, juicios penales, juicio sobre pensiones alimenticias, de familia o disolución de régimen matrimonial".* Asimismo, se exceptúan las publicaciones de datos estadísticos que, por su generalidad, no permitan la individualización de declaraciones, informaciones o personas (Art. 47 Párrafo I, inciso 2º). Es decir, se exige que para estos casos se utilice un procedimiento de disociación de los datos.

En suma, se establece un deber de reserva para la Administración Tributaria respecto de la información entregada a ésta a través de las declaraciones, y de la obtenida de los contribuyentes por cualquier medio. Además de ello se señala un límite a la utilización de esos datos, el cual está dado por los fines propios de la Administración Tributaria.

3. Bienes Jurídicos Protegidos por la Legislación de Datos Personales

Ante la inexistencia de una ley de protección de datos personales, no nos referiremos a este punto.

4. Principios Informativos de la Legislación de Protección de Datos Personales

Por la misma razón señalada en el número anterior, tampoco nos detendremos en esta materia.

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

Dada la ausencia de una ley general de protección de datos personales en el ordenamiento jurídico dominicano, no nos detendremos en este punto.

6. Modelos de Tutela

En el ordenamiento jurídico dominicano, no existen mecanismos específicos que tutelen los derechos de las personas en materia de datos personales. Por su parte, la Constitución tampoco se pronuncia respecto de mecanismos de tutela general a los

derechos fundamentales. Por nuestra parte, tampoco tenemos noticias de legislación especial de amparo. En razón a este escenario jurídico, no podremos detenernos a analizar este punto.

7. Mecanismos de Control

Como consecuencia de la inexistencia de una ley de protección de datos personales en la República Dominicana que prevea órganos de control, tampoco nos podremos referir a este tema.

8. Transmisión Internacional de Datos

En esta materia sólo conocemos la disposición transitoria en materia tributaria del párrafo 1, artículo 3 de la Ley Nº 11-01 del año 2001, la cual señala que a partir del primero de enero del 2001, la Dirección General de Impuestos internos iniciará un operativo de valoración de patrimonios de las personas físicas, *"utilizando las informaciones obtenidas a través de acuerdos de intercambio de información fiscal firmados con otros países"*.

De la disposición anterior se deduce, a lo menos, la intención legislativa de concretar acuerdos de intercambio de información fiscal, cuya naturaleza jurídica desconocemos. La norma señalada, en principio estaría acorde con la propia disposición legal que establece las excepciones al deber de secreto fiscal, pues dada la amplitud de aquélla (Art. 47), cualquier impedimento de fiscalización podría caber dentro del término "*obstáculo para promover la transparencia del sistema tributario"*. Ciertamente, es criticable tal disposición, pues deja entregado al arbitrio del Estado cuando respetar o no la norma legal del secreto, la que en definitiva se vuelve inoperante y sólo tendría un valor puramente nominal.

9. Régimen de Responsabilidad

En materia de responsabilidad, y dada la falta de legislación general y sectorial en materia de datos personales, sólo nos referiremos a las reglas contenidas en algunas de las leyes señaladas más arriba en el punto Nº 2.2.2. En materia penal, haremos referencia a dos delitos relacionados con el derecho a la intimidad y la vida privada; uno contemplado en laLey sobre Expresión y Difusión del Pensamiento y el segundo, en el Código Penal.

9.1 Responsabilidad Administrativa

En materia de responsabilidad administrativa revisaremos tres estatutos sectoriales, éstos se señalan a continuación.

9.1.1) Código Tributario

Este cuerpo legal trata en el artículo 258 del incumplimiento de los deberes formales de

los funcionarios y empleados de la administración tributaria, disponiendo que: *"incurre en esta infracción el funcionario o empleado de la Administración Tributaria que violando los deberes de su cargo, en especial los establecidos en este Código, provoque un perjuicio económico al fisco o al contribuyente o responsable"*.

A renglón seguido, el artículo 259 señala que constituyen, entre otros, casos de incumplimiento de los deberes formales: *"(…) 1. Divulgar hechos o documentos que conozca en razón de su cargo y que por su naturaleza o por disposición de la ley tengan carácter de reservados".* Las sanciones a los incumplimientos de deberes de secreto están previstas en el artículo 260, el cual prescribe que: *"(…) procederá la suspensión sin disfrute de sueldo hasta por tres meses o la destitución de su cargo, de acuerdo con la gravedad del caso".* Por ultimo, el artículo 262 aclara que: *"las sanciones procederán sin perjuicio de las que se establezcan en las leyes administrativas o Ley Penal Común".*

9.1.2) Ley General de Bancos

El artículo 34 de esta ley establece tanto el deber de secreto respecto de los datos recogidos por la Superintendencia de Bancos, como la sanción correspondiente a la infracción de ese deber, disponiendo al efecto que: *"La revelación por los funcionarios y empleados de la Superintendencia, de la Secretaria de Estado de Finanzas o del banco central, de cualesquiera informaciones obtenidas en el desempeño de funciones, será sancionada con la destitución, sin perjuicio de las otras penas aplicables".*

9.1.3) Código para la Protección de Niños, Niñas y Adolescentes

El artículo 66 de este estatuto, prescribe que todos los documentos y actuaciones administrativas o jurisdiccionales propios del proceso de adopción serán reservados por el término de treinta años. En caso de violarse esta prohibición, el inciso 2º prescribe que: *"El o la funcionario(a) que permitiere el acceso a los documentos referidos o que expidiere copia de los mismos a personas no autorizadas en este artículo incurrirá en exceso de poder y será sancionado(a) con la destitución del cargo".*

9.2 Responsabilidad Civil

En materia de responsabilidad civil no existen reglas especiales aplicables, por lo cual entendemos que deberían aplicarse las reglas generales de la responsabilidad civil delictual o cuasidelictual, así como también a las reglas de la responsabilidad contractual según sea el caso. Con todo no podemos referirnos a ellas dada la falta de información al respecto.

9.3 Responsabilidad Penal

En materia penal revisaremos dos estatutos; la Ley sobre Expresión y Difusión del pensamiento y el Código Penal.

9.3.1) Ley sobre Expresión y Difusión del Pensamiento

Esta ley -como ya se señaló- sanciona en el artículo 43, la difusión de todo texto o de

toda ilustración concerniente a la identidad y la personalidad de los menores de dieciséis años que se hubieren separado de sus padres, su tutor, la persona o la institución encargada de su custodia o a la cual se le confiera el cuidado de dichos menores. La sanción respectiva consiste en multa de RD$50.OO a RD$300.00.

9.3.2) Código Penal [526]

En una disposición un tanto confusa, el artículo 337 del Código Penal dominicano señala lo siguiente:

Artículo 337.- *"Se castiga con prisión de seis meses a un año y multa de veinticinco mil a cincuenta mil pesos el hecho de atentar voluntariamente contra la intimidad de la vida privada, el o las personas que por medio de cualquiera de los procedimientos siguientes: 1- Capten, graben o transmitan sin el consentimiento de su autor, palabras pronunciadas de manera privada o confidencial; 2- Capten, graben o transmitan, sin su consentimiento, la imagen de una persona que se encuentra en un lugar privado; Cuando los actos mencionados en el presente artículo han sido realizados con el consentimiento de los interesados sin que se hayan opuesto a ello, su consentimiento se presume".*

Por su parte, el artículo 337-1 dispone que: *"Se castiga con la misma pena el hecho de conservar, llevar o dejar llevar a conocimiento del público o de un tercero, o utilizar, de cualquier manera que sea, toda grabación o documento obtenido con ayuda de uno de los actos previstos en el artículo precedente. (…) Cuando la infracción prevista en el párrafo precedente es cometida por vía de la prensa escrita o audiovisual, se aplican las disposiciones particulares de la Ley No. 6132 sobre Expresión y Difusión del Pensamiento, del año 1962, en cuanto concierne la determinación de las personas responsables".*

En suma, las disposiciones anteriores tendrían como bien jurídico protegido la intimidad de las personas, cuestión que no deja de llamar la atención pues, se reconoce este derecho en sede penal, pero nada se dice al respecto en materia constitucional.

10. Conclusiones

El ordenamiento jurídico de la República Dominicana, no contempla a nivel constitucional ni infraconstitucional previsión específica en materia de protección a los datos personales. La Constitución, apenas se encarga de reconocer indirectamente el derecho a la vida privada. Por otra parte, tampoco se establece ningún medio de tutela que resguarde los derechos fundamentales consagrados por el Constituyente. Esta estrechez normativa, creemos debe ser suplida a través de la aplicación de las disposiciones contenidas en la Convención Americana de Derechos Humanos, la cual el Estado dominicano la hizo derecho propio el año 1978.

En materia legal sólo existen disposiciones específicas que en general establecen deberes de confidencialidad de ciertas informaciones, de las cuales por lo cierto, no se deduce principio alguno en materia de tratamiento y transmisión de datos personales.

[526] **[En línea] < http://www.iijusticia.edu.ar/privacidad/RD.htm#EDP > [consulta: 3 de Enero 2003].**

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN URUGUAY

1. Generalidades

El ordenamiento jurídico uruguayo no posee disposiciones constitucionales ni infraconstitucionales que se refieran a la protección de los datos personales. La ley Fundamental sólo reconoce indirectamente el derecho a la vida privada y a la intimidad y, en el ámbito legal, solamente cuenta con disposiciones sectoriales que se encargan de resguardar la confidencialidad de ciertos datos personales. Con todo, en la actualidad existen diversos Proyectos de Ley encaminados a salvar estos vacíos, pero en ninguno de ellos se avista un tratamiento general de la materia en estudio.

2. Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional

La Constitución Política uruguaya de 1967 [527] , no contiene previsión alguna directamente relacionada con la protección a los datos personales. En consecuencia, ésta no dispone de un derecho a la protección de datos o hábeas data. Aún más, tampoco existe un reconocimiento constitucional directo y expreso del derecho a la vida privada e intimidad. A pesar de las deficiencias anteriores, existe una disposición que complementa y suple las falencias que pudiera contener el texto de la Carta Fundamental, pero no el espíritu de ésta. La disposición en comento, es el artículo 72 y prescribe que: *"La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno".*

Por otra parte, debemos hacer presente que el Estado uruguayo ha ratificado la Convención Americana de Derechos Humanos así como también ha otorgado competencia a la Corte Interamericana en esta materia [528] . Por lo tanto, la protección de los derechos humanos en el Uruguay, se ha visto reforzada en razón de la incorporación

527 [En línea] < http://www.georgetown.edu/pdba/Constitutions/Uruguay/uruguay96.html > [consulta: 22 de Noviembre 2002].

528 La ratificación del Pacto de San José de Costa Rica, data del 26 de Marzo de 1985. El reconocimiento de competencia a la Corte Interamericana de DD.HH, se realizó en la misma fecha anterior y su texto señala que "en el instrumento de ratificación de fecha 26 de marzo de 1985, depositado el 19 de abril de 1985 en la Secretaría General de la OEA, el gobierno de la República Oriental del Uruguay declara que reconoce la competencia de la Comisión Interamericana de Derechos Humanos por tiempo indefinido y de la Corte Interamericana de Derechos Humanos sobre todos los casos relativos a la interpretación o aplicación de esta Convención, bajo condición de reciprocidad, de acuerdo a lo establecido en sus artículos cuarenta y cinco párrafo tres, y sesenta y dos, párrafo dos". [En línea] < http://www.oas.org/juridico/spanish/firmas/b-32.html > [consulta: 20 de Marzo 2003].

de este tratado internacional de fundamental importancia. Para nuestro estudio, esto implica el reconocimiento del derecho a la vida privada y su derivado, el derecho a la intimidad. A continuación, se señalarán las disposiciones constitucionales relacionadas con la protección de los bienes jurídicos vida privada e intimidad, contenidas en el Capítulo I, Sección II denominada "Derechos, Deberes y Garantías".

El artículo 7° de la Carta Fundamental uruguaya dispone que: *"Los habitantes de la República tienen derecho a ser protegidos en el goce de su vida, honor, libertad, seguridad, trabajo y propiedad. Nadie puede ser privado de estos derechos sino conforme a las leyes que se establecieron por razones de interés general".*

Más adelante, el artículo 28 reconoce la inviolabilidad de la correspondencia y de los documentos privados en los siguientes términos: *"Los papeles de los particulares y su correspondencia epistolar, telegráfica o de cualquier otra especie, son inviolables, y nunca podrá hacerse su registro, examen o interceptación sino conforme a las leyes que se establecieron por razones de interés general".*

Finalmente, dentro del Capítulo IV, existe una disposición que cierra el catálogo de derechos individuales. Ella se contiene en el artículo 332 que señala: *"Los preceptos de la presente Constitución que reconocen derechos a los individuos, así como los que atribuyen facultades e imponen deberes a las autoridades públicas, no dejarán de aplicarse por falta de la reglamentación respectiva, sino que ésta será suplida, recurriendo a los fundamentos de leyes análogas, a los principios generales de derecho y a las doctrinas generalmente admitidas".* Esta regla, viene a señalar que las disposiciones constitucionales son aplicables directamente sin necesidad de reglamentación alguna, utilizándose al efecto la analogía y la interpretación sistemática del ordenamiento jurídico para hacer valer y proteger tales derechos.

Dentro del ámbito constitucional, se ha dicho por Palazzi -citando a Delpiano-que cierta doctrina sostiene que, si bien el hábeas data no está previsto a texto expreso en el derecho uruguayo, por aplicación de la norma del artículo 72 de la Constitución "puede considerarse que está incluido en el marco normativo, y podría ser hecho valer, en razón de los intereses protegidos que se condicen con sendos principios generales de derecho, que son admitidos por nuestra Constitución en su existencia previa y superior a si misma, en tanto que nuestra Carta recoge una marcada posición iusnaturalista" [529] . Finalmente, agrega que las mayores dudas se presentan a la hora de determinar el procedimiento judicial pertinente para sustanciar la acción de hábeas data. A este respecto señala que podría canalizarse a través de la Ley de Amparo Nº 16.011 [530] .

En suma, si bien las disposiciones constitucionales sólo establecen de manera indirecta una protección a los derechos vida privada e intimidad, la estrechez de tales disposiciones puede entenderse que han sido suplidas tanto por la propia regla del artículo 332, como por la Convención Americana de DD.HH. Por lo tanto, a partir de ellas podría fundamentarse una protección a los datos personales. En cuanto a la opinión de

[529] Palazzi, Pablo (2) [En línea] < http://www.ulpiano.com/Recursos_Privacy_LatinAmerica.htm#Uruguay > [consulta: 22 de Noviembre 2002].

[530] *Ibídem*.

Delpiano recién citada, nos parece que, en general, ella es acertada con lo cual es posible afirmar que la acción de amparo a falta de otra previsión legal podría ser idónea vía de tutela para el control de la información personal tratada tanto por organismos públicos como privados. En cuanto a la afirmación acerca del marcado carácter iusnaturalista que tendría la Constitución uruguaya, no nos pronunciamos.

2.2 Protección Legal de los datos Personales

En materia legal, el ordenamiento jurídico uruguayo no dispone de una ley de protección de datos personales sino que sólo cuenta con algunas normas específicas sectoriales, como la bancaria y tributaria que establecen deberes secreto respecto de cierta información personal. A pesar de lo anterior, cabe consignar que en la actualidad, se encuentran en tramitación legislativa diversos Proyectos de Ley relacionados con la protección a los datos personales. Llama la atención el hecho de no haberse pensado en un proyecto que pudiera tener el carácter de ley general y que concentrara en un solo cuerpo normativo, tanto la organización y funcionamiento de los bancos de datos, como la regulación general de los derechos, mecanismos de control pertinentes y sanciones [531] . A continuación se señalarán las reglas relacionadas con la protección de los datos personales en materia financiera y tributaria.

2.2.1) Ley sobre el Sistema de Intermediación Financiera (Ley Nº 15.322) [532]

Esta ley dispone en el artículo 25, titulado “Secreto profesional”, que toda persona pública no estatal o privada que realice intermediación financiera, así como también las instituciones estatales que por la índole de sus operaciones queden comprendidas en esta ley, *“no podrán facilitar noticia alguna sobre los fondos o valores que tengan en cuenta corriente, depósito o cualquier otro concepto, pertenecientes a persona física o jurídica determinada”*. Se agrega además que tampoco podrán dar a conocer *“informaciones confidenciales que reciban de sus clientes o sobre sus clientes. Las*

[531] Los Proyectos de Ley de los cuales tenemos noticia son los siguientes: 1) Proyecto de Ley que regula el Funcionamiento de los Bancos de Datos, presentado en Mayo de 2000. Su texto y tramitación puede consultarse [en línea] < http://www.parlamento.gub.uy/Repartidos/Camara/D2000050141-00.htm > [consulta: 5 de Febrero 2003]; 2) Proyecto de Ley que regula los Bancos de Datos de Información de Cumplimiento de Créditos o de Obligaciones de Tracto Sucesivo, presentado en Mayo de 2000. Su texto y tramitación puede consultarse [en línea] < http://www.parlamento.gub.uy/Repartidos/Camara/D2000050112-00.htm > [consulta: 5 de Febrero 2003]; 3) Proyecto de Ley sobre Personas Físicas o Jurídicas que Administren, Gestionen u Obtengan Información de cualquier Base de Datos, presentado en Octubre de 2000. Su texto y tramitación puede consultarse [en línea] < http://www.parlamento.gub.uy/Repartidos/Camara/D2000100351-00.htm > [consulta: 5 de Febrero 2003]; 4) Proyecto de Ley sobre el Derecho a la Información y Acción de "Hábeas Data", presentado en Mayo de 2000 (aprobado por la Cámara de Representantes en el año 2002). Su texto y tramitación puede consultarse [en línea] < http://www.parlamento.gub.uy/Repartidos/Camara/D2000050114-00.htm > [consulta: 5 de Febrero 2003] y, 5) Proyecto de Ley sobre la Creación de un Registro Nacional de Deudores Alimentarios, presentado en Abril de 2000. Su texto y tramitación pueden consultarse [en línea] < http://www.parlamento.gub.uy/Repartidos/Camara/D2000040062-00.htm >[consulta: 5 de Febrero 2003].

[532] [En línea] < http://www.parlamento.gub.uy/Leyes/Ley15322.htm > [consulta: 9 de Abril 2003].

operaciones e informaciones referidas se encuentran amparadas por el secreto profesional y sólo pueden, ser reveladas por autorización expresa y por escrito del interesado o por resolución fundada de la Justicia Penal o de la Justicia competente si estuviera en juego una obligación alimentaria y en todos los casos, sujeto a las responsabilidades más estrictas por los perjuicios emergentes de la falta de fundamento de la solicitud". Finalmente, se añade que no se admitirá otra excepción que las establecidas en esta ley.

De lo señalado por el legislador se deduce un doble deber de secreto; el primero, relativo a las operaciones pasivas de los clientes de las instituciones financieras, y el segundo, relativo a cualquier información confidencial recibida por estas empresas de parte de sus clientes.

2.2.2) Código Tributario [533]

Este código, no establece un deber de secreto vinculante para los funcionarios de la Administración Tributaria respecto de las informaciones suministradas por los contribuyentes o terceros, sino que solamente se establece por el artículo 47 una obligación de secreto respecto de las "actuaciones" realizadas por la Administración Tributaria y los funcionarios que de ella dependen, los cuales *" están obligados a guardar secreto de las informaciones que resulten de sus actuaciones administrativas o judiciales".* El inciso 2º, contempla como excepciones a ese deber, las informaciones proporcionadas a la Administración Tributaria y a los Tribunales de Justicia en materia penal, de menores, o aduanera cuando esos órganos entendieran que fuera imprescindible para el cumplimiento de sus funciones y los solicitaren por resolución fundada. Sin embargo, estimamos que esta disposición no es clara en cuanto a la protección de la confidencialidad de los datos personales de los contribuyentes, pues más bien ésta sería consecuencia del carácter reservado de las actuaciones dentro de un procedimiento de investigación tributaria, cuestión distinta del secreto tributario propiamente tal.

3. Bienes Jurídicos Protegidos por la Legislación de Datos Personales

Ante la inexistencia de una ley de protección de datos personales, no nos referiremos a este punto en la materia.

4. Principios Informativos de la Legislación de Protección de Datos Personales

Por la misma razón señalada en el número anterior, tampoco nos detendremos en esta materia.

[533] [En línea] < http://www.ciat.org/doc/docu/leg/cod/lal_urugu_02_codigo_tributario.doc > [consulta: 10 de Abril 2003].

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

Ante la ausencia de una ley general de protección de datos en el ordenamiento jurídico uruguayo, no nos detendremos en este punto.

6. Modelos de Tutela

En el ordenamiento jurídico uruguayo, no se observan mecanismos específicos que tutelen los derechos de las personas en la materia. Alguna doctrina, ha señalado que en ausencia de normativa específica es factible poder canalizar la tutela a los datos personales a través de la Ley de Amparo Nº 16.011 [534] . En nuestra opinión y, dada la amplitud como está concebida la acción de amparo, también creemos que a falta de mecanismo jurídico específico de tutela, la acción de amparo sería por el momento el medio más eficaz de protección a los datos personales.

6.1 La acción de Amparo [535]

La Ley Nº 16.011, que establece la acción de amparo (en adelante LDA) señala en su encabezamiento que: *"se dictan normas para que cualquier persona física o jurídica, publica o privada, pueda deducir la acción de amparo contra todo acto, omisión o hecho de las autoridades estatales o paraestatales, así como particulares que lesionen con ilegitimidad manifiesta sus derechos y libertades"*. De la sola lectura de lo prescrito por el legislador, ya se da a entender el ámbito de aplicación que esta acción tendría; es ejercitable tanto contra el Estado como contra los particulares, sean personas jurídicas o naturales.

6.1.1) Procedencia de la Acción

El artículo 1º de la LDA señala que cualquier persona física o jurídica, pública o privada, podrá deducir la acción de amparo: *"contra todo acto, omisión o hecho de las autoridades estatales o paraestatales, así como de particulares que en forma actual o inminente, a su juicio, lesione, restrinja, altere o amenace, con ilegitimidad manifiesta, cualquiera de sus derechos y libertades reconocidos expresa o implícitamente por la Constitución (artículo 72), con excepción de los casos en que proceda la interposición del recurso de habeas corpus"*. Acá, la referencia al artículo 72 es muy importante pues abre la posibilidad de tutelar derechos que no estén expresamente establecidos por el Constituyente. Si dentro de éstos podría entenderse incluido el derecho a la autodeterminación informativa, es una cuestión de difícil respuesta, pues resulta complejo fundamentar un derecho de tal entidad dentro de un sistema jurídico que ni siquiera reconoce de manera directa y

534 [En línea] < http://www.ulpiano.com/Recursos_Privacy_LatinAmerica.htm#Uruguay > [consulta: 22 de Noviembre 2002].

535 [En línea] < http://www.parlamento.gub.uy/leyes/ley16011.htm > [consulta: 21 de Enero 2003].

expresa el derecho a la intimidad y a la vida privada. Con todo, queda abierta la discusión, dado el tenor del comentado artículo 72.

Según en el inciso 2º del artículo 1º, la acción de amparo no procederá en ningún caso: *"A) Contra los actos jurisdiccionales, cualquiera sea su naturaleza y el órgano del que emanen. Por lo que refiere a los actos emanados de los órganos del Poder Judicial, se entiende por actos jurisdiccionales, además de las sentencias, todos los actos dictados por los Jueces en el curso de los procesos contenciosos; B) Contra los actos de la Corte Electoral, cualquiera sea su naturaleza; C) Contra las leyes y los decretos de los Gobiernos Departamentales que tengan fuerza de ley en su jurisdicción".*

Por otra parte, el artículo 2º establece otro requisito para que sea procedente la acción de amparo disponiendo que: *"sólo procederá cuando no existan otros medios judiciales o administrativos que permitan obtener el mismo resultado previsto en el literal B) del artículo 9º o cuando, si existieren, fueren por las circunstancias claramente ineficaces para la protección del derecho. Si la acción fuera manifiestamente improcedente, el Juez la rechazará sin sustanciarla y dispondrá el archivo de las actuaciones"* [536] .

Finalmente, cabe anotar que el artículo 4º inciso 1º establece un plazo para la interposición de la acción, prescribiéndose al efecto que: *"en todos los casos deberá ser interpuesta dentro de los treinta días a partir de la fecha en que se produjo el acto, hecho u omisión caracterizados en el artículo 1º. No le correrá el término al titular del derecho o libertad lesionados si estuviere impedido por justa causa".*

6.1.2) Legitimación Activa

En esta materia, el artículo 1º dispone que la acción de amparo puede ser ejercida por *"cualquier persona física o jurídica, pública o privada".* Más adelante, el artículo 4º precisa lo recién señalado disponiendo que la acción de amparo *"deberá ser deducida por el titular del derecho o libertad lesionados o amenazados, pero si éste estuviera imposibilitado de ejercerla podrá, en su nombre, deducirla cualquiera de las personas referidas en el artículo 158 del Código de Procedimiento Civil, sin perjuicio de la responsabilidad de éstas, si hubieren actuado con malicia o con culpable ligereza".* De lo anterior, se deduce que puede ser ejercida la acción de amparo tanto por el propio ofendido, como por un tercero en su nombre.

6.1.3) Legitimación Pasiva

La ley se refiere a los legitimados pasivos de la acción de amparo en el artículo 1º. Ellos son: la autoridad estatal o paraestatal o el particular en su caso, que en forma actual o inminente, lesione, restrinja, altere o amenace, con ilegitimidad manifiesta, cualquiera de los derechos y libertades reconocidos expresa o implícitamente por la Constitución.

6.1.4) Competencia

[536] La referencia al artículo 9º, dice relación a que pueda obtenerse por otra vía una resolución que determine precisamente lo que deba o no deba hacerse y fije el plazo por el cual dicha resolución regirá, si es que correspondiere fijarlo.

En esta materia, el artículo 3º dispone que serán competentes: *"los Jueces Letrados de Primera Instancia de la materia que corresponda al acto, hecho u omisión impugnados y del lugar en que éstos produzcan sus efectos. El turno lo determinará la fecha de presentación de la demanda".* La competencia en segunda instancia está limitada sólo en caso que se apele en contra de la sentencia definitiva y de la que rechaza la acción por ser manifiestamente improcedentes (Art. 10).

6.1.5) Procedimiento Aplicable

El procedimiento al cual se sujeta el amparo podemos sintetizarlo de la siguiente forma:

a) *Demanda* : la demanda debe presentarse con las formalidades señaladas en materia procesal civil, en cuanto corresponda, indicándose, además, los medios de prueba a utilizar. La prueba documental se acompañará necesariamente con la demanda (Art. 5º).

b) *Audiencia pública* : el Juez convocará a las partes a una audiencia pública dentro del plazo de tres días a partir de la fecha de la presentación de la demanda, salvo en el caso previsto en la oración final del artículo 2º. En dicha audiencia se oirán las explicaciones del demandado, se recibirán las pruebas y se producirán los alegatos. El Juez, que podrá rechazar las pruebas manifiestamente impertinentes o innecesarias, presidirá la audiencia so pena de nulidad e interrogará a los testigos y a las partes, sin perjuicio que aquéllos sean, a su vez, repreguntados por los abogados. Gozará de los más amplios poderes de policía y de dirección de la audiencia. En cualquier momento podrá ordenar diligencias para mejor proveer. La sentencia se dictará en la audiencia o, a más tardar, dentro de las veinticuatro horas de su celebración. Sólo en casos excepcionales podrá prorrogarse la audiencia por hasta tres días (Art. 6º).

c) *Medidas cautelares* : éstas serán procedente si de la demanda o en cualquier otro momento del proceso resultare, a juicio del Juez, la necesidad de su inmediata actuación, en amparo del derecho o libertad presuntamente violados (Art. 7º).

6.1.6) La Sentencia

El artículo 9º dispone que la sentencia que haga lugar al amparo deberá contener:

a) La identificación concreta de la autoridad o el particular a quien se dirija y contra cuya acción, hecho u omisión se conceda el amparo;

b) La determinación precisa de lo que deba o no deba hacerse y el plazo por el cual dicha resolución regirá, si es que correspondiere fijarlo;

c) El plazo para el cumplimiento de lo dispuesto, que no podrá exceder de veinticuatro horas continuas a partir de la notificación.

El inciso final del artículo 9º prescribe que sin perjuicio de lo establecido, la sentencia podrá disponer las sanciones pecuniarias conmutativas dispuestas por el Decreto Ley 14.978 de 14 de diciembre de 1978.

El artículo 10º señala que será apelable la sentencia definitiva y la que rechaza la acción por ser manifiestamente improcedente.

En cuanto a los efectos de la sentencia de amparo, el artículo 11 dispone que una vez ejecutoriada ésta *"hace cosa juzgada sobre su objeto, pero deja subsistente el ejercicio de las acciones que pudieren corresponder a cualquiera de las partes con independencia del amparo".* Por lo tanto, sólo produce el efecto de cosa juzgada formal y no material.

6.2 Otras Acciones

Como ya se ha señalado, no existen otras acciones que puedan brindar una tutela a los derechos que podrían fundamentar una protección a los datos personales.

7. Mecanismos de Control

A consecuencia de la inexistencia de una ley de protección de datos personales, tampoco nos podremos referir a esta materia.

8. Transmisión Internacional de Datos

No tenemos conocimiento de legislación especial que se ocupe de regular esta modalidad de transferencia de datos personales.

9. Régimen de Responsabilidad

En materia de responsabilidad, a falta de ley general de protección de datos personales, nos referiremos a algunas reglas contenidas en los estatutos sectoriales vistos en el punto Nº 2.2.2 de este análisis. En materia civil, se hará referencia a las reglas generales e responsabilidad extracontractual y, en el ámbito penal se hará referencia a delitos contemplados en el Código del ramo referidos a los bienes jurídicos intimidad y vida privada.

9.1 Responsabilidad Administrativa

Respecto de esta clase de responsabilidad, sólo podemos decir que el Código Tributario en el inciso final del artículo 47, señala que la violación por los funcionarios de la Administración Tributaria del deber de guardar secreto de las informaciones que resulten de sus actuaciones administrativas o judiciales, *"apareja responsabilidad y será causa de destitución para el funcionario infidente".*

9.2 Responsabilidad Civil

En materia de responsabilidad no existen reglas especiales vinculadas a la protección de datos. A falta de ellas, creemos deberían aplicarse las reglas generales de la responsabilidad civil extracontractual, contenidas en el Libro Cuatro del Código Civil uruguayo (De las Obligaciones), Capítulo II, Sección II [537] . Por otra parte, debemos hacer presente que a nivel constitucional el artículo 24 establece la responsabilidad civil del

Estado en los siguientes términos: "*El Estado, los Gobiernos Departamentales, los Entes Autónomos, los Servicios Descentralizados y, en general, todo órgano del Estado, serán civilmente responsables del daño causado a terceros, en la ejecución de los servicios públicos, confiados a su gestión o dirección".* De lo anterior, se sigue que en el evento que el Estado o sus funcionarios causen daño en el ejercicio de sus funciones, será obligado a reparar los perjuicios. En materia de protección de datos personales, cabría por ejemplo responsabilidad del Estado en caso de vulnerar algún derecho relacionado con la facultad de control de la propia información personal, fundamentada tanto en el derecho a la vida privada como en el derecho a la intimidad, a falta de una consagración específica del hábeas data.

9.3 Responsabilidad Penal

En materia criminal, revisaremos las disposiciones contempladas tanto en la ley sectorial sobre el Sistema de Intermediación Financiera como en la ley común penal uruguaya.

9.3.1) Ley sobre el Sistema de Intermediación Financiera

Este estatuto sectorial establece en el artículo 25 -como se dijo-, un doble deber de secreto; el primero relativo a las operaciones activas de los clientes de las instituciones financieras, y el segundo, relativo a cualquier información confidencial recibida por estas empresas por parte de sus clientes. El inciso final de esta disposición prescribe que quienes incumplan esos deberes de secreto, *"serán sancionados con tres meses de prisión a tres años de penitenciaría".*

9.3.2) Código Penal [538]

El Código Penal uruguayo sólo contempla delitos vinculados con los bienes jurídicos vida privada e intimidad sin referencia alguna a los datos personales. Estos delitos se señalan a continuación:

a) Violación de domicilio:

Artículo 294.-*"El que se introdujera en morada ajena, o en sus dependencias, contra la voluntad expresa o tácita del dueño o del que hiciera sus veces, o penetrare en ella, clandestinamente o con engaño, será castigado con tres a veinticuatro meses de prisión.*

La misma pena se aplicará al que se mantuviera en morada ajena, contra la voluntad

[537] El artículo 1.319, que encabeza la Sección II intitulada "De los Delitos y Cuasidelitos" dispone que: *"Todo hecho ilícito del hombre que causa a otro un daño, impone a aquel por cuyo dolo, culpa o negligencia ha sucedido, la obligación de repararlo. (…) Cuando el hecho ilícito se ha cumplido con dolo esto es, con intención de dañar constituye un delito; cuando falta esa intención de dañar, el hecho ilícito constituye un cuasidelito. (…) En uno y otro caso, el hecho ilícito puede ser negativo o positivo, según que el deber infringido consista en hacer o no hacer".* [En línea] < http://www.parlamento.gub.uy/Codigos/CodigoCivil/1996/l4P1T1.htm > [consulta: 10 de Abril 2003].

[538] [En línea] < http://www.unifr.ch/derechopenal/legislacion/uy/cp_uruguay.htm > [consulta: 10 de Abril 2003].

expresa del dueño de quien hiciera sus veces, o clandestinamente o con engaño".

b) Violación de correspondencia escrita:

Artículo 296.-"*Comete el delito de violación de correspondencia el que, con la intención de informarse de su contenido, abre un pliego epistolar, telefónico o telegráfico, cerrado, que no le estuviere destinado.*

Este delito se castiga con 20 UR (veinte unidades reajustables) a 400 UR (cuatrocientas unidades reajustables) de multa.

Los que abran, intercepten, destruyan u oculten correspondencia, encomiendas y demás objetos postales con la intención de apropiarse de su contenido o interrumpir el curso normal de los mismos, sufrirán la pena de un año de prisión a cuatro de penitenciaría.

Constituye circunstancia agravante de este delito, en sus dos formas, el que fuera cometido por funcionario público perteneciente a los servicios de que en cada caso se tratare".

c) Interceptación de noticia, telegráfica o telefónica:

Artículo 297.- "*El que, valiéndose de artificios, intercepta una comunicación telegráfica o telefónica, la impide o la interrumpe, será castigado con multa de 20 UR (veinte unidades reajustables) a 400 UR (cuatrocientas unidades reajustables) de multa".*

d) Revelación del secreto de la correspondencia y de la comunicación epistolar, telegráfica o telefónica:

Artículo 298.- *"Comete el delito de revelación de correspondencia epistolar, telegráfica o telefónica, siempre que causare perjuicio:*

1° El que, sin justa causa, comunica a los demás lo que ha llegado a su conocimiento, por alguno de los medios especificados en los artículos anteriores.

2° El que, sin justa causa, publica el contenido de una correspondencia, epistolar, telegráfica o telefónica que le estuviere dirigida y que por su propia naturaleza debiera permanecer secreta.

Este delito será castigado con 20 UR (veinte unidades reajustables) a 200 UR (doscientas unidades reajustables)".

e) Conocimiento fraudulento de documentos secretos:

Artículo 300.- *"El que, por medios fraudulentos, se enterare del contenido de documentos públicos o privados, que por su propia naturaleza debieran permanecer secretos, y que no constituyeran correspondencia, será castigado, siempre que del hecho resultaren perjuicios, con 20 UR (veinte unidades reajustables) a 400 UR (cuatrocientas unidades reajustables) de multa".*

f) Revelación de documentos secretos:

Artículo 301.- *"El que, sin justa causa, revelare el contenido de los documentos que se mencionan en el artículo precedente, que hubieren llegado a su conocimiento por los medios en él establecidos o en otra forma delictuosa, será castigado con tres meses de prisión a tres años de penitenciaría".*

g) Revelación de secreto profesional ***:***

Artículo 302.- *"El que, sin justa causa, revelare secretos que hubieran llegado a su conocimiento, en virtud de su profesión, empleo o comisión, será castigado, cuando el hecho causare perjuicio, con 100 UR (cien unidades reajustables) a 600 UR (seiscientas unidades reajustables) de multa".*

10. Conclusiones

El ordenamiento jurídico de la República Oriental del Uruguay, no contempla a nivel constitucional ni infraconstitucional previsión específica en materia de protección a los datos personales. La Constitución sólo reconoce indirectamente el derecho a la vida privada. Estos vacíos normativos, creemos deben ser suplidos a través de la aplicación extensiva de la norma del artículo 72 de la Constitución y de las disposiciones contenidas en la Convención Americana de Derechos Humanos, la cual ha sido ratificada por el Estado uruguayo en el año 1985.

En materia legal, sólo existen disposiciones sectoriales que en general establecen deberes de confidencialidad o secreto de ciertas informaciones, de las cuales, por lo cierto, resulta difícil deducir principios en materia de tratamiento y transmisión de datos personales. Con todo, actualmente están en tramitación parlamentaria diversos Proyecto de Ley relacionados a la tutela de los datos personales; el más avanzado es el proyecto de acceso a la información y hábeas data (aprobado por la Cámara de Representantes), otros, se ocupan de la regulación de los bancos de datos.

ANÁLISIS DE LA PROTECCIÓN A LOS DATOS PERSONALES EN VENEZUELA

1. Generalidades

El ordenamiento jurídico venezolano destaca por la normativa constitucional del año 1999, la cual consagra la garantía del hábeas data y establece límites al uso de la informática. No obstante lo anterior, el legislador aún no ha dictado una ley de protección de datos personales ni ha regulado el ejercicio de la acción constitucional del hábeas data. En consecuencia, Venezuela sólo cuenta con disposiciones sectoriales que, como

en la mayoría de los países latinoamericanos, sólo establecen ciertos deberes de confidencialidad respecto de información de carácter personal. En el ámbito de la actividad legislativa, tampoco estamos al tanto de alguna iniciativa legal que tenga por finalidad regular los derechos señalados en la Constitución venezolana.

2. Niveles de Protección Jurídica a los Datos Personales

2.1 Protección Constitucional

La Constitución Política del año 1999 [539] , introduce disposiciones directamente relacionadas con la protección a los datos personales. Así, ha consagrado la garantía del hábeas data específicamente dentro del título referido a los Derechos Humanos y a las garantías de éstos (Título III), a continuación de la acción de amparo. Además, en el Capítulo dedicado a los "Derechos Civiles", el Constituyente se ha encargado de establecer limitaciones al uso de la informática; no puede vulnerar el honor ni la intimidad personal y familiar de los ciudadanos y ciudadanas, respetando el pleno ejercicio de sus derechos. La tarea de limitar el uso de la informática ha sido endosada por el Constituyente al legislador.

Por otra parte, ya en el Capítulo relativo al "Poder Público", la Constitución consagra el derecho de acceso a la información respecto de los actos de la administración del Estado. Si bien este derecho no se relaciona con la protección a los datos personales -pues su objetivo es la transparencia de los actos de gobierno y de la gestión pública- lo señalamos para resaltar la diferencia conceptual de su garantía con el hábeas data, con el cual a veces se ha tendido a confundir. Como ya se ha dicho, la garantía del derecho de acceso a la información pública, se le ha denominado doctrinariamente como hábeas data impropio.

Reseñado el marco actual constitucional venezolano, pasaremos a analizar las respectivas disposiciones que consagran la protección a los datos personales a través del hábeas data y otras normas.

Como ya se adelantó, existe una disposición fundamental en materia de protección de datos personales, ésta es la del artículo 28 y dispone lo siguiente:

Artículo 28.-"*Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley".*

De la configuración constitucional anterior, claramente inclinada a un reconocimiento

[539] [En línea] < http://www.tsj.gov.ve/legislacion/constitucion1999.htm > [consulta: 21 de Noviembre 2002].

de un derecho a la protección de datos, podría entenderse que se estuviera instaurando un proceso específico de tutela a ese derecho, independiente del amparo tradicional, por cuanto su ubicación dentro del texto constitucional se inserta inmediatamente después de la disposición que establece la acción de amparo. La idea anterior podría ser discutible, pues la acción de amparo venezolana tutela aún aquellos derechos inherentes a la persona que no figuren expresamente en la Constitución o en los instrumentos internacionales sobre derechos humanos (Art. 27). En este último sentido podría encuadrarse alguna jurisprudencia en lo contencioso-administrativo, que ha definido el hábeas data como "aquella categoría del género de amparo, que cualquier persona, natural o jurídica, puede interponer solicitando el acceso, corrección, destrucción, supresión, actualización o confidencialidad de aquellos datos relacionados con su persona que consten en documentos que reposan en archivos oficiales o privados, cuando tales datos o informaciones sean erradas o falsas e ilegítimamente vulneren o menoscaben de cualquier forma o en cualquier sentido sus derechos al honor, reputación, dignidad, propia imagen, vida privada, etc." [540] . De lo anterior, se desprendería una concepción del hábeas data entendida como una especie del amparo, que denota en los sentenciadores una postura que no logra ver la acción de hábeas data como independiente, desligada del amparo tradicional.

Alguna doctrina, analizando en su momento la Propuesta sobre el Derecho a la Libertad Informática y al Hábeas Data del Anteproyecto de Constitución Nacional elaborado por la Asamblea Nacional Constituyente venezolana [541] , ha señalado que, "consideramos que para que el recurso de Hábeas Data pueda lograr sus fines, es decir, garantizar el ejercicio efectivo de los derechos de la libertad informática, en la configuración posterior del procedimiento que realizará el legislador, éste deberá tener como norte los principios de sencillez, transparencia, economía y celeridad procesal de tal manera que constituya un mecanismo eficaz que permita al individuo el acceso fácil, expedito y económico a sus datos personales, puesto que de no ser así se desnaturalizaría la *ratio legis* de dicha garantía al impedir su realización práctica" [542] . De esta opinión se desprendería una postura contraria a la señalada por la jurisprudencia citada. El nuevo punto de vista concibe el procedimiento para hacer efectiva la acción de

[540] Sentencia de amparo constitucional de la Corte Primera en lo Contencioso-Administrativa, de fecha 28 de marzo de 2000, redactada por el Magistrado Carlos Mouriño Vaquero. [En línea] < http://www.veedores.org/_VBiblioteca/Biblioteca_jurisprudencia/decision_sobre_habeas_data_INSACA.htm > [consulta: 16 de Diciembre 2002].

[541] El texto del Anteproyecto difiere solamente del constitucional en las excepciones al ejercicio de la acción de hábeas data, el cual no contemplaba expresamente a las fuentes de información periodística ni al secreto profesional. El texto de aquélla disposición señalaba: Artículo 28.- "Toda persona tiene derecho de acceder a la información y a los datos que sobre si misma o sobre sus bienes consten en registros oficiales o privados de carácter público, así como de conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos. De la misma manera podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas". En Álvarez B. de Bozo, Miriam 'et al': *"La Libertad Informática: Derecho Fundamental en la Constitución Venezolana"*,[en línea] < http://ulpiano.com/Recusos_habeasData_venezuela1999.htm > [consulta: 21 de Noviembre 2002].

hábeas data como diverso al amparo, con reglas específicas que impidan su desnaturalización. Refuerza lo dicho, la siguiente afirmación de estos mismos autores quienes señalan que: "se observa en la propuesta constitucional la consagración expresa tanto del derecho a la libertad informática como de su garantía o tutela, con la acción de Habeas Data" [543] . De lo expuesto, se desprende además una opción acerca del bien jurídico protegido por la disposición, cual sería, la tutela de la libertad informática o derecho a la autodeterminación informativa a través de la consagración de su garantía específica, la acción de hábeas data. Por nuestra parte, nos sumamos a esta última opinión, y estimamos que el Constituyente habría establecido el hábeas data como una garantía independiente del amparo general, lo cual requeriría una especial reglamentación, cuestión que aún no ocurre en Venezuela.

Siguiendo con el análisis constitucional, cabe ahora referirse a la disposición del artículo 60, ubicado dentro del Capítulo "De los Derechos Civiles", el cual dispone lo siguiente:

Artículo 60.- *"Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación.*

La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos".

La disposición anterior, a todas luces, estaría basada en la Constitución española de 1978; el inciso primero del texto venezolano difiere sólo gramaticalmente del Nº 1 del artículo 18 del texto español y, el inciso 2º del texto venezolano es idéntico al Nº 4 del mismo artículo español [544] .

La norma en comento tiene gran importancia, pues complementa y refuerza el reconocimiento de la garantía del hábeas data, y abre camino al desarrollo de una legislación con sólida base constitucional, lo que ahorra esfuerzos argumentativos a la hora de conflictos interpretativos. Si bien el Constituyente ha encargado privativamente al legislador la tarea de regular el uso de la informática, no tenemos noticias aún de una ley de protección de datos personales que cumpla con los requerimientos constitucionales.

542 En ese entonces se señalaba por Álvarez y otros, que "la propuesta del derecho a la libertad informática y del habeas data contenido en el artículo 28 del proyecto de Constitución Nacional elaborado por la Asamblea Nacional Constituyente constituye un avance en la configuración de los derechos de la parte dogmática del texto constitucional e implica la pretensión de nuestro constituyente de ponerse en sintonía con los avances en materia de derecho fundamentales, especialmente con las nuevas libertades en las sociedades tecnológicas". *Ibídem.*

543 *Ídem*.

544 El artículo 18 de la Constitución española señala: "*1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.* 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. *4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".* [En línea] < http://www.congreso.es/funciones/constitucion/titulo_1_cap_2_sec1.htm > [consulta: 10 de Abril 2003].

En cuanto a la disposición que consagra el derecho de acceso a la información pública, puede señalarse que ésta se ubica en el Capítulo III, Título IV denominado "Del Poder Público", disponiéndose al efecto que:

Artículo 143.- *"Los ciudadanos y ciudadanas tienen derecho a ser informados e informadas oportuna y verazmente por la Administración Pública, sobre el estado de las actuaciones en que estén directamente interesados e interesadas, y a conocer las resoluciones definitivas que se adopten sobre el particular. Asimismo, tienen acceso a los archivos y registros administrativos, sin perjuicio de los límites aceptables dentro de una sociedad democrática en materias relativas a seguridad interior y exterior, a investigación criminal y a la intimidad de la vida privada, de conformidad con la ley que regule la materia de clasificación de documentos de contenido confidencial o secreto. No se permitirá censura alguna a los funcionarios públicos o funcionarias públicas que informen sobre asuntos bajo su responsabilidad".*

De lo señalado en el artículo recién visto, se desprende una intención de publicidad y transparencia de la gestión pública, lo cual favorece el fortalecimiento de las instituciones públicas a través del control de sus actividades por los propios ciudadanos. En suma, beneficia la institucionalidad de un Estado democrático.

Por otra parte, y en lo relativo a la tutela de los derechos reconocidos por el Constituyente, creemos que es pertinente detenernos en la disposición que consagra la acción de amparo, pues aunque el Constituyente haya establecido la acción de hábeas data, no se ha encargado de señalar procedimiento alguno para su ejercicio. Además, tampoco el legislador se ha pronunciado al respecto, por lo que a nuestro juicio y pese a todo lo dicho, la acción de amparo aparece en la práctica como el medio más efectivo de tutela a los derechos protegidos por el hábeas data [545] .

El artículo 27 inciso1º de la Constitución venezolana, dispone en materia de amparo que: *"toda persona tiene derecho a ser amparada por los tribunales en el goce y ejercicio de los derechos y garantías constitucionales, aun de aquellos inherentes a la persona que no figuren expresamente en esta Constitución o en los instrumentos internacionales sobre derechos humanos"* (sic).

La amplitud de la disposición anterior, sin duda permite una operatividad que la convierte en una herramienta procesal de máxima importancia, pues no limita su alcance sino por el contrario, lo extiende a aquellos derechos consagrados en los instrumentos internacionales sobre derechos humanos, como por ejemplo, el Pacto de San José de Costa Rica [546] . Debemos añadir en esta materia, que el artículo 281 Nº 3 señala dentro

[545] Al respecto se ha señalado por la Comisión Andina de Juristas que: "corresponderá en consecuencia a la legislación y la jurisprudencia precisar si para la protección de los derechos reconocidos en el Artículo 28º de la Constitución se aplicarán las normas generales sobre el amparo o si se establecerá un proceso especial al cual se le denomine hábeas data. En todo caso, no puede desconocerse que en relación a la protección de estos derechos se hace necesario establecer algunas disposiciones especiales, como la prevista en el último párrafo del mismo Artículo 28º de la ley fundamental" (sic). [En línea] < http://www.cajpe.org.pe/rij/bases/temario/data.htm > [consulta: 16 de Diciembre 2002].

[546] En el caso del Estado venezolano, la ratificación de este Pacto, data de 21 de Enero de 1978. [En línea] < http://www.oas.org/juridico/spanish/firmas/b-32.html > [consulta: 20 de Marzo 2003].

de las atribuciones del Defensor o Defensora del Pueblo, la facultad deinterponer las acciones de inconstitucionalidad, amparo, hábeas corpus*, "hábeas data"* y las demás acciones o recursos necesarios para ejercer las atribuciones señaladas en los numerales anteriores, cuando fuere procedente de conformidad con la ley [547] .

Finalmente, debemos referirnos a una disposición que nos parece muy interesante desde el punto de la protección y promoción de los derechos humanos, ésta es la señalada en el artículo 31 y dispone: *"toda persona tiene derecho, en los términos establecidos por los tratados, pactos y convenciones sobre derechos humanos ratificados por la República, a dirigir peticiones o quejas ante los órganos internacionales creados para tales fines, con el objeto de solicitar el amparo a sus derechos humanos"*. Luego, el inciso 2º de este artículo agrega que: *"El Estado adoptará, conforme a procedimientos establecidos en esta Constitución y la ley, las medidas que sean necesarias para dar cumplimiento a las decisiones emanadas de los órganos internacionales previstos en este artículo".*

Sin duda que lo establecido por la Constitución venezolana se condice con la importancia del tema y más aún, refleja el estado de madurez que la sociedad venezolana ha alcanzado en esta materia. La impronta garantista de la Carta Fundamental venezolana, comparado con otras Constituciones latinoamericanas, nos pone de manifiesto la gran brecha existente entre países de un mismo continente y con historias sociales y políticas similares. Lo anterior, debe llamar a la reflexión e instar para que pueda estrecharse esa diferencia en los niveles de desarrollo constitucional de los países latinoamericanos, incluido el chileno.

2.2 Protección Legal de los Datos Personales

En materia legal, se puede afirmar que si bien Venezuela cuenta con un ordenamiento constitucional que reconocería un derecho a la protección de datos personales y que dispone reglas que establecen límites generales al uso de la informática en resguardo de los derechos de las personas, aún no dispone de una ley de protección de datos que desarrolle lo preceptuado por el Constituyente. En este nivel encontramos disposiciones sectoriales que se ocupan en general de establecer deberes de confidencialidad de cierta información personal. A continuación señalaremos las disposiciones pertinentes en la materia y además, reseñaremos un estatuto de dudosa vigencia en la actualidad, dictado por la Junta de Emergencia Financiera venezolana del año 1998 (Resolución Nº 001-06-98), que establece normas relativas al funcionamiento del Sistema de Información Central de Riesgos (SICRI).

547 Los respectivos numerales anteriores, señalan que son atribuciones del Defensor o Defensora del Pueblo: "1. Velar por el efectivo respeto y garantía de los derechos humanos consagrados en esta Constitución y en los tratados, convenios y acuerdos internacionales sobre derechos humanos ratificados por la República, investigando de oficio o a instancia de parte las denuncias que lleguen a su conocimiento. 2. Velar por el correcto funcionamiento de los servicios públicos, amparar y proteger los derechos e intereses legítimos, colectivos o difusos de las personas, contra las arbitrariedades, desviaciones de poder y errores cometidos en la prestación de los mismos, interponiendo cuando fuere procedente las acciones necesarias para exigir al Estado el resarcimiento a las personas de los daños y perjuicios que les sean ocasionados con motivo del funcionamiento de los servicios públicos (…)".

2.2.1) Ley del Banco Central de Venezuela [548]

Esta ley del año 2002, establece dentro del Capítulo II normas relativas a la seguridad y protección de la información que es manejada por el Banco Central. Al respecto se señala por el inciso 2º del artículo 39 que el Banco Central de Venezuela *"deberá satisfacer las peticiones formuladas por los ciudadanos en ejercicio del derecho de acceso a los registros y archivos administrativos previstos en el artículo 143 de la Constitución, salvo por lo que respecta a los documentos e informaciones calificados como secretos o confidenciales".*

Las excepciones al ejercicio del hábeas data impropio recién señaladas, al parecer han sido dejadas a criterio del propio Banco Central, pues además de no remitirse a un texto legal que determine cuál información es de carácter secreta o confidencial, el texto de la ley habla de "calificar" con lo que podría desprenderse que dicho juicio no quedaría entregado precisamente al legislador sino al propio órgano del Estado, a través de su Directorio.

Las reglas anteriores si bien se refieren directamente al ejercicio del derecho de acceso a la información pública o hábeas data impropio, hemos decido señalarlas por la eventual relación con la disposición del artículo siguiente.

A renglón seguido, el artículo 40 dispone que el Directorio del Banco Central de Venezuela *"dictará normas sobre el tratamiento automatizado de datos personales, a fin de salvaguardar los derechos de las personas previstos en la Constitución".* Esta disposición, circunscrita obviamente al propio ámbito de funcionamiento del Banco Central, nos parece que no se condice con el tenor del propio texto de la Constitución, el cual entrega al legislador la tarea de limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos (Artículo 60 inciso 2º). Si se encarga por el Constituyente a la ley la tarea de establecer la regulación respectiva, no se entiende que esta facultad sea dejada en este caso a un órgano de carácter administrativo como lo es el Directorio del Banco Central. Aquí se nota la falta de una ley de protección de datos personales que esté en consonancia con el espíritu de la Constitución de 1999.

2.2.2)Ley General de Bancos y Otras Instituciones Financieras [549]

Esta ley del año 2001 que regula todo lo relativo al funcionamiento del mercado financiero, sólo se refiere al secreto bancario en los siguientes términos:

Artículo 252.- *"El secreto bancario, el secreto profesional o confidencialidad debida no es oponible en modo alguno, a las solicitudes de información realizadas por la Superintendencia de Bancos y Otras Instituciones Financieras en el ejercicio de sus funciones".*

[548] **[En línea] < http://comunidad.derecho.org/pantin/lbcentral.html > [consulta: 10 de Abril 2003].**

[549] **[En línea] < http://comunidad.derecho.org/pantin/bancos.html > consulta: 10 de Abril 2003].**

De lo previsto por el legislador, se entiende que si bien se reconoce este deber de secreto, no se señala en qué consiste ni cuál es la extensión de el, lo cual plantea dificultades para entender a cabalidad una serie de disposiciones que establecen excepciones al deber de secreto. Esas excepciones se señalan a continuación.

El artículo 226, insertado dentro del capítulo relativo a la organización de la Superintendencia de Bancos, dispone que ésta *"tendrá una Unidad Nacional de Inteligencia Financiera a través de la cual podrá solicitar, recibir, analizar, archivar y transmitir a las autoridades de policía de investigación penal competentes y a los fiscales del Ministerio Público la información financiera que requieran para realizar sus investigaciones; así como los reportes de actividades sospechosas sobre legitimación de capitales que deben efectuar a estos organismos de investigación penal todos los entes regidos por el presente Decreto Ley y todos aquellos sujetos regidos por leyes especiales, sometidos a su control".* Agrega el inciso 2º que: *"toda la información requerida por la Superintendencia de Bancos y Otras Instituciones Financieras a través de la Unidad Nacional de Inteligencia Financiera, tendrá carácter confidencial en los términos que señalen las normas que dicte al efecto la Superintendencia de Bancos y Otras Instituciones Financieras".*

De las reglas anteriores, se desprende en primer lugar que el deber de información que tienen las instituciones del sistema financiero para con la Unidad de Inteligencia Financiera sería un caso de excepción al secreto bancario, pues la propia ley obliga a ello. Por otra parte, respecto de la información recibida por esa Unidad se establece un deber general de secreto –entendemos que para los funcionarios de esa Unidad- según los términos o las condiciones dictadas por la propia Superintendencia. A este respecto, debemos señalar que nos parece más propio que el alcance de los deberes de confidencialidad que pesan sobre los funcionarios de la Unidad de Inteligencia Financiera, sean regulados por el legislador y no por la autoridad administrativa. Con ello se ganaría en seguridad jurídica en una materia compleja, como lo es la investigación de presuntos ilícitos de lavado o blanqueo de capitales.

Otras excepciones al secreto bancario se establecen en este mismo Capítulo, así el artículo 233 intitulado "Confidencialidad de la Información" dispone que, sin perjuicio de lo establecido en este Decreto Ley o en otras disposiciones legales, los datos o informaciones obtenidos por la Superintendencia de Bancos y Otras Instituciones Financieras en sus funciones de inspección, supervisión y vigilancia, serán suministrados a una serie de funcionarios y organismos del Estado que señala, previa la correspondiente solicitud [550] . De éstos, llama la atención tanto la mención a la

[550] Los sujetos y organismos del Estado respecto de los cuales no rige el secreto bancario son los siguientes: Presidente de la República, Vicepresidente Ejecutivo de la República, Presidente de la Asamblea Nacional, Defensor del Pueblo, Procurador General de la República, Contralor General de la República, Magistrados Presidentes de las Salas del Tribunal Supremo de Justicia, Fiscal General de la República, Ministro de Finanzas, Presidente del Banco Central de Venezuela, Presidente del Fondo de Garantía de Depósitos y Protección Bancaria, Presidente de la Comisión Nacional de Valores y el Superintendente de Seguros, para fines oficiales. También se agrega a la lista el Ministro del Interior y de Justicia, el Ministro de la Defensa, los órganos del Poder Judicial, y a la administración tributaria, según las leyes, así como a los organismos a que se refieran los acuerdos de cooperación suscritos con otros países (Artículo 233).

Administración Tributaria como a los organismos a que se refieran los acuerdos de cooperación suscritos con otros países; respecto de la Administración Tributaria, nos parece excesivo que tengan tales facultades pues se amplía aún más la cantidad de datos personales en manos del Estado sin ley reguladora. En relación con la excepción referida a "organismos" sin más, nos parece francamente un exceso legislativo, pues no precisa ni el tipo de organismo ni la naturaleza jurídica de los "acuerdos" que autorizarían la cesión de datos, con lo cual se abre indiscriminadamente la puerta a la transmisión internacional de datos personales. Aún más, el penúltimo inciso del artículo 233 señala que: "*cuando las circunstancias lo requieran, la información a que se refiere el párrafo anterior podrá ser suministrada al Presidente del Consejo Bancario Nacional y a organismos de supervisión bancaria y financiera de otros países".* Con ello, en definitiva, la oportunidad, la calidad y el tratamiento de los datos personales que en principio están cubiertos por el secreto bancario, queda entregado al buen criterio de la autoridad administrativa correspondiente, es decir, a la Superintendencia de Bancos.

Finalmente, el artículo 234 establece una obligación de confidencialidad respecto de los organismos y sujetos a quienes se les haya transmitido la información sujeta a secreto bancario, señalado que: *"los receptores de la información a que se refiere el artículo anterior, deberán utilizarla sólo a los fines para los cuales fue solicitada, y responderán de conformidad con las leyes por el incumplimiento de lo aquí establecido".* De esta disposición destaca, al menos, la referencia a la finalidad del uso de la información, con lo cual se morigera en parte las falencias de las normas ya señaladas.

2.2.3) Código Orgánico Tributario [551]

El Código Orgánico Tributario, establece en el artículo 126 que las informaciones y documentos que la Administración Tributaria obtenga por cualquier medio, *"tendrán carácter reservado y sólo serán comunicadas a la autoridad judicial o a cualquier otra autoridad en los casos que establezcan las leyes. El uso indebido de la información reservada dará lugar a la aplicación de las sanciones respectivas".*

En este caso, si bien se establece el deber de secreto, la excepción relativa a cualquier otra autoridad facultada por ley, abre la puerta para que la regla general se transforme en definitiva en la excepción.

Lo recién señalado se agrava con la disposición del artículo 124, la que establece un deber general de cooperación para con la Administración Tributaria, y que pesa sobre diversos organismos e instituciones tanto fiscales como particulares respecto de información general o particular que les sea requerida por el órgano de la administración tributaria [552] . Con todo, se señala por la ley que la información entregada, *"será utilizada única y exclusiva para fines tributarios, y será suministrada en la forma, condiciones y oportunidad que determine la Administración Tributaria"*. Además, se dispone que el incumplimiento de la obligación de informar *"no podrá ampararse en el secreto bancario"*, así como tampoco podrán ampararse *"en el secreto profesional los sujetos que se encuentren en relación de dependencia con el contribuyente o responsable"* (Art. 124, parágrafo único).

551 **[En línea] < http://comunidad.vlex.com/pantin/cot.html > [consulta: 20 de Abril 2003].**

Las disposiciones anteriores, si bien consagran el secreto fiscal o tributario, por otra parte favorecen desmedidamente al fisco en su labor recaudatoria de impuestos, pues no rige para la Administración Tributaria ni el secreto bancario, ni el secreto profesional respecto de los dependientes del contribuyente o responsable del cual se solicita información. En nuestra opinión, una legislación como la señalada -lo cual vale para cualquier sistema jurídico con estas características- pareciera ser excesiva, pues se otorga a un organismo del Estado que de por sí ya cuenta con amplias facultades de control y prevención, desmedidas atribuciones en pos de una mayor recaudación tributaria, lo cual va en detrimento de la vida privada de los contribuyentes. Esto conduce en definitiva a un panoptismo del Estado que a estas alturas debería quedar sólo reducido a la literatura.

2.2.4) Ley de Registro de Antecedentes Penales [553]

Esta ley del año 1979, dispone en el artículo 6° que: *"el Registro de Antecedentes Penales es secreto y los datos que en el consten sólo podrán ser suministrados en los casos determinados por esta Ley"*. Luego agrega que, solamente se expedirán copias simples o certificadas del Registro de Antecedentes Penales, *"a las autoridades públicas, por motivo de la función del proceso penal o por razones de seguridad o de interés social en los casos establecidos por la ley. Las autoridades policiales o administrativas no podrán expedir certificaciones relativas a las faltas policiales o administrativas de las que hayan conocido, sino únicamente al Ministerio de Justicia, cuando este lo considere conveniente"* (Art. 7°).

El artículo 8° a su turno, establece una prohibición de exigir por parte de cualquier persona la exhibición de los antecedentes penales para efectos laborales. Al respecto se señala: *"queda prohibido a cualquier empresa o persona, exigir a los particulares, con ocasión de las ofertas de trabajo y en materia relacionada con el reclutamiento laboral, la presentación de los Antecedentes Penales"*. Sin duda, esta norma tiene por finalidad evitar la discriminación de las personas que han sido condenadas por delitos. Creemos que la regla no puede ser absoluta, pues existen ciertas actividades laborales en las cuales pareciera del todo razonable exigir antecedentes penales, al menos, respecto de ciertos delitos, como por ejemplo, los abusos sexuales en caso de oferta laboral en establecimientos educacionales. Las sanciones a la violación de estas normas se señalarán más abajo en el punto relativo a la responsabilidad penal (Nº 9.3).

Resolución Nº 001-06-98 de la Junta de Emergencia Financiera que establece

[552] Artículo 124.- *"Las autoridades civiles, políticas, administrativas y militares de la República, de los estados y municipios, los colegios profesionales, asociaciones gremiales, asociaciones de comercio y producción, sindicatos, bancos, instituciones financieras, de seguros y de intermediación en el mercado de capitales, los contribuyentes, responsables, terceros y en general cualquier particular u organización, están obligados a prestar su concurso a todos los órganos y funcionarios de la Administración Tributaria y suministrar, eventual o periódicamente, las informaciones que con carácter general o particular se le requieran. Asimismo, los sujetos mencionados en el encabezamiento de este artículo, deberán denunciar los hechos de que tuvieran conocimiento que impliquen infracciones a las normas de este Código, leyes y demás disposiciones de carácter tributario"*.

[553] [En línea] < http://comunidad.derecho.org/pantin/registropenales.html > [consulta: 21 de Noviembre 2002].

normas relativas al funcionamiento del Sistema de Información Central de Riesgos (SICRI) [554]

La normativa que se analizará ahora, fue dictada en 1998 por la Junta de Emergencia Financiera, en uso de las atribuciones que le confería el artículo 3 de la Ley de Regulación de la Emergencia Financiera en concordancia con lo dispuesto en la Ley General de Bancos y otras Instituciones Financieras, entre otras normas. Al respecto, cabe hacer una prevención; tenemos serias dudas acerca de la vigencia de esta normativa dentro del ordenamiento jurídico actual venezolano, pues desde el año 2001 existe una nueva Ley de Bancos que en ninguna parte se refiere al Sistema de Información Central de Riesgos, por lo que la normativa legal en que descansaba uno de los fundamentos jurídicos que autorizaron la regulación que se señala ya no existen [555] .Por otra parte, el texto de la Constitución de 1999 supera la estrechez de la regulación sectorial, por lo cual estimamos que esta Resolución habría sido derogada tácitamente el Constituyente. Con todo, cabe agregar que en la actualidad puede constatarse la existencia de una página Web de la Superintendencia de Bancos venezolana en donde se señala que "toda persona natural o jurídica podrá obtener su información financiera en forma detallada del Sistema de Información Central de Riesgos (SICRI)" [556] , informando además a los usuarios del sistema financiero cómo obtener la información financiera personal, por lo que entendemos que a pesar de nuestros reparos, se seguiría aplicando en la práctica la normativa de 1998. En razón de lo señalado, sólo revisaremos las normas más importantes de esa Resolución a modo de ilustración de ésta.

a) Objeto del SICRI

El articulo 1 inciso 1º de la Resolución Nº 001-06-98 de la Junta de Emergencia Financiera (en adelante la Resolución), dispone que el Sistema de Información Central de Riesgos (SICRI), previsto en el artículo 304 de la Ley General de Bancos (hoy derogada) tiene por objeto: *"la recepción, compilación, procesamiento y posterior suministro, de acuerdo con las disposiciones de las presentes normas, de la información relativa a las obligaciones que cualquier persona natural o jurídica mantenga en calidad de deudor principal o como garante, fiador o avalista, con los bancos, instituciones financieras, entidades y demás entes integrantes del Sistema, a los fines de efectuar un monitoreo adecuado de los niveles de riesgo del sistema financiero nacional".*

b) Integración del SICRI

554 [En línea] < http://www.iijusticia.edu.ar/privacidad/Paises.htm#VE > consulta: 10 de Abril 2003].

555 Por otra parte, dentro de las disposiciones derogatorias de la nueva Ley de Bancos, se señala en el artículo 522 que: *"se derogan las disposiciones contenidas en la normativa prudencial dictada por la Superintendencia de Bancos y Otras Instituciones Financieras, que contravengan este Decreto Ley"*. Si bien la reglamentación no fue dictada por ninguna de las dos instituciones, sí fue dictada por una Junta de Emergencia Financiera, por lo que tenemos dudas acerca del carácter de la normativa dictada en esas condiciones.

556 [En línea] < http://128.58.69.243/sudeban/sicri/reqsicri.htm > [consulta: 10 de Abril 2003].

Según el artículo 3 de la Resolución, el Sistema de Información Central de Riesgos (SICRI) será integrado por: 1). Los bancos e instituciones financieras regidas por la Ley General de Bancos y otras Instituciones Financieras o por leyes especiales; 2) Las Entidades de Ahorro y Préstamo regidas por la Ley del Sistema Nacional de Ahorro y Préstamo, la Ley General de Bancos y otras Instituciones Financieras o por leyes especiales y, 3) Los entes o instituciones no financieras, cuyas leyes especiales les permitan o atribuyan facultades crediticias, previa autorización de la Superintendencia de Bancos y otras Instituciones Financieras [557] .

Por otra parte, compete a la Superintendencia de Bancos y otras Instituciones Financieras regular mediante normas dictadas al efecto, *"todo lo relativo a los detalles sobre el funcionamiento y operación del Sistema, precisando las diferentes vías de comunicación, mecanismos, medidas, fases y pasos a seguir para la compilación, procesamiento, manejo y posterior suministro de los datos e informaciones procesados por el Sistema; así como determinar en cada caso particular su esfera de actuación"* (Articulo 3).

Del tenor de la disposición anterior ya podemos apreciar que nuevamente la normativa iría en contra del texto constitucional, el cual sólo faculta al legislador para regular el uso de la informática (damos por sentado que el procesamiento actual de la información se hace a través de medios informáticos).

c) Funcionamiento del Sistema

El artículo 5 dispone que los integrantes del Sistema, *"estarán obligados a suministrar a la Superintendencia de Bancos y otras Instituciones Financieras, con la periodicidad y en los términos que ésta indique, información sobre sus deudores".* Por su parte, la Superintendencia *"suministrará a los integrantes del Sistema la información procesada, la cual incluirá los datos de identificación del beneficiario del crédito, si se trata de un deudor principal o de un garante, fiador o avalista, que comprenda además un resumen de la deuda y situación de morosidad; en ningún momento se identificarán a las Instituciones acreedoras"* (Art. 6).

Creemos que lo señalado por la disposición resulta de interés, pues introduce un elemento importante a la hora de evaluar el riego de un determinado crédito, cual es, incorporar en el registro información no sólo del deudor principal, sino que también de los terceros que han caucionado esa obligación.

El artículo 8, establece límites en el uso de la información crediticia señalando que los integrantes del Sistema, *"deberán velar por el correcto uso de la información consolidada; la cual se utilizará a los únicos fines de la evaluación crediticia. Por lo tanto, se prohíbe a los mismos, suministrar total o parcialmente a sus clientes o a terceras*

[557] El artículo 4 a su vez, agrega eventualmente a otras instituciones dentro del sistema como el Banco Central de Venezuela u otros entes u organismos. Al efecto se señala: *"La Superintendencia de Bancos y otras Instituciones Financieras incorporará dentro del Sistema de Información Central de Riesgos (SICRI) al Banco Central de Venezuela, el cual podrá igualmente utilizar la información obtenida para fines estadísticos. (…) La Superintendencia de Bancos y otras Instituciones Financieras podrá incorporar al Sistema de Información Central de Riesgos (SICRI) a otros entes u organismos cuando lo considere conveniente".*

personas la información recibida con fines distintos".

A renglón seguido, el artículo 9 establece que: *"toda la información que se obtenga a los fines de alimentar el Sistema de Información Central de Riesgos (SICRI), así como aquella resultante de la posterior compilación, procesamiento y manejo de la información obtenida, es de estricto carácter confidencial. En consecuencia, la Superintendencia de Bancos y otras Instituciones Financieras implementará los mecanismos y medidas internas que garanticen de forma absoluta la confidencialidad de los datos e informaciones que forman parte del Sistema".*

De lo anterior de vislumbran los principio de seguridad y confidencialidad de los datos, consagrados en l a Directiva 95/46 CE.

d) Derecho de acceso, rectificación y supresión de la información

El artículo 10 de la Resolución señala que los deudores tendrán derecho a obtener del Sistema, una *"relación detallada sobre su situación, a los fines de poder proceder a regularizar la misma con las Instituciones acreedoras, y obtener las rectificaciones o supresiones adecuadas, cuando la información existente en el Sistema sea injustificada o inexacta".* Se agrega que "la relación" -o reporte de crédito- se emitirá previa solicitud debidamente motivada por el particular. En el caso de las personas naturales, el trámite podrá ser realizado por el interesado o a través de persona debidamente autorizada; en el caso de las personas jurídicas, dicho trámite será realizado por el Representante Legal de dicha sociedad, debidamente facultado por los Estatutos Sociales de la misma (Art. 10 inciso 2º).

Claramente se establece en la disposición anterior un derecho de acceso parcial -pues no cumple con todos requisitos generalmente admitidos por la doctrina-, así como también un derecho de rectificación y supresión de los datos que no sean veraces o no estén actualizados. Con todo, la acción constitucional de hábeas data, supera con creces el estrecho derecho reconocido por esta Resolución.

El plazo en que debe entregarse la información por parte de los bancos, instituciones financieras, entidades de ahorro y préstamo y otros entes integrantes del Sistema no se señala en la Resolución, sino que ésta sólo dice que: *"debe ser cumplida en los términos que al efecto establezca la Superintendencia de Bancos y otras Instituciones Financieras".* Por último, se agrega que: "*el incumplimiento de la misma acarreará la sanción administrativa contemplada en el artículo 276 ejusdem y en el artículo 88 de la Ley del Sistema Nacional de Ahorro y Préstamo. Igualmente, determinará el diferimiento de la prestación del servicio al miembro del Sistema que se encuentre en el supuesto aquí previsto, hasta tanto no se regularice el cumplimiento de la obligación señalada en este artículo"* (Art. 11).

Por lo tanto, en materia de plazos para cumplir con el deber de información, la Resolución se remite a lo que señale la autoridad administrativa, omitiéndose toda referencia a los plazos en que se deberá rectificar o suprimir la información inexacta o injustificada.

Finalmente, el artículo 13 señala que las dudas que se presenten con motivo de la interpretación y aplicación de la presente Resolución, así como de los casos no previstos,

"serán resueltos por la Superintendencia de Bancos y otras Instituciones Financieras".

En suma, todo el sistema creado por la Resolución del año 1998 gira en torno a la autoridad administrativa Superintendencia de Bancos, con lo cual la resolución de los eventuales conflictos entre los clientes de las instituciones financieras y éstas, suscitados por la información contenida en los reportes de crédito, se resolvería por la vía administrativa según las propias reglas fijadas por la Superintendencia. En esta materia, creemos que tal como está la Resolución, ella no se condice con la normativa constitucional del artículo 28 que consagra un hábeas data de carácter amplio, por lo que en definitiva la normativa de la Resolución limitaría los derechos reconocidos por el Constituyente. Ante esta situación, estimamos que la jurisprudencia debería hacer primar el texto de la Constitución y aplicar directamente sus disposiciones, aunque no exista regulación al respecto, pues en nuestra opinión la regulación parcial y sectorial transitoria de 1998 habría sido derogada tácitamente por el Constituyente en el año 1999. En razón de lo anterior, sólo se incluye en este análisis parcial pero no la consideraremos para otros efectos.

3. Bienes Jurídicos Protegidos por la Legislación de Datos Personales

En esta materia, sólo nos referiremos a la normativa constitucional, dada la falta de ley de protección de datos.

Como se recordará, el artículo 28 de la Constitución venezolana reconoce el derecho a la protección de datos o hábeas data. Respecto de esa configuración se ha dicho por Álvarez y otros (refiriéndose la disposición del Anteproyecto de Constitución), que se observa la consagración expresa tanto del derecho a la libertad informática como de su garantía o tutela, con la acción de hábeas data. Se resalta además por estos autores el reconocimiento de la libertad informática como un "derecho fundamental, autónomo, inherente a la persona humana y de rango constitucional expreso, así como el de su garantía para su tutela efectiva, lo cual supone un avance indiscutible en el proceso de positivización de los derechos que conforman la parte dogmática o material del texto constitucional, con lo cual nuestro constituyente se articula con la tendencia de las más recientes producciones constitucionales latinoamericanas y por otra parte se reconoce uno de los más significativos "derechos humanos de tercera generación", como respuesta a las exigencias de libertad del hombre frente a las nuevas realidades tecnológicas" (sic) [558].

Una jurisprudencia de la Corte Primera de lo Contencioso Administrativo venezolana, conociendo de una acción de amparo constitucional ha señalado que "es pertinente precisar que el hábeas data, como forma de protección en cuanto a los derechos al honor, la reputación y dignidad, tiene un significado y una justificación equivalente al del hábeas corpus como medio de protección de la libertad, en virtud de la naturaleza y jerarquía de los derechos o bienes jurídicos protegidos por cada una de dichas instituciones. Ambas instituciones de rango y previsión constitucional justifican su

[558] Alvarez ''et al''. *op. cit*. [en línea].

existencia en que los derechos por ellas tutelados son esencialísimos y de vital importancia para cualquier persona que interactúa en la sociedad" [559] .

Por otra parte, cabe recordar el artículo 60 de la Constitución, el cual complementa lo dispuesto en el artículo 28 constitucional y señala que: *"Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. (…) La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos".*

Si interpretamos sistemáticamente la configuración constitucional del derecho a la protección de datos venezolana, podemos ver claramente la vinculación de los bienes jurídicos honor, intimidad, vida privada, imagen, confidencialidad y reputación, con la garantía del hábeas data. Junto a éstos, podríamos estimar incluido el derecho a la autodeterminación informativa, que según se desprende del artículo 28 y, en base a lo señalado por la doctrina, constituiría uno de los principales bienes tutelados, pero no el único. Consideramos que el hábeas data venezolano tutela también los bienes jurídicos señalados por el artículo 60 y que estarían implícitamente incluidos en el propio artículo 28 de la Constitución, pues señala que procederá la acción de hábeas data en su versión de actualización, rectificación o destrucción de los datos personales si éstos *"fuesen erróneos o afectasen ilegítimamente sus derechos"* [560] . Por lo tanto, al incluir el término genérico *"derechos"*, no se circunscribiría el Constituyente a la sola protección de un bien jurídico, lo cual en general ha sido constatado por alguna doctrina [561] .

4. Principios Informativos de la Legislación de Protección de Datos Personales

Dada la inexistencia de legislación de protección de datos personales que desarrolle lo preceptuado por el Constituyente y, en atención a la dudosa vigencia de la regulación reglamentaria relativa al funcionamiento del Sistema de Información Central de Riesgos (SICRI), no nos detendremos en este punto.

[559] Sentencia de amparo constitucional de la Corte Primera en lo Contencioso-Administrativa, de fecha 28 de marzo de 2000, redactada por el Magistrado Carlos Mouriño Vaquero. [En línea] < http://www.veedores.org/_VBiblioteca/Biblioteca_jurisprudencia/decision_sobre_habeas_data_INSACA.htm > [consulta: 16-12-2002].

[560] Cabe hacer presente, que aunque el artículo 28 no hable de "hábeas data", éste término si es utilizado expresamente por el artículo 281 de la Carta Fundamental, al otorgarle competencia al Defensor o Defensora del Pueblo para interponer entre otras, la acción *"(..)de hábeas data (…) cuando fuere procedente de conformidad con la ley"*. En virtud de lo anterior, hablamos derechamente de la acción de hábeas data del artículo 28.

[561] En este sentido se pronuncia, Palazzi, para quien el hábeas data protege un complejo de derechos personalísimos, que incluyen la privacidad y la identidad, relacionados a su vez con la imagen y con los conceptos de verdad e igualdad: en Gozaíni, Osvaldo (coord.), *op. cit.,* pág. 29.

5. Regulación Diferenciada o Indiferenciada del Sector Público y Privado

Debido a la ausencia de una legislación general de protección de datos personales en el ordenamiento jurídico venezolano, no nos referiremos a esta materia.

6. Modelos de Tutela

En materia de protección de datos personales, la Constitución de Venezuela contempla expresamente la garantía del hábeas data en el artículo 28. Si bien la acción de hábeas data se establece como un mecanismo independiente del amparo tradicional, cuya reglamentación ha sido entregada a la ley por el Constituyente, aún no se ha dictado la normativa que regule procesalmente esa acción. De lo señalado por la jurisprudencia ya citada en este análisis, se entiende que el ejercicio del hábeas data constitucional, a falta de ley regulatoria, ha de ser encauzada a través de la acción de amparo contemplada en el artículo 27 de la Constitución, y regulada por la Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales de 1988 (en adelante LOADGC) [562] .

continuación se analizará la acción de hábeas data en relación con el procedimiento señalado para la acción de amparo constitucional, dada la omisión legislativa ya señalada en materia de hábeas data.

6.1 La acción de hábeas data

De lo prescrito por el artículo 28 de la Constitución venezolana, se ha entendido que ésta consagra la garantía del hábeas data aunque no utilice precisamente esa denominación. Reafirma lo dicho, lo dispuesto por el artículo 281 Nº 3, el cual se refiere a la acción de hábeas data en forma expresa, señalando que dentro de las atribuciones del Defensor del Pueblo se encuentra la de interponer estas acciones.

6.1.1) Procedencia de la Acción

Como se recordará el artículo 28 constitucional señala que: "*Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos (…)".*

Se ha señalado por Álvarez y otros, comentando el Anteproyecto constitucional, que acertadamente no se hace mención en éste a la condición de que los datos personales se encuentren en archivos o registros automatizados, "con lo cual se deja la posibilidad de otorgar protección a los datos personales contenidos en archivos públicos o privados

[562] [En línea] < http://www.tsj.gov.ve/legislacion/loadgc.html > [consulta: 21 de Noviembre 2002].

con carácter público, no automatizados; es decir, la tutela se otorga independientemente de que los datos se encuentren contenidos en soportes informáticos y con la previsión anterior, se recoge la tendencia de la protección europea de la libertad informática en el sentido que la tutela se otorga sin tomar en cuenta la modalidad que pueda revestir el almacenamiento de los datos personales" [563] . No concordamos con lo señalado por estos autores, pues nos parece preferible que se haga directa alusión por Constituyente tanto a los archivos o registros manuales y automatizados, dado que se gana en claridad y se ahorra todo tipo de interpretaciones que pudiesen restringir el ejercicio del hábeas data del artículo 28.

6.1.2) Legitimación Activa

El texto constitucional, en lo relativo al sujeto activo del hábeas data habla de *"toda persona"* sin distinguir entre personas naturales o jurídicas. Sobre este punto, ya se ha pronunciado alguna jurisprudencia, señalando que "(…) esta Corte declara, que es perfectamente factible la interposición de pretensiones de amparo para garantizar el honor, reputación, etc., así como el habeas data, inclusive cuando sean personas jurídicas las pretendidas víctimas de tales infracciones de derechos constitucionales" (sic) [564] . Sin duda, la discusión anterior pasa primeramente por dilucidar los bienes jurídicos tutelados por el hábeas data para luego determinar si están legitimadas para accionar las personas jurídicas. Por nuestra parte, estimamos que el instituto del hábeas data tutela no sólo a la libertad informática, sino que también otros derechos de la personalidad, como la vida privada e intimidad, incluso el honor. Por lo tanto, no se encontrarían excluidas las personas jurídicas como sujetos activos de la acción de hábeas data, en tanto ésta sólo se fundamente en el derecho a la autodeterminación informativa o libertad informática, mas no en el derecho a la intimidad, la vida privada o el honor, pues estamos con la doctrina que estima que estos derechos sólo son predicables respecto de las personas naturales.

6.1.3) Legitimación Pasiva

Son legitimados pasivos de la acción de hábeas data los responsables de los *"registros oficiales o privados"* (Art. 28). En esta materia, se ha señalado por Álvarez y otros, que el Constituyente parece entender por registros oficiales aquellos archivos bajo la responsabilidad y organización de la Administración Pública en sentido lato (central y descentralizada)" [565] . Debemos hacer presente a este respecto, que el texto original del Anteproyecto constitucional, hablaba de "registros oficiales o privados de carácter público". Las razones de la ulterior modificación no la conocemos, pero entendemos que con la redacción actual, se amplía el ámbito de los sujetos pasivos a los responsables de todo tipo de registro privado, sin distinción [566] .

[563] Alvarez 'et al', *op. cit.*, [en línea].

[564] Sentencia del Primer Tribunal Contencioso Administrativo, *op cit.*, [En línea].

[565] Alvarez 'et al', *op. cit.*, [en línea].

6.1.4) Competencia

En materia de competencia, el Constituyente no se pronuncia y sólo se limita a señalar que podrá solicitarse la actualización, la rectificación o la destrucción de datos, si fuesen erróneos o afectasen ilegítimamente sus derechos *"ante el tribunal competente"*. Por otra parte, el legislador tampoco ha señalado el tribunal competente para conocer de las acciones de hábeas data. Con todo, y dado que los derechos constitucionales no pueden quedar sin protección por falta de regulación legal, se ha admitido la tramitación del hábeas data por la vía del amparo constitucional [567] . Por lo tanto, y haciendo aplicación de las reglas especiales para la tramitación del amparo, serían competentes para conocer del hábeas data "los Tribunales de Primera Instancia que lo sean en la materia afín con la naturaleza del derecho o de la garantía constitucionales violados o amenazados de violación, en la jurisdicción correspondiente al lugar donde ocurrieren el hecho, acto u omisión que motivaren la solicitud de amparo" (Art. 7 LOADGC).

6.1.5) Procedimiento Aplicable

Por aplicación del texto constitucional en materia de amparo (Art. 27), el procedimiento de amparo será oral, público, breve, gratuito y no sujeto a formalidad. Además, la autoridad judicial competente tendrá potestad para restablecer inmediatamente la situación jurídica infringida o la situación que más se asemeje a ella. Todo tiempo será hábil y el tribunal lo tramitará con preferencia a cualquier otro asunto. A nivel legal, la LOADGC regula el procedimiento del amparo. Éste se resume a continuación:

1) *Demanda* **:** la solicitud de amparo se deberá contener: a) Los datos concernientes a la identificación de la persona agraviada y de la persona que actúe en su nombre, y en este caso con la suficiente identificación del poder conferido; b) Residencia, lugar y domicilio, tanto del agraviado como del agraviante; c) Suficiente señalamiento e identificación del agraviante, si fuere posible, e indicación de la circunstancia de localización; d) Señalamiento del derecho o de la garantía constitucionales violados o amenazados de violación; e) Descripción narrativa del hecho, acto, omisión y demás circunstancias que motiven la solicitud de amparo y, f) Cualquiera explicación complementaria relacionada con la situación jurídica infringida, a fin de ilustrar el criterio jurisdiccional. En el caso de instancia verbal, se exigirán, en lo posible, los mismos requisitos (Art. 18).

2) *Restablecimiento de la situación jurídica infringida*: el Tribunal que conozca del amparo tendrá potestad para restablecer la situación jurídica infringida, prescindiendo de

[566] Comentando el texto del Anteproyecto constitucional, se señala por Alvarez y otros autores, que debe entenderse por registros privados con carácter público, "aquellos organizados y dirigidos por personas de carácter privado, pero que por razones de interés general, se requiera la publicidad del tratamiento de los datos personales, como podría ser el caso de las bases de datos administradas por los bancos comerciales y las empresas aseguradoras del sector privado". De lo anterior, entendemos que tal como estaba pensado el hábeas data en el Anteproyecto, no se contemplaba el ejercicio de las acciones de hábeas data respecto del responsable de cualquier archivo de carácter privado.

[567] En este sentido se enmarca la sentencia de amparo tantas veces citada en este análisis, [en línea].

consideraciones de mera forma y sin ningún tipo de averiguación sumaria que la preceda. En este caso, el mandamiento de amparo deberá ser motivado y estar fundamentado en un medio de prueba que constituya presunción grave de la violación o de la amenaza de violación (Art. 22).

3)*Informe :* si el Juez no optare por restablecer inmediatamente la situación jurídica infringida, conforme al artículo 22, ordenará a la autoridad, entidad, organización social o a los particulares imputados de violar o amenazar el derecho o la garantía constitucionales, que en el término de cuarenta y ocho horas, contadas a partir de la respectiva notificación, informe sobre la pretendida violación o amenaza que hubiere motivado la solicitud de amparo. La falta de informe correspondiente se entenderá como aceptación de los hechos incriminados (Art. 23).

4) *Audiencia pública*: el Juez que conozca del amparo, fijará dentro de las noventa y seis horas siguientes a la presentación del Informe por el presunto agraviante o de la extinción del término correspondiente, la oportunidad para que las partes o sus representantes legales expresen, en forma oral y pública, los argumentos respectivos. Efectuado dicho acto, el Juez dispondrá de un término improrrogable de veinticuatro horas para decidir la solicitud de amparo constitucional (Art. 26).

6.1.6) La Sentencia

En cuanto a la sentencia de amparo -que en verdad debiera ser de hábeas data-, debe aplicarse lo preceptuado en el artículo 32 de la LOADGC, el cual señala que la sentencia que acuerde el amparo constitucional deberá cumplir las siguientes exigencias formales: a) Mención concreta de la autoridad, del ente privado o de la persona contra cuya resolución o acto u omisión se conceda el amparo; b) Determinación precisa de la orden a cumplirse, con las especificaciones necesarias para su ejecución y, c) Plazo para cumplir lo resuelto.

Se agrega por la Ley, que contra la decisión dictada en primera instancia sobre la solicitud de amparo se concede recurso de apelación en un solo efecto. Si transcurridos tres días de dictado el fallo, las partes, el Ministerio Público o los procuradores no interpusieren apelación, el fallo será consultado con el Tribunal Superior respectivo, al cual se le remitirá inmediatamente copia certificada de lo conducente. Este Tribunal decidirá dentro de un lapso no mayor de treinta días (Art. 35).

En cuanto a los efectos de la sentencia firme de amparo, se dispone que ésta producirá efectos jurídicos respecto al derecho o garantía objetos del proceso, sin perjuicio de las acciones o recursos que legalmente correspondan a las partes (Art. 36). De lo anterior se sigue que el fallo produce sólo el efecto de cosa juzgada formal.

Finalmente, debemos señalar que el rechazo del amparo no afecta la responsabilidad civil o penal en que hubiese podido incurrir el autor del agravio, ni prejuzga sobre ninguna otra materia (Art. 37), con lo que se reafirma lo señalado recién en cuanto a los efectos de la sentencia de amparo. Con todo, creemos que esos efectos no deben coincidir con los de una acción de hábeas data, la cual debiera producir el efecto de cosa juzgada material.

6.2 Otras Acciones

Dentro del ordenamiento jurídico venezolano, no se contemplan otras acciones pertinentes para la tutela de los bienes jurídicos que fundamentan una protección a los datos personales.

7. Mecanismos de Control

Como consecuencia de la inexistencia de una ley de protección de datos personales que contemple organismos de control de la ley, no nos podremos referir a este punto.

8. Transmisión Internacional de Datos

En materia de transmisión internacional de datos no existe una regulación de carácter general en Venezuela. A pesar de lo anterior, sí encontramos al menos una disposición contenida en la Ley General de Bancos y Otras Instituciones Financieras que al establecer excepciones al secreto bancario se refiere al tema. La excepción se circunscribe a los acuerdos de cooperación suscritos con otros países que permitan la transmisión de datos sujetos al secreto bancario (Art. 233). Como ya se señalara más arriba (punto Nº 2.2.2), esta excepción referida a "organismos" sin más, nos parece francamente un exceso legislativo, pues no precisa ni el tipo de organismo ni la naturaleza jurídica de los "acuerdos"que autorizarían la cesión de datos, con lo cual se abre indiscriminadamente la puerta a la transmisión internacional de datos personales. Aún más, el penúltimo inciso del artículo 233 señala que: "*cuando las circunstancias lo requieran, la información a que se refiere el párrafo anterior podrá ser suministrada al Presidente del Consejo Bancario Nacional y a organismos de supervisión bancaria y financiera de otros países".* Con ello, en definitiva la oportunidad, la calidad y el tratamiento de los datos personales que en principio están cubiertos por el secreto bancario, queda entregado al buen criterio de la autoridad administrativa correspondiente, es decir, a la Superintendencia de Bancos.

9. Régimen de Responsabilidad

En materia de responsabilidad, sólo revisaremos las reglas contenidas en algunos de los estatutos jurídicos más arriba indicados (punto Nº 2.2). Sólo en materia penal se hará referencia a delitos contemplados tanto en leyes sectoriales como en la ley común penal venezolana (Código Penal).

9.1 Responsabilidad Administrativa

En este punto, revisaremos las sanciones establecidas en algunas de las leyes ya analizadas. En el ámbito de la responsabilidad funcionaria y en aquellas materias en las cuales no se señalan sanciones específicas, entendemos que debería aplicarse el estatuto de carácter general que rija a los funcionarios de las entidades públicas, del cual

no disponemos mayor información.

9.1.1) Ley del Banco Central de Venezuela

El artículo 127 de esta ley sectorial, dispone que sin menoscabo de otras responsabilidades que pudieran tener lugar, *"aquel que infrinja el deber de secreto establecido en la presente Ley será sancionado por una cantidad de hasta cuatro mil (4.000) unidades tributarias".* Se agrega que, en la eventualidad que el infractor sea personal al servicio del Banco Central de Venezuela, *"la transgresión será además causal de destitución o despido, según el caso".* El inciso tercero dispone por su lado, que si la infracción es cometida por la firma encargada de la auditoría externa prevista en esta Ley, *"dicha empresa quedará además inhabilitada para realizar auditorías en el Banco Central de Venezuela durante los diez (10) años siguientes a la realización de aquella".* El inciso final de este artículo prescribe que en estos casos, el Directorio del Banco Central de Venezuela determinará la cuantía de la sanción y proveerá su liquidación. De la respectiva sanción se notificará al Ejecutivo Nacional, a la Asamblea Nacional y a la Superintendencia de Bancos y Otras Instituciones Financieras para los fines pertinentes.

Ley General de Bancos y Otras Instituciones Financieras

En lo que respecta a la responsabilidad administrativa de los funcionarios de la Superintendencia de Bancos y Otras Instituciones Financieras, el artículo 279 establece sanciones a conductas genéricas, señalando que las infracciones en que incurran los funcionarios, serán sancionadas conforme a lo establecido en la ley que regule la función pública, sin perjuicio de lo dispuesto en las sanciones establecidas en el Título VII de la Ley. Por su parte, el artículo 416 del Título VII de esa normativa, prescribe que los bancos, entidades de ahorro y préstamo, otras instituciones financieras y casas de cambio, serán sancionados con multa desde el cero coma uno por ciento (0,1%) hasta el cero coma cinco por ciento (0,5%) de su capital pagado cuando: *"(…) 5. Infrinjan las limitaciones y prohibiciones previstas en este Decreto Ley, o con la normativa prudencial que dicte el Banco Central de Venezuela o la Superintendencia de Bancos y Otras Instituciones Financieras".* Por lo tanto, entendemos que las violaciones al deber de secreto bancario, serían sancionadas administrativamente en virtud de las disposiciones recién señaladas.

9.2 Responsabilidad Civil

En esta materia no existen reglas especiales, por lo que deberá estarse a las reglas generales de la responsabilidad civil delictual o cuasidelictual. En este sentido, deben aplicarse las normas de la Sección V (De los Hechos Ilícitos) del Código Civil venezolano, cuyo artículo 1.185 da comienzo a la regulación legal y prescribe:*"El que con intención, o por negligencia o por imprudencia, ha causado un daño a otro, está obligado a repararlo".(…) Debe igualmente reparación quien haya causado un daño a otro, excediendo, en el ejercicio de su derecho, los límites fijados por la buena fe o por el objeto en vista del cual le ha sido conferido ese derecho"* [568] .

[568] [En línea] < http://comunidad.vlex.com/pantin/codigocivil.html > [consulta: 11 de Abril 2003].

9.3 Responsabilidad Penal

A continuación se señalaran tanto los delitos contemplados en leyes sectoriales como en el Código Penal de Venezuela, relacionados con los bienes jurídicos intimidad y vida privada, a falta de normas específicas que tutelen penalmente el derecho a la autodeterminación informativa o derecho a la protección de datos.

9.3.1)Ley General de Bancos y Otras Instituciones Financieras

Esta normativa sanciona en el artículo 444 la revelación de la información confidencial de la siguiente forma: *"Los miembros de la junta administradora, directores, administradores, funcionarios o empleados del banco, institución financiera o casa de cambio, o cualesquiera de las personas sometidas al control de la Superintendencia de Bancos y Otras Instituciones Financieras en virtud de el presente Decreto Ley, que en beneficio propio o de un tercero utilicen, modifiquen, revelen o difundan datos reservados de carácter confidencial que se hallen registrados en medios escritos, magnéticos o electrónicos, serán penados con prisión de ocho (8) a diez (10) años".*

Por otra parte también se sanciona la apropiación de información de los clientes de las instituciones financieras utilizándose medios informáticos, prescribiéndose que:*"Quien a través de la manipulación informática o mecanismo similar, se apodere o altere documentos, cartas, mensajes de correo electrónico o cualquier otro documento o efecto personal remitido por un banco, institución financiera o casa de cambio, a un cliente o usuario de dicho ente, será penado con prisión de ocho (8) a diez (10) años"* (Art. 446).

9.3.2) Código Orgánico Tributario

El artículo 115 de este cuerpo legal señala que constituyen ilícitos sancionados con pena restrictiva de libertad: *"(…) 3 La divulgación o el uso personal o indebido de la información confidencial proporcionada por terceros independientes que afecte o pueda afectar su posición competitiva, por parte de los funcionarios o empleados públicos, sujetos pasivos y sus representantes, autoridades judiciales y cualquier otra persona que tuviese acceso a dicha información".* Esta norma debe entenderse complementada por la del artículo 119 que dispone: *"Los funcionarios o empleados públicos, los sujetos pasivos y sus representantes, las autoridades judiciales y cualquier otra persona que directa o indirectamente, revele, divulgue o haga uso personal o indebido, a través de cualquier medio o forma, de la información confidencial proporcionada por terceros independientes que afecte o pueda afectar su posición competitiva, serán penados con prisión de tres (3) meses a tres (3) años".*

9.3.3) Ley Especial Contra los Delitos Informáticos [569]

Esta ley del año 2001, tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes, o los cometidos mediante el uso

[569] **[En línea] < http://www.tsj.gov.ve/legislacion/ledi.htm > [consulta: 21 de Noviembre de 2002].**

de dichas tecnologías (Art. 1). Los tipos delictivos relacionados con los bienes jurídicos que permiten fundamentar una protección de los datos personales se señalan a continuación.

i) Violación de la privacidad de la data o información de carácter personal:

El artículo 20 dispone que: *"El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias".* Se agrega por el inciso 2º de esta norma que: *"La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero".*

Esta norma permitiría la tutela a los datos personales que formaran parte de un sistema computacional, como podría serlo la contenida en un banco de datos. Lo anterior, dado que puede entenderse que el bien jurídico protegido primariamente por la disposición del artículo 20 es la integridad del sistema computacional, y no los derechos de los titulares de los datos, los cuales aparecen tutelados directamente por el inciso 2º recién señalado.

ii) Violación de la privacidad de las comunicaciones:

Por su parte, el artículo 21 sanciona al que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, con la pena de *"prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias".*

Claramente este artículo tiene por finalidad resguardar la inviolabilidad de las comunicaciones, por lo que sería una norma especial en esta materia. De la tipificación, destacan los particulares medios que pueden ser utilizados para vulnerar ese derecho, cuales son, las tecnologías de la información.

iii) Revelación indebida de data o información de carácter personal:

Finalmente, debemos señalar que el artículo 22 de esta Ley preceptúa que: *"El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aún cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias"*. Se añade por el inciso 2º que si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, *"la pena se aumentará de un tercio a la mitad".* En esta última parte se aumenta la penalidad por agregarse otro desvalor del injusto, como lo es el actuar para lucrarse o perjudicando a un tercero que no es el titular de los datos.

9.3.4 Ley de Registro de Antecedentes Penales

Esta ley, señala en el artículo 13° que sin perjuicio de la aplicación de las sanciones establecidas en la Ley de Carrera Administrativa, el funcionario que revele, comunique o publique los datos contenidos en el Registro de Antecedentes Penales, será sancionado con la pena de tres a quince meses de prisión.

Ley sobre Protección a la Privacidad de las Comunicaciones [570]

Esta normativa del año 1991 tiene por objeto proteger la privacidad confidencialidad, inviolabilidad y secreto de las comunicaciones que se produzcan entre dos o más personas (Articulo 1). Cabe recordar que la Ley Especial Contra los Delitos Informáticos, contempla delitos especiales relacionados con la violación de las comunicaciones privadas, por lo que estimamos no cabría posibilidad de concurso de leyes por una misma conducta en esta materia. Los delitos contemplados en esta ley relacionados con los bienes jurídicos intimidad y vida privada se señalan a continuación.

i) Violación de comunicación:

El articulo 2 de esta Ley dispone que: *"El que arbitraria, clandestina o fraudulentamente grabe o se imponga de una comunicación entre dos personas, la interrumpa o impida, será castigado con prisión de tres (3) a cinco (5) años".* El inciso 2º agrega por su parte que: *"En la misma pena incurrirá, salvo que el hecho constituya delito más grave, quien vele, en todo o en parte, mediante cualquier medio de información, el contenido las comunicaciones indicadas en la primera parte de este articulo".*

Debe entenderse que para la aplicación de esta norma no debe haberse utilizado alguna de las tecnologías de la información, pues si ese fuera el caso entendemos se aplicaría la ley especial ya vista.

Cabe destacar por otra parte, la disposición que sanciona el hostigamiento de las personas utilizando los datos obtenidos ilícitamente. Al respecto el articulo 5 de esta ley dispone: *"El que perturbe la tranquilidad de otra persona mediante el uso de información obtenida por procedimientos condenados en esta Ley y creare estados de angustia, incertidumbre, temor o terror, será castigado con prisión de seis (6) a treinta (30) meses".* Sin duda, esta disposición logra dimensionar el daño psicológico que puede causarse a las personas por el hecho de ser perturbadas con informaciones obtenidas ilícitamente sobre su persona. Entendemos que la información obtenida tiene carácter de privada o íntima, pues no se justificaría que se predicara lo anterior de información pública, aunque puede admitirse que el punto es discutible.

ii) Interrupción, interceptación, grabación comunicaciones por la autoridad policial:

El articulo 6 de esta Ley señala que las autoridades policiales, como auxiliares la administración de justicia podrán impedir, interrumpir, interceptar o grabar

[570] [En línea] < http://www.iijusticia.edu.ar/privacidad/Paises.htm#VE > [consulta: 10 de Abril 2003].

comunicaciones, únicamente a los fines investigación de los siguientes hechos: a) Delitos contra la seguridad o independencia del Estado; b) Delitos previstos en la Ley Orgánica de Salvaguarda del Patrimonio Público; c) Delitos contemplados en la Ley Orgánica sobre Sustancias Estupefacientes o Psicotrópicas; y d) Delitos de secuestro y extorsión [571].

El artículo 8 por su lado, establece un deber de secreto respecto de la información obtenida por la policía, señalando que: *"Toda grabación autorizada conforme a lo previsto en la presente Ley, será de uso exclusivo de las autoridades policiales y judiciales encargadas de su investigación y procesamiento, quedando en consecuencia prohibido a tales funcionarios divulgar la información obtenida".* Finalmente, se dispone que si los funcionarios policiales y judiciales infringen la disposición antes señalada serán castigados con la pena establecida en el artículo 2 de esta Ley aumentada hasta las dos terceras partes.

Las disposiciones anteriores destacan por la importancia asignada a la protección de los derechos de las personas sujetas a la restricción de sus derechos como consecuencia de un proceso judicial incoado en su contra, en especial a los derechos a la vida privada e intimidad. Sin embargo la eventual aplicación de esas normas debe ser estudiada a fondo por los especialistas en la materia.

9.3.6) Código Penal [572]

El Código Penal venezolano, tipifica algunos delitos relacionados con la protección de los bienes jurídicos intimidad y vida privada, con lo cual se completa el catálogo de penas señaladas para los delitos contra estos bienes. Ellos son los siguientes.

a) Violación de domicilio:

Artículo 184.- "*Cualquiera que, arbitraria, clandestina o fraudulentamente se introduzca o instale en domicilio ajeno, o en sus dependencias, contra la voluntad de quien tiene derecho a ocuparlo, será castigado con prisión de quince días a quince meses.*

Si el delito se ha cometido de noche o con violencia a las personas, o con armas, o con el concurso de varios individuos, la prisión será de seis a treinta meses.

571 Luego, el articulo 7 dispone que en los casos señalados en el artículo anterior: "*las autoridades de policía, como auxiliares de la administración de justicia "solicitarán razonadamente al Juez de Primera Instancia en lo Penal, que tenga competencia territorial en el lugar donde se realizaría la intervención, la correspondiente autorización, con expreso señalamiento del tiempo de duración, que no excederá de sesenta (60) días, pudiendo acordarse prórrogas sucesivas mediante el mismo procedimiento y por lapsos iguales de tiempo, lugares, medios y demás extremos pertinentes. El Juez notificará, de inmediato, de este procedimiento al Fiscal del Ministerio Público"* (Artículo 7 inciso 1º). Se agrega además que "*excepcionalmente, en caso de extrema necesidad y urgencia, los órganos de policía podrán actuar sin autorización judicial previa, notificando de inmediato al Juez en Primera Instancia en lo Penal, sobre esta actuación, en acta motivada que se acompañará a las notificaciones y a los efectos de la autorización que corresponda, en un lapso no mayor de ocho (8) horas."* (Artículo 7 inciso 2º). En caso de inobservancia del procedimiento legal, *"la intervención, grabación o interceptación será ilícita y no surtirá efecto probatorio alguno y los responsables serán castigados con prisión de tres (3) a cinco (5) años"* (Artículo 7 inciso final).

572 **[En línea] < http://www.unifr.ch/derechopenal/legislacion/ve/cpveneidx.htm > [consulta: 20 de Abril 2003].**

El enjuiciamiento no se hará lugar sino por acusación de la parte agraviada".

Artículo 185.- "*El funcionario público que con abuso de sus funciones o faltando a las condiciones o formalidades establecidas por la ley, se introduzca en domicilio ajeno o en sus dependencias, será castigado con prisión de cuarenta y cinco días a dieciocho meses.*

Si el hecho fuere acompañado de pesquisas o de algún otro acto arbitrario, la prisión será de seis a treinta meses.

Si consta que el culpable ha obrado por causa de algún interés privado, las penas se aumentarán en una sexta parte".

b) Violación de secreto:

Artículo 186.- *"El que indebidamente abra alguna carta, telegrama o pliego cerrado que no se le haya dirigido, o que indebidamente lo tome para conocer su contenido, aunque no esté cerrado, perteneciendo a otro, será castigado con arresto de ocho a veinte días.*

Si divulgando el contenido, el culpable ha causado algún perjuicio, la pena será de quince días a diez meses de arresto".

Artículo 187.- "*Cualquiera que haya suprimido indebidamente alguna correspondencia epistolar o telegráfica que no le pertenezca, aunque estando cerrada no la hubiera abierto, será castigado con arresto de uno a seis meses.*

Si el hecho ha ocasionado algún perjuicio, el arresto no podrá bajar de cuarenta y cinco días".

Artículo 188.- "*Cualquiera que teniendo una correspondencia epistolar o telegráfica, no destinada a la publicidad, la hiciere indebidamente pública, aunque le haya sido dirigida, siempre que el hecho pueda ocasionar algún perjuicio, será castigado con multa de cincuenta a mil bolívares".*

Artículo 189.- "*El que estando empleado en el servicio de correos o telégrafos, con abuso de su oficio, se adueñare de alguna carta, telegrama, comunicación o cualquiera otra correspondencia no cerrada, o que, estándolo, la abra para conocer su contenido, o la retenga o revele su existencia o contenido a otra persona distinta del título de su destino, será castigado con prisión de quince días a quince meses.*

La misma pena se impondrá al que en servicio y con abuso de los mencionados oficios, suprima alguna de las dichas correspondencias.

Si alguno de los hechos previstos en el presente artículo causare algún perjuicio, la pena de prisión será de tres meses a dos años".

Artículo 190.- "*El que teniendo por razón de su estado, funciones, profesión, arte u oficio, conocimiento de algún secreto cuya divulgación pueda causar algún perjuicio, lo revele, no obstante, sin justo motivo, será castigado con prisión de cinco a treinta días".*

Artículo 191.- *"En lo que concierne a los delitos previstos en los artículos 186, 187, 188 y 190, siempre que el hecho no hubiere ocasionado algún perjuicio que interese al orden público, el enjuiciamiento no se hará lugar sino por acusación de la parte*

agraviada".

10. Conclusiones

El ordenamiento jurídico de la República Bolivariana de Venezuela contempla a nivel constitucional una protección a los datos personales a través de la garantía del hábeas data pero sin señalar procedimiento alguno para el ejercicio de la acción. En este sentido, la tutela del derecho a la protección de datos ha quedado entregada, en la práctica, a los Tribunales de Justicia a través de la acción de amparo, a falta de regulación específica de la acción de hábeas data. Asimismo, el Constituyente también reconoce una protección de los derechos de las personas ante el uso de la informática, entregándose al legislador la tarea de regular la utilización de ésta, cuestión que tampoco se ha llevado a cabo hasta ahora.

En materia legal, Venezuela no posee una ley de protección de datos sino que sólo se prevén disposiciones sectoriales que en general establecen deberes de confidencialidad de ciertas informaciones, de las cuales por cierto, no es posible deducir principios generales en materia de tratamiento y transmisión de datos personales. Por último, cabe hacer presente que no tenemos noticias de Proyectos de Ley en la materia que actualmente se tramiten por el Poder Legislativo. En razón de todo lo anterior, y dada la configuración constitucional del derecho a la protección de datos o hábeas data, urge que el legislador venezolano dicte las normas legales correspondientes que desarrollen las modernas disposiciones constitucionales en la materia.

CAPITULO III. TABLAS COMPARATIVAS

Tabla Nº 1: Identificación de las Normas de Protección de Datos Personales y Naturaleza Jerárquica

PAÍS	IDENTIFICACIÓN DE LAS NORMAS	JERARQUÍA
Argentina	Constitución Política: arts. 18,19, 43 Nº 3 y 75 Nº 22.	Constitucional
	Ley Nº 25.326 (Ley de Protección de Datos Personales).	Legal Federal
	Decreto Reglamentario 1.558/01 de la Ley de Protección de Datos Personales.	Reglamentaria
	Código Civil: arts. 1.071 bis y 1.109 y ss.	Legal Federal
	Ley Nº 21.526 (Ley de Entidades Financieras): arts. 39 y 40.	Legal Federal
	Ley Nº 11.683 (Ley de Procedimientos Fiscales): art. 101.	Legal Federal
	Ley Nº 25.065 (Ley de Tarjetas de Crédito): art. 53.	Legal Federal
	Ley 25.322 (Ley del Registro Nacional de Donantes de Células Hematopoyéticas): art. 4.	Legal Federal
	Comunicación "A" 3.630 del 10.06.02: art. 8.1, del Banco Central de la República.	Comunicación Banco Central
	Ley Nº 712 de la Ciudad Autónoma de Buenos Aires sobre Garantías del Patrimonio Genético Humano: art. 5.	Legal Provincial
	Ley 23.798 (Ley sobre Prevención y Lucha contra el Síndrome de Inmunodeficiencia Adquirida **): arts. 2 y 11.**	Legal Federal
	Decreto Reglamentario Nacional Nº 1.244/91 de la Ley 23.798.	Reglamentaria
	Código Penal: arts. 117 bis y 150 a 157 bis.	Legal Federal
Bolivia		

	Constitución Política: arts. 6º II, 19, 20, 120 y 127.	Constitucional
	Código Civil: arts. 18, 19, 21, 23 y, 984 y ss.	Legal
	Código del Niño, Niña y Adolescente (Ley Nº 2.026-1999): arts. 10 y 229.	Legal
	Ley de Bancos e Instituciones Financieras (Ley Nº 1.488-1993): arts. 86,87 y 89.	Legal
	Ley del Estatuto del Funcionario Público (Ley Nº 2.027-1999): art. 9.	Legal
	Ley de la Abogacía (DL Nº 16.793-1979): art. 10.	Legal
	Código Tributario: arts. 124 a 126 y 132.	Legal
	Ley del Tribunal Constitucional: arts. 94 y ss.	Legal
	Código Penal: arts. 298 a 302	Legal
PAÍS	IDENTIFICACIÓN DE LAS NORMAS	JERARQUÍA
Brasil	Constitución Política: arts. 5; X, XI, XII, LXXII, LXXVII, XXXIII, 105 1.b) y, 108 Ic).	Constitucional
	Ley de Protección al Consumidor (Ley Nº 8.078): arts. 43, 44 y 56.	Legal Federal
	Estatuto del Niño y Adolescente (Ley Nº 8.069): art. 247.	Legal Federal
	Ley Complementaria Nº 105 de 2001 sobre el sigilo de las operaciones de las instituciones financieras: arts. 1, 2 y 10.	Legal Federal
	Resolución Nº 2.724/00 del Banco Central de Brasil.	Resolución
	Ley sobre el Sistema Tributario Nacional (Ley Federal Nº 5.172-1966): arts. 198 y 199.	Legal Federal
	Ley que Regula el Derecho de Acceso a las Informaciones disciplinando la Acción de Hábeas Data (Ley Nº 9.507-1997).	Legal Federal
	Código Penal: arts. 150, 151, 153 y 154.	Legal Federal
Chile		

	Constitución Política: arts. 5 inciso 2º; 19 Nº 4, 5, 26 y art. 20.	Constitucional
	Ley Nº 19.628 sobre Protección de la Vida Privada.	Legal
	Decreto Supremo Nº 779/2000 del Ministerio de Justicia.	Reglamentaria legal
	Decreto Supremo Nº 950/1928 del Ministerio de Hacienda.	Reglamentaria autónoma
	Código Sanitario: arts. 127 y 174.	Legal
	Código Tributario: arts. 6, letra A 6º, 30 inciso 4º y 101.	Legal
	Ley General de Bancos: art. 154.	Legal
	Circular Nº 2.544 de 8 de junio de 1990,Superintendencia de Bancos e Instituciones Financieras.	Otras
	Código del Trabajo: arts. 2º inciso 6º, 154 bis y 477.	Legal
	L.O.C. de Bases Generales de la Administración del Estado: art. 18.	Orgánica Constitucional
	Ley Nº 19.477 (Ley Orgánica del Servicio de Registro Civil e Identificación): art. 4.	Legal
	Código Civil: arts. 1.546, 1.547, 1.556, 1558 y 2.314 y ss.	Legal
	Ley N º 19.223 que tipifica figuras penales relativas a la informática: arts. 2 y 4.	Legal
	Código Penal: arts. 144, 146, 155, 156, 161-A, 246 y 247.	Legal
PAÍS	IDENTIFICACIÓN DE LAS NORMAS	JERARQUÍA
Colombia		

	Constitución Política: arts. 15 y 86.	Constitucional
	Ley Nº 550-1999 (Establece régimen que promueva y facilite la reactivación empresarial): art. 76.	Legal
	Ley Nº 510-1999: art. 114.	Legal
	Ley General de Procedimiento Tributario: arts. 583, 585, 586, 587 y 679.	Legal
	Ley Nº 546, año 1999 (Regula el Financiamiento de las Viviendas): art. 52.	Legal
	Decreto Nº 2.591-1991 (Acción de Tutela).	Decreto con Rango Legal
	Decreto Nº 306-1992 (Reglamenta Decreto Nº 2.591).	Legal
	Código Contencioso Administrativo: art. 76.	Legal
	Código Civil: art. 2.341.	Legal
	Código Penal: arts. 189- 191, 192, 194 y 195.	Decreto Reglamentario
Costa Rica	Constitución Política: arts. 24 y 48.	Constitucional
	Código de Comercio: art. 615.	Legal
	Código Tributario: arts. 115 y 117.	Legal
	Código de la Niñez y la Adolescencia: art. 25.	Legal
	Ley sobre Justicia Penal Juvenil (Ley Nº 7.576): arts. 20 y 21.	Legal
	Ley que Crea el Sistema de Emergencias 911 (Ley Nº 7.566): arts. 12 y 13.	Legal
	Ley de la Jurisdicción Constitucional.	Legal
	Código Civil: arts. 1.045 y 1.046.	Legal
	Código Penal: arts. 196, 196 bis, 197, 198, 201, 202, 203 y 339.	Legal
Cuba	Constitución Política: arts. 9, 56, 57, 62 y 63.	Constitucional
	Normas Generales y Procedimientos Tributarios (Decreto-Ley Nº 169-1997) art. 22.	Legal
	Estatutos del Banco Central de Cuba: art. 35º.	Otros
	Decreto-Ley Nº 173 (sobre Bancos e Instituciones Financieras no bancarias): art. 21 y 81.	Legal
	Código Penal: arts. 287-290.	Legal

PAÍS	IDENTIFICACIÓN DE LAS NORMAS	JERARQUÍA
Ecuador	Constitución Política: arts. 16, 17, 18, 19, 23 Nº 8; 12; 13; 21 y, artículo 94.	Constitucional
	Ley de Control Constitucional.	Legal
	Codificación de la Ley General de Instituciones del Sistema Financiero: arts. 88, 89, 90, 91, 92, 94 y 95.	Legal
	Código Tributario: art. 99 y 101.	Legal
	Ley Nº 67-2002 (Ley de Comercio Electrónico, Firmas y Mensajes de Datos): arts. 5, 9, 32 y disposición general novena.	Legal
	Código Civil: arts. 1.480 y 2.241.	Legal
	Código Penal: arts. 191, 192 y 197-202.	Legal
El Salvador	Constitución Política: arts. 2, 6, 18, 20, 24, 174, 246 y 247.	Constitucional
	Ley de Bancos: arts. 61 y 232.	Legal
	Código Tributario: art. 28.	Legal
	Ley Orgánica de la Superintendencia del Sistema Financiero de El Salvador: art. 37.	Legal
	Código Civil: arts. 2.067 y 2.080.	Legal
	Código Penal: arts. 184-189, 300 y 301.	Legal
	Ley de Procedimientos Constitucionales.	Legal
Guatemala	Constitución Política: arts. 22, 23, 24, 25, 31, 35, 44, 46, 265, 272, 275 y 276.	Constitucional
	Ley de Bancos y Grupos Financieros: art. 63.	Legal
	Ley Orgánica del Banco de Guatemala: arts. 49 y 50.	Legal
	Código Tributario: arts. 30 y 96.	Legal
	Código Penal: arts. 206, 217, 218, 219, 220, 222 y 223.	Legal
	Ley de Amparo, Exhibición Personal y Constitucionalidad (Decreto Nº 1 de 1986)	Decreto con Rango de Ley Constitucional
Honduras	Constitución Política: arts. 16, 18, 59, 63, 64, 70, 76, 99, 100, 183 y 319 Nº 8.	Constitucional
	Código Tributario: arts. 49 y 61.	Legal
	Código Penal: arts. 202,203, 214 y 215.	Legal
PAÍS	IDENTIFICACIÓN DE LAS NORMAS	JERARQUÍA

México	Constitución Política: arts. 6, 7, 8, 16, 103 y 107.	Constitucional
	Ley de Imprenta: art. 9.	Legal Federal
	Ley de Instituciones de Crédito: arts. 17, 112 bis y 118.	Legal Federal
	Código Fiscal de la Federación: arts. 63, 69, 87 y 88.	Legal Federal
	Ley Federal de Protección al Consumidor: arts. 16, 18, 126 y 127.	Legal Federal
	Ley de Protección y Defensa al Usuario de Servicios Financieros: arts. 13, 14 y 15.	Legal Federal
	Ley para regular las Sociedades de Información Crediticia.	Legal Federal
	Ley de Amparo	Legal Federal
	Código Civil: arts. 1.910 y ss.	Legal Federal
	Código Penal: arts. 173, 177, 211 bis y 285.	Legal Federal
Nicaragua	Constitución Política: arts. 26, 29, 45, 182 y 184.	Constitucional
	Legislación Tributaria Común (Decreto Legislativo Nº 713-1962): art. 12.	Legal
	Ley General de Bancos, Instituciones Financieras no Bancarias y Grupos Financieros: arts. 109 y 110.	Legal
	Ley de Amparo.	Legal
	Código Penal: arts. 238, 239, 240, 242, 244 y 248.	Legal
Panamá	Constitución Política: arts. 17, 26, 29, 41 y 50.	Constitucional
	Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores o Clientes (Ley Nº 24-2002).	Legal
	Ley Nº 6-2002 de Transparencia en la Gestión Pública, establece la acción de Hábeas Data y dicta otras disposiciones.	Legal
	Código Fiscal: art. 722.	Legal
	Código Penal: arts. 163-170.	Legal
	Ley Bancaria: arts. 84, 85 y 86.	Legal
Paraguay		

	Constitución Política: arts. 24, 28, 33, 34, 45 y 135.	Constitucional
	Ley que Regula la Información Privada (Ley Nº 1.682).	Legal
	Ley que establece el Nuevo Régimen Tributario paraguayo (Ley Nº 125/91): art. 190.	Legal
	Ley General de Bancos, Financieras y Otras Entidades de Crédito: arts. 84-91.	Legal
	Código Penal: arts. 141-148.	Legal
PAÍS	IDENTIFICACIÓN DE LAS NORMAS	JERARQUÍA
Perú	Constitución Política: arts. 2º Nº 5, 6, 7, 9, 10 y, 18; 3º y, 200º Nº 3.	Constitucional
	Ley que regula las Centrales Privadas de Información de Riesgos y de Protección al Titular de la Información (Ley Nº 27.489).	Legal
	Ley de Transparencia y Acceso a la Información Pública (Ley Nº 27.806).	Legal
	Ley General de la Persona con Discapacidad: art. 12.	Legal
	Ley que crea la Unidad de Inteligencia Financiera-Perú: arts. 3, 12 y 13.	Legal
	Código Tributario: arts. 85 y 186.	Legal
	Ley de Protección al Consumidor: art. 39	Legal
	Ley General del Sistema Financiero y del Sistema de Seguros: arts. 140-143.	Legal
	Ley Orgánica de la Defensoría del Pueblo: art. 9 inciso 2º.	Legal
	Código Civil: arts. 1321 y 1969 y ss.	Legal
	Código Penal: arts. 154, 156, 157, 159, 160, 161, 162 y 165.	Legal
República Dominicana	Constitución Política: art. 8 Nº 3, 9 y 10.	Constitucional
	Ley de Expresión y Difusión del Pensamiento (Ley Nº 6.132): art. 43.	Legal
	Ley General de Bancos: arts. 33 y 34.	Legal
	Código para la Protección de Niños, Niñas y Adolescentes: art. 66.	Legal
	Código Penal: arts. 337 y 337-1.	Legal
	Código Tributario: arts. 47, 258, 259, 260 y 262.	Legal
Uruguay	Constitución Política: arts. 7, 28, 72 y	Constitucional

	332.	
	Ley sobre el Sistema de Intermediación Financiera (Ley Nº 15.322): art. 25.	Legal
	Código Tributario: art. 47.	Legal
	Código Penal: arts. 294, 296, 297, 298, 300, 301 y 302.	Legal
	Ley que establece la Acción de Amparo (Ley Nº 16.011).	Legal
PAÍS	IDENTIFICACIÓN DE LAS NORMAS	JERARQUÍA
Venezuela	Constitución Política: arts. 27, 28, 31, 60 y 143.	Constitucional
	Ley del Banco Central de Venezuela: arts. 39,40 y 127.	Legal
	Ley General de Bancos y Otras Instituciones Financieras: arts. 226, 233, 234, 252, 279, 416, 444 y 446.	Legal
	Código Orgánico Tributario: arts. 115, 119, 124 y 126.	Legal
	Ley de Registro de Antecedentes Penales: arts. 6, 7, 8 y 13.	Legal
	Resolución Nº 001-06-98 de la Junta de Emergencia Financiera que establece normas relativas al funcionamiento del Sistema de Información Central de Riesgos (SICRI).	Resolución
	Ley Especial Contra los Delitos Informáticos: arts. 20-22.	Legal
	Código Civil: art. 1.185 y ss.	Legal
	Código Penal: arts. 184-190.	Legal
	Ley sobre Protección a la Privacidad de las Comunicaciones: arts. 2, 6 y 8.	Legal
	Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales	Legal Orgánica

Tabla Nº 2: Bienes Jurídicos Protegidos por las Normas de Protección de Datos Personales [573]

Tabla Nº 3: Principios Informativos de la Legislación General de Protección de Datos y de la Sectorial Compleja Inspirada en Principios Internacionales Sobre el Tratamiento de Datos.

[573] Sólo en países que cuentan con normas constitucionales y/o con leyes especiales generales o sectoriales complejas en la materia, en base a lo señalado por la doctrina. A falta de doctrina, sólo se indica nuestra opinión en atención a lo preceptuado por cada ordenamiento jurídico, la que irá antecedida del signo (**).

Tabla Nº 3: Principios Informativos de la Legislación General de Protección de Datos y de la Sectorial Compleja Inspirada en Principios Internacionales Sobre el Tratamiento de Datos.	Licitud y lealtad de los archivos de datos	Calidad de los datos	Consentimiento informado del titular de los datos	Seguridad de los datos	**Confidencialidad de los datos**	**Consentimient para la cesión de los datos**
PRINCIPIOS ►						
PAÍSES ▼						
Argentina	-Ley 25.326: art. 3º.	-Ley 25.326: arts. 4º y 23º -Reglamento: art. 4º.	-Ley 25.326: arts. 5º y 6º. -Reglamento: art. 5º.	-Ley 25.326: art. 9º. -Reglamento: art. 9º.	-Ley 25.326: art. 10º.	-Ley 25.326: art 11. -Reglamento art. 11º.
Bolivia	-	-	-	-	-	-
Brasil	-	-Ley de Protección al Consumidor: parágrafo 1º, art. 43.	-	-	-	-
Chile	-Ley 19.628: arts.1º, 2º y 4º.	-Ley 19.628: arts. 6º, 9º, 18 y 21º.	-Ley 19.628: arts. 3º y 4º.	-Ley 19.628: arts. 5º y 11º.	-Ley 19.628: art. 7º	-Ley 19.628: art 4º.
Colombia	-	-	-	-	-	-
Costa Rica	-	-	-	-	-	-
Cuba	-	-	-	-	-	-

PRINCIPIOS ►	Licitud y lealtad de los archivos de datos	Calidad de los datos	Consentimiento informado del titular de los datos	Seguridad de los datos	**Confidencialidad de los datos**	**Conse para la de los**
PAÍSES ▼						
Ecuador	-Ley de	-	-Ley de	-Ley de	-Ley de Comercio	-Ley de

	Comercio Electr., Firmas y Mensajes de Datos: art. 9. -Ley de Control Constitucional: indirectamente, art. 39.		Comercio Electr., Firmas y Mensajes de Datos: art. 9. .	Comercio Electr., Firmas y Mensajes de Datos: indirectamente, art. 32. - Ley de Control Constitucional: indirectamente, art. 39.	Electr., Firmas y Mensajes de Datos: arts. 5, 9, y disposición gral. 9ª.	Elec Mer Dat inci
El Salvador	-	-	-	-	-	-
Guatemala	-	-	-	-	-	-
Honduras	-	-	-	-	-	-
México	-Ley para regular las Sociedades de Información Crediticia: arts. 5, 18 y 20.	-Ley para regular las Sociedades de Información Crediticia: arts. 36, 45 y 47.	-Ley para regular las Sociedades de Información Crediticia: art. 28.	-Ley para regular las Sociedades de Información Crediticia: arts. 7º Nº 5.4 y 22.	-Ley para regular las Sociedades de Información Crediticia: arts. 29 y 38.	-Ley las de Cre
Nicaragua	-	-	-	-	-	-

PRINCIPIOS ► PAÍSES ▼	Licitud y lealtad de los archivos de datos	Calidad de los datos	Consentimiento informado del titular de los datos	Seguridad de los datos	**Confidencialidad de los datos**	**C p d**
Panamá	-Ley Servicio de Información Historial de Crédito de Consumidores: art. 11.	-Ley Servicio de Información Historial de Crédito de Consumidores: arts. 4, 23 Nº 2, 28 N^{OS}. 1 y 3 y, 29 Nº 1.	-Ley Servicio de Información Historial de Crédito de Consumidores: arts. 23 Nº 4º y 24.	-Ley Servicio de Información Historial de Crédito de Consumidores: art. 5	-Ley Servicio de Información Historial de Crédito de Consumidores: art. 6.	-L In H C C ar
Paraguay	-Ley Nº 1.682: arts. 1, 2, 3, 4, 5, y 6.	-Ley Nº 1.682: arts. 7 y 9.	-Ley Nº .682: indirecta y débilmente, art. 5.	-Ley Nº 1.682: indirectamente, arts. 3 y 9.	-	-L ar
Perú	-Ley Centrales Privadas de Información de Riesgos: art. 9.	-Ley Centrales Privadas de Información de Riesgos: arts. 1 y 9	-Ley Centrales Privadas de Información de Riesgos: débilmente, art. 8.	-Ley Centrales Privadas de Información de Riesgos: arts. 5 y 12.	-Ley Centrales Privadas de Información de Riesgos: art. 1.	-L P In R

R. Dominicana	-	-	-	-	-	-
-------Uruguay	-	-	-	-	-	-

D: Existencia de regulación legal diferenciada	1
ID: Inexistencia de regulación legal diferenciada	1
IL: Inexistencia de regulación legal en la materia	1

Tabla Nº 6: Modelos de Tutela Judicial

1: Consentimiento para el tratamiento de datos personales	1
2: Consentimiento para la transmisión o cesión de datos personales	1
3: Tratamiento de los datos sensibles	1
4: Derechos de los titulares de los datos personales	1
5: Excepciones al ejercicio de los derechos de los titulares de datos	1
6: Creación y registro de los archivos, o bancos de datos personales	1
7: Archivos, registros o bancos de datos relativos a encuestas	1
8: Tratamiento manual o automatizado de datos	1
9: Personas jurídicas como titulares de datos	1
10: Transmisión internacional de datos personales	1

Tabla Nº 6: Modelos de Tutela Judicial

PAÍSES	MODELOS DE TUTELA JUDICIAL	
	Específicos	Generales
Paraguay	-Acción de hábeas data (Art. 135 C. Política y art. 8 Ley 1.682).	-Acción de amparo (Art. 134 C. Pol.).
Perú	-Acción de hábeas data (Art. 200 Nº 3 C. Pol. y Ley de Transparencia y Acceso a la Información Pública) -Acción especial hábeas de data (Ley para Regular las Sociedades de Información Crediticia, art. 17).	-Acción de amparo (Ley 23.506).
Rep. Dominicana	-	-
Uruguay	-	-Acción de amparo (Ley de Amparo Nº 16.011).
Venezuela	-	-Acción de amparo (Art. 27 C. Pol. y Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales): a falta de ley que regule el ejercicio de la garantía del hábeas data del art. 28 de la C. Pol.

Tabla Nº 7: Mecanismos de Control

PAÍSES	MECANISMOS DE CONTROL	
	Jurídico	Deontológico
Argentina	-Dirección Nacional de Protección de Datos (Art. 29, Ley 25.326 y art. 29 Reglamento)	- Códigos de conducta (Art. 30, Ley 25.326 y art. 30 Reglamento).
Bolivia	-	-
Brasil	-	-
Chile	-	-
Colombia	-	-
Costa Rica	-	-
Cuba	-	-
Ecuador	-	-
El Salvador	-	-
Guatemala	-	-
Honduras	-	-
México	-Sólo se contemplan mecanismos de control de carácter sectorial (Ley para Regular las Sociedades de Información Crediticia y Ley de Protección al Consumidor).	-
Nicaragua	-	-
Panamá	-Sólo se contemplan mecanismos de control de carácter sectorial (Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores).	-
Paraguay	-	-
Perú	-Sólo se contemplan mecanismos de control de carácter sectorial (Ley para Regular las Sociedades de Información Crediticia).	-
Rep. Dom.	-	-
Uruguay	-	-
Venezuela	-	-

Tabla Nº 8: Regulación de la Transmisión Internacional De Datos Personales

PAÍSES	TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES	
	Sector Público	Sector Privado

Argentina	-Artículo 12, Ley 25.326 y art. 12 Reglamento.	-Artículo 12, Ley 25.326 y art. 12 Reglamento.
Bolivia	-	-
Brasil	-	-
Chile	- Sólo se contempla regulación de carácter parcial sectorial (Art. 6 Letra A Nº 6 Código Tributario).	-
Colombia	-	-
Costa Rica	-	-
Cuba	-	-
Ecuador	-	-
El Salvador	-	-
Guatemala	-	-
Honduras	-	-
México	- Sólo se contempla regulación de carácter parcial sectorial (Art. 69 Código Fiscal de la Federación y art. 117 Bis Ley de Instituciones de Crédito).	-
Nicaragua	- Sólo se contempla regulación de carácter parcial sectorial (Art. 109 de la Ley General de Bancos).	-
Panamá	-	-
Paraguay	-	-
Perú	- Sólo se contempla regulación de carácter parcial sectorial (Art.15, Ley 27.693 que crea la Unidad de Inteligencia Financiera del Perú).	-
Rep. Dominicana	- Sólo se contempla regulación de carácter parcial sectorial (Párrafo 1, artículo 3 de la Ley tributaria Nº 11-01 del año 2001).	-
Uruguay	-	-
Venezuela	- Sólo se contempla regulación de carácter parcial sectorial (penúltimo inciso del artículo 233, Ley General de Bancos y Otras Instituciones Financieras).	-

Tabla Nº 9: Régimen General de Responsabilidad

PAÍSES	CLASES DE RESPONSABILIDAD		
	Administrativa	Civil	Penal

Argentina	*Legislación especial*: -Ley 25.326: art. 31. -Reglamento Ley 25.326: art. 31. *Legislación sectorial*: -Ley sobre Entidades Financieras (Ley Nº 21.526): art. 41. -Ley sobre sistema de Tarjetas de Crédito, Compra y Débito (Ley Nº 25.065): art. 48. *Legislación común*: -Sin información.	*Legislación especial*: -Ley 25.326: art. 11 Nº 4. -Reglamento Ley 25.326: art. 11. *Legislación común*: -Código Civil: arts. 1.071 y ss. (Reglas grales. responsabilidad civil extracontractual).	*Legislación especial*: - Ley 25. 326: art. 32 (introduce en el C. **Penal los arts. 117 bis y 157 bis .** *Legislación sectorial:* Ley de Procedimientos Fiscales: art. 101 inc. 4º en rel. Art. 157 C. Penal. *Legislación común:* -Código Penal: arts. 150-157.
Bolivia	*Legislación sectorial*: -Ley de Bancos e Instituciones Financieras: art. 89. -Código Tributario: arts. 124-126. *Legislación común*: -Estatuto del Funcionario Público: art 9º.	*Legislación común*: -Código Civil: arts. 24 y 984 (Reglas grales responsabilidad civil extracontractual).	*Legislación común*: -Código Penal: arts. 298 al 302.
Brasil	*Legislación sectorial:* -Ley de Protección al Consumidor: art. 56. -Ley de Protección del Niño y del Adolescente: art. 247. -Ley sobre el Sistema Tributario Nacional (Ley Federal Nº 5.172-1966): art. 198. *Legislación común*: -Sin	*Legislación sectorial:* -Ley Complementaria 105 (establece el sigilo bancario): art. 11. *Legislación común:* -Sin información.	*Legislación sectorial:* -Ley Complementaria 105 (establece el sigilo bancario): art. 10. *Legislación común:* -Código Penal: arts. 150, 151,153 y 154.

	información.		

Tabla Nº 9

PAÍSES	CLASES DE RESPONSABILIDAD		
	Administrativa	Civil	Penal
Chile	*Legislación especial:* -Ley 19.628: art. 16 inciso 5º. -Código Sanitario: art. 174. -Código del Trabajo: art. 477. *Legislación sectorial:* -Código Tributario: art. 101. -Ley General de Bancos: art. 19. *Legislación común:* -LOC de Bases Generales de la Administración del Estado: arts. 4 y 18	*Legislación especial:* -Ley 19.628: arts. 11 y 23. *Legislación común:* -Código Civil: arts. 1.546, 1.547, 1.556, 1558 y 2.314 y ss.	*Legislación sectorial:* -Código Tributario: art. 30. -Ley General de Bancos: art. 154. -Ley Nº 19.223: arts. 2 y 4. *Legislación común:* -Código Penal: arts. 144, 146, 155, 156, 161-A, 161-B, 246 y 247.
Colombia	*Legislación común:* -Código Contencioso Administrativo: art. 76º. *Legislación sectorial:* -Ley General de Procedimiento Tributario: art. 679.	*Legislación común*: -Código Civil: art. 2.341 (Reglas grales. responsabilidad civil extracontractual).	*Legislación común:* -Código Penal: arts. 189, 190, 191, 192, 194 y 195.
Costa Rica	-Sin información.	*Legislación común:* -Código Civil: arts. 1.045 y 1.046 (Reglas grales. responsabilidad civil extracontractual)	*Legislación sectorial:* Código Tributario: art. 115. *Legislación común:* -Código Penal: arts. 196, 196 bis, 197, 198, 201, 202, 203 y 339.
Cuba	-Sin información.	*Legislación común:* -Sin información.	*Legislación común:* -Código Penal: arts. 287, 288, 289 y 290.
Ecuador	*Legislación especial:* -Ley de Control	*Legislación común:* -Código Civil: arts. 1.480 y	*Legislación sectorial compleja:* -Ley de

	Constitucional: arts. 42 y 43. *Legislación sectorial:* -Ley General de Instituciones del Sistema Financiero: art. 95. -Código Tributario: art. 101. *Legislación común*: -Sin información.	2.241 (reglas grales. responsabilidad civil extracontractual).	Comercio Electrónico, Firmas y Mensajes de Datos: arts. 57 y 58. *Legislación sectorial:* -Ley Gral. del Sistema de Inst. Financieras: art. 94. *Legislación común*: -Código Penal: arts 191, 192, 197, 198, 199, 200 y 201.

Tabla Nº 9

PAÍS	CLASES DE RESPONSABILIDAD		
	Administrativa	Civil	Penal
El Salvador	*Legislación sectorial:* -Ley Orgánica de la Superintendencia del Sistema Financiero: art. 37. - Código Tributario: art. 28. *Legislación común*: -Sin información.	*Legislación común:* -Código Civil: arts. 2.067 y 2.080 (reglas grales. responsabilidad civil extracontractual).	*Legislación común*: -Código Penal: arts. 184, 185, 186, 187, 188, 189, 300 y 301.
Guatemala	*Legislación sectorial:* -Ley de Bancos: art. 63. -Ley Orgánica del Banco de Guatemala: art. 50. -Código Tributario: art. 96. *Legislación común*: -Sin información.	-Sin información	*Legislación común:* -Código Penal: arts. 206, 217, 218, 219, 220, 222 y 223.
Honduras	-Sin información.	-Sin información	*Legislación sectorial:* -Código Tributario, art. 49. *Legislación común*: -Código Penal: arts. 202, 203, 214 y 215.
México	*Legislación sectorial compleja:* -Ley para regular las Sociedades de Información Crediticia: arts. 53, 54, 55 y 56. *Legislación sectorial* -Código Fiscal de la Federación, art. 88. -Ley Federal de Protección al	*Legislación sectorial compleja*: -Ley para regular las Sociedades de Información Crediticia: arts. 51 y 52. *Legislación sectorial* -Ley de Protección y Defensa al Usuario de Servicios Financieros, art. 15. -Ley de	*Legislación sectorial*: -Ley de Instituciones de Crédito: art. 112 bis. -Ley de Imprenta: art. 10 y 12. *Legislación común:* -Código Penal: arts. 173, 177, 210, 211 bis y 285.

	Consumidor, arts. 126 y 127. *Legislación común*: -Sin información.	Instituciones de Crédito: art. 118. *Legislación común:* -Código Civil, art. 1.910 y ss. (reglas grales. responsabilidad extracontractual).	
Nicaragua	*Legislación sectorial:* -Ley General de Bancos: art. 110. *Legislación común:* -Sin información.	-Sin información.	*Legislación común*: -Código Penal: arts. 238, 239, 240, 242, 244 y 248.

Tabla Nº 9

PAÍS	CLASES DE RESPONSABILIDAD		
	Administrativa	Civil	Penal
Panamá	*Legislación especial*: -Ley de Transparencia en la Gestión Pública: arts. 20 y 22. *Legislación sectorial compleja*: -Ley Servicio de Información Historial de Crédito de Consumidores: arts. 38, 39, 40 y 42. *Legislación sectorial:* -Ley Bancaria: art.86. *Legislación común*: -Sin información.	*Legislación especial*: -Ley de Transparencia en la Gestión Pública art. 21. *Legislación sectorial compleja*: -Ley Servicio de Información Historial de Crédito de Consumidores: arts. 2 y 9. *Legislación común*: -Sin información.	*Legislación común:* -Código Penal: arts. 163, 164, 165, 166, 167, 168, 169 y 170.
Paraguay	*Legislación especial*: -Ley que Regula la Información Privada (Ley Nº 1.682): art. 10. *Legislación sectorial:* -Ley que establece el Nuevo Régimen Tributario: art. 190. -Ley General de Bancos: art. 88. *Legislación común*: -Sin información.	*Legislación común*: -Código Civil: art. 1.833 (Reglas grales. responsabilidad civil extracontractual).	*Legislación común*: -Código Penal: arts. 141, 142, 143, 144, 145, 146, 147 y 148.
Perú	*Legislación especial:* -Ley de Transparencia y Acceso a la Información Pública: arts. 4 y 14. *Legislación sectorial*	*Legislación sectorial compleja*: -Ley para Regular las Sociedades de Información Crediticia: art. 18. *Legislación*	*Legislación común*: -Código Penal: arts. 154, 156, 157, 159, 160, 161, 162 y 165.

	-Ley para Regular las Sociedades de Información Crediticia: arts. 20-22. *Legislación sectorial:* -Ley General del Sistema Financiero y del Sistema de Seguros: art. 141. -Código Tributario, art. 186. *Legislación común*: -Sin información.	*común*: -Código Civil: arts. 1321 y 1969 y ss. (Reglas grales. responsabilidad civil contractual y extracontractual).	

Tabla Nº 9

PAÍS	CLASES DE RESPONSABILIDAD		
	Administrativa	Civil	Penal
Rep. Dominicana	*Legislación sectorial*: -Código Tributario: arts. 258, 259, 260 y 262. -Ley General de Bancos, art. 34. -Código para la Protección de Niños, Niñas y Adolescentes: art. 66. *Legislación común*: -Sin información.	-Sin información.	*Legislación sectorial*: -Ley sobre Expresión y Difusión del Pensamiento: art. 43. *Legislación común*: -Código Penal: arts. 337 y 337-1.
Uruguay	*Legislación sectorial*: -Código Tributario: art. 47. *Legislación común*: -Sin información.	*Legislación común*: -Código Civil: arts. 1.919 y ss. (Reglas grales. responsabilidad civil extracontractual	*Legislación sectorial*: -Ley sobre el Sistema de Intermediación Financiera: art. 25. *Legislación común:* -Código Penal: arts. 294, 296, 297, 298, 300, 301 y 302.
Venezuela	*Legislación sectorial*: -Ley del Banco Central de Venezuela: art. 127. -Ley General de Bancos y Otras Instituciones Financieras: arts., 279 y 416. *Legislación común*: -Sin información.	*Legislación común*: -Código Civil: arts. 1.185 y ss. (Reglas grales. responsabilidad civil extracontractual).	*Legislación sectorial*: -Código Orgánico Tributario: arts. 115 y 119. -Ley de Registro de Antecedentes Penales, art. 13. -Ley General de Bancos y Otras Instituciones Financieras: arts. 444 y 446. -Ley Especial Contra los Delitos Informáticos, arts. 20, 21 y 22. -Ley sobre Protección a la Privacidad de las Comunicaciones:

			arts, 2, 6 y 8. *Legislación común*: -Código Penal: arts. 184, 185, 186, 187, 188, 189, 190 y 191.

CAPITULO IV. ANÁLISIS COMPARATIVO DE LA PROTECCIÓN JURÍDICA A LOS DATOS PERSONALES EN LATINOAMÉRICA

1. Introducción

A lo largo de todo el Capítulo II de esta investigación, fuimos analizando particularmente cada uno de los diecinueve ordenamientos jurídicos latinoamericanos comprendidos en ella, desarrollando diversas áreas temáticas en materia de protección a los datos personales. Esas explicaciones han servido a la vez de base para la elaboración de las tablas comparativas presentadas en el capítulo anterior, las cuales apoyarán el análisis que más adelante desarrollamos.

En este capítulo, específicamente llevaremos a cabo un análisis general del estado actual de la legislación latinoamericana de protección de datos personales, tocando los puntos temáticos más importantes en la materia, para lo cual nos apoyaremos en las tablas comparativas ya vistas, complementadas con la información particular de cada

ordenamiento jurídico, la cual puede consultarse en el Capítulo II de esta memoria.

2. Normativa Latinoamericana de Protección de Datos Personales

A través de nuestro estudio, hemos constatado diversas formas jurídicas de protección a los derechos de los titulares de los datos personales frente al tratamiento de éstos por el Estado y por los particulares. Según la fuente normativa de tal protección, es posible hablar de dos grandes niveles: el constitucional y el infraconstitucional. Cada uno de esos dos niveles presenta a su vez diversos grados de desarrollo; en el ámbito constitucional, puede observarse en Latinoamérica un rango máximo representado por aquellos ordenamientos que prevén expresamente una garantía del hábeas data -algunos incluso estableciendo límites a la informática-, y un rango mínimo, presente en aquellos ordenamientos jurídicos que apenas reconocen indirectamente el derecho a la vida privada. En lo que respecta al plano infraconstitucional, específicamente el legal, los ordenamientos jurídicos latinoamericanos también presentan diversos niveles de complejidad y desarrollo en la materia de nuestro estudio. Así, algunos sistemas cuentan con estatutos de carácter general, plasmados en leyes de protección de datos que pretenden regular la mayor cantidad de ámbitos temáticos a través de normas de carácter sustantivo y procedimental; estas últimas destinadas a la efectiva protección de los derechos de los titulares de los datos. Debemos hacer presente que se ha observado, que comúnmente, tanto las formas de regulación legal general como sectorial de los países estudiados, tienden a coexistir dentro de un mismo ordenamiento jurídico. Por ello, la categorización utilizada no es mutuamente excluyente. Ejemplo de lo anterior puede apreciarse claramente en la Argentina, país que además de contar con una desarrollada ley de protección de datos personales, a su vez dispone de legislación sectorial que complementa el estatuto de carácter general.

Descrita a grandes rasgos la panorámica normativa latinoamericana en relación a la protección de datos personales, pasaremos a analizar en particular el estado de aquélla en los ordenamientos jurídicos estudiados.

2.1 Protección Constitucional

Como hemos visto, de los ordenamientos jurídicos latinoamericanos estudiados casi la mitad de ellos prevé disposiciones constitucionales en materia de protección de datos. Sin embargo, el alcance y extensión de esas normas varía de un país a otro.

Para realizar un análisis comparativo de las diversas formas como se ha reconocido a nivel constitucional el instituto del hábeas data en los ordenamientos jurídicos latinoamericanos estudiados, nos centraremos en tres puntos temáticos específicos, a saber: clases de archivos o bancos de datos objeto de regulación, tipo de tratamiento de los datos personales, y alcance de los derechos reconocidos a los titulares de los datos

personales.

En base a la clase de archivos o bancos de datos (públicos o privados) comprendidos por las normas constitucionales de hábeas data, hemos agrupado los ordenamientos jurídicos latinoamericanos en tres tipos: i) El primer tipo, está compuesto por aquellos ordenamientos que reconocen constitucionalmente el hábeas data tanto respecto de los registros o bancos de datos públicos como privados; ii) El segundo, por aquellos sistemas que junto con alcanzar a los archivos de carácter público o estatales, incluyen sólo algunos archivos o bancos de datos de carácter privado y, iii) Por último, el tercer tipo lo componen sólo los ordenamientos que circunscriben el ámbito objetivo de protección a los registros de carácter públicos o estatales. Los ordenamientos jurídicos no comprendidos en ninguna de las clasificaciones anteriores, obviamente son aquéllos que nada dicen a nivel constitucional en materia de hábeas data, lo cual no significa que en sus respectivas legislaciones no se otorgue tutela a los derechos de las personas ante el tratamiento de sus datos personales.

Dentro de cada uno los tres tipos de ordenamientos jurídicos que disponen de normas constitucionales de hábeas data, tocaremos a la vez los otros dos puntos arriba enunciados, los que servirán de base para nuestro análisis comparativo. Ellos son: a) El punto relativo al tipo de tratamiento de datos, el cual puede ser manual o automatizado, y b) El contenido del derecho reconocido por el Constituyente, el cual puede comprender el solo reconocimiento de un simple derecho de acceso a los datos, hasta la rectificación, actualización, supresión o cancelación de ellos. A continuación se situarán los diversos sistemas jurídicos que prevén normas de protección de datos, según la clasificación ya señalada.

2.1.1) Sistemas Jurídicos cuyas Disposiciones Constitucionales de Protección de Datos Abarcan como Ámbito Objetivo tanto a los Archivos, Registros o Bancos de Datos Públicos como Privados.

Los países cuyos ordenamientos jurídicos incluyen dentro del ámbito objetivo de protección a los datos personales, tanto a los archivos o bancos de datos públicos como privados sin restricción alguna son los siguientes:

a) Colombia: la Constitución colombiana dispone en la materia que todas las personas tienen derecho a *"conocer, actualizar y rectificar"* las informaciones que se hayan recogido sobre ellas "*en bancos de datos y en archivos de entidades públicas y privadas".* Se añade, que en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución (Art. 15 C. Pol.).

La norma colombiana aparece con una configuración bastante amplia, lo cual permite una adecuada tutela a los derechos de los titulares de los datos. Ella no distingue entre tratamiento manual o automatizado de la información, por lo cual entendemos que incluiría a ambos. Cabe criticar de dicho texto el que no haya incluido expresamente el derecho de supresión o eliminación de datos personales. Sin embargo, consideramos que dado el carácter de derecho fundamental atribuido al hábeas data en el ordenamiento jurídico colombiano, podría ampliarse interpretativamente la extensión de la disposición del artículo 15 de la Constitución.

b) Ecuador: en esta materia la Constitución ecuatoriana señala en el artículo 94 que toda persona tendrá *"derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito".* Se añade por la misma que podrá solicitarse ante el funcionario respectivo, la "*actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos"* (Art. 94 inc. 2º C. Pol.).

La configuración del hábeas data ecuatoriano es amplia y permite una adecuada tutela a los derechos de los titulares, pues comprende toda clase de bancos de datos, sin distinguir entre tratamiento mecánico o automatizado de datos. Por otra parte, destaca que no se limiten los derechos de los titulares de los datos, quienes pueden solicitar: el acceso a éstos, lo cual implica conocer tanto el uso como la finalidad que se le de a los datos; la actualización; la rectificación y, la eliminación o anulación de aquéllos.

c) Perú: de lo señalado por el Constituyente peruano en el artículo 200 Nº 3 en relación con el artículo 2º numerales 5º y 6º, podemos afirmar que la "Acción de Hábeas Data", tutela el derecho: a) A solicitar por el titular de los datos sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Salvo las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional (Art. 2º Nº 5º), y b) A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar (Art. 2º Nº 6º).

Si bien lo dicho por el Constituyente peruano no es muy claro, entendemos que del derecho garantizado en el numeral 5º del artículo 2º, se desprendería que el ámbito objetivo de aplicación de la norma comprendería a los archivos, registros y bancos de datos personales cuyo responsable sea el Estado. Luego, de lo prescrito en el numeral 6º, indirectamente se reconocería la procedencia de la acción de hábeas data respecto de los responsables de archivos tanto públicos como privados, pues una de las formas más efectivas de poder controlar que esos archivos no suministren informaciones que afecten la intimidad personal y familiar es otorgando a los respectivos titulares una acción que, a lo menos, permita el acceso a esos datos. De lo contrario, la finalidad de la disposición no se lograría a cabalidad. Por otra parte, se entiende que en cuanto al tipo de tratamiento de datos realizado, la configuración es amplia, pues incluye en el numeral 6º a toda clase de servicios informáticos, sea computarizado o no. Lo anterior no deja de llamar la atención, dado que parecería un contrasentido afirmar la existencia de un servicio informático que no sea computarizado. Al parecer, el término se utilizaría más bien como sinónimo de servicio de información.

Finalmente, puede observarse que si bien el Constituyente peruano ha establecido expresamente la acción de hábeas data, ella sólo sería procedente en la variante de acceso, más no en lo que toca al derecho de rectificación, actualización supresión o eliminación de datos. Con todo, una interpretación extensiva de la garantía permitiría suplir la deficiencia normativa.

d) Venezuela: la previsión constitucional de protección a los datos personales en este ordenamiento jurídico señala en el artículo 28 que toda persona tiene el derecho de

"acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, *así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos"*. También dispone que, queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley. Lo anterior, debe ser complementado con la disposición del artículo 60 la cual señala en el inciso 2º que: *"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos"*.

La configuración constitucional de la protección de datos en Venezuela aparece como la más completa de las ya reseñadas, pues comprende diversos ámbitos que son muy importantes para una regulación legal de la materia, la cual aún no se concreta. Así, el ámbito objetivo de tutela de la norma abarca tanto a los registros oficiales como a los privados, sin distinguir tipos de tratamiento de datos, por lo que comprendería tanto a los archivos mecánicos como automatizados. En lo relativo a los derechos de los titulares, la disposición venezolana alcanza no sólo el acceso, sino que también los derechos de actualización, rectificación o destrucción de los datos o información, si fuesen erróneos o afectasen ilegítimamente los derechos de aquéllos, incluyéndose dentro del derecho de acceso, la facultad de conocer el uso y la finalidad dada a los datos por el responsable del archivo o banco de datos. Por otra parte, el Constituyente venezolano ha endosado al legislador la tarea de establecer las excepciones al derecho de acceso, lo que implica que éste deberá tener en cuenta la importante regla que se desprende del tenor del artículo 60, cual es, que la actividad informática -que deberá regular el legislador- no podrá atentar en contra el honor, la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos, todo lo cual se traduce a la vez en una limitación a la actividad legislativa en la materia.

2.1.2) Sistemas Jurídicos cuyas Disposiciones Constitucionales de Protección de Datos Abarcan como Ámbito Objetivo a los Archivos o Bancos de Datos de Carácter Público o Estatal y sólo algunos Archivos o Bancos de Datos de Carácter Privado.

Los ordenamientos jurídicos latinoamericanos que poseen textos constitucionales con estas características son los siguientes:

a) Argentina: elartículo 43 inciso tercero de la Constitución Argentina, a renglón seguido de la acción de amparo constitucional, dispone que toda persona podrá interponer esta acción para *"tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos"*. Se agrega que no podrá afectarse el secreto de las fuentes de información periodística.

De lo preceptuado por el Constituyente trasandino, se desprende claramente la exclusión de los archivos o bancos de datos de carácter privado, limitación que creemos

no favorece al control del tratamiento de los datos sensibles, el cual como regla general, se encuentra prohibido desde el año 2000 por el artículo 7º de la Ley 25.326. Por lo tanto, no procede en principio, la acción de hábeas data respecto de los responsables de archivos privados, sino sólo de aquéllos destinados a proveer informes. Estimamos que lo anterior es, sin duda, el punto oscuro de la normativa argentina, la cual ha privilegiado el derecho a la inviolabilidad de los papeles privados ante la defensa de la intimidad. Sin embargo, creemos que esa restricción no puede ser obstáculo para negar protección a un titular de datos sensibles afectado por el tratamiento ilegal de éstos por un particular, aunque no provea informes, pues la sola tenencia o control fáctico de ese tipo de datos ya genera un riesgo de utilización indebida. En cuanto al tipo de tratamiento de datos, el Constituyente no distingue, por lo que se entiende que abarcaría tanto a los archivos mecánicos como automatizados (lo confirma la Ley 25.326). Finalmente, destaca de la normativa trasandina el que se comprenda en el derecho de acceso la facultad del titular de los datos para exigir se le informe por el responsable del banco de datos acerca del uso y finalidad de éstos.

b) Brasil: como se recordará, el ordenamiento jurídico brasileño contempla en el artículo 5 LXXII la acción de hábeas data, señalando al efecto que se concederá esta acción: i) Para asegurar el conocimiento de informaciones relativas a las personas solicitantes, constantes en registros o bancos de datos de entidades gubernamentales o de carácter público y ii) Para la rectificación de datos, cuando no se prefiera hacerlos por proceso secreto, judicial o administrativo.

De lo dispuesto por la Constitución del Brasil, se desprende que la acción de hábeas data sólo es procedente respecto de los responsables de los archivos o bancos de datos estatales o de carácter público, por lo que en principio, se excluirían a los archivos de carácter privados. Esta disposición ha sido morigerada por el legislador (Ley de Protección al Consumidor) y la doctrina, concluyéndose, en general, que la acción es procedente no sólo respecto de los órganos del Estado sino que también respecto de aquellas entidades y personas jurídicas privadas que prestan servicios de interés público o servicios para el público. En lo relativo al tipo de tratamiento de datos objeto de la norma, nada se señala, pero entendemos que dada la finalidad de la disposición comprendería a los archivos manuales y automatizados. Por otra parte, cabe hacer presente que la disposición del artículo 5º restringe la extensión del hábeas data sólo al derecho de acceso y rectificación, guardando silencio respecto de la actualización, supresión, cancelación o eliminación de datos. En este punto, pensamos debió haberse puesto mayor acento y reconocer en esta sede las facultades omitidas que cercenan en parte la finalidad del hábeas data. Sin embargo, estimamos que el espíritu de la disposición actual permitiría una interpretación extensiva del instituto. Así lo ha entendido en parte el legislador, el que amplía el objeto del hábeas data, a la "anotación" en los registros o bancos de datos de explicaciones sobre datos verdaderos y justificables que solicite el titular de los datos, aduciendo juicio pendiente o arbitraje, es decir, se faculta al titular a solicitar una mención aclaratoria en el registro impugnado en tanto no se resuelva el litigio respectivo (Art. 7 Ley 9.507).

c) Paraguay: la Constitución del Paraguay como se recordará dispone en el artículo 135 intitulado "Del Hábeas Data" que: *"Toda persona puede acceder a la información y a*

los datos que sobre si misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos".

La disposición anterior, no permite que se ejercite una acción de hábeas data respecto de archivos o bancos de datos particulares. La razón de tal restricción -al igual que en la Argentina-, tiene su base en considerar preeminente al derecho a la inviolabilidad de los papeles privados por sobre el hábeas data o derecho a la protección de datos, cuestión que se discutió y zanjó en el seno del Comisión Constituyente. Reiteramos no compartir esa restricción a nivel constitucional, pues estimamos que ante un conflicto de derechos fundamentales tan intrínsecamente vinculados entre sí (vida privada e intimidad), el decidir entre la tutela de uno u otro, es labor que sólo pueden realizar y resolver los jueces caso a caso, una vez que ha nacido un conflicto de esa entidad y no ex ante. En lo relativo al tipo de tratamiento de datos afectado por la norma, nada se dice, pero al igual que en los demás ordenamientos jurídicos entendemos que debe incluirse tanto a los archivos de carácter manual como automatizados. En cuanto a la extensión de los derechos reconocidos por el hábeas data paraguayo, ellos se ajustan en general a la naturaleza del instituto, cubriendo el derecho de acceso -incluida la facultad de exigir información respecto del uso y finalidad de los datos-, y los derechos de actualización, rectificación y destrucción de los datoscuando fuesen erróneos o afectaren ilegítimamente los derechos del titular.

2.1.3) Sistemas Jurídicos cuyas Disposiciones Constitucionales de Protección de Datos Abarcan como Ámbito Objetivo solamente los Archivos, Registros o Bancos de Datos Públicos.

Dentro de esta categoría sólo se encuentran dos países centroamericanos, los que se señalan a continuación.

a) Guatemala: el ordenamiento jurídico constitucional guatemalteco, como ya lo señalamos en el capítulo II de este trabajo, dispone en el artículo 31 intitulado "Acceso a archivos y registros estatales" que: *"Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos".*

De lo previsto por la norma anterior, se desprende que el derecho de hábeas data reconocido por el Constituyente, sólo puede ser reclamable respecto de los responsables de archivos, fichas o cualquier otra forma de registros estatales. De lo anterior, pensamos que podrían abarcarse tanto a los archivos manuales como automatizados. Estos últimos, quedarían comprendidos bajo el término "cualquier otra forma de registros". En cuanto a la exclusión de los registros o archivos particulares, ello resulta claramente perjudicial para los intereses de los titulares de los datos, dado que el tratamiento de éstos realizado por los privados sin cortapisa jurídica, obviamente también puede vulnerar los derechos de las personas. En lo relativo a la extensión de los derechos reconocidos por la

disposición, destaca la amplitud de éstos, pues comprende el derecho de acceso, incluida la facultad de exigir se informe por el Estado acerca de la finalidad a que se dedica esa información, así como también el derecho de corrección, rectificación y actualización de los datos. Finalmente, cabe destacar de la disposición analizada la expresa prohibición de formación de archivos y registros de filiación política, de la cual podría ciertamente fundamentarse una protección más intensa a los datos sensibles en general.

b) Nicaragua: el Constituyente nicaragüense, reconoce en el Nº 4 del artículo 26, el derecho de toda persona a "*conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información".*

Si bien la configuración anterior es la más modesta de todas las analizadas, no deja de llamar la atención que ella se inserte en la misma disposición que reconoce expresamente el derecho a la intimidad, a la vida privada, el derecho al honor y a la reputación. Dicha configuración podría eventualmente ampliar el área de tutela a los datos personales. La disposición nicaragüense, nada dice respecto del tipo de tratamiento de datos objeto de ella, sin embargo, creemos que al hablarse de "toda información", la forma de tratamiento pasa a ser secundaria, por lo que incluiría tanto a los archivos mecánicos como automatizados. En cuanto a las facultades reconocidas por el hábeas data en Nicaragua, se aprecia que ésta sólo comprendería el derecho de acceso, el cual incluye la facultad de exigir se informe por el Estado el por qué se tiene la información y qué finalidad se le dará a ella.

En suma, de lo anteriormente señalado se desprende que el nivel de protección a los datos personales en sede constitucional en Latinoamérica no es homogéneo, pues dentro de las configuraciones constitucionales que prevén normas expresas en la materia de estudio, cada una presenta características particulares que, en general, parecieran obedecer a patrones propios. La situación anterior, debe entenderse con independencia de la regulación legal respectiva dentro de cada ordenamiento, pues el que un país posea normas constitucionales más o menos desarrolladas en materia de hábeas data, no es indiciario de una regulación legal en la materia de las mismas características. Por el contrario, la realidad muestra que de los países latinoamericanos estudiados que disponen de normas de hábeas data a nivel constitucional, sólo Argentina prevé a nivel legal una legislación de protección de datos de carácter general, seguida muy por debajo de ésta por Paraguay, con una legislación que si bien tiene pretensiones de generalidad, pareciera ser más bien una ley sectorial compleja.

2.2 Protección Legal

A nivel infraconstitucional, el panorama latinoamericano de la protección a los datos personales no es muy alentador. Como ya se hizo presente, el hecho de existir normas de protección de datos a nivel constitucional no significa que el ordenamiento jurídico respectivo contemple una legislación que desarrolle la materia o, al menos regule el ejercicio de la acción de hábeas data constitucional en los países en que éste se prevea. En esta materia podemos mencionar dos casos que ilustrarán lo dicho. Como se recordará, el ordenamiento jurídico Venezolano dispone de dos importantes normas

constitucionales; una establece la garantía del hábeas data (Art. 28 C. Pol.) y la otra señala límites al uso de la informática (Art.60 C. Pol.) en una disposición casi idéntica a la del artículo 18 de la Constitución española de 1978. Ahora bien, no obstante lo prescrito por la Ley Fundamental venezolana, no existe una ley de protección de datos personales que cumpla con el mandato del Constituyente de establecer las excepciones al derecho de acceso y de señalar las limitaciones al uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos. Cabe agregar, que a nivel regional, esta situación no es aislada ni la excepción, pues situaciones similares son constatables también en Brasil, Colombia, Ecuador, Guatemala, Nicaragua y Perú. Por lo que en definitiva, en estos ordenamientos jurídicos todo el instituto ha quedado por el momento entregado al desarrollo jurisprudencial, que salvo el caso de Colombia, no es muy fructífero.

El caso inverso al recién señalado podemos constatarlo en nuestro propio ordenamiento jurídico. Como sabemos, la Constitución del ’80 no contiene previsión alguna referida expresamente al derecho a la protección de datos o hábeas data, sino que sólo reconoce entre otros, los derechos a la vida privada e intimidad de las personas, así como el honor de ellas. A pesar de lo anterior, cuenta desde al año 1999 con una ley de protección de datos personales (Ley Nº 19.628), que si bien presenta ciertas deficiencias, cabe concederle a modo de consuelo el que haya sido la primera ley de protección de datos en Latinoamérica y, junto con la ley argentina (Ley Nº 25.326), las únicas que se ocupan del tema de un modo general no sectorial en la región. No incluimos en esta categoría a la ley paraguaya del año 2000 (Ley Nº 1.682), pues estimamos que no responde al carácter de ley general en la materia, sino más bien a una de carácter híbrida referida más bien al tratamiento de la información relativa a los datos comerciales y patrimoniales.

Dentro de algunos sistemas jurídicos analizados, se ha podido apreciar que varios de ellos disponen de leyes de carácter procedimental que regulan el ejercicio de acciones constitucionales de hábeas data (propio como impropio) y otros, que establecen esas normas procedimentales de manera autónoma a la existencia de una norma constitucional de hábeas data. En el primer caso, se encuentran las legislaciones de Brasil (Ley 9.507), Ecuador (Ley de Control Constitucional) y Perú (Ley 26.301). En el segundo, sólo Panamá (Ley Nº 6-2002).

Otros ordenamientos latinoamericanos estudiados, disponen a nivel legal de estatutos sectoriales que podríamos clasificar en dos grandes grupos: 1) Estatutos sectoriales simples, no inspirados por principios internacionales sobre el tratamiento de datos y, 2) Estatutos sectoriales complejos eventualmente inspirados o influidos por principios y normas internacionales sobre el tratamiento de datos. Dentro del primer grupo mencionado se inserta, en general, la legislación que establece el secreto y la reserva bancaria y financiera, el secreto y la reserva tributaria o fiscal y, variados deberes de cargo que imponen un deber de confidencialidad de cierta clase de información personal, en atención al estado o situación particular de los titulares. Junto a ellos, destacan otros cuerpos legales sectoriales que también establecen algunas reglas de protección de datos, circunscritas a la mínima regulación de las bases de datos de los proveedores de bienes y servicios, y de los derechos de los clientes o consumidores. De la legislación

analizada disponen de esta clase de estos estatutos sectoriales: Brasil (Ley de Protección al Consumidor) y México (Ley Federal de Protección al Consumidor y Ley de Protección y Defensa al Usuario de Servicios Financieros). En lo que respecta al segundo grupo de estatutos sectoriales latinoamericanos -los de carácter complejo-, podemos afirmar que éstos se ocupan comúnmente de regular el mercado de la información comercial, crediticia o de solvencia patrimonial, materializada a través de los denominados 'informes de crédito' o 'reportes de crédito'. Una legislación sectorial compleja que escapa a tal categorización es la ley ecuatoriana de comercio electrónico, firmas y mensajes de datos, la que a propósito de regular la mensajería de datos establece algunas normas de protección de datos personales probablemente influenciada por algunos principios y normas internacionales en la materia. Los ordenamientos jurídicos latinoamericanos exponentes del grupo de estatutos sectoriales complejos eventualmente inspirados en principios internacionales sobre el tratamiento de datos personales, son los siguientes: Ecuador (Ley de Comercio Electrónico, Firmas y Mensajes de Datos), México (Ley para regular las Sociedades de Información Crediticia), Panamá (Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores o Clientes) y Perú (Ley que regula las Centrales Privadas de Información de Riesgos y de Protección al Titular de la Información).

En síntesis, la protección legal dispensada a los datos personales a nivel latinoamericano no es homogénea, siendo la regla general la sola existencia de estatutos sectoriales simples no inspirados en principios internacionales sobre el tratamiento de datos personales, como lo es la legislación que establece el secreto bancario y financiero, así como también la reserva tributaria. En un estadio intermedio, se ubican aquellos ordenamientos jurídicos que conjuntamente con los estatutos recién señalados prevén aquéllos de carácter sectorial complejo eventualmente inspirados en principios internacionales sobre el tratamiento de datos. Estos últimos, significan un cierto avance en la materia a pesar de su restringido ámbito de aplicación normativo, pues en nuestro concepto algunas de esas disposiciones influenciadas eventualmente tanto por las normas internacionales de protección de datos (Directiva 95/46 CE) como por las leyes chilena y argentina, podrían servir de herramienta interpretativa a la hora de salvar vacíos legales a causa de la inexistencia de leyes generales de protección de datos en los respectivos sistemas jurídicos. Finalmente, debemos agregar que en el grado de desarrollo legal más avanzado, se sitúan los ordenamientos jurídicos que poseen leyes más o menos generales de protección de datos personales; algunas de éstas sólo regulan aspectos procesales, otras en cambio, se ocupan también de aspectos sustantivos. De estas últimas, solamente tres sistemas jurídicos disponen de ellas, el argentino, el chileno y el paraguayo. Sin embargo, la ley del Paraguay se ubicaría por debajo de las anteriores dado que aparece como un estatuto híbrido que regula sustantivamente el mercado de la información crediticia y muy sintéticamente el tratamiento de datos en general, siendo casi nula la regulación procedimental de la acción de hábeas data, por lo que en algunos aspectos se acerca bastante más a la categoría de estatuto sectorial complejo.

3. Bienes Jurídicos Protegidos por las Normas de Protección de Datos Personales.

A lo largo del desarrollo de esta investigación, nos hemos percatado de la imposibilidad de centrar o condensar en un sólo bien jurídico todo el derecho a la protección de datos personales o hábeas data, pues como ya se ha dicho, en general, este instituto es concebido a su vez por la doctrina y jurisprudencia como tributario de una serie de derechos y principios que no son exclusivamente reconducibles a la intimidad o a la autodeterminación informativa. La situación anterior se ve reafirmada por aquella doctrina que ha entendido que también el derecho a la protección de datos tutela algo más que la intimidad y la vida privada, salvo que pudiera entenderse el concepto de autodeterminación informativa como omnicomprensivo de cada uno de los diversos intereses reclamados de tutela ante el tratamiento de los datos personales.

En los sistemas jurídicos latinoamericanos que disponen de normas constitucionales y/o leyes de protección de datos personales, podría decirse que, comúnmente, domina la idea que el derecho a la intimidad es el centro de gravedad del hábeas data o derecho a la protección de datos y, que a partir de aquél, se derivarían o agregarían otros bienes jurídicos. Es decir, existirían puntos comunes o áreas tangenciales en materia de bienes jurídicos en donde el derecho a la intimidad, sin duda, es el predominante, secundado por el derecho a la vida privada o 'privacidad'. Ocupa un lugar destacado también en materia de bienes jurídicos, el derecho al honor y el derecho a la propia imagen. Las alusiones expresas al derecho a la autodeterminación informativa en el plano normativo latinoamericano son nulas. En el caso de Chile, debemos recordar que el legislador patrio tuvo la oportunidad de reconocer expresamente el derecho a la autodeterminación informativa en la Ley 19.628, pero dicha propuesta sucumbió ante los embates del gobierno de turno que no se atrevió a dar el paso completo en la materia, cuestión que creemos habría sido de gran importancia para una sólida construcción dogmática del derecho a la protección de datos no sólo en Chile, sino que en toda Latinoamérica, pues como la realidad nos muestra, los modelos jurídicos traspasan fronteras y son eventualmente asimilados en otras latitudes. Sin embargo, debemos recordar que existe alguna doctrina latinoamericana que ha concebido este derecho, al menos, como uno de los bienes jurídicos protegidos por las normas constitucionales algunos países, como: Argentina (según Puccinelli), Brasil (según Morales), Chile (según Nogueira) y Venezuela (según Álvarez y otros). Finalmente, en el ámbito jurisprudencial destaca el caso de Colombia, país en el cual ha sido la propia Corte Constitucional la que ha señalado que el núcleo fundamental del hábeas data estriba en la defensa de la autodeterminación informativa [574] .

Como se ha podido observar a lo largo de este trabajo, la labor de determinación de los bienes jurídicos protegidos en materia de protección de datos, ha sido llevada a cabo

[574] Ver Capítulo II, Análisis de la Protección a los Datos Personales en Colombia, punto Nº 3.

en Latinoamérica mayoritariamente por la doctrina, seguida también de alguna jurisprudencia. Lo anterior, puede ser indiciario de la dificultad del tal cometido, pues para emitir una opinión fundada obviamente no basta el texto de la norma sino que se requiere un profundo y sistemático estudio de cada sistema jurídico en particular. Dicho lo anterior, debemos aclarar que nuestro análisis se limitará a reproducir lo señalado por la doctrina y jurisprudencia que se ha pronunciado en la materia, y a la cual hemos tenido acceso, y sólo en aquellos países en los cuales no disponemos de tales referencias señalaremos nuestra opinión, la que ha sido tomada de los análisis particulares de cada ordenamiento jurídico desarrollado en el Capítulo II de esta memoria. A continuación revisaremos lo señalado por la doctrina y alguna jurisprudencia en materia de bienes jurídicos tutelados por las disposiciones constitucionales y/o leyes especiales en materia de protección de datos personales en Latinoamérica.

De la totalidad de los sistemas jurídicos estudiados en este trabajo y que disponen de normas de protección a los datos personales, sean éstas de carácter constitucional o legal, el derecho a la intimidad ha sido señalado por la doctrina de cada país como uno de los bienes jurídicos tutelados. Estos ordenamientos corresponden a los siguientes países: Argentina, Brasil, Chile, Colombia, Paraguay, Perú y Venezuela. En los ordenamientos jurídicos latinoamericanos en los cuales no hemos encontrado doctrina o jurisprudencia que se pronuncie sobre la materia de estudio, hemos estimado que también estarían presentes en las normas de protección de datos tanto el derecho a la intimidad como el derecho a la vida privada, en lo siguiente países: Guatemala, México, Nicaragua y Panamá.

En lo que respecta al derecho a la vida privada o privacidad como bien jurídico protegido, podemos señalar que además de los sistemas jurídicos recién señalados, la doctrina sólo los menciona respecto de los ordenamientos de Argentina y Chile. Lo anterior, no deja de llamar la atención pues como se ha dicho, es generalizada la doctrina que concibe a la intimidad contenida dentro del ámbito del derecho a la vida privada, entendida como una dimensión más estricta de ésta [575] .

En lo relativo al derecho a la autodeterminación informativa o libertad informática, tenemos que señalar que éste ha sido señalado por alguna doctrina como bien jurídico presente en: Argentina, Brasil, Chile, Colombia y Venezuela. En nuestra opinión, este derecho eventualmente estaría reconocido en los sistemas jurídicos del Perú y del Paraguay.

Por otra parte, el derecho al honor también ha sido mencionado por alguna doctrina latinoamericana como uno de los bienes jurídicos tutelados por las normas de protección de datos en los ordenamientos jurídicos de Argentina, Chile, Colombia, Ecuador y Venezuela.

Se agrega a la lista de bienes jurídicos en Latinoamérica, el derecho a la imagen, el cual ha sido igualmente señalado como uno de los bienes jurídicos protegidos en los ordenamientos jurídicos de Argentina, Chile, Colombia, Ecuador y Paraguay.

Aisladamente, se ha mencionado también el derecho a la identidad en los sistemas

[575] En este sentido, Nogueira Alcalá, Humberto, 1998, *op. cit*., pág. 68.

jurídicos de Argentina y Ecuador. Se ha añadido por otra parte, el derecho a la dignidad en los ordenamientos de Paraguay y Venezuela. Asimismo, el derecho a la reputación ha sido indicado por alguna doctrina en Ecuador y Venezuela. También se ha dicho que se tutelaría –sin mayores fundamentos y de manera más bien liviana a nuestro juicio-la integridad psicofísica en Argentina. Por último, se ha aducido que la libertad y seguridad de las personas, la inviolabilidad del patrimonio documental y el derecho a la libre expresión de la personalidad serían bienes jurídicos protegidos por las normas existentes en Paraguay.

En suma, en materia de bienes jurídicos tutelados por las normas constitucionales o legales de protección de datos personales, no existe unanimidad de pareceres, lo que en general nos lleva a concluir que no existiría un solo bien tutelado sino que por el contrario confluirían diversos bienes jurídicos o intereses encaminados aun mismo objetivo, cual es, proteger a la persona tanto en el ámbito de su libertad como de su dignidad. Sin embargo, puede señalarse que, comúnmente, el derecho a la intimidad se erige como el gran núcleo alrededor del cual se desarrollan los distintos fundamentos doctrinales en materia de protección de datos. En lo relativo al bien jurídico autodeterminación informativa, pensamos que aún no se ha logrado superar el solapado temor de las legislaciones, doctrina y jurisprudencia de convertirlo en la sustancia de la protección de datos, lo cual conllevaría superar y desplazar al derecho a la intimidad del sitial que actualmente ocupa. En tanto ello no suceda, los legítimos intereses de las personas jurídicas o morales quedan en una desmejorada situación que puede perjudicarlos, pues un derecho a la protección de datos basado fundamentalmente en la tutela de la intimidad o la vida privada excluiría del ámbito de protección a los intereses de esas entidades.

4.Principios Informativos de las Leyes de Protección de Datos y de los Estatutos Sectoriales Complejos

Para el análisis de los principios informativos de las diversas normativas latinoamericanas de protección de datos, nos hemos servido de siete principios generales que han sido tomados a modo de guía, tanto de la Directiva 95/46/CE de Protección de Datos Personales, como de la Resolución 45/95 de la Asamblea General de la ONU de 14 de Diciembre de 1990, la cual establece los denominados “Principios Rectores para la Reglamentación de los Ficheros Computarizados de Datos Personales”. Estos principios sin duda están presentes con mayor fuerza en las leyes de protección de datos de Chile y Argentina, aventajando esta segunda a la primera. Por su parte la ley paraguaya de información privada también reconoce ciertos principios pero circunscritos, en general, al tratamiento de datos comerciales, económicos o de situación patrimonial. En tocante a los estatutos sectoriales complejos o más desarrollados en materia de protección de datos, también se visualizan algunos principios, referidos comúnmente a los datos de carácter comercial, económico o de solvencia patrimonial, es decir, contemplados en estatutos que regulan el mercado de la información crediticia. Otros cuerpos legales sectoriales en que hemos avistado principios en la materia, son aquellos referidos a la protección de los

derechos del consumidor. En definitiva, los ordenamientos jurídicos que disponen de cuerpos legales que a tales principios se refieren son los siguientes: Argentina (Ley 25.326 y su respectivo Reglamento), Brasil (Ley de protección al Consumidor), Chile (Ley 19.628 y D.S. 779-2000), Ecuador (Ley de Comercio electrónico, Firmas y Mensajes de Datos), México (Ley para regular las Sociedades de Información Crediticia), Panamá (Ley que regula el Servicio de Información del Historial de Crédito de los Consumidores), Paraguay (Ley 1.682) y Perú (Ley que regula las Centrales Privadas de Información de Riesgos).

A continuación se señalarán los principios informativos y la respectiva normativa en que éstos se han plasmado.

4.1 Principio de la Licitud y Lealtad de los Archivos de Datos.

En base al desarrollo de los análisis particulares de cada legislación latinoamericana comprendida en este estudio, hemos estimado que el principio de la licitud y lealtad de los archivos de datos se encontraría contenido en los siguientes ordenamientos jurídicos y normas respectivas: a) Argentina (Art. 3º Ley 25.326); b) Chile (Arts.1º, 2º y 4º Ley 19.628); c) Ecuador (Art. 9 Ley de Comercio Electrónico y art. 39, Ley de Control Constitucional); d) México (Arts. 5, 18 y 20 Ley para regular las Sociedades de Información Crediticia); e) Panamá (Art. 11, Ley que regula el Servicio de Información del Historial de Crédito de los Consumidores; f) Paraguay (Arts. 1, 2, 3, 4, 5, y 6 Ley Nº 1.682) y, g) Perú (Art. 9 Ley que regula las Centrales Privadas de Información de Riesgos).

De los estatutos recién señalados, el más garantista del principio que revisamos y en el que con mayor fuerza lo expresa, es la ley argentina sobre protección de datos personales (Ley 25.326). Esta Ley lo refuerza a través de la obligatoriedad de la inscripción de los registros de datos en el Registro público que para el efecto lleva la Dirección Nacional de Protección de Datos. En el caso chileno, el legislador sólo ha establecido la obligatoriedad de registro de los bancos de datos a cargo de organismos públicos, pero curiosamente no ha señalado sanción alguna para el caso del incumplimiento de este mandato (Art. 22 Ley 19.628 y D.S.779-2000). La ley paraguaya por su parte, no señala ningún deber de registro de los archivos, más aún establece como regla general la libertad de recopilación de información para uso estrictamente privado (Art. 2 Ley 1.682).

En lo que respecta a las legislaciones de carácter sectorial compleja, si bien la ley panameña que regula el Servicio de Información del Historial de Crédito de los Consumidores no exige la inscripción de los archivos, si establece como requisito para que puedan operar las agencias de información de crédito, la autorización y el registro de éstas ante el órgano de control respectivo, lo cual es condición necesaria para que sea lícita la prestación de los servicios de crédito por parte de esas empresas, con lo cual igualmente se tiende a reforzar el principio en comento(Artículo 11).

4.2 Principio de la Calidad de los Datos

En lo relativo a este principio, podemos señalar que de los análisis particulares a las legislaciones que prevén normas sobre protección de datos, concluimos que se encuentra presente el principio de la calidad de los datos en los siguientes ordenamientos jurídicos y disposiciones respectivas: a) Argentina (Arts. 4º y 23º Ley 25.326 y art. 4º Reglamento); b) Brasil (parágrafo 1º del art. 43, Ley de Protección al Consumidor); c) Chile (Arts. 6º, 9º, 18 y 21º Ley 19.628); d) México (Arts. 36, 45 y 47 Ley para regular las Sociedades de Información Crediticia); e) Panamá (Arts. 4, 23 Nº 2, 28 N^{os} 1 y 3 y, 29 Nº 1, Ley que regula el Servicio de Información Historial de Crédito de Consumidores); f) Paraguay (Arts. 7 y 9 Ley Nº 1.682), y g) Perú (Arts. 1 y 9 Ley Centrales Privadas de Información de Riesgos).

Debemos recordar que de las normas recién señaladas solamente las previstas en los ordenamientos jurídicos argentino y chileno son de aplicación general, es decir, rigen a toda clase de dato susceptible de tratamiento, lo que se traduce normativamente en relación a este principio, en un deber de cuidado o estándar de conducta que pesa sobre los responsables de los registros, archivos y bancos de datos respecto de los titulares de éstos, cual es: mantener las bases de datos actualizadas, con información veraz y exacta.

En el ordenamiento jurídico brasileño, llama la atención que el principio de la calidad de los datos sólo se reconozca en un estatuto sectorial, como lo es la Ley de Protección al Consumidor (Art. 43 parágrafo 1º), y no en una ley general, lo cual sería más consecuente con la disposición constitucional que reconoce el hábeas data (Art. 5º LXXII C. Pol.).

Con mayor claridad, se visualiza el principio de la calidad de los datos en aquellos estatutos sectoriales complejos circunscritos al tratamiento de datos de carácter económico, comercial o de solvencia patrimonial, en donde sólo tiene un área de aplicación de carácter restringido. Destaca de este tipo de legislación la panameña que regula el Servicio de Información del Historial de Crédito de los Consumidores, la cual reconoce expresamente el derecho de los consumidores a la fidelidad de la información (Art. 23 Nº 2). Sin embargo, estimamos que el reconocimiento del principio de la calidad de los datos, aunque se haga dentro de un estatuto de restringida aplicación, podría hacerse extensivo de un modo general a las demás categorías de datos, a fin de salvar la falta de legislación especial y de proteger debidamente los derechos de los titulares en caso de situaciones jurídicas no abarcadas por la normativa sectorial. En este sentido, estimamos que la labor interpretativa extensiva se hará más fácil en aquéllos ordenamientos que dispongan de normas constitucionales que reconozcan el derecho a la protección de datos o hábeas data, como sucede en el caso de Brasil y Perú.

4.3 Principio del Consentimiento Informado del Titular de los Datos

Este tercer principio informativo en materia de tratamiento de datos personales, se encuentra presente en diversos ordenamientos jurídicos latinoamericanos, tanto a través de leyes generales como a través de estatutos sectoriales complejos. Esos estatutos y las respectivas disposiciones legales en las cuales se plasma el principio del consentimiento informado del titular de los datos se señalan a continuación: a) Argentina (Arts. 5º y 6º, Ley 25.326 y, art. 5º del Reglamento); b) Chile (Arts 3º y 4º, Ley 19.628); c) Ecuador (Art.

9 Ley de Comercio Electrónico); d) México (Art. 28 Ley que regula las Sociedades de Información Crediticia) y, e) Panamá (Arts. 23 Nº 4º y 24 Ley que regula el Servicio de Información del Historial de Crédito de los Consumidores). Cabe agregar que este principio se aprecia de manera indirecta en Paraguay (Art. 5 Ley Nº 1.682) y débilmente en Venezuela (Art. 8 Ley que regula las Centrales Privadas de Información de Riesgos).

Debemos hacer presente en relación al principio del consentimiento informado del titular de los datos, que la operatividad de éste, en general, no es amplia. En otras palabras, el que el legislador contemple la exigencia del consentimiento del titular de los datos para que pueda calificarse de lícita su recolección y posterior tratamiento, no significa que esa disposición constituya al mismo tiempo la regla general en la materia. Lo recién dicho se ve claramente reflejado en la generalidad de las leyes de protección de datos, las cuales si bien sientan el principio, también contemplan disposiciones que hacen excepción a ella. En el caso de Argentina, la Ley 25.326 dispone que no se requiere el consentimiento del titular de los datos cuando: 1) La obtención de los datos provenga de fuentes de acceso público irrestricto; 2) Los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de obligación legal; 3) Se trate de listados de datos limitados al nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; 4) Se deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios su cumplimiento y, 5) Se refieran a operaciones que realicen las entidades financieras ,y a las informaciones que reciban de sus clientes afectas al secreto bancario, entre otras (Art. 5º inciso 3º Ley 25.326).

La ley chilena de protección de datos por su parte, si bien contempla el principio del consentimiento informado del titular de los datos en el artículo 4º, también señala excepciones a éste, por lo que en definitiva las excepciones pasan a ser en verdad la regla general y no la salvedad, vaciando de contenido el principio. De esta forma, no se precisa la autorización del titular para el tratamiento de los datos personales: a) Provenientes o recolectados de fuentes accesibles al público: i) Cuando sean de carácter económico, financiero, bancario o comercial; ii) Cuando 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 y iii) Cuando sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios (Artículo 4 inciso 5º) y, b) Que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos (Artículo 4 inciso 6º). Tampoco se necesita el consentimiento del titular de los datos personales cuando el Estado, a través de sus organismos públicos, recabe datos respecto de las materias de su competencia y sujetándose a la Ley 19.628 (Art. 20).

La ley paraguaya en tanto, sólo se referiría indirectamente a este principio, al reconocer en parte el principio del consentimiento informado para la cesión o transmisión de datos que revelen, describan o estimen la situación patrimonial de las personas, su solvencia económica o el cumplimiento de sus obligaciones comerciales (Art. 5º). Al efecto, se señala que los datos tanto de las personas físicas como jurídicas, podrán ser

publicados o difundidos solamente: a) Cuando esas personas hubiesen otorgado autorización expresa y por escrito para que se obtengan datos sobre el cumplimiento de sus obligaciones no reclamadas judicialmente b) Cuando se trate de informaciones o calificaciones que entidades estatales o privadas deban publicar o dar a conocer en cumplimiento de disposiciones legales específicas y, c) Cuando consten en las fuentes públicas de información. De lo recién expuesto es claro que el alcance como principio es más bien restringido. A lo anterior, debe sumarse lo previsto en el artículo 6º, el cual señala en una norma poco clara que podrán ser publicados y difundidos: a) Los datos que consistan únicamente en nombre y apellido, documento de identidad, domicilio, edad, fecha y lugar de nacimiento, estado civil, ocupación o profesión, lugar de trabajo y teléfono ocupacional; b) Cuando se trate de datos solicitados por el propio afectado; y, c) Cuando la información sea recabada en el ejercicio de sus funciones, por magistrados judiciales, fiscales, comisiones parlamentarias o por otras autoridades legalmente facultadas para ese efecto. En definitiva, el principio aparecería reconocido débilmente sólo circunscrito a la información señalada en el artículo 5, siendo más bien de carácter excepcional su aplicación.

En suma, si bien puede afirmarse que las dos leyes más importantes a nivel latinoamericano en materia de protección de datos personales reconocen el principio del consentimiento informado, la operatividad de éste se ve entrabada en el realidad, pues los legisladores argentino y chileno establecen tantas excepciones a él, que como se ha dicho, el principio pasa a quedar vacío de contenido.

La gravedad de la situación anterior, no es dimensionada en una regulación sectorial, la cual por regla general, necesitará de márgenes que escapen al principio del consentimiento del titular para lograr que la actividad que se regula funcione sin el necesario concurso del titular de los datos. Con todo, destaca dentro de la legislación sectorial compleja, la ley panameña que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores, la cual establece como uno de los derechos de los consumidores, el consentir expresamente la recopilación y transmisión de la información (Art. 23 Nº 4).

4.4 Principio de la Seguridad de los Datos

En materia de seguridad de los datos, debemos señalar que diversas leyes se refieren a este principio, tanto de carácter general como sectorial. Algunas veces, el principio es reconocido explícitamente en normas específicas y en otras aparecería de manera indirecta, debiendo deducirse de ciertos deberes o estándares de conducta. De las legislaciones analizadas, podemos señalar que contemplan este principio en mayor o menor grado los siguientes ordenamientos jurídicos: a) Argentina (Art. 9 Ley 25.326 y art. 9º del Reglamento); b) Chile (Arts. 5º y 11º Ley 19.628); c) Ecuador, de manera indirecta (Art. 32 Ley de Comercio Electrónico, Firmas y Mensajes de Datos y art. 39 Ley de Control Constitucional); d) México (Arts. 7º Nº 5.4 y 22 Ley que regula las Sociedades de Información Crediticia); e) Panamá (Art. 5 Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores); f) Paraguay, se forma indirecta (Arts. 3 y 9 Ley Nº 1.682) y, Perú (Arts. 5 y 12 Ley que regula las Centrales Privadas de Información

de Riesgos).

De las legislaciones mencionadas, la argentina se empina como la más protectora y desarrollada en este ámbito, pues establece con claridad los deberes que pesan sobre los responsables de los datos, prohibiendo todo tratamiento que no de seguridades al debido cuidado y manejo de los datos (Art. 9 Ley 25.326). Por su parte, la ley chilena sólo se limita a señalar 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. Estimamos que ese deber debe hacerse extensivo también a quienes recolectan e ingresan la información, pues la actividad que realizan también representa un riesgo de utilización indebida de éstos, salvo que se trate de datos accesibles al público en general. Se evidencia en la ley chilena poca claridad y determinación al respecto. Por último, la ley paraguaya, a pesar de ser concebida como ley general, no contempla directamente reglas al respecto, sino que el principio de seguridad de los datos más bien debe deducirse de otras normas, por lo que estimamos que no estaría suficientemente garantizado.

Por su parte, debemos señalar que las leyes sectoriales complejas latinoamericanas se ocupan de la seguridad de los datos, en general, de manera consistente. Así, la ley mexicana que regula las Sociedades de Información Crediticia (Arts. 7º Nº 5.4 y 22º) señala el deber de adoptar por las Sociedades las medidas necesarias de seguridad y control para evitar el uso indebido de la información, el cual se ve reforzado por la obligación de presentar manuales operativos ante el órgano de control, que establezcan las medidas mínimas de seguridad. La ley panameña, a su vez, reconoce expresamente el principio de seguridad de los datos señalando que los agentes económicos y las agencias de información de datos, deben adoptar las medidas o controles técnicos necesarios para evitar la alteración, pérdida, tratamiento o acceso no autorizado de los datos sobre historial de crédito que manejen o mantengan en sus respectivas bases o bancos de datos (Art. 5). Por último, la ley peruana que regula las Centrales Privadas de Información de Riesgos también dispone de norma expresa en la materia, señalando que las CEPIRS deberán adoptar las medidas de índole técnica y administrativa destinadas a garantizar la seguridad de la información que manejen, a fin de evitar su alteración, pérdida, tratamiento o acceso no autorizado (Arts. 5 y 12).

Finalmente, cabe referirnos a la ley sectorial ecuatoriana de Comercio Electrónico, Firmas y Mensajes de Datos y a la Ley de Control Constitucional, la cual si bien no señala reglas que consagren expresamente el principio de seguridad de los datos, dispone de normas que podrían servir de base para desarrollar el principio y dar una adecuada protección a los titulares de los datos ante el riesgo del uso indebido de éstos.

4.5 Principio de la Confidencialidad de los Datos

Este cuarto principio ha sido previsto también por algunas de las legislaciones que ya hemos señalado. La extensión es variada, por lo que no existe un criterio homogéneo en la materia. Las respectivas normas legales se señalan a continuación precedidas por el país al cual pertenecen: a) Argentina (Art. 10º Ley 25.326); b) Chile (Art. 7º Ley 19.628); c) Ecuador (Arts. 5, 9, y disposición general 9ª Ley de Comercio Electrónico, Firmas y

Mensajes de Datos); d) México (Arts. 29 y 38 Ley para regular las Sociedades de Información Crediticia); e) Panamá (Art. 6 Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores) y, f) Perú (Art. 1 Ley que regula las Centrales Privadas de Información de Riesgos).

De los estatutos que contemplan este principio podemos afirmar nuevamente que la Ley 25.326 argentina es la más clara y amplia, a la vez que desarrolla acertadamente el principio, al disponer como regla general que el responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos, obligación que subsistirá aún después de finalizada su relación con el titular del archivo de datos (Artículo 10º inciso 1º). Por su parte, la ley chilena si bien de similar alcance a la trasandina, entra a distinguir situaciones y no habla de personas que intervengan en el procesamiento de datos, sino de personas que trabajen o hayan cesado sus actividades (Art. 7, Ley 19.628). Respecto de esto último, creemos que es más preciso utilizar la frase de la ley argentina, pues facilita la aplicación de la regla a toda persona que intervenga en el proceso de tratamiento de datos, desde su inicio hasta el final. En lo que respecta a la ley paraguaya en el tema, ésta no se pronuncia.

De las normas sectoriales ya señaladas y referidas al principio de la confidencialidad de los datos, cabe decir que en el caso del Ecuador, la ley de comercio electrónico y mensajería de datos señala expresamente en el artículo 9º que la recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política y la misma Ley. En lo relativo a los estatutos sectoriales complejos, debemos señalar que la ley mexicana establece un amplio deber de secreto respecto de los Usuarios de los servicios proporcionados por las Sociedades de Información de Crédito, sus funcionarios, empleados y prestadores de servicios, los cuales deben guardar confidencialidad sobre la información contenida en los Reportes de Crédito a los que tengan acceso (Arts 29 y 38 Ley para regular las Sociedades de Información Crediticia). En la ley panameña por su lado, se reconoce expresamente el principio, apreciándose similares alcances a los previstos por la ley mexicana, pues dispone por aquélla que tanto los funcionarios públicos como privados que con motivo de los cargos que desempeñen, tengan acceso a la información objeto de esa ley, quedarán obligados a guardar la debida reserva, aún cuando cesen en sus funciones (Artículo 6 inciso 2º). Finalmente, debemos anotar que la ley peruana sólo menciona la confidencialidad dentro de los objetivos de la ley, pero no desarrolla el tema (Art.1º).

4.6 Principio del Consentimiento para la Cesión de Datos

El penúltimo principio que hemos incluido en nuestro análisis señala que la transferencia o transmisión de datos debe estar precedida por la autorización expresa de su titular. Lo que implica además, que los datos sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario, debiendo informarse al titular sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo. De los ordenamientos estudiados, sólo algunos prevén reglas que directamente se refieren a este principio, mientras que otros más bien

disponen de normas de las cuales debe deducirse o entenderse implícito tal principio. Los estatutos en los cuales hemos avistado en mayor o menor medida el principio del consentimiento para la cesión o transmisión se datos se señalan a continuación precedidos de ordenamiento al cual pertenecen: a) Argentina (Art. 11 Ley 25.326 y art. 11º del Reglamento); b) Chile (Art. 4º Ley 19.628); c) Ecuador (Art. 9 y 58 inciso 5º de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos); d) México (Art. 28 Ley para regular las Sociedades de Información Crediticia); e) Panamá (Art. 24 Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores); f) Paraguay (Art. 5 Ley Nº 1.682) y, g) Perú (Art. 8 Ley que regula las Centrales Privadas de Información de Riesgos).

En cuanto a la materia que se analiza, debemos hacer nuevamente presente, al igual como lo hicimos en relación al principio del consentimiento informado para el tratamiento de datos, que no debe confundirse el carácter de principio con la mayor o menor operatividad de éste, pues paradójicamente la regla general en los países que disponen de una ley de protección de datos en Latinoamérica, pasa a ser la cesión o transmisión de datos sin el consentimiento del titular. Así, por ejemplo, si bien la ley argentina del año 2000 reconoce el principio en toda su extensión en el artículo 11 de la Ley 25.326, establece al mismo tiempo en el inciso 3º, diversas excepciones. Ellas son: la autorización legal, la cesión de datos realizada entre dependencias de los órganos del Estado en forma directa dentro de sus respectivas competencias, la cesión de datos relativos a la salud por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, preservándose la identidad de los titulares de los datos mediante mecanismos de disociación adecuados y, la cesión de datos personales en que se haya aplicado un procedimiento de disociación de la información que garantice la no identificación del titular. En el caso de la ley chilena el panorama no es tan alentador como el trasandino, pues la configuración del principio es de carácter tenue y vaga. Entendiéndose por parte de la doctrina chilena que no existe una obligación general de requerir el consentimiento inequívoco y específico del titular para efectuar una comunicación a terceros [576] . Las excepciones al principio, pasan a ser en definitiva la regla general, pues son tan diversas que casi queda sin aplicación el principio [577]

Por su parte, la ley paraguaya Nº 1.682 sólo contempla una disposición de aplicación restringida a los datos que describan la situación patrimonial, solvencia o el cumplimiento de obligaciones comerciales de las personas, en la cual se reconocería el principio del consentimiento para la cesión de los datos. Nuevamente, si bien aparentemente pudiera entenderse que sería de amplia aplicación, en definitiva pasa a convertirse en una regla excepcional de mínima aplicación (Art. 51 letra a Ley 1.682).

En cuanto a las leyes latinoamericanas de carácter sectorial compleja, debemos señalar que tanto en el caso de la ley mexicana que regula las Sociedades de Información Crediticia (Art. 28) como en la legislación panameña que también regula los Servicios de información sobre el historial crediticio de los consumidores (Art. 24), ambas

[576] Herrera Bravo, Rodolfo, op. cit., pág. 25.

[577] Ver Capítulo II, Análisis de la Protección a los Datos Personales en Chile, N[os] 4 y 5.2.3

prevén normas que reconocen el principio en comento y que se traducen en general en que los usuarios de esos servicios o agentes económicos sólo podrán consultar la información existente en una base o banco de datos de una agencia de información de datos, con la autorización escrita del consumidor o cliente. En ambos casos la regla opera ampliamente. En la ley peruana, a su vez, entendemos que el principio estaría reconocido implícitamente en los casos que las Centrales Privadas de Información de Riesgos recolecten esa información directamente de los titulares, pues necesariamente deben informar, entre otras cosas, la existencia del banco de datos, la finalidad de la recolección de la información y *"los potenciales destinatarios de ésta"* (Artículo 8º). Finalmente, la ley ecuatoriana que regula el comercio electrónico y la mensajería de datos, entre otros tópicos, reconocería este principio en el artículo 9 de la Ley 67-2002, al señalar que para la elaboración, transferencia o utilización de bases de datos -obtenidas directa o indirectamente del uso o transmisión de mensajes de datos- se requerirá el "consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros" (Art. 9 inc 1º). Lo anterior se refuerza en el inciso 2º, el cual dispone que los datos personales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. Finalmente, debemos hacer presente que llama la atención que este principio encuentre una tutela a nivel penal en el artículo 58 inciso 5º de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, el cual dispone que: "*La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica".* Sin duda, creemos que esta disposición aparecería claramente tutelando a nivel penal, el principio del consentimiento del titular para la transmisión de datos. Queda, sin embargo, la duda en cuanto al ámbito de aplicación de la respectiva norma, pues ella está circunscrita a la mensajería de datos.

4.7.-Principio de la Finalidad

Este último principio se vincula estrechamente con los anteriormente señalados, por cuanto la operatividad de él se traduce en un deber de conducta que pesa sobre los responsables de un registro, archivo o banco de datos, quienes están obligados a utilizar los datos de un modo correspondiente a la finalidad para la cual fueron recolectados, lo cual debe especificarse y justificarse. Junto con ello, y en el momento de la creación del fichero, éste debe ser objeto de una medida de publicidad o ponerse en conocimiento de la persona interesada a fin de poder posteriormente comprobarse que: a) todos los datos personales reunidos y registrados siguen siendo pertinentes a la finalidad perseguida, b) que ninguno de esos datos personales es utilizado o revelado sin el consentimiento de la persona interesada, con un propósito incompatible con el que se haya especificado y, c) que el período de conservación de los datos personales no excede del necesario para alcanzar la finalidad con que se han registrado.

Precisados los alcances del principio de la finalidad, debemos hacer presente una situación que sin duda es de máxima importancia para el desarrollo del principio de la

finalidad a nivel legal en no pocos países de Latinoamérica; a lo largo de este estudio hemos podido constatar que a nivel constitucional, diversos ordenamientos jurídicos reconocen como derecho de los titulares de datos -unido principalmente al derecho de acceso- el conocer el uso y la finalidad que se dará a éstos, ya sea por los responsables de archivos, registros o bancos de datos de carácter estatal o privados, según sea la configuración del derecho a la protección de datos particular de cada sistema jurídico. La importancia de ello radica en que el propio Constituyente reconoce el ámbito central del principio de la finalidad, el cual sin duda puede ser desarrollado en toda su extensión a nivel infraconstitucional. Por lo tanto, entendemos que el reconocimiento del principio de la finalidad en esa sede, generalmente en carácter de garantía, implica que éste debe aplicarse directamente y obliga a interpretarlo extensivamente, exista o no ley de protección de datos. Tal situación ocurriría en diversos países de los estudiados, y curiosamente, en varios que no disponen ni de leyes generales ni sectoriales en la materia. Los ordenamientos jurídicos en los cuales estimamos se reconocería el principio de la finalidad a nivel constitucional son los siguientes: Argentina (Art. 43 inc. 3º C. Pol.), Ecuador (Art. 94 C. Pol.), Guatemala (Art. 31 C.Pol.), Paraguay (Art. 135 C.Pol.), Nicaragua (Art. 26 Nº 4 C.Pol.) y Venezuela (Art. 28 C. Pol.). Por último, debemos aclarar que en este punto de análisis sólo se comprenderá la legislación general o sectorial en materia de protección de datos, teniendo presente, cuando corresponda, la normativa constitucional recién señalada referida al principio de la finalidad.

A continuación, pasaremos a enunciar los ordenamientos jurídicos latinoamericanos comprendidos en este estudio que de alguna forma reconocen en sus respectivas legislaciones de protección de datos -sean éstas generales o sectoriales- el principio en estudio. Estos son los siguientes: Argentina (Arts. 3º, 4º,6º, 11º y 22 Ley 25.326 y, arts. 3º y 4º del Reglamento), Brasil de manera indirecta (Parágrafo 2º del artículo 43 Ley de Protección al Consumidor), Chile (Arts. 3º, 4º, 5º, 9 y 22 Ley 19.628 y, art. 3º del Reglamento), Ecuador (Disposición Gral. 9ª y Glosario de Ley de Comercio Electrónico, Firmas y Mensajes de Datos y, art. 39 Ley de Control Constitucional), México (Art. 22 y 28 Ley para regular las Sociedades de Información Crediticia y, art. 18 Ley de Protección al Consumidor), Panamá (Art. 23 Nº 1 Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores), Paraguay (Art. 8 Ley Nº 1.682) y Perú (Art. 8 Ley Centrales Privadas de Información de Riesgos).

De los estatutos jurídicos enunciados, nuevamente aparece la normativa argentina como la más clara y desarrollada en el tema, la cual además está reforzada por la disposición constitucional, que -como se vio anteriormente- expresamente reconoce el principio de la finalidad como integrante del hábeas data o derecho a la protección de datos. La Ley 25.326, a través de diversas disposiciones va configurando y dando fuerza al principio, lo que normativamente se traduce en los siguientes mandatos: los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública; los datos personales que se recojan a los efectos de su tratamiento no deben ser excesivos en relación al ámbito y finalidad para los que se hubieren obtenido; los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención; cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara entre otras cosas la

finalidad para la que serán tratados, entre otros.

En el caso de la ley chilena de protección de datos, el principio de la finalidad no está claramente desarrollado. Si a ello le sumamos el hecho de no contar con una norma constitucional que reconozca entre otros este principio, podríamos aventurarnos a concluir que los derechos de los titulares de los datos no estarían debidamente resguardados por la Ley 19.628. Prueba de lo anterior es la forma como concibe el legislador el principio en estudio, lo cual se plasma en una disposición que señala que los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público (Art. 9 inc. 1º). El hecho de incluir tal excepción, estimamos, desnaturalizaría el principio, pues da a entender que todos los datos que no sean de acceso restringido o reservado al público (o sea, la regla general) escapan al principio y, por lo tanto, podrían ser utilizados para los más variados fines, sin que el titular pudiere saber *ex ante* esa finalidad. Por otra parte, las demás disposiciones que hacen referencia al principio de la finalidad del uso de los datos, no se traducen en la práctica en la regla general. Incluso la norma del artículo 5, que aparentemente reforzaría el principio, al final traiciona las nobles intenciones declaradas en un comienzo, cuales son, establecer ciertas condiciones para la transmisión y recepción de datos mediante procedimientos automatizados. De las condiciones que se mencionan, dos se encaminan a resguardar el principio: quela transmisión guarde relación con las tareas y finalidades de los organismos participantes y, que sólo pueden utilizarse los datos personales para los fines que motivaron la transmisión a través del procedimiento automatizado. Lamentablemente, las excepciones que se señalan a la aplicación de esas condiciones, convierten en la actualidad a la disposición del artículo 5º en una norma de casi nula aplicación, dado que Chile no ha suscrito tratados internacionales en materia de transmisión internacional de datos y dado que los datos personales accesibles al público en general constituyen la regla general en nuestra legislación [578] .

Creemos que el legislador chileno eventualmente pudo morigerar de una manera muy simple las consecuencias de las falencias anotadas anteriormente, al momento de consagrar el derecho de acceso en el artículo 12 de la Ley 19.628. Como se recordará, dicho artículo señala que toda persona tiene derecho a exigir al responsable de un banco de datos personales, que se dedique en forma pública o privada al tratamiento de éstos, a que se le informe 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. En esta disposición, estimamos que debió utilizarse derechamente el vocablo 'finalidad' en vez del término 'propósito', pues habría estado más acorde con las demás disposiciones legales referidas al principio, lo cual permitiría desarrollar una interpretación más favorable a los derechos de los titulares de datos, incluso de aquéllos de carácter no restringido o reservado. Tal como está actualmente la ley chilena, podría eventualmente darse el caso que ante el ejercicio de una acción de protección de datos, el demandado (un particular cualquiera), se oponga a revelar el "propósito" del archivo, obviando el artículo 12 y fundando tal negativa en que la propia ley permite una utilización distinta de los datos a los fines para los cuales se

[578] Ver Capítulo II, Análisis de la Protección a los Datos Personales en Chile, Punto Nº 4.

hubieren recolectado. Aún más, podría aducir que el exigírsele por la ley que informe acerca del propósito de su archivo privado, adolecería de inconstitucionalidad por vulnerar su derecho a la inviolabilidad de sus documentos privados (Art. 19 Nº 5º C. Pol.) e incluso su propia intimidad, si no se aduce para tal efecto otra norma jurídica constitucional que así lo permita. Esta argumentación que podría parecer absurda en nuestro ordenamiento jurídico, es completamente justificada al menos en Paraguay, y eventualmente en Argentina, en los cuales los archivos de datos de uso estrictamente privado, o no destinados a proveer informes, están expresamente excluidos de la acción de hábeas data. Un caso hipotético como el recientemente planteado, si bien puede parecer extremo, no sería de extrañar en nuestro país, pues tal interpretación, tan alejada al espíritu de una ley de protección de datos sólo tiene cabida donde se la permite. En definitiva, creemos que la ley chilena aun le queda por desarrollar adecuadamente el principio de la finalidad.

Por su parte, la Ley 1.682 del Paraguay se limita a repetir lo señalado por el Constituyente en el artículo 135, en el sentido que toda persona podrá conocer el uso que se haga de los datos o su finalidad (Art. 18). La diferencia con el texto constitucional radica en los sujetos pasivos de la eventual acción de hábeas data, ahora ampliados por la ley a entidades que suministren información sobre solvencia económica y situación patrimonial de las personas. A partir de la previsión constitucional, creemos podría desarrollarse adecuadamente el principio de la finalidad. Queda entonces la tarea entregada al legislador paraguayo pues la ley 1.682 está todavía muy lejos de reconocer el principio en toda su dimensión.

En lo que respecta a los estatutos legales sectoriales complejos, debemos señalar que en Brasil no se reconoce explícitamente el principio de la finalidad, sino más bien éste podría deducirse de lo señalado en la Ley de Protección al Consumidor, relativo a que la apertura del registro o ficha de datos personales y de consumo debe ser comunicada por escrito al consumidor cuando no sea solicitado por él (parágrafo 2º del artículo 43º). Pensamos que tal comunicación incluiría la información respectiva acerca de la finalidad del fichero. Con todo, aún así no puede decirse con propiedad que se reconozca este principio, por lo tanto, en este punto la legislación brasileña presenta serios vacíos.

La legislación ecuatoriana, por su parte, está subordinada al mandato constitucional de la garantía del hábeas data, la cual reconoce el derecho de conocer la finalidad y uso de los datos personales. La Ley de Control Constitucional se hace cargo de ello al disponer que declarado con lugar el recurso de hábeas data, las entidades o personas requeridas entregarán toda la información y, bajo juramento, una explicación detallada que incluya por lo menos el uso dado a los datos y el que se pretenderá dar a éstos (Art. 39). De lo recién señalado de desprendería al menos una intención de reconocer en parte el principio, lo cual obviamente debe ser desarrollado en un ley sustantiva y no en una de carácter procedimental de amparo especial como lo es la señalada. Con más claridad, se aprecia el principio de la finalidad en la ley de comercio electrónico y mensajería de datos pues al definir los ‘datos personales autorizados’ señala que son aquéllos que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente

señalado y ser aceptado por dicho titular (Disposición gral. 9ª). En síntesis, creemos que la legislación ecuatoriana reconoce expresamente el principio de la finalidad, aunque se falta un mayor desarrollo de éste.

La legislación mexicana a su turno, reconocería este principio en la Ley de protección al Consumidor al establecer la prohibición a las empresas dedicadas a la investigación de crédito o de mercadotecnia y a sus clientes de utilizar la información con fines diferentes a los crediticios o mercadotécnicos (Art. 18). Además de ese estatuto, la Ley que regula la Sociedades de Información Crediticia reconocería indirectamente el principio en el artículo 28, al disponer que sólo pueden entregarse reportes de crédito si el Cliente ha dado expresa autorización al Usuario, debiendo además constar de manera fehaciente que el Cliente tiene pleno conocimiento de la naturaleza y alcance de la información que la Sociedad proporcionará al Usuario que así la solicite y del uso que dicho Usuario hará de tal información. En suma, si bien aparece vislumbrado el principio de la finalidad, ello no es suficiente, y por lo mismo, obliga a que el legislador se ocupe de desarrollar adecuadamente una legislación que contenga inequívocamente el principio de la finalidad.

En el caso de la ley panameña, el principio en estudio se encuentra contenido en la disposición que establece el derecho del consumidor o cliente al “Buen manejo de la información”, lo cual implica que los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recopilados. Lo anterior, claramente refleja la presencia del principio de la finalidad, lo cual se complementa con uno de los objetos de la ley panameña sobre el historial crediticio de los consumidores o clientes; el buen manejo de los datos personales de consumidores o clientes (Art. 23 Nº 3).

Finalmente, cabe anotar que la ley peruana reconocería el principio de la finalidad implícitamente al disponer que en los casos que las Centrales Privadas de Información de Riesgos recolecten la información directamente de los titulares, necesariamente deben informar, entre otras cosas, la existencia del banco de datos, la finalidad de la recolección de la información y los potenciales destinatarios de ésta (Artículo 8º). Con todo, la aplicación de la norma anterior es más bien excepcional, pues existen otras fuentes de información que no precisan el consentimiento del titular (Art. 7º), y consecuencialmente el deber de informar la finalidad de la recolección, por lo que estimamos faltaría un mayor desarrollo de la legislación para que pudiera afirmarse que el principio de la finalidad es reconocido ampliamente.

En síntesis, como comentario general del punto analizado, podemos señalar que tanto a nivel de legislación general de protección de datos como sectorial compleja existe normativa que con mayor o menor énfasis reconoce el principio de la finalidad. Si bien pudiera pensarse que a nivel de leyes generales el principio estaría adecuadamente desarrollado, ello queda desvirtuado específicamente en el caso de Paraguay y Chile, ordenamientos en que la finalidad aparece muy débilmente tratada; el primero limitándose a repetir lo señalado por el Constituyente, y en el caso de nuestro país, de forma poco clara y sin fuerza suficiente. En lo relativo a los estatutos latinoamericanos sectoriales, sorprende en general la mayor claridad de algunas leyes en la materia a pesar de su restringido campo de aplicación; el mercado de la información crediticia y la

protección de los consumidores. Una forma de regulación extravagante a estas normas, aparece en el caso de Ecuador, mediante la Ley de Comercio Electrónico, Firma Electrónica y Mensajería de Datos, la cual a través de reglas generales aplicables a este último ámbito sienta de forma clara el principio de la finalidad, reforzado tanto por la Ley de Control de Constitucionalidad que regula procesalmente el hábeas data, como por la propia Constitución.

5. Derechos Reconocidos a los Titulares de los Datos Personales

Una de los puntos más importantes en materia de protección de datos es el relativo a los derechos reconocidos a los titulares de los datos por los respectivos ordenamientos jurídicos. Antes de revisar de un modo general tales derechos en Latinoamérica, debemos aclarar el lugar de tratamiento que le hemos dado ellos a lo largo de nuestro trabajo. En el Capítulo II de este estudio, analizamos fundamentalmente en dos puntos diferentes los derechos de los titulares de los datos: dentro del análisis de la protección legal a los datos personales y dentro del análisis referido a los modelos de tutela. En el primero de esos puntos de análisis, se señalaron los procedimientos administrativos o informales establecidos por las leyes para hacer efectivos los derechos de cada titular de datos. En cambio, en el análisis relativo a los modelos de tutela, sólo nos circunscribimos a las acciones y los procedimientos de carácter judicial, previstos tanto a nivel constitucional como legal por los diversos ordenamientos jurídicos para hacer efectivos los derechos de los titulares de datos.

A continuación, enunciaremos los sistemas jurídicos que reconocen ciertos derechos a los titulares de los datos personales, identificándolos junto con la normativa respectiva que le sirve de fundamento.

En la Argentina, se reconocen al titular de los datos los derechos de acceso, rectificación o modificación, cancelación o supresión, bloqueo y confidencialidad, los cuales pueden ejercerse en contra de los responsables de archivos, registros o bancos de datos públicos y de los privados destinados a proveer informes, lo cual debe llevarse a cabo primero, de manera informal o administrativa ante el responsable del archivo y, agotada esa vía, a través de la acción de protección de datos o hábeas data (Art. 43 inc. 3º C. Pol.; arts. 13, 14, 16 y 33 Ley 25.326). Cabe agregar que en materia sectorial, se dispone de una norma que reconoce a los clientes de las instituciones financieras el derecho de acceso a la información relativa a la clasificación asignada a aquéllos por estas instituciones, relativa al comportamiento crediticio, junto con los fundamentos que justifican tal clasificación de los clientes. La institución anterior ha sido denominada por alguna doctrina como el hábeas data financiero, y se ejerce directamente ante la institución financiera (Art. 8.1 Comunicación “A” 3.630 del Banco Central). Entendemos que de no prosperar tal mecanismo, quedaría expedita la acción de protección de datos contemplada en la Ley 25.326.

Por su parte, en el ordenamiento jurídico del Brasil, se reconocen expresamente sólo los derechos de acceso e información y rectificación de datos, los cuales sólo pueden reclamarse ante los responsables de registros o bancos de datos de entidades gubernamentales o de carácter público; primeramente a través de la vía administrativa y agotada ésta, a través de la acción de hábeas data (Art. 5º LXXII C. Pol. y art. 7º Ley Nº 9.507). Además de la normativa constitucional, en materia de derechos del consumidor, la ley respectiva reconoce los derechos de acceso e información y el derecho de corrección inmediata de los datos personales inexactos, los cuales deben ejercerse informalmente o extrajudicialmente ante el encargado del archivo o banco de datos que preste servicios de información de crédito. Estos archivos son considerados por la ley como entidades de carácter público, con la finalidad de hacer aplicables las normas que regulan el hábeas data constitucional a esos bancos de datos, los cuales sin esa corrección legal, en principio quedarían excluidos como sujetos pasivos de la acción de hábeas data (Art. 43 yparágrafo 3 Ley de Protección al Consumidor).

En el caso del ordenamiento jurídico chileno, se reconocen sólo a nivel legal los derechos de acceso e información, modificación, cancelación, y bloqueo de datos. Estos derechos deben ser ejercidos por el titular, primeramente, de manera directa ante el responsable del registro o banco de datos y, agotada esa vía administrativa o extrajudicial, queda abierta la posibilidad de ejercer judicialmente la acción de amparo a los derechos del titular de los datos (Arts. 12-16 Ley 19.628).

Colombia por su parte, sólo reconoce a nivel constitucional los derechos de acceso e información, rectificación o modificación y actualización de datos. Sin embargo, no se contempla una acción específica que haga efectiva la garantía del hábeas data. A falta de ella, la vía utilizada es la acción de tutela (Arts. 15 y 86 C. Pol.).

El sistema jurídico del Ecuador, también reconoce a nivel constitucional ciertos derechos a los titulares de datos personales, como lo son los derechos de acceso e información, rectificación, eliminación o anulación de datos (Art. 94 C. Pol. y art. 35 Ley de Control Constitucional).

Por su parte, el ordenamiento jurídico guatemalteco, únicamente reconoce a nivel constitucional los derechos de acceso e información, corrección, rectificación y actualización. Sin embargo, ellos sólo son reclamables respecto de los responsables de los archivos estatales (Art. 31 C. Pol.). El ejercicio de tales derechos no se encuentra regulado por ley general ni especial al efecto.

México dispone de un sistema jurídico que reconoce sólo a nivel legal sectorial algunos derechos a los titulares de datos. Así, la Ley para regular las Sociedades de Información Crediticia, reconoce a los clientes de las entidades financieras y de las empresas comerciales, los derechos de acceso e información, rectificación, cancelación y accesoriamente a ello, a que como medida de publicidad de una impugnación de los registros se incluya una leyenda en tal sentido hasta que se resuelva la controversia entre el cliente y la institución financiera o empresa comercial. El ejercicio de tales derechos, debe efectuarse extrajudicialmente ante la unidad especializada de la Sociedad de Información Crediticia que hubiera emitido el reporte de crédito respectivo (Arts. 39-43). En materia de protección a los consumidores, el estatuto respectivo contempla los

derechos de acceso e información y rectificación o corrección de datos, los cuales pueden ser ejercidos directamente por los consumidores respecto de las empresas dedicadas a la investigación de crédito o la recopilación de información sobre consumidores con fines de mercadotecnia o marketing (Art.16 Ley de Protección al Consumidor).

Del ordenamiento jurídico de la República de Nicaragua cabe solamente decir que se reconoce a nivel constitucional el derecho de acceso a la información registrada por las autoridades estatales, sin establecerse una regulación legal que desarrolle tal estrecho precepto (Art. 26 Nº 4 C. Pol.).

Más adelantado que el sistema anterior se encuentra Panamá, aunque sólo disponga de normas legales en materia de protección de datos. Un primer estatuto que contempla ciertos derechos a los titulares de datos es la Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores, la cual reconoce los derechos de acceso e información, rectificación, eliminación y actualización de los datos de los consumidores o clientes. Estos derechos deben ejercerse personalmente o a través de mandatario directamente ante el agente económico (proveedores de bienes y servicios que registran, suministran y obtienen información de una base o banco de datos) o ante la Comisión de Libre Competencia y Asuntos de Consumidor (CLICAC), es decir, a través de un procedimiento de carácter extrajudicial en la primera alternativa señalada y de carácter administrativo en la segunda (Arts. 23 y 31). Por otra parte, la Ley de Transparencia en la Gestión Pública, también reconoce algunos derechos a los titulares de datos personales contenidas en archivos, registros o expedientes que mantengan las instituciones del Estado. Éstos son, el derecho de acceso e información, corrección y eliminación de datos, los cuales deben ser ejercidos primeramente a través del procedimiento administrativo que la Ley dispone al efecto. Agotada esa vía, se abre la posibilidad de accionar judicialmente de hábeas data ante los Tribunales Superiores de justicia (Arts. 3 y 4).

En el sistema jurídico paraguayo, a nivel Constitucional se reconoce a los titulares de los datos los derechos de acceso e información, actualización, rectificación y destrucción de éstos, que obren en registros oficiales o privados de carácter público, los cuales deberán ejercitarse ante el magistrado competente (Art. 135 C. Pol). En el plano legal, la Ley Nº 1.682, malamente regula lo preceptuado por el Constituyente, pues trata diferenciadamente el derecho de acceso de los demás derechos sin señalar el procedimiento judicial ni el tribunal competente que deberá conocer de la acción de hábeas data. En cuanto al trato diferenciado, podemos señalar que en el derecho de acceso, se amplía el ámbito objetivo de aplicación de la disposición constitucional a los registros de entidades que suministren datos sobre la solvencia económica y situación patrimonial de las personas. En lo relativo a los derechos de actualización, rectificación y destrucción, únicamente los circunscribe la Ley al ejercicio de ellos por los titulares, ante los responsables de los registros de datos sobre la solvencia económica y situación patrimonial de las personas, omitiendo toda referencia a los responsables de otra clase de archivos (Arts. 7 y 8). En definitiva, si bien el Constituyente ha establecido a nivel de garantía el hábeas data, el legislador no ha cumplido debidamente su tarea de regular y desarrollar adecuadamente el mandato de la Ley Fundamental.

Del análisis al sistema jurídico del Perú, hemos podido constatar que si bien el Constituyente establece expresamente la acción de hábeas data, ésta sólo abarca al derecho de acceso e información (Art. 200 Nº 3 en relación con el art. 2º Nº 5 y 6 C. Pol.). A nivel legal, existen tres estatutos que desarrollan la estrecha configuración constitucional del hábeas data. El primero de ellos, regula transitoria y escuetamente el ejercicio de la acción de hábeas data y en lo no previsto por ella se remite a la acción de amparo (Ley 26.301). El segundo estatuto es la Ley de Transparencia y Acceso a la Información Pública, la cual hace eco de lo señalado en la Constitución y, por lo tanto, se refiere nada más que al derecho de acceso, el cual primeramente debe ejercerse a través del procedimiento administrativo señalado en la misma Ley. Agotada esa vía, resulta procedente entablar la acción de hábeas data regulada deficientemente en la Ley 26.301 (Arts. 7, 10 y 12 Ley Transparencia y Acceso a la Información Pública). El tercer estatuto legal que reconoce ciertos derechos a los titulares de datos es la Ley que regula las Centrales Privadas de Información de Riesgos. Esta ley, si bien es una normativa de carácter sectorial, contiene disposiciones dignas de destacar, las cuales permiten el desarrollo del instituto del hábeas data a pesar de la limitada configuración constitucional. Dispone esta ley que de manera enunciativa, mas no limitativa, los titulares de la información registrada en los bancos de datos administrados por las Centrales Privadas de Información de riesgos (CEPIRS) tienen los siguientes derechos: de acceso e información, modificación, cancelación, rectificación y actualización (Art. 13). La importancia de la norma anterior radica en no limitar los derechos de los titulares, por lo tanto, pueden solicitarse medidas no señaladas en la ley y que tiendan a resguardar los derechos de los titulares de datos. El ejercicio de estos derechos se hace valer a través de un procedimiento extrajudicial ante las CEPIRS. Entendemos que la procedencia de la acción de hábeas data ante la magistratura, está supeditada al agotamiento de la vía previa ante aquellas instituciones (Arts. 13-17).

Finalmente, cabe exponer la situación venezolana en materia de derechos de los titulares de los datos. Al respecto, debemos señalar que sólo a nivel constitucional se reconocen los derechos de acceso, actualización, rectificación y destrucción de los datos que consten en registros oficiales o privados. El Constituyente agrega a lo dicho, que esos derechos no podrán ejercerse en los casos de excepción que señale la ley. Como no existe ley de protección de datos que establezca tales excepciones, entendemos que la regla Constitucional operaría ampliamente (Art. 28 C. Pol.). El ejercicio de la acción respectiva, a falta de regulación especial, ha quedado entregada en definitiva, según la doctrina y alguna jurisprudencia, al procedimiento de amparo, en tanto no se dicte la ley respectiva [579].

6. Modelos de Tutela

En el análisis particular a los diversos ordenamientos jurídicos, realizado a lo largo del

[579] Ver Capítulo II, Análisis de la Protección a los Datos Personales en Venezuela, punto Nº 2.2.

Capítulo II de este estudio, nos detuvimos a reseñar los mecanismos de tutela judicial previstos en éstos para hacer efectivos los derechos de los titulares de los datos, es decir, las acciones establecidas por cada ordenamiento jurídico para la protección a los datos personales. Esos mecanismos jurídicos de tutela, podríamos clasificarlos en dos grupos: a) Modelos de tutela específicos y, b) Modelos de tutela generales. Los modelos de tutela específicos estarían representados por las acciones de hábeas data o acciones de protección de datos para cuyo ejercicio, por regla general, se dispone de un procedimiento especial. El segundo grupo, es decir, los modelos de tutela general, estarían circunscritos a las acciones constitucionales de amparo, tutela o protección de los derechos y garantías constitucionales reconocidos en cada ordenamiento jurídico. Estas acciones y los respectivos procedimientos, entrarían a operar en aquellos ordenamientos jurídicos en los cuales no existan disposiciones que reconozcan expresamente el derecho a la protección de datos, o cuando incluso reconociéndose ellos, no se señale la acción ni el procedimiento específico para hacer efectivos los derechos de los titulares de datos, y también, cuando el reconocimiento del hábeas data es limitado, es decir, circunscrito a determinadas situaciones o ejercitable respecto de determinados sujetos pasivos. Por último, estimamos que excepcionalmente podría recurrirse a la acción de amparo, tutela o protección, en los casos en que a pesar de contemplarse la acción de hábeas data y su respectivo procedimiento especial, no se garantizare a través de éste la oportuna y adecuada protección a los derechos de los titulares de datos.

En los ordenamientos jurídicos en que por diversos motivos se haga aplicación del procedimiento contemplado para la acción de amparo o tutela, si bien podría afirmarse que quedarían resguardados los derechos de los titulares de datos, debe tenerse presente que las disposiciones que regulan esta acción, no necesariamente reflejan la amplitud e independencia predicada de la acción de hábeas data, con lo cual las buenas intenciones de reconocer el derecho a la protección de datos se diluyen en la práctica. Uno de los aspectos negativos del amparo o tutela, que no cuadra con la mecánica del hábeas data, es la limitación temporal al ejercicio de los derechos afectados, pues por regla general aquellas acciones están sujetas a plazos de caducidad, cuestión del todo ajena a la finalidad del hábeas data.

Sin perjuicio de la clasificación relativa a los modelos de tutela presentes en las legislaciones latinoamericanas comprendidas en este trabajo, debemos agregar que en la práctica esos modelos se relacionan, y muchas veces se confunden en el más general, dado que sintetiza las normas sustantivas del derecho a la protección de datos o hábeas data, con la acción constitucional de amparo. Es decir, existiría una tendencia a reconducir la tutela jurídica a los datos personales, al modelo general de protección de los derechos y garantías constitucionales, cual es la acción de amparo, la que en algunos casos tutelará el derecho a la protección de datos o hábeas data, y en otros, el derecho a la intimidad, vida privada, honor, o cualquier otro bien jurídico que permita fundamentar la defensa de las personas ante el tratamiento de sus datos personales. A continuación, señalaremos los ordenamientos jurídicos que contemplan mecanismos de tutela -tanto específicos como generales- en materia de protección de datos personales, en base a la tabla comparativa Nº 6 contenida en el Capítulo III [580] .

Los ordenamientos jurídicos que contemplan expresamente acciones de hábeas data o de protección de datos personales, y que además establecen un procedimiento específico para el ejercicio de ésta son los siguientes: Argentina (Art. 43 inc.3º C. Pol. y arts. 33-43, Ley 25.326), Brasil (Art. 5º LXXII C. Pol. y Ley Nº 9.507), Chile (Art. 16 y 23 Ley 19.628), Ecuador (Art. 94 C. Pol. y Ley de Control Constitucional), Panamá (Ley de Transparencia en la Gestión Pública) y, Perú (Art. 200 Nº 3 C. Pol., Ley de Transparencia y Acceso a la Información Pública, y art. 17 Ley para Regular las Sociedades de Información Crediticia).

En los ordenamientos latinoamericanos que no reconocen el derecho a la protección de datos personales o hábeas data, pero que sí lo hacen respecto de otros derechos señalados por la doctrina y jurisprudencia como bienes jurídicos protegidos por el hábeas data, la acción constitucional de amparo o tutela se erige como la más apta para la defensa de esos derechos. En esos sistemas jurídicos, estimamos que la fundamentación a la protección solicitada puede basarse no sólo en los expresos o implícitos derechos reconocidos por las respectivas Cartas Fundamentales, sino que también en los reconocidos en los tratados internacionales de protección a los derechos humanos, como lo es el Pacto de San José de Costa Rica. La situación anteriormente descrita, es constatable en los países que se señalan a continuación: Bolivia (Art. 19 C. Pol. y Ley Tribunal Constitucional), Costa Rica (Ley de la Jurisdicción Constitucional), El Salvador (Art. 247 C. Pol. y Ley de Procedimientos Constitucionales), Honduras (Art. 183 C. Pol.), México (Art. 103 y 107 C. Pol. y Ley de Amparo), Panamá (Art. 50 C. Pol.) y, Uruguay (Ley de Amparo Nº 16.011). Dicho lo anterior, sólo nos cabe agregar que el Pacto de San José de Costa Rica ha sido ratificado por todos los Estados ya nombrados, con lo cual creemos que se suplirían las deficiencias en materia de derechos fundamentales que puedan servir de base para impetrar una tutela constitucional.

En los sistemas jurídicos en que se reconoce el derecho a la protección de datos o hábeas data pero no se señala ni la acción ni el procedimiento específico destinado a tutelar tal derecho, se ha estimado en general por la doctrina y alguna jurisprudencia que debería aplicarse supletoriamente el procedimiento previsto para la acción de amparo constitucional. Estos ordenamientos son los siguientes: Colombia (Art. 15 en relación con el art. 86 C. Pol. y Decreto Nº 2.591 de 1991), Guatemala (Art. 31 y 265 C. Pol. y Ley de Amparo, Exhibición Personal y Constitucionalidad), Nicaragua (Art. 26 Nº 4 en relación con art. 184 C. Pol y Ley de Amparo) y Venezuela (Art. 27 C. Pol. y Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales).

Finalmente, estimamos que igualmente sería procedente la acción de protección o amparo en aquellos sistemas jurídicos en que se reconoce un hábeas data limitado, para cubrir los ámbitos excluidos del derecho (como por ejemplo ciertos ficheros) y, en aquellos en que contemplándose una acción de hábeas data, en determinadas situaciones, ésta no sea el medio más expedito y eficaz para la adecuada protección de los derechos de los titulares de los datos. Este es el caso de Chile, pues si bien la Ley 19.628 establece una acción de amparo a ciertos derechos consagrados expresamente, creemos que ante una situación como la recién descrita ello no obstaría al ejercicio de la

[580] Ver Capítulo III, Tabla Nº 6

acción de protección del artículo 19 Nº 20 de la Constitución Política.

7. Mecanismos de Control

En este punto, trataremos de dilucidar el nivel de protección a los datos personales en las legislaciones latinoamericanas, en lo relativo a los mecanismos de control implementados a efecto de velar por el respeto y aplicación de la normativa general o sectorial compleja de protección a los datos personales. En esta materia, debemos recordar que los mecanismos de control previstos por la normativa comunitaria europea (Directiva 95/46 CE), son de dos clases o tipos, a los cuales llamaremos mecanismos de control jurídico y mecanismos de control deontológico. Los primeros se caracterizan entre otras cosas, porque las normas que componen el sistema de control que vela por el respeto y aplicación de la normativa de protección de datos, es jurídicamente vinculante y de carácter general, es decir obliga a todos. Ahora bien, para que puedan operar los sistemas de control previstos por la ley, debe existir un órgano de control administrativo encargado de llevar a cabo la tarea de vigilar el estricto cumplimiento de la normativa de protección de datos, el que además deberá ofrecer garantías de imparcialidad e independencia respecto de las personas u organismos responsables del procesamiento de datos o de su aplicación y de la competencia técnica de éstos. El sistema de control deontológico por su parte, se caracteriza principalmente por su naturaleza normativa no jurídica, basado en normas acordadas por quienes participan de un sector profesional específico en materia de tratamiento de datos y, por lo tanto, obliga sólo a quienes han decidido someterse voluntariamente a ellas. Estas normas de autorregulación de una actividad profesional sectorial, reciben el nombre de normas de buena práctica profesional y se recogen en los denominados códigos de conducta o códigos deontológicos.

Del análisis general de cada ordenamiento jurídico latinoamericano, lo cual se grafica en la Tabla Comparativa Nº 7 del Capítulo III [581] , podemos afirmar que sólo uno de ellos posee mecanismos de control que se adecuan a las normas internacionales en materia de protección de datos, tanto en la vertiente jurídica como deontológica: este es el caso de Argentina, país que en su Ley 25.326 de protección de datos personales, establece la creación de un órgano de control cuyo deber es realizar todas las acciones necesarias para el cumplimiento de los objetivos y las disposiciones contenidas en la propia Ley (Art. 29 Ley 25.326). Ese órgano de control es la Dirección Nacional de Protección de Datos Personales. Por otra parte, el legislador trasandino también ha contemplado la existencia de mecanismos de control deontológicos, plasmados en los denominados códigos de conducta de práctica profesional, los cuales podrán establecer normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la Ley (Art. 30 Ley 25.326). Aún más, la Ley le encomienda al propio órgano de control, es decir, a la

[581] Ver Capítulo III, Tabla Nº 7

Dirección Nacional de Protección de Datos Personales, alentar la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones legales y reglamentarias (Art. 30 Reglamento Ley 253.26). Cabe señalar que estos códigos deben ser inscritos en el registro que al efecto lleva el órgano de control, el cual podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia.

No obstante lo señalado en el párrafo anterior, cabe agregar que en el ámbito legal sectorial complejo o influido por los principios internacionales sobre protección de datos, existen tres ordenamientos jurídicos que en sus respectivos estatutos contemplan la intervención de organismos administrativos encargados entre otras cosas, de velar por el cumplimiento de las disposiciones relativas a la protección de los derechos de los titulares de los datos. En razón de lo anterior, estimamos que estos organismos administrativos actuarían sin duda como órganos de control, restringidos al ámbito de las respectivas leyes que les otorgan competencia.

Dicho lo anterior, debemos señalar que en México, tanto la Ley para Regular las Sociedades de Información Crediticia como la Ley de Protección al Consumidor prevén órganos encargados de velar por el cumplimiento de los respectivos estatutos jurídicos, facultándoles en algunos casos para aplicar sanciones administrativas y actuar como árbitros en la resolución de conflictos. La primera de estas leyes establece como órgano de control a la Comisión Nacional Bancaria y de Valores, la cual está facultada para aplicar sanciones administrativas tanto a los funcionarios de las Sociedades, Entidades Financieras como también a los Usuarios (Arts 53-56). Por su parte, la Ley de Protección al Consumidor contempla como órgano de control a la Procuraduría Federal del Consumidor, la cual está encargada de promover y proteger los derechos e intereses del consumidor y procurar la equidad y seguridad jurídica en las relaciones entre proveedores y consumidores (Art.20). Dentro las facultades que se le reconocen, se encuentra la de aplicar las sanciones establecidas en la propia Ley (Art. 24).

En el caso de Panamá, la Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores, otorga competencia a dos órganos administrativos que de manera conjunta cumplen un rol de órganos de control de la aplicación de la Ley: el primero es el Ministerio de Comercio e Industrias, el cual tiene la facultad de inspeccionar y verificar que las agencias de información de datos cumplan con los requisitos de seguridad, confiabilidad y actualización de los datos de los consumidores y clientes. Asimismo, este Ministerio tiene la facultad de sancionar a las agencias de información de datos que infrinjan lo establecido en la señalada Ley. El segundo órgano de control previsto por la Ley panameña de Información sobre el Historial de Crédito de los Consumidores, es la Comisión de Libre Competencia y Asuntos del Consumidor (CLICAC), la cual conoce y atiende las quejas de los consumidores o clientes, supervisa e investiga las prácticas de los agentes económicos y las agencias de información de datos, así como también está facultada para sancionar a los agentes económicos y a las agencias de información de datos que, en virtud de la investigación de las quejas que se le presenten, se les compruebe que han infringido los derechos del consumidor o cliente señalados en la Ley (Art. 8).

Finalmente, debemos consignar que en el ordenamiento jurídico peruano, la Ley para

Regular las Sociedades de Información Crediticia otorga competencia a la Comisión de Protección al Consumidor del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), como órgano administrativo, para conocer de las infracciones a la Ley e imponer tanto sanciones administrativas como medidas correctivas a las que hubiere lugar (Art. 21).

En suma, puede concluirse que de los ordenamientos jurídicos estudiados, el único que prevé mecanismos de control, tanto jurídicos como deontológicos, a través de una ley general de protección de datos, es el argentino. Le siguen a éste, sólo con mecanismos de control jurídico, algunos estatutos jurídicos sectoriales complejos de México, Panamá y Perú, los cuales contemplan organismos de control para la defensa de los derechos de los clientes y consumidores, y los que además están facultados para sancionar a quienes infrinjan las disposiciones legales respectivas.

8. Transmisión Internacional de Datos Personales

En materia de regulación legal de la transmisión internacional de los datos personales en los ordenamientos jurídicos estudiados, en general se observa un disímil desarrollo de las legislaciones; la regla general es la inexistencia de normativa al respecto. En un término medio se ubicarían aquellos países (sólo seis) que disponen de normas legales sectoriales no influidas por los principios internacionales de protección de datos, referidas comúnmente a la transmisión internacional de datos de carácter financiero y tributario, que asimismo constituyen excepciones al deber general de reserva o secreto de esos datos. Por último, debemos señalar que es la excepción en Latinoamérica la existencia de un sistema jurídico que disponga de una ley de protección de datos personales, y que además regule con carácter general la transmisión internacional de éstos. De todos los países estudiados sólo Argentina constituye la honrosa excepción, país que dispone de una legislación muy influida por las normas internacionales de protección de datos, en particular por la Directiva europea 95/46 CE.

La ley argentina Nº 25.326 establece en el artículo 12 como regla general, la prohibición de la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados. Las excepciones a la regla prohibitiva, son desarrolladas en el mismo artículo 12 de la Ley, las que se fundan en un interés superior, como por ejemplo, en casos de colaboración judicial internacional, intercambio de datos de carácter médico, acuerdos internacionales suscritos y la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico. Ahora bien, qué entiende la ley por “niveles de protección adecuados”, es una pregunta cuya respuesta la da el artículo 12º del Decreto Reglamentario de la Ley 25.326 ya analizado en el capítulo II al cual nos remitimos [582] .

En el caso chileno, la Ley 19.628 sólo se refiere a la transmisión internacional de

[582] Ver Capítulo II, Análisis de la Protección a los Datos Personales en Argentina, punto Nº 8.

datos en dos disposiciones; en la primera de manera vaga, al definir qué se entiende por transmisión y tratamiento de datos (Art.1º letras c y o), y en la segunda directamente, a propósito de las excepciones a las condiciones para la transmisión electrónica de datos personales (Art. 5º inciso final). Lo anterior, junto con lo señalado en la historia de la Ley 19.628 ha sido interpretado en el sentido que todo lo relativo a la transmisión internacional de datos debe ser regulado vía tratados internacionales [583] . No obstante lo anterior, a nivel de legislación sectorial, el Código Tributario faculta al Director de Impuestos Internos en el artículo 6 letra A, Nº 6º a mantener canje de informaciones con Servicio de Impuestos de otros países para los efectos de determinar la tributación que afecte a determinados contribuyentes, el cual deberá llevarse a cabo sobre la base de reciprocidad, quedando amparado por las normas relativas al secreto de las declaraciones tributarias. Con todo, y como ya lo señalamos en el análisis respectivo, estimamos que la disposición anterior eventualmente podría entrar en contradicción con lo señalado por la Ley 19.628, pues tanto de la historia fidedigna del establecimiento de ella como de su tenor literal, se desprende que todo lo relativo a la transmisión internacional de datos personales habría sido dejado a la regulación vía tratados internacionales y no a través de convenios entre organismos tributarios administrativos.

En lo que respecta a los ordenamientos jurídicos que sólo cuentan con normas sectoriales en la materia, aparece como común denominador que la operatividad de la transmisión internacional de datos quede entregada al criterio de la autoridad administrativa facultada por la ley para tal efecto. Así por ejemplo, en el caso de México, la Ley de Instituciones de Crédito autoriza a la Comisión Nacional Bancaria y de Valores para proporcionar a autoridades financieras del exterior, información sobre las operaciones y servicios, que por regla general están sujetos al secreto bancario, siempre que existan acuerdos basados en el principio de la reciprocidad (Art. 117 bis), quedando a juicio del órgano administrativo la determinación de cuándo debería o no realizarse la transferencia en virtud de tales acuerdos. Por otra parte, el artículo 69 del Código Fiscal de la Federación mexicana señala que mediante acuerdo de intercambio recíproco de información, suscrito por el Secretario de Hacienda y Crédito Público, se podrá suministrar la información a las autoridades fiscales de países extranjeros, “siempre que se pacte que la misma sólo se utilizará para efectos fiscales y se guardará el secreto fiscal correspondiente por el país de que se trate”. De lo recién señalado, aparece claro que los acuerdos de intercambio de información sujeta a secreto fiscal o tributario son celebrados por las propias autoridades administrativas, facultadas al efecto por la ley.

Por su parte, el ordenamiento jurídico nicaragüense en el artículo 109 de la Ley General de Bancos, establece como excepción al sigilo bancario el suministro de información que se canalice a través de convenios de intercambio y de cooperación suscritos por el Superintendente con autoridades supervisoras financieras de otros países. Como ya lo hicimos presente en el análisis respectivo, la facultad conferida a la autoridad administrativa sin más explicaciones ni requisitos, en nuestro concepto, implicaría un serio riesgo para los derechos de las personas, dado que nada asegura que el uso de esos datos una vez trasmitidos se corresponda con la finalidad para la cual han sido cedidos, pues ello no aparece garantizado.

583 Ver Capítulo II, Análisis de la Protección a los Datos Personales en Chile, punto Nº 8.

En el caso del Perú, la Ley 27.693 que crea la Unidad de Inteligencia Financiera del Perú (UIF) regula la transmisión internacional de datos con el fin de facilitar la operatividad de dicha Unidad, a la cual se faculta para colaborar o intercambiar información con las autoridades competentes de otros países que ejerzan competencias análogas, en el marco de convenios y acuerdos internacionales suscritos en materia de lavado de dinero o de activos, agregándose que la colaboración e intercambio de información se condicionará a lo dispuesto en los tratados y convenios internacionales y, en su caso, al principio general de reciprocidad y al sometimiento por las autoridades de dichos países a las mismas obligaciones sobre secreto profesional que rigen para las nacionales (Art.15).

La República Dominicana por su parte, contempla una disposición transitoria en materia tributaria, dentro del Párrafo 1 del artículo 3 de la Ley Nº 11-01 del año 2001, la cual señala que a partir del primero de enero del 2001, la Dirección General de Impuestos internos iniciará un operativo de valoración de patrimonios de las personas físicas, utilizando las informaciones obtenidas a través de acuerdos de intercambio de información fiscal firmados con otros países. Como no se distingue en cuanto a la naturaleza jurídica de las normas que fundamentarían ese intercambio de información, se entiende que podría fundarse a lo menos en un acuerdo de carácter administrativo, cuestión que no compartimos y hemos criticado con anterioridad.

Por último, en Venezuela la Ley General de Bancos y Otras Instituciones Financieras se refiere a la transmisión internacional de datos, al establecer excepciones al secreto bancario. La operatividad de la excepción, y consecuencialmente la posible transmisión internacional de datos sujetos al secreto bancario, está supeditada a la existencia de acuerdos de cooperación suscritos con otros países que así lo permitan (Art. 233). Como ya lo hemos planteado, el que norma legal se refiera a “organismos” sin más, nos parece francamente un exceso legislativo, pues no precisa ni el tipo de organismo ni la naturaleza jurídica de los “acuerdos” que autorizarían la cesión de datos, con lo cual se abre indiscriminadamente la puerta a la transmisión internacional de datos personales. Aún más, de lo señalado en el penúltimo inciso del artículo 233, se desprende que cuando las circunstancias lo requieran, la información sujeta a secreto bancario podrá ser suministrada al Presidente del Consejo Bancario Nacional y a organismos de supervisión bancaria y financiera de otros países.Con ello, la oportunidad, la calidad y el tratamiento de los datos personales que en principio están cubiertos por el secreto bancario, queda entregado al buen criterio de la autoridad administrativa, es decir, a la Superintendencia de Bancos.

En suma, a nivel latinoamericano se observa en general una ausencia de regulación general en materia de transmisión internacional de datos personales, siendo el caso de la Ley argentina el único de excepción. Muy por detrás le sigue la ley chilena, la cual no desarrolla el tema sino que endosa todo lo relativo a la materia a una regulación a través de tratados internacionales. Dentro de un estadio intermedio de regulación de la transmisión internacional de datos, podríamos situar a los ordenamientos jurídicos que disponen de algunos estatutos sectoriales que se refieren a la materia en aspectos precisos, circunscritos por lo general a la cooperación internacional en materia financiera, tributaria y de lucha contra el lavado de dinero y otros delitos. Llama la atención de estos

estatutos, el que se permita que las decisiones de transmisión de datos queden entregadas al criterio de la autoridad administrativa respectiva. En este punto se nota la brecha más amplia entre una regulación legal de carácter general y la sectorial, donde la primera señala claros parámetros para tal efecto y entrega al órgano de control un rol activo en la determinación de cuándo un determinado país posee niveles de protección adecuados a los datos, paso previo a la transmisión internacional de éstos. Lo anterior está claramente desarrollado por la ley argentina de protección de datos y su respectivo reglamento (Art. 12 de Ley 25.326 y art. 12 del Reglamento).

9. Regulación Diferenciada o Indiferenciada del Sector Público y Privado por las Leyes Generales de Protección de Datos en Latinoamérica

De los países comprendidos en este estudio, a nivel infraconstitucional, sólo tres de ellos disponen de estatutos generales o leyes de protección de datos. Dado el carácter más o menos general que esos estatutos presentan, ha sido de interés para nuestra investigación el indagar acerca del carácter de la regulación del sector público, representado por el Estado y sus organismos, y la regulación del sector privado o de los particulares. Es decir, hemos intentado conocer en qué específicas áreas el legislador ha optado por reglamentar de forma diferenciada una misma situación jurídica, en atención a la función pública o privada que realiza alguno de los sujetos obligados por la norma. Un esquema de los resultados obtenidos se aprecia en la Tabla comparativa Nº 5 inserta en el Capítulo III [584] de este trabajo. A continuación, comentaremos los resultados reflejados en la Tabla ya señalada, los cuales están circunscritos a lo previsto en los ordenamientos jurídicos que disponen de leyes generales de protección de datos, es decir a las leyes de protección de datos de Argentina, Chile y Paraguay.

9.1 Consentimiento para el Tratamiento de Datos

En este tema, tanto las leyes de protección de datos argentina Nº 25.326 como la chilena Nº 19.628, y parcialmente la paraguaya Nº 1.682 contemplan una regulación diferenciada tanto para el sector público como privado en materia de excepciones al requisito-principio del consentimiento para el tratamiento de los datos.

Cabe destacar que para el sector público, no rige en general el requisito del consentimiento del titular de los datos cuando es el Estado quien realiza el tratamiento de éstos, siempre que ello se enmarque dentro de las funciones que le son propias, o cuando la recolección se hace en virtud de una disposición legal. En el caso de Argentina, ello se plasma en el artículo 5º Nº 2 letra b, y en el artículo 23 Nº 2 de la Ley 25.326. En Chile, debemos consignar que el artículo 20 de la Ley 19.628 establece tales

584 Ver Capítulo III, Tabla Nº 5

prerrogativas para el Estado. De forma más restringida puede apreciarse tal situación en Paraguay, lo cual se desprende de lo preceptuado en el artículo 6º letra c de la Ley 1.682.

Por su parte, el sector privado o los particulares también poseen una regulación especial en materia de consentimiento para el tratamiento de datos, la cual comúnmente se ocupa solamente de las excepciones legales al requisito del consentimiento. En el caso argentino, ello está presente en los artículos 5 Nº 2 y 26 Nº 2 de la Ley 25.326 [585] . La Ley chilena por su parte, establece excepciones al principio del consentimiento que se aplican sólo a los particulares o privados en los incisos 5º y 6º del artículo 4º de la Ley 19.628. Finalmente, hemos constatado que en la ley paraguaya, no es tan marcada la diferenciación pues, en general, no se desarrollan los ámbitos en los cuales el Estado puede actuar en materia de tratamiento de datos. Con todo, pareciera ser que la regla del artículo 5º letra a) se aplicaría particularmente al sector privado. Esta norma señala que los datos de personas físicas o jurídicas individualizadas que revelen, describan o estimen su situación patrimonial, su solvencia económica o el cumplimiento de sus obligaciones comerciales, podrán ser publicados o difundidos solamente: *"a) Cuando esas personas hubiesen otorgado autorización expresa y por escrito para que se obtengan datos sobre el cumplimiento de sus obligaciones no reclamadas judicialmente (…)"*.

9.2 Consentimiento para la Transmisión o Cesión de Datos Personales

En cuanto al requisito-principio del consentimiento para la cesión o transferencia de datos, podemos señalar que en la ley argentina, a propósito de las excepciones a este requisito, se aprecian diferencias de tratamiento entre el sector público y privado. De ellas, al menos una es de aplicación exclusiva para el sector público, representado por el Estado y sus organismos; sólo éstos pueden obviar la prohibición de la cesión de los datos personales sin el consentimiento del titular cuando: 1) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal y, 2) Cuando se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus propias funciones (Art.11). El Reglamento por su parte, dispone en el artículo 11, que para la cesión masiva de datos personales de registros públicos a registros privados se requerirá autorización legal o autorización del funcionario responsable, si los datos son de acceso público y se ha garantizado el respeto a los principios de protección establecidos en la Ley Nº 25.326.

Por su parte, la ley chilena de 1999, también a propósito de una excepción al requisito general del consentimiento para la transmisión de datos, establece una regla que se aplica sólo al sector público y que está implícita en la regulación de la transmisión de los datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias; éstos pueden ser comunicados, no obstante estar prescrita la acción penal o administrativa, o cumplida o prescrita la pena o sanción, sin límite temporal a los tribunales de justicia u otros organismos públicos dentro del ámbito de su competencia

[585] Ver Capítulo II, Análisis de la Protección a los Datos Personales en Argentina, punto Nº 5.1.1.

(Art. 21).

En el caso del Paraguay, existe una disposición legal sólo aplicable a determinados organismos públicos que hacen excepción al requisito del consentimiento para la transmisión de datos: el artículo 6º de la Ley 1.682, el cual dispone que podrán ser publicados y difundidos datos: *"c) Cuando la información sea recabada en el ejercicio de sus funciones, por magistrados judiciales, fiscales, comisiones parlamentarias o por otras autoridades legalmente facultadas para ese efecto".*

En lo relativo a las normas que sólo se aplican al sector privado, la ley argentina dispone en materia de excepción al requisito del consentimiento para la cesión o transmisión de datos, que la prestación de servicios de información crediticia *"no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios"* (Art. 26º Nº 5 Ley 25.326). La ley chilena por su parte, en ese mismo ámbito de excepciones al requisito del consentimiento del titular para la cesión de datos, autoriza la comunicación de información que verse sobre algunas obligaciones de carácter económico, financiero, bancario o comercial (Art. 17 Ley 19.628), lo que se aplica sólo al sector privado, pues es el único que realiza la actividad de tratamiento y transmisión o cesión de esa clase de datos personales.

Finalmente, en la ley paraguaya la única disposición que exige tal requisito es la letra a) del artículo 5º, el cual más bien es excepcional. En esta norma, eventualmente se avista un trato diferenciado sólo aplicable al sector privado, salvo que el Estado esté facultado para regirse en sus relaciones patrimoniales con los particulares por tal disposición, lo cual desconocemos.

9.3 Tratamiento de los Datos Sensibles

En materia de tratamiento de los datos sensibles, podemos señalar que en la ley argentina 25.326, existe una norma que establece una regulación privilegiada para el Estado en la materia, por cuanto se reserva exclusivamente a éste la facultad de recolectar y tratar datos relativos a antecedentes penales o contravencionales, a través de sus autoridades públicas competentes (Art.7 Nº 4).La Ley chilena, por su parte, también establece una normativa sólo aplicable al sector público en materia de tratamiento de datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, los cuales sólo pueden ser tratados por organismos públicos (Art. 20 Ley 19.628). En el caso de la legislación paraguaya, no se dispone norma como las ya señaladas.

En cuanto a la normativa aplicable al sector privado, debemos decir que en Argentina la Ley 25.326 faculta expresa y excepcionalmente sólo a los particulares para recolectar algunos tipos de datos sensibles. Este es el caso de las instituciones religiosas, los partidos políticos y las organizaciones sindicales, las cuales pueden llevar registros de sus miembros (Art.7 Nº 3). En el caso de Chile la Ley 19.628 no dispone de una regla como la anterior en materia de datos sensibles, sino que sólo se señala a modo de regla de excepción al requisito del consentimiento del titular de los datos que: *"Tampoco*

requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos" (Art. 4º inc. Final). Sin embargo, creemos que no podría estimarse que esa disposición pudiera ser aplicable a los datos sensibles, pues la regla general en Chile es la prohibición del tratamiento de ellos. En consecuencia, si se llegara a sostener que las excepciones señaladas en el artículo 10 de la Ley (ley que lo autorice, consentimiento del titular o datos necesarios para la determinación u otorgamiento de beneficios de salud a los titulares) son aplicables al tratamiento de los datos sensibles por los particulares, estimamos que tal proposición no tendría asidero legal por cuanto esas excepciones deberían necesariamente hacer expresa referencia al carácter de sensibles de esos datos, cuestión que no aparece en el inciso final del artículo 4º de la ley chilena. En suma, estimamos que en esta materia la ley chilena no ha establecido ninguna regla de aplicación diferenciada a los particulares relativa al tratamiento de los datos sensibles.

Finalmente, debemos señalar que si bien la ley paraguaya establece una prohibición de carácter general de "difusión" de los datos sensibles, y que por ende afecta tanto al Estado como a los particulares, nada dice respecto de la recolección y tratamiento de éstos. Si lo anterior lo concordamos con la disposición del artículo 2º de la Ley 1.682, la cual establece que: *"toda persona tiene derecho a recolectar, almacenar y procesar datos personales para uso estrictamente privado"*, cabría entender que no existiría prohibición de almacenar y procesar datos sensibles si ello se realiza para en uso estrictamente privado. Por lo tanto, de lo señalado por la Ley 1.682 se desprende que existiría un tratamiento diferenciado respecto de los particulares, en virtud del cual éstos no tendrían impedimento legal para recolectar, almacenar y procesar datos sensibles siempre que lo hagan para 'uso estrictamente privado'. Lo anterior, estimamos no regiría para el Estado, salvo que alguien pudiera predicar de éste un ámbito de derecho a la vida privada, y en consecuencia un uso de datos sensibles de los ciudadanos para fines estrictamente privados del Estado, lo cual nos parecería absurdo.

9.4 Derechos de los Titulares de los Datos Personales

En relación a los derechos de los titulares de los datos, podemos señalar que se aprecia en la ley argentina Nº 25.326 la existencia de un tratamiento diferenciado en cuanto a la procedencia de la acción de hábeas data. En el caso que ésta se ejerza en contra de los responsables de archivos, registros o bancos de datos de carácter privado, sólo es procedente respecto de aquéllos *"destinados a proporcionar informes"*. En cambio, la acción de hábeas data en contra de archivos, registros o bancos de datos públicos procede, en principio, sin restricciones salvas las excepciones legales.

Dentro de la ley chilena de protección de datos personales, hemos observado que en materia de derechos de los titulares, no se establecen diferencias de trato entre el sector público y el privado. Por lo tanto, el ámbito de aplicación de tales normas es indiferenciado y afecta tanto a los responsables de bancos de datos públicos como privados (Art. 12 Ley 19.628).

El ordenamiento jurídico paraguayo por su parte, en lo relativo al derecho de acceso

e información, establece en la Ley 1.682 un trato diferenciado similar al existente en la Argentina, pues en relación al sector público el derecho opera ampliamente, a diferencia del sector privado o particulares, los cuales no pueden ser sujetos pasivos de una acción de hábeas data informativo si la recolección y procesamiento de datos es de uso estrictamente privado (Art. 8 en relación con el art. 2º Ley 1.862). Por otra parte, en lo que se refiere al ejercicio de los derechos constitucionales de actualización, rectificación y destrucción de datos personales (Art. 135 C. Pol.), éstos sólo aparecen regulados legalmente respecto de los datos sobre la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales, con lo cual se aprecia claramente una diferenciación injustificada excluyente de los archivos públicos (Art. 7 Ley 1.862).

9.5 Excepciones al Ejercicio de los Derechos de los Titulares de Datos

En materia de excepciones al ejercicio de los derechos de los titulares, la Ley argentina Nº 25.326, establece una regulación diferenciada la cual sólo pueden reclamarla los organismos del Estado. La disposición pertinente señala que los organismos del Estado que sean responsables o usuarios de bancos de datos públicos, pueden por decisión fundada *"denegar el acceso, rectificación o supresión"* de los datos personales, en función: 1) De la protección de la defensa de la nación; 2) Del orden público; 3) De la seguridad pública y, 4) De la protección de los derechos e intereses de terceros. Asimismo, pueden denegarse estos derechos cuando pudiere obstaculizarse actuaciones judiciales o administrativas en curso que se vinculen a: i) La investigación sobre cumplimiento de obligaciones tributarias o previsionales; ii) El desarrollo de funciones de control de la salud y del medio ambiente; iii) La investigación de delitos penales y, iv) La verificación de infracciones administrativas. Con todo, se permite el acceso a los registros en el momento en que se ejerza el derecho a defensa por el titular de los datos (Art.17).

En el caso chileno, cabe señalar que las excepciones que establece la Ley 19.628 a los derechos de información, modificación, cancelación o bloqueo de datos personales, operan en general respecto de los organismos públicos. Así, en el ámbito de las instituciones públicas, el artículo 15 dispone que no procederá el ejercicio de los derechos de información, modificación, cancelación o bloqueo de datos en los siguientes casos: 1) Cuando se impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido; 2) Cuando se afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias; 3) Cuando afecte la seguridad de la Nación, 4) Cuando se afecte el interés nacional y, 5) Cuando los datos personales sean almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva. Esta última hipótesis, interpretada *a contrario sensu* reconocería que sólo podría ejercerse el derecho de información respecto de los datos almacenados por mandato legal (Art. 15 inciso final).

En lo que respecta a la ley paraguaya, debemos hacer presente que no se aprecian excepciones al ejercicio de los derechos de los titulares, sino más bien una deficiente regulación de la materia, razón por la cual concluimos que en este punto no existiría un tratamiento diferenciado entre el sector público y el privado.

En el ámbito de los particulares o sector privado, del análisis de la Ley argentina del año 2000 se desprende que los derechos de acceso, rectificación y actualización de datos personales operan sin excepción. No obstante lo anterior, no pueden afectarse en ningún caso las fuentes de información periodísticas (Artículo 43 C. Pol.).

Por otra parte, del estudio de la ley chilena de 1999 se entiende que en el ámbito del sector privado los derechos de acceso, rectificación, actualización y supresión de datos personales también operan sin excepción (Artículo 13). Es decir, la operatividad de la acción de amparo del artículo 16 de la Ley 19.628 es amplia respecto de los sujetos que se dediquen en forma privada al tratamiento de datos (Art. 12).

Finalmente, cabe decir que en la ley paraguaya no se aprecian excepciones al ejercicio de los derechos de los titulares, y por ende, tampoco diferencias de regulación entre lo público y lo privado.

9.6 Creación y Registro de los Archivos, o Bancos de Datos Personales

En materia de creación y registro de los archivos y bancos de datos personales, se aprecian en la ley argentina de protección de datos ciertas diferencias en el tratamiento del sector público y del sector privado. Para el sector público, representado por el Estado y sus organismos, el artículo 22 de la Ley dispone que: *"las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos, deben hacerse por medio de disposición general publicada en el Boletín oficial de la Nación o diario oficial"*. Luego, la misma disposición señala una serie de indicaciones que deben contener las normas legales de creación, modificación o supresión de los archivos o bancos de datos de éstos organismos. En el caso que los particulares formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal, éstos deberán inscribirse en el Registro que para tal efecto lleva la Dirección Nacional de Protección Datos (Art.24), al igual que todos los archivos públicos (Art. 21). En suma, los bancos de datos, registros o archivos de uso exclusivamente personal, no están sujetos a la obligación general de inscripción.

La ley chilena por su parte, dispone que el tratamiento de datos personales por los organismos públicos solamente puede efectuarse respecto de las materias de su competencia y con sujeción a las normas de la Ley 19.628. En esas condiciones, no necesitará el consentimiento del titular para el tratamiento (Artículo 20). Por otro lado, se prescribe en el artículo 22, que el Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de los organismos públicos, el cual tendrá carácter público. En este registro debe hacerse constar respecto de cada uno de los bancos de datos: 1) El fundamento jurídico de su existencia; 2) Su finalidad; 3) Los tipos de datos almacenados y, 4) Una descripción del universo de personas que comprende. La ley dispone a la vez, que todo lo anterior debe ser definido por reglamento. El reglamento respectivo si bien regula la materia, no establece sanción alguna en caso de no cumplirse lo preceptuado por éste (Decreto Nº 779/2000 Min. Justicia). Agrega finalmente la Ley 19.628, que el organismo público responsable del

banco de datos debe proporcionar esos antecedentes al Servicio de Registro Civil e Identificación cuando se inicien las actividades del banco de datos, y comunicar cualquier cambio dentro de los quince días desde que se produzca (Artículo 22 inciso final). En relación a los particulares o sector privado, la ley chilena no contempla la creación de un registro de bancos de datos personales, ni menos la obligación de inscribir éste por los particulares que sean responsables de esos bancos de datos.

Finalmente, en el caso paraguayo, debemos señalar que la respectiva ley no contempla disposiciones al respecto.

9.7 Archivos, Registros o Bancos de Datos Relativos a Encuestas

Respecto de los archivos o bancos de datos relativos a encuestas, la ley argentina Nº 25.326 dispone en el artículo 28, que no serán aplicables sus disposiciones a las encuestas de opinión, mediciones y estadísticas, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable. En esta materia, podríamos señalar que al sector público, en lo relativo a las mediciones y estadísticas realizadas a través del censo nacional, tampoco se le aplicaría la Ley 25.326, pues esa actividad se rige por una ley especial, la Nº 17.622. En los demás casos, la regla operaría ampliamente tanto respecto del sector público como el privado. Por lo tanto, sí existiría un ámbito de regulación diferenciada.

En lo relativo a la legislación chilena, debemos consignar que ella no hace referencia explícita a un sector u otro como ámbito objetivo de aplicación, respecto de los archivos, registros o bancos de datos relativos a encuestas (Art. 3º Ley 19.628). La misma situación anterior es constatable en la legislación paraguaya, dado que el artículo 3º de la Ley 1.682 se limita a señalar que es lícita la recolección, almacenamiento, procesamiento y publicación de datos o características personales, que se realice con fines científicos, estadísticos, de encuestas y sondeos de la opinión pública o de estudio de mercados, siempre que en las publicaciones no se individualicen las personas o entidades investigadas. Por lo tanto, entendemos que dicha norma es aplicable tanto al sector público como a los particulares.

9.8. Tratamiento Manual o Automatizado de Datos

En lo relativo al carácter del tratamiento de los datos, el legislador argentino ha sido bastante claro, pues incluye dentro del ámbito objetivo de la regulación legal de protección de datos, tanto al tratamiento de datos automatizado como manual, lo cual se refleja además en el carácter de los archivos, registros, o bancos o bases de datos personales. En cuanto a la forma de regular la materia, no se aprecian diferencias entre el sector público y el privado. Por lo tanto, podemos afirmar que tanto el tratamiento manual como el automatizado de datos personales que realice el Estado, o los particulares con el fin de proporcionar informes, están sujetos de igual manera a la normativa de la Ley 25.326.

La ley chilena por su parte, no es tan explícita en este tema como la ley argentina, pero en definitiva la respuesta es la misma, pues se desprende de la amplia definición legal del "tratamiento de datos", así como también de la definición de "registro o banco de datos", que el ámbito objetivo de aplicación de la Ley 19.628 abarca tanto a los registros o bancos de datos manuales como automatizados, sin establecer diferencias en cuanto al carácter público o privados de ellos (Art. 2º).

La ley del Paraguay a su vez, tampoco es tan clara como la argentina y más se parece a la chilena. Con todo, no es difícil llegar a concluir que el ámbito de aplicación de la ley alcanza tanto al tratamiento manual como automatizado de datos. Ello se desprende de lo señalado por el artículo 1º, el cual dispone que el objeto de la ley es regular la recolección, almacenamiento, distribución, publicación, modificación, destrucción, duración y, en general, el tratamiento de datos personales contenidos en archivos, registros, bancos de datos *"o cualquier otro medio técnico de tratamiento de datos"*. En definitiva, estimamos que la regla operaría tanto respecto del sector público como privado sin diferencias de tratamiento.

9.9 Personas Jurídicas como Titulares de Datos

La regulación legal de este punto en los tres ordenamientos jurídicos que disponen de leyes más o menos generales de protección de datos no es uniforme. El legislador argentino, expresamente reconoce como titulares de los derechos consagrados en la Ley a las personas jurídicas (Art. 2º) sin distinguir entre las de derecho público o de derecho privado. La ley chilena, en cambio, sólo reconoce como titulares de datos personales a las personas naturales o físicas**.** Lo anterior, queda claro en el artículo 2º letra f de la Ley 19.628, al leerse la definición de "datos de carácter personal o datos personales". Por lo tanto, expresamente se ha dejado fuera de la protección de la Ley chilena a los datos o información relativa a las personas jurídicas o morales. En este sentido, la exclusión es amplia e incluye tanto a las personas jurídicas de derecho privado como de derecho público.

Finalmente, debemos decir que al respecto, la ley paraguaya no se pronuncia sino que sólo habla de "toda persona" en el artículo 8 de la Ley 1.682. Por lo tanto, para efectos de este análisis estimaremos que la materia no está regulada y en consecuencia no cabría hablar de trato diferenciado entre el sector público y el sector privado.

9.10 Transmisión Internacional de Datos Personales

En materia de transmisión o transferencia internacional de datos personales, podemos señalar que la ley argentina establece un trato diferenciado para algunos organismos del Estado, a los cuales faculta para transmitir datos personales fuera del territorio argentino (sin necesidad de consentimiento del titular y, aunque el país receptor no contemple niveles de protección adecuados a esos datos). Los casos establecidos por la Ley son los siguientes: 1) Colaboración judicial internacional; 2) Cuando la transferencia se hubiere acordado en el marco de tratados internacionales en que el Estado argentino fuere parte; y 3) Cuando la transferencia tenga por objetivo la cooperación internacional entre

organismos de inteligencia para la lucha contra el crimen organizado, terrorismo o narcotráfico (Art.12).

En la ley chilena de protección de datos, la materia no ha sido regulada por ésta sino que se ha dejado la tarea al Derecho Internacional para que a través de tratados internacionales se desarrolle todo lo relativo al tema (Art. 5º inc. Final).

Por último, analizada la ley paraguaya Nº 1.682 podemos afirmar que ésta no hace ninguna referencia a la materia, por lo cual entendemos que la transmisión internacional de datos no ha sido objeto de regulación legal.

10. Régimen General de Responsabilidad

En este último punto del Capítulo IV, analizaremos el régimen de responsabilidad adoptado por los diversos ordenamientos jurídicos latinoamericanos abarcados por este estudio, en materia de protección de datos personales. Como se vio en el Capítulo II, el análisis del régimen de responsabilidad en cada país se dividió en tres clases: administrativa, civil y penal. Luego, en cada una de ellas y dependiendo del mayor o menor desarrollo legal en la materia, para efectos de la exposición gráfica de los datos en la Tabla comparativa Nº 9 del Capítulo III [586] , hemos agrupado a la vez en cuatro tipos la legislación existente: especial, sectorial compleja, sectorial y común. Dentro de la legislación especial, se han incluido las leyes generales de protección de datos y las leyes que regulan el ejercicio de las acciones de hábeas data o de acceso a la información, que prevén al mismo tiempo sanciones para quienes violen sus disposiciones. Por otro lado, agrupamos dentro del término legislación sectorial compleja, a aquellos estatutos legales que regulan sectorialmente la protección de los datos personales y en los cuales es posible visualizar en mayor o menor medida la influencia de las normas y principios internacionales sobre el tratamiento de datos. Estos estatutos, por lo general, se circunscriben a regular el mercado de la información crediticia. El uso del término legislación sectorial, lo hemos circunscrito para referirnos a aquellos estatutos que abordan la protección de datos por áreas específicas, parcialmente, y sin visualizarse en éstos la influencia de las normas y principios internacionales en la materia de estudio. Entre éstos estatutos destacan comúnmente las leyes que regulan ciertas actividades sectoriales, como la financiera y tributaria, las que en materia de protección de datos se limitan a establecer deberes de reserva o secreto de cierta información personal, tanto de los clientes como de los sujetos pasivos de la obligación tributaria respectivamente. Finalmente, utilizaremos el término legislación común para referirnos a aquella normativa que a falta de normas especiales o sectoriales, o junto con ellas, sería aplicable para hacer efectivas las responsabilidades de quienes lesionan los derechos de las personas; sea en el ámbito específico de la protección de datos, o en cuanto a los bienes jurídicos que fundamentan o podrían fundamentar tal protección, como lo es la intimidad, la vida privada e incluso el honor. A continuación, revisaremos el régimen de responsabilidad en

[586] Ver Capítulo III, Tabla Nº 9

atención al carácter de los estatutos que desarrollan las respectivas normas, para lo cual nos hemos basado en la Tabla comparativa Nº 9, incluida en el Capítulo III [587] de este estudio.

10.1 Legislación Especial

De los ordenamientos jurídicos comprendidos en esta investigación, sólo la menor parte de ellos dispone de estatutos especiales o leyes generales de protección de datos, que prevean además normas especiales de responsabilidad.

Comparativamente, de los sistemas jurídicos que disponen de leyes generales de protección de datos, sin duda que el sistema argentino se asoma como el más desarrollado en materia de responsabilidad. Como se recordará, la Ley 25.326, contempla sanciones administrativas y penales, así como también establece una regla especial en materia de responsabilidad civil. Las sanciones administrativas son aplicadas por el órgano de control denominado Dirección Nacional de Protección de Datos, las cuales pueden consistir en: apercibimiento, suspensión, multa de mil pesos a cien mil pesos, clausura o cancelación del archivo, registro o banco de datos (Art. 31 Ley 25.326 y 31 del Reglamento). En materia civil, se establece un regla especial de responsabilidad referida a la cesión o transferencia de datos, en virtud de la cual, el cesionario queda sujeto a las mismas obligaciones legales y reglamentarias del cedente, respondiendo además este último solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate (Art. 11 Nº 4 Ley 25.326 y art. 11º Reglamento). Finalmente, en materia penal debemos recordar que se introdujeron dos artículos en el Código del ramo argentino, los cuales sancionan con penas privativas de libertad: 1) A quienes proporcionen a un tercero, a sabiendas, información falsa contenida en un archivo de datos personales (Arts. 117 bis); 2) A quien sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales (Art. 157 bis Nº 1) y, 3) A quienes revelaren a otro, información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley (Art. 157 bis Nº 2).

Por su parte, la ley chilena de protección de datos establece sanciones de dudoso carácter -que en definitiva hemos entendido como de carácter administrativo- consistentes en multas y suspensión de funciones de ciertos funcionarios públicos renuentes a cumplir las órdenes del Tribunal que conoce de una acción de amparo o hábeas data, las cuales pueden ser aplicadas por el propio juez civil que conoce de esta acción (Art. 16 inciso 5º Ley 19.628). Junto con ellas, se introdujeron por la Ley 19.628 y por la Ley 19.812 modificatoria de la anterior, disposiciones al Código Sanitario y al Código del Trabajo respectivamente en materia de protección de datos. En el primero, se estableció el carácter de reservado de las recetas médicas y los análisis o exámenes de salud, cuya violación se sanciona administrativamente por el Director General de Salud (Art. 127 incisos 2º y 3º y, art. 174 C. Sanitario). En el Código del Trabajo, por su parte, se instituyó una regla que impone un deber de reserva al empleador respecto de los datos

[587] Ver Capítulo III, Tabla Nº 9

privados del trabajador que tenga acceso con ocasión de la relación laboral (Art. 154 bis). También se introdujo una regla de no discriminación en la contratación de los trabajadores basada en sus antecedentes comerciales (Art. 2º inc. 6º). Las infracciones a las disposiciones señaladas se sancionan administrativamente por la Dirección de Trabajo (Art. 477 C. del Trabajo). En materia civil, la Ley 19.628 repite las reglas generales de la responsabilidad, destacando la disposición que reconoce expresamente la procedencia de la indemnización tanto del daño patrimonial como moral que se causare a las personas naturales a consecuencia del tratamiento indebido de sus datos personales (Art. 23 Ley 25.326). Finalmente, debemos recordar que la ley chilena no estableció delitos que castiguen conductas que atenten en contra de los derechos de los titulares de los datos personales.

En la República del Ecuador, hemos constatado que la Ley de Control Constitucional de 1997 que regula el ejercicio de la acción constitucional del hábeas data, establece sanciones al parecer de carácter administrativo para quienes incumplieren las resoluciones expedidas por los jueces o Tribunales que concedan el hábeas data. Estas sanciones pueden consistir en la prohibición a las personas jurídicas o naturales deejercer directa o indirectamente las actividades que venían desarrollando y que dieron lugar al hábeas data por el lapso de un año (Art. 42), y en la destitución por el juez o Tribunal, sin más trámite de su cargo o empleo, a los funcionarios públicos de libre remoción que se nieguen a cumplir con las resoluciones que expidan esos jueces o Tribunales dentro del procedimiento de hábeas data (Art. 43).

El ordenamiento jurídico de Panamá por su parte, cuenta con un estatuto legal especial denominado Ley de Transparencia en la Gestión Pública, la cual establece dos disposiciones en materia de responsabilidad administrativa, atingentes al ejercicio de la acción de hábeas data respecto de los archivos o registros públicos. La primera de ellas, prescribe que se sancionará al funcionario que, requerido por el Tribunal que conoce del recurso de hábeas data, incumpla con la obligación de suministrar la información. En este caso, se incurrirá en desacato y será sancionado con multa mínima equivalente al doble del salario mensual que devengue y, en caso de reincidencia, el funcionario será sancionado con la destitución del cargo (Art. 20). La segunda disposición que establece sanciones administrativas es el artículo 22, y prescribe que el funcionario que obstaculice el acceso a la información, destruya o altere un documento o registro, será sancionado con multa equivalente a dos veces el salario mensual que devenga, sin perjuicio de las demás sanciones pertinentes. En lo que respecta a la responsabilidad civil, la Ley de Transparencia en la Gestión Pública establece en el artículo 21 una regla que exime de responsabilidad al Estado por el hecho de sus funcionarios, disponiendo que la persona afectada por habérsele negado el acceso a la información, una vez cumplidos los requisitos y trámites legales, tendrá derecho a demandar civilmente al servidor público responsable por los daños y perjuicios que se le hayan ocasionado. La norma anterior, sin duda no parece razonable, pues desconoce toda la construcción dogmática que está detrás de la consideración del Estado como sujeto pasivo de responsabilidad por la falta o deficiencia del servicio, lo que además redunda en un serio perjuicio para el afectado, el que sólo tendrá el patrimonio del funcionario público para resarcirse y compensar los daños provocados por éste en el ejercicio de sus funciones.

La ley paraguaya Nº 1.682 que reglamenta la información privada, contempla por su parte algunas sanciones -al parecer de carácter administrativo- consistentes en multas; algunas son aplicables exclusivamente a las personas físicas o jurídicas que publiquen o distribuyan información sobre la situación patrimonial, solvencia económica o cumplimiento de obligaciones comerciales y financieras (Art. 10 letras a y b), y otras, son de aplicación general pero circunscritas a la denegación o retardo de la entrega de información ante el ejercicio extrajudicial del derecho de acceso (Art. 10 letra c). Con todo, la Ley 1.682 no señala el procedimiento ni el juez competente para conocer tanto las acciones de hábeas data como la aplicación de las sanciones respectivas.

En el ordenamiento jurídico peruano, laLey de Transparencia y Acceso a la Información Pública, que regula el ejercicio del hábeas data respecto de archivos públicos, sanciona a los funcionarios o servidores públicos que incumplan con las disposiciones de esta Ley, así como también a aquéllos que de modo arbitrario obstruyan el acceso del solicitante a la información requerida, o la suministren en forma incompleta u obstaculicen de cualquier modo el cumplimiento de la Ley, lo que será considerado como falta grave (Art. 4 y 14).

A partir de lo anterior, podemos afirmar que son escasos en Latinoamérica los estatutos legales de carácter general, que en el ámbito de la protección de datos contemplan normas específicas en materia de responsabilidad, estableciendo sanciones para quienes violen los derechos de los titulares a causa del tratamiento de sus datos.

10.2 Legislación Sectorial Compleja

Dentro de esta clasificación, hemos incluido a todos aquellos estatutos latinoamericanos que regulan el tratamiento de datos personales de forma sectorial específica, dentro de los cuales es posible visualizar, comúnmente, ciertas influencias tanto de la legislación como de los principios internacionales sobre protección de datos. A continuación señalaremos esos cuerpos legales y los regímenes de responsabilidad que ellos consagran.

En el ordenamiento jurídico ecuatoriano, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos [588] , establece diversos tipos penales de los cuales al menos uno, se acercaría bastante al bien jurídico autodeterminación informativa, pues sanciona a quien obtuviere información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares (Artículo 58 inciso 5º). En esta disposición aparecería claramente tutelado a nivel penal el principio del consentimiento del titular de los datos para la transmisión de éstos, quedando la duda en cuanto al ámbito de aplicación de la respectiva norma, pues está circunscrita a la mensajería de datos. Por otra parte, la Ley castiga también: 1) A quien empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información, para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad

[588] Como se recordará el objeto de esta Ley es: regular los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.(Art.1º)

(Artículo 58 inciso 1º); 2) A quien empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información, para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad (Artículo 58 inciso 1º) y, 3) A quien encargado de la custodia o utilización legítima de la información, y cometiendo las acciones descritas en el inciso 1º del artículo 58º, la divulgare o la utilizare fraudulentamente (Artículo 58 inciso 4º). En suma, la ley de comercio electrónico se limita a tipificar como delitos determinadas conductas lesivas a los derechos de los titulares de datos personales,enviados, recibidos, comunicados o archivados por medios electrónicos y que pueden ser intercambiados por cualquier medio transmitidos a través de las nuevas tecnologías (Disposición Gral. 9ª Ley de Comercio Electrónico ...).

Por su parte, el ordenamiento jurídico mexicano dispone a nivel sectorial complejo con una ley que regula las Sociedades de Información Crediticia, la cual establece normas de responsabilidad civil, y prevé además sanciones administrativas para quienes infrinjan sus disposiciones. En lo relativo a las sanciones administrativas, podemos señalar que éstas son aplicables tanto a los usuarios como a las sociedades de información que violen el deber de secreto que pesa sobre ellos respecto de los datos personales crediticios y comerciales que utilizan. El deber de secreto financiero, se extiende a los empleados de las Sociedades y a los de las Entidades Financieras, quienes en caso de violar la obligación que sobre ellos, se exponen a ser sancionados por la ComisiónNacional Bancaria y de Valores con la inhabilitación para desempeñar un empleo, cargo o comisión dentro del sistema financiero mexicano, por un periodo de seis meses a diez años (Art. 53). También se sanciona con multa aplicada administrativamente por dicha Comisión, a las Sociedades que: 1) No envíen el Reporte de Crédito Especial al Cliente, los Reportes de Crédito y los informes dentro de los plazos legales (Art. 54); 2) Alteren, eliminen o modifiquen algún registro de sus bases de datos, sin algún motivo que así lo justifique (Art. 54); 3) Proporcionen el nombre, domicilio y cualquier otro dato del Cliente contenido en su base de datos a un Usuario o a un tercero, sin contar con la autorización del Cliente (Art. 55); 4) Hagan uso o manejo indebido de la información (Art. 55). Por último, en lo relativo a las sanciones administrativas, debemos señalar que las comisiones encargadas de la inspección y vigilancia de las Entidades Financieras, podrán sancionar a las mismas con una multa cuando soliciten información de los clientes o consumidores sin contar con la autorización prevista en la Ley (Art. 56).

En materia de responsabilidad civil, la Ley mexicana que regula las Sociedades de Información Crediticia, establece normas especiales que modifican el régimen general, pues limita la reparación de los daños causados por esas Sociedades al proporcionar la información de crédito, sólo en el evento de existir culpa grave, dolo o mala fe en el manejo de la base de datos (Art. 51). Como ya lo hemos hecho presente, estimamos que el régimen de responsabilidad establecido por esta Ley es inadecuado, pues implica una limitación a la responsabilidad tanto de los usuarios del sistema (instituciones financieras en general y las empresas comerciales) como de las sociedades de información crediticia, sin una justificación razonable para ello. En suma, creemos que restringir la responsabilidad civil de aquellos que están en la mejor posición para evitar los riesgos, sólo a los hechos dolosos, implica desconocer toda la fundamentación de justicia que se erige tras la atribución de responsabilidad por negligencia.

Otro ordenamiento jurídico que dispone de una legislación sectorial compleja en materia de datos personales, y que a la vez establece reglas de responsabilidad, es el panameño. En efecto, la Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores establece un catálogo de conductas constitutivas de infracción a la Ley, distinguiendo según la entidad de ellas, en infracciones de carácter leve, grave y muy grave (Art. 39-41). A éstas, se aparejan respectivamente tres clases de sanciones administrativas, las cuales sonaplicadas por la Comisión de Libre Competencia y Asuntos del Consumidor (CLICAC); las infracciones leves son sancionadas la primera vez con amonestación escrita y en caso de existir reincidencia, las subsiguientes son consideradas graves. Las infracciones graves, son sancionadas la primera vez con multa de mil balboas a cinco mil balboas y en caso de existir reincidencia, las subsiguientes son consideradas muy graves. Por último, cabe decir que las infracciones muy graves son sancionadas con multa de cinco mil balboas con un centésimo a diez mil balboas (Art. 42) [589] . Como comentario final diremos que debe tenerse en cuenta, quela CLICAC sanciona el desacato o desobediencia a las órdenes de hacer o no hacer, emitidas a través de resoluciones, con multa de quinientos balboas a mil balboas, la cual es reiterativa y se comete por día, hasta que se cumpla con lo ordenado (Artículo 42 inciso final).

La última normativa correspondiente a este punto, es la ley peruana que regula las Centrales Privadas de Información de Riesgos y vela por la protección del titular de la información (Ley de CEPIRS). Este estatuto establece reglas de responsabilidad administrativa y civil. Respecto de las primeras, diremos que en el artículo 20 se prescribe un catálogo de conductas constitutivas de infracciones administrativas en las cuales pueden incurrir las Centrales Privadas de Información de Riesgos (Art. 15), respecto de las cuales son objetivamente responsables, sin perjuicio de la responsabilidad que pudiera corresponder a las fuentes de las que hubieran recolectado información (Art. 20). Las sanciones respectivas son aquellas establecidas por la Ley de Protección al Consumidor, y son aplicadas por la Comisión de Protección al Consumidor. Por lo tanto, en virtud del artículo 40 de la señalada Ley, los proveedores infractores podrán ser sancionados administrativamente con una amonestación o con una multa. Además de estas sanciones, se prevé por el legislador la aplicación de medidas correctivas, las cuales tienen por objeto revertir los efectos que las conductas infractoras hubieran ocasionado o evitar que éstas se produzcan nuevamente en el futuro (Art. 40 Ley de Protección al Consumidor en relación con el art. 22 Ley de CEPIRS). Esas medidas son las siguientes: 1) La modificación o cancelación de la información de riesgos registrada en los bancos de datos de las CEPIRS y, 2) La rectificación de la información comercial de riesgos difundida en el mercado, por cuenta y costo del infractor, en la forma que determine la Comisión. Por otro lado, se señala en el inciso 2º del artículo 22º que adicionalmente a las sanciones administrativas a que hubiera lugar respecto de las CEPIRS, la Comisión de Protección al Consumidor impondrá sanciones a las fuentes proveedoras de la información que incurran en alguna infracción a la Ley y, en general, a las terceras personas que hayan proporcionado información de riesgos a las CEPIRS y que resulte ilegal, inexacta, errónea o caduca. En materia civil, la Ley de CEPIRS peruana establece respecto de estas empresas un régimen de responsabilidad estricta u

[589] Ver Capítulo II, Análisis de la Protección a los Datos Personales en Panamá, punto Nº 9.1.1.

objetiva, facultándose a las Centrales a repetir en contra de las fuentes proveedoras de información cuando el daño sea ocasionado como consecuencia del tratamiento de información realizada por éstas (Art. 18.1). En cambio, para los usuarios y receptores de los reportes de crédito, el régimen de responsabilidad establecido por la ley es por culpa o negligencia (Art. 18.2).

En suma, del análisis comparativo de los diversos estatutos sectoriales complejos presentes en Latinoamérica referidos al tratamiento y difusión de información de crédito de los consumidores, no existe homogeneidad en materia de responsabilidad, presentando diverso desarrollo tales regímenes. Llama la atención en ellos, la asimetría del tratamiento de la responsabilidad civil, la cual puede ir desde una exclusión de ésta por los daños causados con culpa o negligencia (Ley mexicana que regula las Sociedades de Información Crediticia) hasta un régimen de responsabilidad estricta u objetiva (Ley peruana de CEPIRS). En cuanto a las sanciones administrativas, puede vislumbrarse cierta dificultad para articularlas, pues en general se recurre a organismos de control relacionados con la defensa de los consumidores que no son especializados en la materia y a los cuales por añadidura se les ha encomendado legalmente velar por los derechos de los titulares de los datos. La falta de una legislación general de protección de datos así como también de un organismo de control especial se hace notar con fuerza.

10.3 Legislación Sectorial

Dentro de los ordenamientos jurídicos comprendidos en este estudio, los estatutos legales de carácter sectorial constituyen la regla general en materia de protección a los datos personales. Sin embargo, ese mismo carácter estrecho es su mayor debilidad, pues invariablemente las normas relacionadas a la tutela de los datos que se contienen en esos cuerpos legales se traducen en disposiciones que a lo más establecen deberes de confidencialidad o reserva de determinadas informaciones personales, sin desarrollar el tratamiento que a éstas debe darse. Destacan y están presentes en la mayoría de los países abarcados por este trabajo, las leyes generales de bancos e instituciones financieras que establecen la reserva y/o el secreto bancario, y las leyes tributarias que establecen el secreto o reserva fiscal o tributaria. Esa normativa, coexiste a la vez con diversos estatutos, de variados objetivos, cuyo rasgo común es la imposición de un deber de reserva o confidencialidad respecto de cierta información personal, tutelándose la mayoría de las veces tanto el derecho a la intimidad como el derecho a la vida privada. Otra limitación importante que a nuestro juicio presentan este tipo de legislaciones, es el hecho de haber sido establecidas sin tener en cuenta las normas y principios internacionales de protección de datos personales. Más aún, muchas de esas normas han sido dictadas en el siglo pasado y conviven incluso con una legislación general de protección de datos, como ocurre por ejemplo en el caso chileno, donde la discutible actual normativa de la Ley General de Bancos que establece el secreto y la reserva bancaria, proviene del D.F.L. 252 del año 1960, es decir, 39 años antes que naciera la Ley 19.628.

A continuación, señalaremos los diversos estatutos legales sectoriales presentes en

Latinoamérica relacionados a la protección de datos personales y que establecen normas de responsabilidad.

En materia de secreto y/o reserva bancaria, hemos constatado que disponen de normas de responsabilidad, a lo menos, los siguientes ordenamientos jurídicos: Argentina (Ley sobre Entidades Financieras, art. 41), Bolivia (Ley de Bancos e Instituciones Financieras, art. 89), Brasil (Ley Complementaria 105, arts. 10 y 11), Chile (Ley General de Bancos, art. 19 y 154), Ecuador (Ley General de Instituciones del Sistema Financiero, art. 94 y 95), El Salvador (Ley Orgánica de la Superintendencia del Sistema Financiero, art. 37), Guatemala (Ley de Bancos, art. 63 y Ley Orgánica del Banco de Guatemala, art. 50), México (Ley de Instituciones de Crédito, arts. 112 bis y 118), Nicaragua (Ley General de Bancos, art. 110), Panamá (Ley Bancaria, art. 86), Paraguay (Ley General de Bancos, art. 88), Perú (Ley General del Sistema Financiero y del Sistema de Seguros, art. 141), República Dominicana (Ley General de Bancos, art. 34), Paraguay (Ley sobre el Sistema de Intermediación Financiera, art. 25) y, Venezuela (Ley General de Bancos y Otras Instituciones Financieras, arts, 279, 416, 444 y 446).

Por otra parte, cabe hacer presente que también es común encontrar dentro de los ordenamientos jurídicos latinoamericanos normas de responsabilidad vinculadas a las reglas de secreto fiscal o tributario. Entre esos ordenamientos podemos mencionar a lo menos los siguientes: Argentina (Ley de Procedimientos Fiscales, art. 101 inc. 4º), Bolivia (Código Tributario, arts. 124-126), Brasil (Ley sobre el Sistema Tributario Nacional, art. 198), Chile (Código Tributario, arts. 30 y 101), Colombia (Ley General de Procedimiento Tributario, art. 679), Costa Rica (Código Tributario, art. 115), Ecuador (Código Tributario, art. 101), El Salvador (Código Tributario, art. 28), Guatemala (Código Tributario, art. 96), Honduras (Código Tributario, art. 49), México (Código Fiscal de la Federación, art. 88), Paraguay (Ley que establece el Nuevo Régimen Tributario, art. 190), Perú (Código Tributario, art. 186), República Dominicana (Código Tributario, arts. 258, 259, 260 y 262), Uruguay (Código Tributario, art. 47) y, Venezuela (Código Orgánico Tributario, arts. 115 y 119).

Pasando a otra materia, podemos señalar que en dos estatutos legales latinoamericanos de protección a los consumidores, hemos constatado la existencia de normas de responsabilidad en relación al tratamiento de datos personales, los cuales establecen sanciones administrativas que deben ser aplicadas por los respectivos órganos de control de la protección a los consumidores. Estos son: Brasil (Ley de Protección al Consumidor: art. 56 en relación con el art. 43) y México (Ley Federal de Protección al Consumidor, arts. 126 y 127 en relación con arts. 16 y 18).

Debemos hacer presente además, que también hemos evidenciado la existencia algunos estatutos sectoriales que regulan otras áreas del derecho, previendo al mismo tiempo reglas de responsabilidad en materia de datos personales. Estas reglas comúnmente se limitan a sancionar la violación de deberes funcionarios de confidencialidad o reserva, relativos a determinada información personal. En estos casos las sanciones generalmente son aplicadas administrativamente por la autoridad de control. En este párrafo, solamente señalaremos los estatutos latinoamericanos a los cuales hemos accedido vía Internet, haciendo presente que la tarea por localizar toda la legislación sectorial que prevea normas de protección de datos en Latinoamérica es tarea

pendiente y materia de otro estudio más profundo. A continuación, mencionaremos los ordenamientos que disponen de otros estatutos sectoriales que contienen reglas de responsabilidad en la materia de estudio. Estos son: Argentina (Ley sobre sistema de Tarjetas de Crédito, Compra y Débito: art. 48), Brasil (Ley de Protección del Niño y del Adolescente: art. 247), México (Ley de Protección y Defensa al Usuario de Servicios Financieros, art. 15) y República Dominicana (Código para la Protección de Niños, Niñas y Adolescentes: art. 66).

Finalmente, en lo relativo a los estatutos sectoriales que establecen reglas de responsabilidad relacionadas a la protección de los datos personales, tenemos que agregar algunas normas que tipifican como delitos, diversas conductas que atentan en contra de los bienes jurídicos intimidad y vida privada, distintos a los delitos de violación del secreto bancario y tributario. Debe aclararse que la existencia de esas normas, no obedecería a una intención expresa legislativa por proteger los derechos de los titulares de los datos, basado en el reconocimiento de un derecho a la autodeterminación informativa o derecho de control sobre el uso de la propia información, sino que más bien expresarían una repuesta social a los atentados directos o indirectos en contra de la intimidad, los cuales pueden concretarse de diversas formas y a través de variados medios materiales. El hecho que contemplemos en nuestra investigación tales normas penales sólo tiene un afán ilustrativo de la legislación protectora de los bienes jurídicos generalmente reconocidos como objeto de tutela por las normas de protección de datos personales (intimidad y vida privada), por lo que su sola enunciación no significa que los estimemos aptos para amparar en sede penal los derechos de los titulares de datos. En definitiva, los ordenamientos jurídicos que establecen disposiciones penales en leyes especiales desde el punto de vista penal, pero sectoriales según nuestra clasificación, son los siguientes: Chile (Ley Nº 19.223 que tipifica figuras penales relativas a la informática, arts. 2 y 4), México (Ley de Imprenta, arts. 10 y 12), República Dominicana (Ley sobre Expresión y Difusión del Pensamiento: art. 43) y Venezuela (Ley Especial Contra los Delitos Informáticos, arts. 20, 21 y 22; Ley sobre Protección a la Privacidad de las Comunicaciones, arts, 2, 6 y 8 y, Ley de Registro de Antecedentes Penales, art. 13).

10.4 Legislación Común

Hemos agrupado dentro del término legislación común, a todos los estatutos legales que establecen una regulación general, susceptible de ser aplicada supletoriamente, a falta de leyes especiales o sectoriales en materia de responsabilidad por violaciones a los derechos de los titulares de los datos. Estos estatutos se visualizan en tres grandes áreas del derecho: administrativa, civil y penal. Respecto de esta última, debemos recordar que su inclusión sólo responde a la finalidad de ilustrar el estado de la legislación penal en materia de protección a la intimidad y a la vida privada, por lo que no significa que estimemos idónea su eventual aplicación para tutelar directamente los derechos de las personas ante el tratamiento de sus datos personales.

En lo que respecta a las reglas generales de la responsabilidad administrativa, solamente hemos accedido a la legislación de los siguientes ordenamientos jurídicos: Bolivia (Estatuto del Funcionario Público: art 9º), Chile (L.O.C. de Bases Generales de la

Administración del Estado, arts. 4 y 18) y Colombia (Código Contencioso Administrativo: art. 76º). En materia civil, como se ha visto, comúnmente los ordenamientos jurídicos latinoamericanos disponen de reglas generales de responsabilidad civil extracontractual. En base a la información que hemos recolectado, podemos afirmar que serían aplicables ante el evento de daño o perjuicio a los titulares de los datos personales, las reglas generales de la responsabilidad extracontractual, a lo menos en los siguientes sistemas jurídicos: Argentina (Código Civil, arts. 1.071 y ss.), Bolivia (Código Civil, arts. 24 y 984), Chile (Código Civil, arts. 1.546, 1.547, 1.556, 1558 y 2.314 y ss.), Costa Rica (Código Civil, arts. 1.045 y 1.046), Ecuador (Código Civil, arts. 1.480 y 2.241), El Salvador (Código Civil, arts. 2.067 y 2.080), México (Código Civil, art. 1.910 y ss.), Paraguay (Código Civil, art. 1.833), Perú (Código Civil, arts. 1321 y 1969 y ss.), Uruguay (Código Civil, arts., 1.919 y ss.) y Venezuela (Código Civil, arts. 1.185 y ss.).

Finalmente, en lo que respecta a las normas comunes de carácter penal, podríamos aseverar que en todos los ordenamientos jurídicos comprendidos en este estudio, hemos encontrado normas que sancionan conductas que atentan comúnmente en contra de los bienes jurídicos intimidad y vida privada, tipificándose en general el delito de violación de domicilio, violación de la correspondencia y de las comunicaciones privadas, así como también el delito de violación de secretos. Sin embargo, cabe hacer presente que algunas legislaciones presentan un mayor desarrollo en la materia, producto de la introducción de tipos específicos que tutelan la intimidad, como lo es el caso de Chile (Art. 161 A: Delitos contra el respeto y protección a la vida privada y pública de la persona y su familia), Costa Rica (Art. 196 bis:Violación de las comunicaciones electrónicas), El Salvador (Art. 186:Captación de comunicaciones), Paraguay (Art.143: Lesión de la intimidad de la persona), y Perú (Art. 157: Uso indebido de archivos computarizados). Con todo, es necesario tener presente que hemos omitido dentro de la enumeración anterior a los delitos introducidos en el Código Penal argentino por la Ley 25.326, y los delitos agregados por la ley ecuatoriana de comercio electrónico, firmas y mensajería de datos al respectivo Código Penal, dado que fueron tratados dentro del punto relativo a los estatutos legales especiales y sectoriales complejos en materia de protección de datos. No obstante lo anterior, debe destacarse que ellos se han incorporado a la legislación común penal.

En suma, la legislación común latinoamericana a la que hemos podido acceder, aparece como la herramienta subsidiaria para tutelar los derechos de los titulares de los datos personales, a falta de normas especiales o sectoriales que cubran ámbitos específicos. Sin embargo, en materia penal, la conclusión anterior no puede ser sostenida sin un previo estudio en profundidad de los tipos penales respectivos, tarea que obviamente hemos endosado a los penalistas, tanto por la competencia específica en la materia que se discute, como porque excede los límites de esta investigación.

CAPITULO V. CONCLUSIONES

A través del estudio particular y comparativo de los diecinueve ordenamientos jurídicos latinoamericanos incluidos en este trabajo, hemos podido comprobar que tanto a nivel constitucional como legal, el grado de desarrollo de los respectivos sistemas jurídicos en materia de protección de datos personales es diverso, presentando cada uno de ellos particularidades propias.

A nivel constitucional, se han podido observar en Latinoamérica diversos estados de complejidad normativa. El más avanzado, está representado por aquellos ordenamientos latinoamericanos que prevén expresamente la garantía del hábeas data o derecho a la protección de datos, pudiendo constatarse que el más complejo de esos sistemas, el venezolano, incluso establece límites a la utilización de la informática. En el otro extremo, es decir, en el grado mínimo de desarrollo constitucional, se ubican los ordenamientos jurídicos que reconocen indirectamente el derecho a la vida privada y/o el derecho a la intimidad. En esta situación se encuentran actualmente Bolivia, Cuba, México, Panamá, República Dominicana y Uruguay.

Dentro de los ordenamientos de Latinoamérica que disponen de normas constitucionales sobre protección de datos, también se evidencia una diversidad en cuanto al grado de desarrollo en la materia. En efecto, se visualizan por una parte sistemas jurídicos cuyas disposiciones constitucionales de protección de datos abarcan normativamente tanto a los archivos, registros o bancos de datos públicos como privados. Ello ocurre en Colombia (Art. 15 C. Pol.), Ecuador (Art. 94 C. Pol.), Perú (Art. 200 Nº 3, en relación con el artículo 2º Nº 5º y Nº 6º) y Venezuela (Art. 28 C. Pol.). Esta situación

representa el nivel más complejo de regulación constitucional, lo que se traduce en definitiva en la posibilidad de accionar de hábeas data en contra de los responsables de archivos o bancos de datos, sean éstos públicos o privados. Por otra parte, también se verifica la existencia de sistemas jurídicos cuyas disposiciones constitucionales de protección de datos abarcan normativamente a los archivos o bancos de datos de carácter público o estatal y sólo algunos archivos o bancos de datos de carácter privado. Esta situación está presente en los ordenamientos jurídicos de Argentina (Art. 43 inc. 3º C. Pol.), Brasil (Art. 5º LXXII C. Pol.) y Paraguay (Art. 135 C. Pol.), lo cual significa un menor grado de protección a los derechos de los titulares, pues no reconocen como sujetos pasivos de la acción de hábeas data a los responsables de bancos de datos de carácter privado o de uso estrictamente personal. De otra parte, se evidencian sistemas jurídicos cuyas disposiciones constitucionales de protección de datos, abarcan como ámbito normativo objetivo solamente a los archivos, registros o bancos de datos públicos, lo que ocurre en Guatemala (Art. 31 C. Pol.) y Nicaragua (Art. 26 Nº 4 C. Pol.). Una de las posibles consecuencias de tal estrechez normativa, sería limitar el futuro desarrollo de una legislación general de protección de datos –legislación que por el momento no existe-, pues no se reconocen explícitamente derechos a los titulares de datos que puedan hacerlos valer ante los responsables de archivos, registros o bancos de datos privados. Sin embargo, ello no obstaría a que pudiera sostenerse una interpretación extensiva del texto fundamental, basada al menos, en el principio de igualdad ante la ley reconocido en el artículo 23 de la Convención Americana de Derechos Humanos, la cual ha sido ratificada por ambos países. Por último, y agotados los ordenamientos que disponen de normas constitucionales de protección de datos, debemos mencionar a aquéllos que se encuentran en la situación contraria, es decir, los ordenamientos jurídicos que no disponen de normativa constitucional en la materia y que, en definitiva constituyen mayoría en Latinoamérica. Ellos son : Bolivia, Chile, Costa Rica, Cuba, El Salvador, Honduras, México, Panamá, República Dominicana y Uruguay.

Del análisis efectuado a los distintos sistemas jurídicos latinoamericanos, hemos podido corroborar que el estado de progreso de ellos a nivel constitucional, en materia de protección de datos, lamentablemente no va de la mano con el desarrollo de la misma a nivel legal. Es decir, el hecho que un país posea normas constitucionales más o menos extendidas en cuanto a la protección de datos, no es indiciario de una regulación legal de las mismas características. Ejemplo de esta situación se halla en: a) Brasil, país en que existe una ley procedimental que regula la acción de hábeas data constitucional (Ley 9.507) y algunos estatutos sectoriales, del cual destaca la Ley de Protección al Consumidor; b) Colombia, que no tiene ley sustantiva ni procedimental de protección de datos, sino sólo estatutos sectoriales; c) Ecuador, que aún no posee ley general en la materia y, donde la normativa procedimental del hábeas data, además, ha sido duramente cuestionada por la doctrina y jurisprudencia (Ley de Control Constitucional), destacándose sólo una ley sectorial compleja que regula la mensajería de datos (Ley Nº 67-2002); d) Guatemala, donde sólo existe normativa sectorial; e) Nicaragua, en la misma situación anterior; f) Perú, el cual cuenta con una escueta ley procedimental del hábeas data (Ley 26.301), una ley sectorial compleja (Ley que regula las Centrales Privadas de Información de Riesgos) y diversos estatutos sectoriales y, g) Venezuela, que a pesar de presentar el escenario constitucional más favorable en todo Latinoamérica en materia de

protección de datos, no dispone de ley general sustantiva ni procedimental que regule el ejercicio de la garantía del hábeas data, sino solamente una legislación sectorial. Sin duda que la situación anterior llama profundamente la atención, pues las expectativas de los respectivos Constituyentes aún no se han satisfecho y los derechos de las personas quedan en definitiva desprovistos de una tutela adecuada. Los casos de excepción a lo descrito, es decir, aquellos países que junto con disponer de normas constitucionales de protección de datos además cuentan con una ley más o menos general en la materia, sólo están presentes en dos ordenamientos jurídicos: el argentino, que prevé a nivel infraconstitucional una legislación de protección de datos de carácter general (Ley 25.326) y el paraguayo, que cuenta con una legislación que -si bien tiene pretensiones de generalidad- se acerca más a una legislación sectorial compleja, dado que mayoritariamente se ocupa de reglamentar el funcionamiento del mercado de la información crediticia (Ley Nº 1.682). Debemos agregar a lo dicho, que la situación contraria a la señalada en los ordenamientos jurídicos que sí poseen normas de hábeas data puede apreciarse en Chile, donde la Constitución no contiene norma expresa que reconozca el derecho a la protección de datos personales o hábeas data, y sin embargo, ello no ha sido obstáculo para dictar una ley general de protección de datos (Ley Nº 19.628), basada principalmente en los derechos constitucionales a la vida privada e intimidad. Otro caso que destaca en este mismo sentido, es el de Panamá, donde a pesar de no reconocerse directamente el derecho a la intimidad ni contar tampoco con disposición constitucional que reconozca el hábeas data, el legislador se ha ocupado de dictar una ley que permite el acceso y rectificación de los datos personales en poder del Estado y sus organismos (Ley Nº 6-2002), junto con una ley sectorial compleja que regula los servicios de información del historial crediticio de los consumidores (Ley Nº 24-2002).

En el ámbito legal o infraconstitucional, hemos podido verificar que los ordenamientos jurídicos latinoamericanos presentan diversos niveles de complejidad y desarrollo en la materia de estudio. Algunos disponen de estatutos legales de carácter general, que se materializan en leyes de protección de datos, cuyo objetivo es regular la mayor cantidad de áreas vinculadas al tratamiento de éstos y la protección a sus titulares. Para tal cometido, esos estatutos -a los cuales hemos denominado especiales-, prevén normas de carácter sustantivo y procedimental. Estas normas están destinadas a la regulación del ejercicio de las denominadas acciones de hábeas data, de protección de datos o de amparo a los derechos de los titulares de datos. Otros sistemas jurídicos, disponen de cuerpos legales que llamamos estatutos sectoriales simples y estatutos sectoriales complejos; éstos últimos -como se ha dicho- serían aquéllos eventualmente inspirados en principios y normas internacionales sobre el tratamiento de datos. Dentro de la primera denominación, se comprende comúnmente a la legislación que establece el secreto y la reserva bancaria y financiera, el secreto y la reserva tributaria o fiscal y variados deberes de cargo que implican la confidencialidad de cierta información personal. En la denominación de estatutos sectoriales complejos, se comprende la regulación al tratamiento de los datos crediticios o de solvencia patrimonial y, excepcionalmente, una normativa sobre mensajería de datos. Estos cuerpos legales están presentes en los siguientes países: a) México (Ley para regular las Sociedades de Información Crediticia), b) Panamá (Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores o Clientes), y c) Perú (Ley que regula las

Centrales Privadas de Información de Riesgos y de Protección al Titular de la Información). En los casos de Argentina, Chile y Paraguay, si bien no existen este tipo de estatutos sectoriales, las leyes de protección de datos contienen normas específicas en esta materia. Cabe agregar que, como un estatuto sectorial complejo extravagante que establece normas de protección de datos pero de manera adjetiva al fin principal de la regulación, encontramos a la ley ecuatoriana de comercio electrónico, firmas y mensajes de datos, la cual recoge algunos principios generales de protección de datos y establece delitos vinculados al respecto de aquéllos. En los restantes sistemas jurídicos estudiados, sólo se observan estatutos sectoriales simples (secreto bancario y tributario) y de legislación común; éstos últimos reducidos fundamentalmente a las reglas generales de responsabilidad administrativa y civil, dado que en materia penal no se ve factible predicar una tutela directa a los datos personales, dado el principio general del Derecho Penal que sostiene la inexistencia de crimen y pena sin ley (*nullum crimen, nulla poena sine lege; praevia, scripta, srtricta, certa*).

Si bien se ha podido constatar a nivel infraconstitucional la existencia de diversas formas jurídicas de abordar la protección a los datos personales, tanto a través de estatutos especiales (leyes de protección de datos), estatutos sectoriales complejos (leyes sectoriales eventualmente influenciadas por las normas y principios internacionales de protección de datos) como por medio de estatutos simplemente sectoriales, la presencia de éstos en un mismo ordenamiento jurídico, por lo general, no es exclusiva, sino por el contrario la regla es que esos estatutos coexistan y se complementen. Así, por ejemplo, en el caso de Argentina, Chile y Paraguay, sus leyes de protección de datos conviven junto con estatutos sectoriales no abarcados por esas normativas. Sin embargo, la situación de coexistencia no se da entre las leyes generales de protección de datos (Ley 25.326, para Argentina; Ley 19.628 para Chile y, Ley 1.682 para Paraguay) y los estatutos sectoriales complejos, como por ejemplo, aquéllos que regulan el tratamiento de datos de carácter económico, de solvencia patrimonial o de cumplimiento de obligaciones, pues las respectivas normativas especiales se encargan de regular ese ámbito, es decir, las incluyen. Por el contrario, en el caso de los ordenamientos jurídicos que no disponen de leyes generales de protección de datos pero que sí cuentan con leyes sectoriales complejas, éstas coexisten con otros estatutos sectoriales. Tal es el caso de: a) Ecuador (Ley de Comercio Electrónico, Firmas y Mensajes de Datos), b) México (Ley para regular las Sociedades de Información Crediticia), c) Panamá (Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores o Clientes), y d) Perú (Ley que regula las Centrales Privadas de Información de Riesgos). Por último, cabe destacar que la legislación común presente en cada sistema jurídico, sea ella de carácter civil o administrativa, en general aparece como apta para hacer valer la responsabilidad respectiva ante ataques a los derechos de los titulares, aunque no exista norma constitucional ni ley que reconozca el hábeas data o derecho a la protección de datos, pues en última instancia, la fundamentación de la tutela de las personas en lo relativo a la esfera de control sobre sus propios datos podría derivarse de los derechos a la intimidad, vida privada e incluso el honor. No podemos decir lo mismo respecto de la legislación común penal, pues la aplicación de ella se ve limitada -como se ha dicho- por el principio de la legalidad.

En materia de bienes jurídicos tutelados por las normas de protección de datos, pudimos constatar que en los sistemas jurídicos latinoamericanos que disponen de normas constitucionales y/o leyes de protección de datos personales, tanto en base a lo señalado por la doctrina como por alguna jurisprudencia, se desprende que el derecho a la intimidad sería el centro de gravedad del derecho a la protección de datos, a partir del cual, se derivarían o agregarían otros bienes jurídicos. Ello ocurre en los ordenamientos de: Argentina, Brasil, Chile, Colombia, Paraguay, Perú y Venezuela. En aquellos países en los cuales no hemos encontrado doctrina o jurisprudencia que se pronuncie sobre la materia, concluimos, no obstante, que también estaría el derecho a la intimidad presente como bien jurídico tutelado por las normas de protección de datos en Guatemala, México, Nicaragua y Panamá.

En lo que respecta al derecho a la vida privada o privacidad como bien jurídico protegido, la doctrina regional sólo lo menciona respecto de los ordenamientos de Argentina y Chile. Nosotros, a falta de opiniones doctrinales y jurisprudenciales, hemos estimado que este derecho también estaría presente en los sistemas jurídicos de Guatemala, México, Nicaragua y Panamá.

Dentro de los bienes jurídicos más estrechamente ligados al derecho a la protección de datos, el derecho a la autodeterminación informativa aparece doctrinariamente como uno de los más importantes. Sin embargo, la discusión en torno a su independencia o dependencia de otros derechos como la intimidad, aún está pendiente y no existe un consenso al respecto. Lo anterior probablemente ha repercutido en la configuración de los textos autoritativos latinoamericanos, en los cuales ninguna alusión expresa se hace a ese derecho, ni siquiera en los ordenamientos que cuentan con disposiciones constitucionales de hábeas data. En el caso de Chile, ocurrió una situación que pudo cambiar la conclusión anterior, pues el legislador patrio tuvo la oportunidad de reconocer expresamente el derecho a la autodeterminación informativa al tramitarse la Ley 19.628. Sin embargo, dicha propuesta fue criticada y en definitiva desechada debido a la posición del gobierno de turno, el cual no estaba dispuesto a dar el paso completo en la materia, cuestión que creemos habría sido de gran importancia para una sólida construcción dogmática del derecho a la protección de datos no sólo en Chile sino que en toda Latinoamérica.

A pesar de todo lo anterior, alguna doctrina ha señalado este derecho como uno de los bienes jurídicos protegidos por las normas constitucionales de los ordenamientos jurídicos de Argentina (Puccinelli), Brasil (Morales), Chile (Nogueira) y Venezuela (Álvarez). En el caso de Colombia, destaca el hecho que haya sido la jurisprudencia de la Corte Constitucional la que señalara que el núcleo fundamental del hábeas data estriba en la defensa de la autodeterminación informativa. Por nuestra parte, hemos estimado que este derecho eventualmente estaría reconocido en los sistemas jurídicos de Perú y Paraguay.

Han sido señalados también por la doctrina latinoamericana como bienes jurídicos tutelados por las normas de protección de datos: 1) El derecho al honor, en Argentina, Chile, Colombia, Ecuador y Venezuela; 2) El derecho a la imagen, en Argentina, Chile, Colombia, Ecuador y Paraguay; 3) El derecho a la identidad, en los sistemas jurídicos de Argentina y Ecuador; 4) El derecho a la dignidad, en Paraguay y Venezuela; 5) El

derecho a la reputación, en Ecuador y Venezuela; 6) La integridad psicofísica en Argentina, y 7) La libertad y seguridad de las personas, la inviolabilidad del patrimonio documental y el derecho a la libre expresión de la personalidad en Paraguay.

Estimamos que no es posible centrar la protección a los datos personales en Latinoamérica en un solo bien jurídico, sino más bien en un conjunto de ellos, los cuales confluyen. En lo relativo al derecho a la autodeterminación informativa, aún falta una concreción positiva de éste. Su eventual reconocimiento obviamente dependerá de los legisladores respectivos, sin embargo, podemos aventurar una mayor o menor dificultad en ese cometido fundamentalmente en atención al estado de las respectivas constituciones de cada ordenamiento jurídico. Así, por ejemplo, en el caso de Argentina, la tarea podría verse dificultada, dado el carácter restrictivo del texto constitucional trasandino, el cual excluye del hábeas data a los bancos de datos privados que no estén destinados a proveer informes, es decir, aquéllos de carácter privado de uso personal (Art. 43 inc. 3º C. Pol); en Chile, mientras no se modifique la Constitución, más dificultosa se torna la posibilidad de incorporar el derecho a la autodeterminación informativa, dada la expresa negativa del legislador a reconocer este derecho en la Ley 19.628. En el caso de Brasil, también se aprecia una limitación similar a la vista en Argentina, dada la estrechez de texto constitucional. Por el contrario, vemos favorecida la posibilidad de reconocimiento de tal derecho, en Colombia, Ecuador, Perú, y Venezuela, pues sus respectivas constituciones son lo bastante amplias como para permitir un desarrollo del derecho, particularmente en este último país, que además de reconocer la garantía del hábeas data, establece limitaciones a la utilización de la informática, de idéntica forma a la señalada en la Constitución española de 1978.

Se ha evidenciado por otra parte, la existencia de ciertas leyes de protección de datos -sean éstas generales, sectoriales complejas o sectoriales simples- en las cuales es posible encontrar menciones más o menos expresas a alguno o algunos de los principios internacionales sobre el tratamiento de datos personales. Sin embargo, del análisis particular de los estatutos que recogen en mayor o menor medida esos principios, se desprende que no existe homogeneidad en el reconocimiento de ellos. Más aún, la extensión y el desarrollo varía en cada sistema jurídico, dándose situaciones paradojales, como por ejemplo, que los principios del consentimiento para el tratamiento y para la cesión de datos, pasen a constituirse en la práctica como la regla excepcional, perdiendo en definitiva toda la fuerza que ellos podrían imprimirle a las respectivas regulaciones. La situación anterior, a nuestro juicio, no parece tan grave en aquellos ordenamientos jurídicos que sólo disponen de leyes sectoriales complejas circunscritas a la regulación del tratamiento de los datos comerciales, económicos o de situación patrimonial, pues esa información comúnmente es tratada con menos apego a los principios señalados, dado el interés social por incentivar ciertas actividades económicas, como el mercado crediticio, el comercio, y por reducir los costos de transacción. No puede decirse lo mismo respecto de las leyes de protección de datos, que por su naturaleza están llamadas a regular la materia de un modo general, abarcando la mayor cantidad de áreas temáticas posibles.

De los tres estatutos más o menos generales de protección de datos existentes en la región en materia de principios, destaca nuevamente la Ley argentina, la cual contempla

con mayor claridad y fuerza los principios de licitud y lealtad de los archivos, calidad de los datos, seguridad, confidencialidad y finalidad. Sin embargo, ello no ocurre con los principios del consentimiento informado del titular tanto para el tratamiento de datos como para la cesión, los cuales aparecen en la práctica más bien como la regla excepcional, perdiendo en definitiva su fuerza, dada la cantidad de excepciones previstas por la regulación legal. Esta misma situación es constatable en Chile, donde ambos principios si bien aparecen reconocidos más débilmente que en la ley argentina, también han sido prácticamente vaciados de contenido, pues los casos en que se aplican pasan a constituir la regla de excepción según se pudo constatar del análisis de la Ley 19.628. Agrava la situación chilena, el hecho de reconocerse el principio de la finalidad de forma vaga y poco precisa, perdiéndose el sentido que este principio debería impregnarle a la legislación. Si a lo anterior le sumamos la inexistencia de un deber de inscripción de los bancos de datos privados, la falta de sanción para aquellos responsables de bancos de datos públicos que no los inscriban en tiempo y forma y, la inexistencia de un órgano de control, tenemos un escenario muy poco favorable en Chile para la protección efectiva de los derechos de las personas ante el tratamiento de sus datos personales. En el caso del Paraguay, los principios son menos visibles, pues se regula asimétricamente el tratamiento de los datos y los derechos de los titulares, dedicándose mayoritariamente a los datos comerciales, económicos o de solvencia patrimonial. En este ordenamiento aparecen muy débiles los principios de licitud de los archivos, consentimiento del titular para el tratamiento y cesión de datos, seguridad y finalidad, constatándose por último la inexistencia del principio de la confidencialidad. Con todo, si bien el Paraguay no dispone de una legislación sistemática y completa, el texto constitucional permitiría, sin duda, mejorarla sustancialmente. En tanto ello no ocurra, algunos de los principios que aparecen débilmente reconocidos podrían ser suplidos por una labor interpretativa a la luz de la Constitución.

En lo que respecta a los estatutos sectoriales complejos o más desarrollados en materia de protección de datos, también se visualizan en general los principios internacionales sobre el tratamiento de datos personales, circunscritos a los datos de carácter comercial, económico o de solvencia patrimonial, es decir, aquéllos contemplados en leyes que regulan el tratamiento de la información crediticia junto con los derechos de los titulares. Es así como los estatutos sectoriales complejos de México (Ley para regular las Sociedades de Información Crediticia), Panamá (Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores) y Perú (Ley que regula las Centrales Privadas de Información de Riesgos), contienen los siete principios estudiados, cada uno con matices y alcances propios. Entre ellos destaca la ley panameña, la cual reconoce expresamente los principios de calidad de los datos, seguridad y confidencialidad o reserva de información sobre el historial de crédito de los consumidores, y además señala como derechos de éstos: el buen manejo de la información (finalidad), el consentimiento del titular para la recopilación y transmisión de datos y la fidelidad de la información (calidad de los datos).

Dentro de unos pocos estatutos sectoriales latinoamericanos, también es posible visualizar en mayor o menor medida algunos principios en materia de tratamiento de datos personales. En efecto, ley brasileña de protección a los consumidores, reconoce en

cierta medida el principio de la licitud de los archivos y el de la finalidad (Art. 43, parágrafos 1º y 2º). Por otra parte, en Ecuador la Ley de Comercio Electrónico, Firmas y Mensajes de Datos reconoce, en mayor o menor grado, los principios de licitud y lealtad de los archivos, el consentimiento para el tratamiento y cesión de datos, confidencialidad y la finalidad. Destaca además de esta normativa, la protección brindada en sede penal al principio del consentimiento para el tratamiento y cesión de los datos, cuya violación en ciertas circunstancias es constitutiva de delito penal (Art. 58). Finalmente, debemos señalar que en este mismo ordenamiento jurídico, se visualiza indirectamente el principio de la licitud de los archivos, seguridad de los datos y finalidad, en algunas disposiciones de la Ley de Control Constitucional que regula la acción de hábeas data (Art. 39).

Los resultados obtenidos en relación al estudio de los derechos reconocidos a los titulares de los datos personales, en general no difieren mucho de la hipótesis de nuestra investigación, es decir, hemos confirmado que en esta materia también existen diversos niveles de desarrollo normativo, cuyo rango mínimo está dado por aquellos ordenamientos jurídicos que no disponen de normas que reconozcan derechos a los titulares de los datos; el rango máximo está dado por aquéllos que sí lo hacen. Dentro de estos últimos, se presentan las mayores diferencias pues la extensión de los derechos reconocidos también es variable.

Los sistemas jurídicos que reconocen ciertos derechos a los titulares de los datos personales lo hacen de diversa forma y en distintos niveles normativos; algunos sistemas sólo los prevén a nivel constitucional sin mediar ley especial que regule el ejercicio de esos derechos, como ocurre en Colombia, Guatemala, Nicaragua y Venezuela. Otros, más consecuentes, además de establecer reglas constitucionales que los reconozcan, disponen de normas legales que los desarrollan sustantivamente y regulan procesalmente, situación que se presenta en la Argentina de manera extendida y débilmente en el Paraguay, a consecuencia de la estrechez normativa de la Ley 1.682 que regula la información privada. Existen también ordenamientos que junto con las normas constitucionales, disponen de leyes que regulan procesalmente el ejercicio de los derechos reconocidos disponiendo además de algunos estatutos sectoriales que regulan el ejercicio de ciertos derechos, como es el caso de Brasil, Ecuador y Perú. Por último, también se constatan sistemas jurídicos que sólo reconocen derechos a los titulares de los datos a nivel legal, sea a través de leyes generales de protección de datos, de estatutos sectoriales complejos o de estatutos sectoriales simples. En esta categoría sólo se ubican dos países: Chile y México. El primero, a través de una ley general de protección de datos, y el segundo, por la vía de un estatuto sectorial simple y otro complejo.

Se han apreciado también, diferencias en cuanto a la extensión de los derechos reconocidos a los titulares de los datos. El panorama latinoamericano es el siguiente: 1) En Argentina, se reconocen al titular de los datos los derechos de acceso, rectificación o modificación, cancelación o supresión, bloqueo y confidencialidad, los cuales sólo se pueden ejercer en contra de los responsables de archivos, registros o bancos de datos públicos y de los privados destinados a proveer informes; primero, de manera informal o administrativa ante el responsable del archivo y, agotada esa vía, a través de la acción de protección de datos o hábeas data ; 2) En Brasil, en cambio, solamente se reconocen los

derechos de acceso e información y rectificación de datos, los cuales únicamente pueden ejercerse ante los responsables de registros o bancos de datos de entidades gubernamentales o de carácter público; primeramente a través de la vía administrativa y agotada ésta, a través de la acción de hábeas data. En materia de derechos del consumidor, la ley brasileña respectiva también reconoce los derechos de acceso e información y el derecho de corrección inmediata de los datos personales inexactos, los cuales deben ejercerse informal o extrajudicialmente ante el encargado del archivo o banco de datos que preste servicios de información de crédito. Estos archivos son considerados por la Ley de Protección al Consumidor como entidades de carácter público, con la finalidad de hacer aplicables las normas que regulan el hábeas data constitucional a esos bancos de datos, los cuales sin esa corrección legal, en principio quedarían excluidos como sujetos pasivos de la acción de hábeas data; 3) En Chile, se reconocen a nivel legal los derechos de acceso e información, modificación, cancelación, y bloqueo de datos, los cuales deben ser ejercidos por el titular, primeramente, de manera directa ante el responsable del registro o banco de datos y, agotada esa vía administrativa o extrajudicial, judicialmente a través de la acción de amparo a los derechos del titular de los datos; 4) En Colombia, sólo se reconocen a nivel constitucional los derechos de acceso e información, rectificación o modificación y actualización de datos, sin prever una acción específica que haga efectiva la garantía del hábeas data. A falta de ella, la vía utilizada ha sido la acción de tutela; 5) En el caso del Ecuador, se reconocen a nivel constitucional los derechos de acceso e información, rectificación, eliminación o anulación de datos, regulándose procesalmente éstos a nivel legal por la Ley de Control Constitucional; 6) En Guatemala, sólo se reconocen a nivel constitucional los derechos de acceso e información, corrección, rectificación y actualización, respecto de los responsables de los archivos estatales, no encontrándose regulado el ejercicio de ellos por ley general ni especial; 7) En el caso de México, los derechos que se reconocen a los titulares se circunscriben sectorialmente a la Ley para regular las Sociedades de Información Crediticia. Por lo tanto, el carácter de titular sólo es predicable respecto de los clientes de las entidades financieras y de las empresas comerciales a quienes se les reconocen los derechos de acceso e información, rectificación, cancelación. El ejercicio de éstos es de carácter extrajudicial. Junto con la normativa anterior, ahora en materia de protección a los consumidores, el estatuto respectivo mexicano reconoce los derechos de acceso e información y rectificación o corrección de datos, los cuales se ejercen extrajudicialmente ante el órgano de control pertinente, respecto de las empresas dedicadas a la investigación de crédito o a la recopilación de información sobre consumidores con fines de mercadotecnia o marketing; 8) En Nicaragua, sólo se reconoce a nivel constitucional el derecho de acceso a la información registrada por las autoridades estatales; 9) En Panamá, en virtud de la Ley que regula el Servicio de Información de Historial de Crédito de los Consumidores, se reconocen los derechos de acceso e información, rectificación, eliminación y actualización de los datos de los consumidores o clientes. Estos derechos deben ser ejercidos directamente ante el agente económico o ante la Comisión de Libre Competencia y Asuntos del Consumidor. Además de este estatuto sectorial complejo, la Ley de Transparencia en la Gestión Pública reconoce el derecho de acceso e información, corrección y eliminación de datos personales contenidos en archivos, registros o expedientes que mantengan las

instituciones del Estado, los cuales deben ser previamente reclamados administrativamente. Agotada esa instancia, se abre la posibilidad de entablar la acción de hábeas data ante los Tribunales Superiores de Justicia; 10) En Paraguay, la Constitución reconoce los derechos de acceso e información, actualización, rectificación y destrucción de datos, que obren en registros oficiales o privados de carácter público, los cuales deberán ejercitarse ante el magistrado competente. En el plano legal, la Ley 1.682, defectuosamente regula lo preceptuado por el Constituyente, tratando diferenciadamente el derecho de acceso de los demás, sin señalar procedimiento judicial ni tribunal competente que deberá conocer de la acción de hábeas data; 11) En el Perú, se reconoce por el Constituyente sólo el derecho de acceso e información. A nivel legal, existen tres estatutos que desarrollan la estrecha configuración constitucional del hábeas data. El primero, regula transitoria y escuetamente el ejercicio de esa acción, aplicándose en su defecto la ley que regula el amparo constitucional. El segundo estatuto es la Ley de Transparencia y Acceso a la Información Pública, cuyo ámbito de aplicación se restringe al derecho de acceso, el cual previamente debe ejercerse administrativamente y agotada esa vía, a través de la acción de hábeas data. El último cuerpo legal peruano que reconoce ciertos derechos a los titulares de datos es la Ley que regula las Centrales Privadas de Información de Riesgos. Destaca de ella el reconocer los derechos de acceso e información, modificación, cancelación, rectificación y actualización (Art. 13) de manera enunciativa y no limitativa. El ejercicio de estos derechos es extrajudicial ante las CEPIRS y, 12) Venezuela reconoce a nivel constitucional los derechos de acceso, actualización, rectificación y destrucción de los datos que consten en registros oficiales o privados. El ejercicio de éstos a falta de regulación especial, según la doctrina y alguna jurisprudencia, ha quedado entregado en definitiva, al procedimiento de amparo en tanto no se dicte la ley al efecto.

Los modelos de tutela existentes en Latinoamérica en materia de datos personales, en cuanto a sus alcances son disímiles y la regulación de ellos tampoco es homogénea. Esos modelos están representados por dos tipos de acciones: a) Las de hábeas data o acciones de protección de datos (mecanismos específicos) para cuyo ejercicio, por regla general, se dispone de un procedimiento especial, y b) las acciones constitucionales de amparo, tutela o protección a los derechos y garantías constitucionales (mecanismos generales). Hemos estimado que éstas últimas, serían aplicables en aquellos ordenamientos jurídicos en que: 1) No existan disposiciones expresas de hábeas data; 2) Existiendo normas de protección de datos, no se señale la acción ni el procedimiento específico para hacer efectivos los derechos de los titulares; 3) El reconocimiento del hábeas data sea limitado o circunscrito a determinadas situaciones o ejercitable respecto de determinados sujetos pasivos y, 4) Excepcionalmente, en caso que la acción de hábeas data y su respectivo procedimiento, no garantice la oportuna y adecuada protección a los derechos de los titulares de datos. Con todo, existiría una tendencia a reconducir la tutela jurídica de los datos personales, a la acción de amparo o tutela, la cual en algunos casos resguardará el derecho a la protección de datos o hábeas data, y en otros, el derecho a la intimidad, vida privada, honor, o cualquier otro bien jurídico que permita fundamentar la defensa de las personas ante el tratamiento de sus datos personales.

Los ordenamientos jurídicos estudiados que disponen de acciones de hábeas data y que establecen al mismo tiempo un procedimiento específico para el ejercicio de ésta son: Argentina, Brasil, Chile, Ecuador, Panamá y Perú. Por otra parte, los sistemas jurídicos en que si bien se reconoce el derecho a la protección de datos o hábeas data, no se señala acción ni procedimiento que tutele el derecho son: Colombia, Guatemala, Nicaragua y Venezuela. En ellos, el procedimiento a seguir para no dejar indefensos a los titulares de datos, sería el amparo o tutela constitucional que supliría en parte tal deficiencia. También en el caso de los ordenamientos jurídicos que no reconocen un derecho a la protección de datos o hábeas data, la vía de protección a los derechos de los titulares, en defecto de norma especial, sería la acción de amparo o tutela, fundado en cualquiera de los derechos reconocidos generalmente como bienes jurídicos tutelados por el hábeas data, sea el derecho a la intimidad, la vida privada, el honor u otro de los ya señalados en materia de bienes jurídicos. Los países cuyos ordenamientos jurídicos se encuentran en tal situación son: Bolivia, Costa Rica, El Salvador, Honduras, México, Panamá y Uruguay. Con todo, las insuficiencias normativas en lo que respecta al reconocimiento de los derechos a la intimidad o a la vida privada, en definitiva, se suplirían aplicando el Pacto de San José de Costa Rica, el cual ha sido ratificado por todos los Estados ya mencionados.

Analizados los ordenamientos jurídicos latinoamericanos que disponen de leyes más o menos generales de protección de datos, concluimos que sólo Argentina posee mecanismos de control que se adecuan a las normas internacionales en materia de protección de datos; la Ley 25.326 establece la creación de un órgano de control, denominado Dirección Nacional de Protección de Datos Personales, cuyo deber es realizar todas las acciones necesarias para el cumplimiento de los objetivos y las disposiciones contenidas en la propia Ley. Por otra parte, se ha contemplado la existencia de mecanismos de control deontológicos, plasmados en los denominados códigos de conducta de práctica profesional, los cuales tienden a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos por el legislador. Más aún, la propia Ley le encomienda al órgano de control alentar la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones legales y reglamentarias.

Existen tres ordenamientos jurídicos en Latinoamérica, que dentro de sus estatutos legales referidos al funcionamiento de las empresas que prestan servicios de información de crédito de los consumidores, prevén la intervención de organismos administrativos encargados entre otras cosas, de velar por el cumplimiento de las disposiciones relativas a la protección de los derechos de los titulares de los datos. Hemos estimado que ellos actuarían como órganos de control, restringidos al ámbito de las respectivas leyes que les otorgan competencia. Así, en México, tanto la Ley para Regular las Sociedades de Información Crediticia como la Ley de Protección al Consumidor, prevén la creación de órganos encargados de velar por el cumplimiento de los respectivos estatutos jurídicos, facultándolos en algunos casos a aplicar sanciones administrativas y actuar como árbitros en la resolución de conflictos. En Panamá, la Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores, otorga competencia a dos órganos

administrativos que de manera conjunta cumplen un rol de órganos de control de la aplicación de la Ley. Finalmente, en Perú, la Ley para Regular las Sociedades de Información Crediticia otorga competencia a la Comisión de Protección al Consumidor, para conocer de las infracciones a la Ley e imponer tanto sanciones administrativas como medidas correctivas.

La regulación en Latinoamérica de la transmisión internacional de datos personales es escasa y se lleva a cabo principalmente de forma sectorial. El único ordenamiento jurídico que desarrolla el tema en una normativa de carácter general es el argentino, el cual establece como regla, la prohibición de la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados, sin perjuicio de las excepciones que la propia Ley señala, las que comúnmente se establecen en beneficio de la salud pública, la justicia, las operaciones financieras y la cooperación internacional para la prevención de ilícitos. En el caso de Chile, se ha planteado que la Ley 19.628 habría dejado entregado todo lo relativo a la regulación de la transmisión internacional de datos a los tratados y convenios internacionales. Ello se desprende tanto de la historia fidedigna del establecimiento de la Ley como de lo señalado por el inciso final del artículo 5º de la ley chilena. Por su parte, la Ley 1.682 del Paraguay no hace ninguna referencia al respecto. En suma, concluimos que la regla en Latinoamérica es la inexistencia de normativa general que se ocupe de la regulación de la transmisión internacional de los datos personales.

De los ordenamientos jurídicos estudiados que no cuentan con legislación especial de protección de datos, sólo algunos de ellos disponen de normas legales sectoriales en materia de transmisión internacional de datos. Esas normas están referidas, en general, a la transmisión internacional de información de carácter financiero y tributario, lo que al mismo tiempo se constituye en excepción al deber general de reserva o secreto de esa información, y cuya operatividad queda entregada, en definitiva, al criterio de las respectivas autoridades administrativas de control de la legislación sectorial. Los países en los cuales tal situación se presenta son: a) México (Ley de Instituciones de Crédito y Código Fiscal de la Federación), b) Nicaragua (Ley General de Bancos), c) Perú (Ley que crea la Unidad de Inteligencia Financiera), d) República Dominicana (Ley transitoria tributaria Nº 11 de 2001) y, e) Venezuela (Ley General de Bancos y Otras Instituciones Financieras).

El estudio relativo al eventual tratamiento diferenciado o indiferenciado del sector público y privado por las leyes generales de protección de datos en Latinoamérica, sólo pudo llevarse a cabo en los tres ordenamientos jurídicos que disponen de legislación especial en la materia, esto es, en Argentina, Chile y Paraguay. A través de ese examen, pudimos constatar múltiples diferencias en la reglamentación legal, según sea el Estado o los particulares quienes actúen en el tratamiento de los datos personales. De los análisis a los distintos puntos temáticos abordados, podemos señalar que: 1) En lo relativo al requisito del consentimiento para el tratamiento de datos, tanto las leyes de protección de datos argentina Nº 25.326 como la chilena Nº 19.628, y parcialmente la paraguaya Nº 1.682, contemplan una regulación diferenciada tanto para el sector público como privado en materia de excepciones a ese requisito. Esta misma situación se presenta en relación

al consentimiento para la transmisión o cesión de datos personales; 2) En cuanto a la regulación del tratamiento de los datos sensibles, tanto la ley argentina como la chilena establecen normas que privilegian al Estado, por cuanto se reservan la facultad de recolectar y tratar datos relativos a antecedentes penales o contravencionales, a través de sus autoridades públicas competentes. La legislación paraguaya no dispone normas como las anteriores. Por otra parte, la normativa aplicable al sector privado en Argentina faculta expresa y excepcionalmente a algunas organizaciones para recolectar ciertos datos. Tal es el caso de las instituciones religiosas, partidos políticos y organizaciones sindicales, que pueden llevar registros de sus miembros. En Chile, no se dispone de una regla como la anterior en materia de datos sensibles. Por último, en Paraguay existiría un tratamiento diferenciado respecto de los particulares, en virtud del cual éstos no tendrían impedimento legal para recolectar, almacenar y procesar datos sensibles, siempre que lo hagan para 'uso estrictamente privado'; 3) En lo concerniente a los derechos de los titulares de los datos, se observa en la ley argentina la existencia de tratamiento diferenciado, por cuanto la procedencia de la acción de hábeas data respecto de archivos privados está restringida a los responsables de archivos, registros o bancos de datos destinados a proporcionar informes. En cambio, la acción de hábeas data en contra de archivos, registros o bancos de datos públicos procede, en principio, sin restricciones salvas las excepciones legales. En Chile, la Ley 19.628 no establece diferencias de trato entre el sector público y el privado en la materia. En Paraguay, en lo relativo al derecho de acceso e información, la Ley 1.682 establece un trato diferenciado similar al existente en la Argentina, pues en relación al sector público el derecho opera ampliamente, a diferencia del sector privado donde se excluyen del hábeas data los responsables de los archivos de uso estrictamente privado. En cuanto al ejercicio de los derechos constitucionales de actualización, rectificación y destrucción de datos personales, éstos sólo aparecen regulados legalmente en Paraguay respecto de los datos sobre la situación patrimonial, solvencia económica y el cumplimiento de obligaciones comerciales; 4) En lo que respecta a las excepciones al ejercicio de los derechos de los titulares, la ley argentina 25.326 establece una regulación diferenciada, en virtud de la cual los organismos del Estado responsables o usuarios de bancos de datos públicos, pueden por decisión fundada denegar el acceso, rectificación o supresión de datos aduciendo -entre otras razones- la defensa de la nación y el orden público. Respecto de los particulares, el ejercicio de los derechos opera sin excepción. En Chile, también se establece un trato que beneficia los intereses del Estado, por cuanto no procede el ejercicio de los derechos de información, modificación, cancelación o bloqueo de datos cuando se impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras de los organismos públicos, se afecte la reserva o secreto establecido por ley o reglamento, entre otros casos. En el ámbito del sector privado, el ejercicio de los derechos de los titulares opera sin excepción. Por último, en la ley paraguaya, no se aprecian excepciones al ejercicio de los derechos de los titulares, por lo que no existiría un tratamiento diferenciado entre el sector público y el privado; 5) En lo que se relaciona con la creación y registro de los archivos y bancos de datos personales, la ley argentina de protección de datos señala ciertas diferencias en el tratamiento del sector público y del sector privado. Así, las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos, deben hacerse por medio de disposición

general publicada en el Boletín Oficial de la Nación. Los particulares que formen archivos, registros o bancos de datos para fines distintos del uso exclusivamente personal, deben inscribirse -al igual que los bancos de datos públicos- en el Registro que para tal efecto lleva la Dirección Nacional de Protección Datos. La ley chilena, por su parte, dispone que el tratamiento de datos personales por los organismos públicos solamente puede efectuarse respecto de las materias de su competencia y con sujeción a las normas de la Ley 19.628, cuyos bancos de datos deben ser inscritos en el registro a cargo del Servicio de Registro Civil e Identificación, el cual tiene carácter público. En relación a los particulares, no existe deber alguno de inscribir sus bancos de datos personales, ni tampoco en la práctica podría hacerse, pues la Ley sólo reguló la inscripción de los registros o bancos de datos públicos. Por último, en el caso paraguayo, cabe señalar que la respectiva ley no regula la materia; 6) En lo referente a los archivos o bancos de datos relativos a encuestas, debemos señalar que la ley argentina no es aplicable a las encuestas de opinión, mediciones y estadísticas, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable. Al sector público, en lo relativo a las mediciones y estadísticas realizadas a través del censo nacional, tampoco se le aplica la Ley 25.326. La Ley chilena por su parte, no diferencia ámbito objetivo de aplicación, respecto de los archivos, registros o bancos de datos relativos a encuestas, por lo que la regla se aplicaría tanto al sector público como privado. La misma situación anterior se constata en la legislación paraguaya; 7) En cuanto al tipo de tratamiento de datos, la ley argentina incluye expresamente tanto al automatizado como al manual, sin establecer diferencias entre el sector público y el privado. En la ley chilena se llega a la misma conclusión, pero a través de las definiciones legales del tratamiento de datos y del registro o banco de datos. Por su parte, la ley paraguaya tampoco es tan clara como la argentina, asemejándose más a la chilena. Con todo, concluimos que el ámbito de aplicación de la ley alcanza tanto al tratamiento manual como automatizado de datos, lo cual se desprende del objeto de la Ley; 8) En lo que atañe al reconocimiento o no de las personas jurídicas como titulares de datos, se constata que la regulación legal de este punto no es uniforme. En argentina, expresamente reconocen como titulares de los derechos consagrados en la Ley a las personas jurídicas, sin distinguir entre las de derecho público y las de derecho privado. La ley chilena en cambio, sólo reconoce como titulares de datos personales a las personas naturales o físicas. Por último, la ley paraguaya no se pronuncia expresamente en la materia y sólo habla de toda persona, por lo que no cabría hablar de trato diferenciado y, 9) En materia de transmisión o transferencia internacional de datos personales, la ley argentina establece un regulación diferenciada para algunos organismos del Estado, a los cuales faculta para transmitir datos personales fuera del territorio argentino. La ley chilena por su parte no ha regulado la materia y la ley paraguaya 1.682 no hace ninguna referencia al tema.

El último punto de análisis realizado por este estudio, abarcó el régimen de responsabilidad adoptado por los diversos ordenamientos jurídicos latinoamericanos en materia de protección a los datos personales. Para tal efecto, agrupamos en cuatro tipos la legislación existente en materia de responsabilidad administrativa, civil y penal, diferenciando en cada una de ellas, legislación especial, sectorial compleja, sectorial y

común.

De los ordenamientos jurídicos comprendidos en esta investigación, que disponen de estatutos especiales o leyes generales de protección de datos que prevean además normas especiales de responsabilidad podemos señalar que: 1) El sistema argentino aparece como el más desarrollado en la materia, estableciendo una regla especial en materia de responsabilidad civil junto con prever sanciones administrativas y penales para quienes infrinjan las disposiciones de la Ley 25.326; 2) La ley chilena de protección de datos ha establecido sólo sanciones -al parecer de carácter administrativo- para determinadas infracciones a la Ley, así como también en materia civil ha reconocido expresamente la procedencia de la indemnización del daño moral a causa del tratamiento indebido de los datos personales. Destaca además, que se hayan introducido disposiciones que amplían el ámbito de la responsabilidad administrativa. Así, en el Código Sanitario se estableció expresamente el carácter reservado de las recetas médicas y los análisis o exámenes de salud. Luego, la Ley 19.812, en el año 2002, instituyó una regla en el Código del Trabajo de no discriminación en la contratación de los trabajadores basada en sus antecedentes comerciales, cuya violación genera responsabilidad; 3) La ley paraguaya que reglamenta la información privada, contempla ciertas sanciones -al parecer de carácter administrativo-, algunas de aplicación exclusiva a quienes realicen tratamiento de información sobre la situación patrimonial, solvencia económica o cumplimiento de obligaciones comerciales y financieras de las personas, y otras de aplicación general circunscritas a la denegación o retardo de la entrega de información ante el ejercicio extrajudicial del derecho de acceso; 4) La ley ecuatoriana de Control Constitucional que regula el ejercicio de la acción constitucional del hábeas data, establece sanciones -al parecer de carácter administrativo- para quienes incumplieren las resoluciones expedidas por los jueces o Tribunales que concedan el hábeas data; 5) En Panamá, la Ley de Transparencia en la Gestión Pública prevé normas de responsabilidad administrativa y civil, referidas al ejercicio del hábeas data respecto de los archivos o registros públicos y, 6) En el ordenamiento jurídico peruano, laLey de Transparencia y Acceso a la Información Pública, que regula el ejercicio del hábeas data respecto de archivos públicos, sanciona a los funcionarios o servidores públicos que incumplan con las disposiciones de esta Ley.

En lo referente a los estatutos sectoriales complejos latinoamericanos que establecen normas de protección de datos personales y prevén además reglas de responsabilidad, podemos señalar que: 1) En Ecuador, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos sólo tipifica algunos delitos penales que atentan en contra de los derechos de los titulares de datos personales que hayan sidoenviados, recibidos, comunicados o archivados por medios electrónicos, de los cuales destaca el delito que sanciona a quien obtuviere información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular; 2) En México, la Ley que regula las Sociedades de Información Crediticia establece normas de responsabilidad civil y prevé además sanciones administrativas para quienes infrinjan sus disposiciones. Llama la atención que aquéllas disposiciones limiten la procedencia de la responsabilidad civil a la sola existencia de daño por culpa grave, dolo o mala fe en el manejo de la base de datos, lo cual nos parece extremadamente negativo, pues pone de

cargo de los titulares de los datos los riesgos de una actividad potencialmente dañosa, sin justificación jurídica ni económica de peso; 3) En Panamá, la Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores establece un catálogo de conductas constitutivas de infracción a la Ley, las cuales se sancionan administrativamente y, 4) La ley peruana que regula las Centrales Privadas de Información de Riesgos, establece reglas de responsabilidad administrativa y civil. Respecto de las primeras, lo hace a través de un catálogo de conductas constitutivas de infracciones, de las cuales se responde estricta u objetivamente. Junto con ellas, se prevé la aplicación de medidas correctivas cuyo fin es revertir los efectos que las conductas infractoras hubieran ocasionado o evitar que éstas se produzcan nuevamente en el futuro. En materia de responsabilidad civil, la ley peruana establece un régimen de responsabilidad estricta u objetiva que afecta a las Centrales de Información Privada, en cambio, respecto de los usuarios y receptores de los reportes de crédito, el régimen de responsabilidad establecido por la ley es por culpa o negligencia.

Los estatutos legales de carácter sectorial, que constituyen la regla general latinoamericana en materia de protección de datos personales, establecen principalmente reglas de responsabilidad administrativa y penal, destacando las normas de las leyes de bancos e instituciones financieras que sancionan la violación a la reserva y/o el secreto bancario, y las normas tributarias que sancionan la violación del secreto o reserva fiscal. Así, en materia de secreto y/o reserva bancaria, se constató que disponen de normas de responsabilidad, a lo menos, los siguientes ordenamientos jurídicos: Argentina, Bolivia, Brasil, Chile, Ecuador, El Salvador, Guatemala, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Paraguay y Venezuela. Por otra parte, se verificó también que los sistemas jurídicos que disponen de reglas de responsabilidad vinculadas al secreto fiscal o tributario en Latinoamérica son, en principio: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, México, Paraguay, Perú, República Dominicana, Uruguay y Venezuela.

En otros estatutos legales latinoamericanos, ahora referidos a la protección de los consumidores, hemos constatado igualmente la existencia de normas de responsabilidad en relación al tratamiento de datos personales, estableciéndose en ellos sanciones administrativas. Estos estatutos son: la Ley de Protección al Consumidor del Brasil y la Ley Federal de Protección al Consumidor mexicana. Además de ellos, hemos constatado la presencia de estatutos sectoriales que regulan otras áreas del derecho, los cuales comúnmente se limitan a sancionar la violación de deberes funcionarios de confidencialidad o reserva, relativos a determinada información personal. Estos estatutos son: 1) La ley argentina sobre sistema de tarjetas de crédito, compra y débito; 2) La ley brasileña de protección del niño y del adolescente; 3) La ley mexicana de protección y defensa al usuario de servicios financieros, y 4) El código dominicano para la protección de niños, niñas y adolescentes. Por último, se ha verificado también la existencia de normas penales que sancionan conductas que atentan en contra de los bienes jurídicos intimidad y vida privada, distintos a los delitos de violación del secreto bancario y tributario. Sin embargo, la aplicación de estas normas relativas a la protección de datos personales se vería dificultada, en atención a la restricción impuesta por el principio de legalidad en materia penal. Los países en lo cuales se dispone de tales normas son:

Chile (Ley Nº 19.223), México (Ley de Imprenta), República Dominicana (Ley sobre Expresión y Difusión del Pensamiento) y, Venezuela (Ley Especial Contra los Delitos Informáticos, Ley sobre Protección a la Privacidad de las Comunicaciones y Ley de Registro de Antecedentes Penales).

Hemos concluido por otra parte, que las reglas generales de la responsabilidad administrativa y civil, serían susceptibles de ser aplicadas supletoriamente, a falta de leyes especiales o sectoriales que establezcan normas de responsabilidad por violaciones a los derechos de los titulares de los datos. No ocurre lo mismo respecto de la legislación penal común que tutela el derecho a la intimidad y la vida privada de ataques específicos, como la violación de domicilio, violación de correspondencia o la violación de secretos, pues ella no ha sido establecida para los casos de violación a los derechos de los titulares de los datos. Sin perjuicio de ello, destacan algunos tipos penales específicos que tutelan: la intimidad en Chile (Art. 161 A C. Penal) y Paraguay (Art.143 C. Penal); la inviolabilidad de las comunicaciones electrónicas en Costa Rica (Art. 196 bis C. Penal) y El Salvador (Art. 186 C. Penal), y la intimidad, protegiendo los archivos computarizados en Perú (Art. 157 C. Penal).

En definitiva, del análisis comparativo de los diecinueve ordenamientos jurídicos latinoamericanos abarcados por este estudio, se concluye que el nivel de desarrollo normativo en materia de protección de datos personales a nivel latinoamericano es diverso, tanto en el contenido como en la forma y extensión de la regulación, constatándose en general, una ausencia de leyes generales de protección de datos que recojan los principios internacionales en la materia. Constituyen una excepción a lo recién señalado, las leyes de Argentina y Chile sobre protección de datos, junto con la híbrida ley paraguaya que regula la información privada. Asimismo, se ha evidenciado en tres ordenamientos jurídicos la existencia de una regulación sectorial acerca del tratamiento de la información crediticia, que sorprende positivamente, pues todos ellos recogen algunos de los principios internacionales sobre el tratamiento de datos. Si bien estos estatutos no son de aplicación general, estimamos que los principios que se han reconocido en éstos podrían ser utilizados para solucionar aquellos casos aún no legislados. La tarea se vería facilitada al menos en el Perú, país que cuenta con normas constitucionales expresas de hábeas data, pero no así de una ley general en la materia. Las demás leyes sectoriales, que se circunscriben a establecer deberes de secreto o reserva de determinada clase de información, como la bancaria y tributaria, pasan a ser la regla general en Latinoamérica, no obstante los diversos alcances que éstas poseen. Por último, la legislación común aparece eventualmente como apta para perseguir las responsabilidades civiles y administrativas por violación a los derechos de las personas en materia de datos personales. En cuanto a las normas penales, no puede señalarse lo mismo, dada la restricción impuesta por el principio de la legalidad, pilar básico del Derecho Penal.

Estimamos que sería conveniente incentivar en Latinoamérica la dictación de legislaciones fundadas en estándares internacionales de protección de datos, particularmente en aquéllos señalados por la Directiva 95/46 CE. Lo anterior podría verse potenciado con la incorporación de una normativa de derecho internacional regional que estableciera el marco mínimo de regulación que debe implementar cada país signatario,

en miras a la adecuada tutela de los derechos de las personas ante el tratamiento de sus datos personales, y que permitiera, al mismo tiempo, el desarrollo de la sociedad de la información con pleno respeto a los derechos humanos. Antes de ello, creemos sería beneficioso, poder desarrollar con más fuerza el denominado derecho a la autodeterminación informativa y lograr eventualmente su reconocimiento como derecho fundamental, lo cual le daría autonomía y propia fuerza, con la consecuencial ventaja de poder implementar mecanismos de tutela especiales que superen al clásico proceso constitucional de amparo, tutela o protección, pues -como se ha visto- éste no logra comprender adecuadamente las particularidades que se derivan de la naturaleza del derecho a la autodeterminación informativa, entendido éste como la facultad de control de la utilización de la propia información.

Finalmente, cabe señalar que en la presente investigación no han sido abordados diversos aspectos en materia de protección de datos, los cuales, sin duda, convendría desarrollar en futuros trabajos. Entre ellos queremos destacar los siguientes: 1) Analizar con mayor detenimiento la jurisprudencia constitucional a nivel latinoamericano en materia de hábeas data, con el fin de poder dar una respuesta más exacta en lo que respecta a los bienes jurídicos protegidos en cada ordenamiento jurídico; 2) Estudiar el grado de influencia de los principios internacionales de protección de datos en las distintas legislaciones latinoamericanas; 3) Analizar las fuentes materiales de los textos constitucionales latinoamericanos que reconocen la garantía de hábeas data que logren explicar el porqué de las limitaciones que en ellos se establecen; 4) Examinar la idoneidad de la normativa actual de protección de datos para enfrentar el desarrollo de la Internet, y 5) Por último, estudiar la legislación penal y su eventual aplicación en materia de datos personales, lo cual pasa por responder al menos la pregunta sobre la conveniencia o inconveniencia de que el Estado utilice el *ius puniendi* para tutelar a las personas en su ámbito de autonomía de control de su propia información. Ello podría llevar también a explorar la factibilidad de fortalecer el sistema de responsabilidad civil y administrativa, y respecto de la responsabilidad civil, discutir además la pertinencia de optar por un régimen de responsabilidad por culpa, o por uno de responsabilidad estricta u objetiva.

En Santiago de Chile, a 21 días del mes de Julio de 2003.

BIBLIOGRAFÍA

Textos, Libros, Revistas, Referencias de Internet

Álvarez B. de Bozo, Miriam "et al": *"La Libertad Informática: Derecho Fundamental en la Constitución Venezolana"*,[en línea] < http://ulpiano.com/Recusos_habeasData_venezuela1999.htm > [consulta: 21 de Noviembre 2002].

Barros Bourie, Enrique: *"Curso de Derecho de Obligaciones. Responsabilidad civil Extracontractual".* Apuntes preparados con la participación de los ayudantes Eduardo Ugarte D. y Alejandro Vícari V., Universidad de Chile, Facultad de derecho, 2001.

Basterra, Marcela: *"Los Derechos Tutelados por el hábeas data: doctrina y jurisprudencia, en La defensa de la intimidad y de los datos personales a través del hábeas data"*, Gozaíni, Alfredo, Coord., Ediar, Bs. As., 2001.

Benítez, Luis María: *"La Acción de Hábeas Data en el Derecho Paraguayo"*, Revista Ius et Praxis, Universidad de Talca, Año 3 Nº 1, Talca, 1997.

Carranza Torres, Luis: *"Hábeas data. La protección jurídica de los datos personales"*, Averoni Ediciones, Córdoba, 2001.

Carvajal Pérez, Marvin: *"La protección de los datos personales en Costa Rica".* [En

línea] < http://www.democraciadigital.org/derechos/arts/0207datos.html > [consulta: 6 de Febrero 2003].

Chiriboga Zambrano, Galo: *"La acción de amparo y de hábeas data: garantías de los derechos constitucionales y su nueva realidad jurídica"*. [En línea] < http://www.ildis.org.ec/amparo/hab.htm > [consulta: 18 de Noviembre 2002].

Cifuentes Muñoz, Eduardo: *"El Hábeas Data en Colombia"*. En Revista Ius Et Praxis, Universidad de Talca, año 3 Nº 1, Talca, 1997 (1).

Cifuentes Muñoz, Eduardo: *"La Acción de Tutela en Colombia"*, Revista Ius et Praxis, Universidad de Talca, año 3 Nº 1, Talca, 1997 (2).

Comisión Andina de Juristas. [En línea] < http://www.cajpe.org.pe/rij/bases/temario/data.htm > [consulta: 16 de Diciembre 2002].

Corral Talciani, Hernán: *"De los Derechos de las Personas Sobre los Responsables de Bancos de Datos: El Hábeas Data Chileno"*. En Cuadernos de Extensión Jurídica Universidad de los Andes, Nº 5, Santiago, 2001.

Cuervo, José: *"Autodeterminación Informativa"*. [En línea] < http://www.informatica-juridica.com/trabajos/autodeterminacion_informativa.asp#4.%20CONCLU > [consulta: 10 de Diciembre de 2002].

Cumplido Cereceda, Francisco: *"Análisis del Anteproyecto de Ley sobre Protección de datos Personales elaborado por el Ministerio de Justicia (1990-1994)".* En Revista Ius et Praxis, Universidad de Talca, 1997.

Davara Rodríguez, Miguel A.: *"Manual de Derecho Informático"*, Ed. Aranzadi, Pamplona, 1997.

De Abreu, Dalmo: *"El Hábeas Data en Brasil"*, en Revista Ius et Praxis, Universidad de Talca, año 3 Nº 1, Talca 1997.

Diario La Hora de Guatemala, artículo de prensa: *"Congreso inicia ronda de discusión sobre la Ley de libre acceso a la información"*. [En línea] < http://www.lahora.com.gt/02/10/17/paginas/nac_2.htm#n1 > [17 de Enero 2003].

Dubié, Pedro: *"El hábeas data financiero"*, en Revista electrónica Alfa-Redi Nº 39. [En línea] < http://www.alfa-redi.org/revista/data/39-7.asp > [consulta: 27 de Noviembre 2002].

Eguiguren Praeli, Francisco J.: *"El Hábeas Data y su Desarrollo en el Perú"*, Revista Ius et Praxis, Universidad de Talca, año 3 Nº 1, Talca, 1997.

Estadella Yuste, Olga: *"La Protección de la Intimidad Frente a la Transmisión Internacional de Datos Personales"*, Ed. Tecnos, Madrid, 1995.

García Berni, Aída: *"La acción de Hábeas Data"* [en línea] < http://www.dlh.lahora.com.ec/paginas/judicial/paginas/D.Constitucional.18.htm > [consulta: 28 de Febrero 2003].

García Ponce, Temístocles: *"El recurso de Hábeas Data"*. [En línea] < http://www.dlh.lahora.com.ec/paginas/judicial/paginas/D.Constitucional.122.htm > [consulta: 16 de Noviembre 2002].

García-Herreros, Orlando: *"Lecciones de Derecho Administrativo"*, Institución Universitaria Sergio Arboleda, Santa Fe de Bogotá, 1994.

González Hoch, Francisco: *"Modelos comparados de protección de la información digital y la ley chilena de datos de carácter personal, en tratamiento de datos personales y protección de la vida privada"*, Cuadernos de Extensión Jurídica Nº 5, Universidad de Los Andes, Facultad de Derecho, 2001.

Gordón Ormaza, Fredy: "*El hábeas data en la legislación ecuatoriana"*, [en línea] < http://www.dlh.lahora.com.ec/paginas/judicial/paginas/D.Constitucional.172.htm > [consulta: 27 de Febrero 2003].

Gozaíni, Osvaldo (coord.): *"La Defensa de la Intimidad y de los datos personales a través del Habeas Data".* EDIAR, Buenos Aires, 2001.

Heredero Higueras, Miguel: *"La Directiva Comunitaria de Protección de los Datos de Carácter Personal"*, Ed. Aranzadi, Pamplona, 1997.

Herrán Ortíz, Ana: *"El Derecho a la Intimidad en la Nueva Ley Orgánica de Protección de Datos Personales"*, Ed. Dykinson, Madrid, 2002.

Jijena Leiva, Renato: *"La Ley Chilena de Protección de Datos Personales. Una visión crítica desde el punto de vista de los intereses protegidos"*, Cuadernos de Extensión Jurídica, Universidad de Los Andes, Nº 5, 2001.

Magliona M., Claudio: *"Hábeas Data y Protección de Datos Personales en Chile"*. [En línea] < http://www.adi.cl/pdf/magliona2.pdf > [consulta: 30 de Octubre 2002].

Mendoza Zúñiga, Ramiro Alfonso: *"Régimen de los Bancos de datos de organismos Públicos. Una Aproximación del Derecho Administrativo a la Ley Sobre Protección de la Vida Privada"*. En Cuadernos de Extensión Jurídica, Universidad de los Andes, Nº 5, Santiago, 2001.

Miguel Harb, Benjamín: *"Acción de amparo relacionada con la protección de datos personales en el orden jurídico Boliviano".* En Revista Ius Et Praxis*,* Universidad de Talca, año 3 Nº 1, Talca, 1997.

Moeykens, Federico Rafael: *"Derecho a la Libertad Informática: Consecuencia del Habeas Data"* Revista Electrónica Alfa-Redi Nº 48, [en línea] < http://www.alfa-redi.org/revista/data/48-6.asp > [consulta: 27 de Noviembre 2002].

Nino, Carlos S., *"Juicio al Mal Absoluto. Los Fundamentos y la Historia del Juicio a las Juntas del Proceso",* tr. Böhmer, Martín F., Emecé Editores, Buenos Aires, 1997.

Nogueira, Humberto: *"Reflexiones sobre el Establecimiento Constitucional del Hábeas Data y del Proyecto de Ley en Tramitación Parlamentaria sobre la Materia".* En Revista Ius Et Praxis, año 3, N° 1, Talca, 1997.

Nogueira Alcalá, Humberto. *"El Derecho a la Privacidad y a la Intimidad en el Ordenamiento Jurídico Chileno"*. En Revista Ius et Praxis, Universidad de Talca, año 4 Nº 2, Talca, 1998.

Nogueira Alcalá, Humberto: *"Las Constituciones y los Tratados en Materia de Derechos Humanos: América Latina y Chile"*. En Revista Ius et Praxis, Universidad de Talca, año 6 Nº 2, Talca, 2000.

Padilla, Miguel P.: *"Bancos de datos y acción de hábeas data",* Abeledo Perrot, Bs. As., 2001.

Palazzi, Pablo: *"El Hábeas Data en el Derecho Constitucional Argentino"*, en"La defensa de la intimidad y de los datos personales a través del hábeas data", Gozaíni,

Osvaldo (Coord.), Ed. Ediar, Bs.As., 2001.

Palazzi, Pablo: *"La transmisión internacional de datos personales y la protección de la privacidad",* Ed. Ad-Hoc, Bs. As., 2002.

Palazzi, Pablo: *"Protección de Datos Personales, Privacidad y Hábeas Data en América Latina"* [En línea] < http://www.ulpiano.com/Recursos_Privacy_LatinAmerica.htm#Uruguay > [consulta: 22 de Noviembre 2002].

Paván, Luis Carlos, *"La protección del consumidor en el MERCOSUR Análisis comparativo de los sistemas de Argentina, Brasil y Chile"*. [En línea] < http://www.acmp.org.br/docs/proteccion.doc > [consulta: 7 de Febrero 2003].

Pizzolo, Calógero: *"El Hábeas Data en el Derecho Constitucional Latinoamericano*". En "La Defensa de la Intimidad y de los Datos Personales a través del Hábeas Data". Gozaini, Osvaldo (coord.), Ediar, Bs. As., 2001.

Quiroga Lavié, Humberto*, "Hábeas Data"*, Zavalia, Bs. As., 2001.

Rebolledo Delgado, Lucrecio: *"El Derecho Fundamental a la Intimidad"*, Ed. Dykinson, Madrid, 2000.

Ríos Estavillo, Juan José: *"El Hábeas Data: ¿Algún día en México?".* [En línea] < http://legal.terra.com.mx/Legal/EnLinea/Columnas/articulo/31default.asp > [consulta: 15 de Noviembre 2002].

Rodríguez Reichberg, Tamara: *"La protección de los derechos humanos en Guatemala".* [En línea] < http://hcs.harvard.edu/~haciadem/summit/bulletins/Reichberg-CdG-Bulletin.pdf > [consulta: 16 de Marzo 2003].

Roxin, Claus: *"Derecho Penal Parte General, T.I, Fundamentos. La Estructura de la Teoría del Delito"*, tr. Luzón Peña, Diego-Manuel "et al", Ed. Civitas, Madrid, 1997.

Suárez Crothers, Christian: *"Informática, Vida Privada y los Proyectos Chilenos sobre Protección de Datos".* En Revista Ius et Praxis, Universidad de Talca, Año 3 Nº 1, Talca, 1997.

Suñé Llinás, Emilio: *"Tratado de Derecho Informático, Vol. I, Introducción y Protección de Datos Personales"*, Universidad Complutense, Facultad de Derecho e Instituto Español de Informática y Derecho, Madrid, 2000.

Vasquéz Márquez, José Ignacio: *"Análisis crítico sobre la naturaleza jurídica de la ley de protección de la vida Privada"*. En Revista de Derecho Universidad Finis Terrae, año III, Nº 3, Santiago, 1999.

Vial Claro, Felipe: *"La Ley Nº 19.628 sobre Protección de Datos de Carácter Personal una Visión general"*. En Cuadernos de Extensión Jurídica, Universidad de Los Andes, Nº 5, Santiago, 2001.

Viera-Gallo, José: *"Fundamentos y Características del Hábeas Data en Chile"*. En Revista Ius et Praxis*,* Universidad de Talca, año 3 Nº 1, Talca, 1997.

Warren, Samuel D. y Brandeis, Louis D., *"El derecho a la intimidad"*, tr. Baselga, Pilar, Ed. Civitas S.A, Madrid, 1995.

Zúñiga, Francisco: *"El Derecho a la Intimidad y sus Paradigmas"*, en Revista Ius et Praxis, Universidad de Talca, año 3, N° 1. Talca, 1997.

Textos Autoritativos y Otras Fuentes

Argentina. Ley 21.526 sobre Entidades Financieras, [En línea] <http://infoleg.mecon.gov.ar/txtnorma/texactley21526.htm> [consulta: 27 de Diciembre 2002].

Argentina. Constitución Política. [En línea] < http://www.georgetown.edu/pdba/Constitutions/Argentina/argen94.html > [consulta: 27 de Diciembre 2002].

Argentina. Ley Nº 23.798 sobre Prevención y Lucha contra el Síndrome de Inmunodeficiencia Adquirida (SIDA). [En línea] <http://www.iijusticia.edu.ar/privacidad/ley23798.htm> [consulta: 27 de Diciembre 2002].

Argentina. Ley Nº 25.065 que establece normas que regulan diversos aspectos vinculados con el sistema de Tarjetas de Crédito, Compra y Débito, [en línea] < http://infoleg.mecon.gov.ar/txtnorma/texactley25065.htm > [consulta: 27 de Diciembre 2002].

Argentina. Ley Nº 712 de la Ciudad Autónoma de Buenos Aires sobre Garantías del Patrimonio Genético Humano. [En línea] < http://www.msn.com.ar/cbsas/contenidonumero.asp?idfdlcba=7422 > [consulta: 27 de Diciembre 2002].

Argentina. Texto Ordenado y Actualizado de Normas sobre Clasificación de Deudores (última comunicación incorporada: “A” 3.630 del 10 de Junio de 2002. [En línea] < http://www.bcra.gov.ar/folio/t-cladeu.pdf > [consulta: 24 de Enero 2003].

Asamblea General de la ONU, Resolución 45/95, 14 de Diciembre de 1990. Principios Rectores para la Reglamentación de los Ficheros Computarizados de Datos Personales, señalados por al, [en línea] < http://www.onu.org.gt/~oacdh/oacdh/Derechos%20Humanos/CDROM/Normativa/UN/Normas%20C > [consulta: 05-05-2003].

Bolivia. Ley del Estatuto del Funcionario Público (Ley Nº 2.027-1999). [En línea] < http://www.solobolivia.com/politica/leyes/ley2027.shtm > [consulta: 6 de Febrero 2003].

Bolivia. Código Civil. [En línea] < http://www.cajpe.org.pe/rij/bases/legisla/bolivia/ley11.HTM

Bolivia. Código del Niño, Niña y Adolescente (Ley Nº 2.026-1999). [En línea] <http://www.cajpe.org.pe/RIJ/bases/legisla/bolivia/2026.HTM> [consulta: 3 de Febrero 2003].

Bolivia. Código Penal. [En línea] < http://www.unifr.ch/derechopenal/legislacion/bo/cp_bolivia5.pdf > [consulta: 2 de Marzo 2003].

Bolivia. Código Tributario (Ley Nº 1.340-1992). [En línea] < http://www.ferjus.bizland.com/ct.htm > [consulta: 6 de Febrero 2003].

Bolivia. Constitución Política. [En línea] < http://www.georgetown.edu/pdba/Constitutions/Bolivia/consboliv1615.html > [consulta: 17 de Octubre 2002].

Bolivia. Constitución Política. [En línea] < http://www.portal-pfc.org/legislacion/2002/038.html#1 > [consulta: 6 de Febrero 2003].

Bolivia. Ley de Bancos e Instituciones Financieras (Ley Nº 1.488-1993). [En línea] < http://www.solobolivia.com/politica/leyes/ley1488.shtml > [consulta: 2 de Marzo 2003].

Bolivia. Ley de la Abogacía (DL Nº 16.793-1979). [En línea] < http://www.ferjus.bizland.com/abogado.htm > [consulta: 6 de Febrero 2003].

Bolivia. Ley del Tribunal Constitucional (Ley Nº 1.836-1998). En línea] < http://www.cajpe.org.pe/RIJ/bases/ddhh/bo_13.htm > [consulta: 6 de Febrero 2003].

Bolivia. Proyecto de Ley de Necesidad de Reforma a la Constitución Política del Estado. [En línea] < http://www.portal-pfc.org/legislacion/2002/038.html#1 > [consulta: 6 de Febrero 2003].

Brasil. Código Penal. [En línea] < http://www.unifr.ch/derechopenal/legislacion/br/ljbre5.html > [consulta: 8 de Febrero 2003].

Brasil. Constitución Política. [en línea] < http://www.congreso.gob.hn/sil/WEBCONS/c/CBRASIL.htm > [consulta: 7 de Febrero de 2003].

Brasil. Constitución Política. [En línea] < http://www.georgetown.edu/pdba/Constitutions/Brazil/brazil88.html > [consulta: 7 de Febrero 2003].

Brasil. Estatuto del Niño y Adolescente (Ley Nº 8.069). [en línea] < http://www.pge.sp.gov.br/centrodeestudos/bibliotecavirtual/dh/volume%20i/crian%C3%A7alei806 > [consulta: 3 de Enero 2003].

Brasil. LEI Nº 8.078 *"Dispõe sobre a proteção do consumidor, e dá outras providências".* [En línea] < http://www.crea-mg.com.br/infor/legislacao/l8078.htm > [consulta: 3 de Enero 2003].

Brasil. Ley Complementaria Nº 105 de 2001. [En línea] < http://www.planalto.gov.br > [consulta: 7 de Febrero 2003].

Brasil. Ley Nº 4.595 de 1964 sobre Política de las Instituciones Financieras, bancarias y crediticias. [En línea] < http://www.oficinadodireito.com.br/leifederal/4595.htm > [consulta: 3 de Enero 2003].

Brasil. Ley Nº 9.507. [En línea] < http://www.planalto.gov.br/ccivil_03/Leis/L9507.htm > [consulta: 26 de Noviembre 2002].

Brasil. Ley sobre el Sistema Tributario Nacional (Ley Federal Nº 5.172-1966). [En línea] < http://www.sefp.df.gov.br/Legislacao/LeiordinariaFed/lei5172.htm > [consulta: 3 de Enero 2003].

Brasil. Proyecto de Ley Nº 268 del año 1999. [En línea] < http://www.senado.gov.br/lucioalcantara/1999/projetos/indproje.htm# > [consulta: 7 de Febrero 2003].

Brasil. Resolución Nº 2.724/00 del Banco Central de Brasil. [En línea] < http://www.leasingabel.com.br/novosite/juridico/resolucao/res2724.htm > [consulta: 3 de Enero 2003].

Chile. Constitución Política.

Chile. *"Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado recaído en el Proyecto de Ley en tercer Trámite, sobre Protección de la Vida Privada"*, Sesión 18º ordinaria del 5 de Agosto de 1998, Diario de Sesiones del Senado, págs. 2086-2091.

Chile. Código del Trabajo.

Chile. Código Sanitario.

Chile. Código Tributario.

Chile. Decreto Supremo Nº 779/2000 del Ministerio de Justicia.

Chile. Decreto Supremo Nº 950/1928 del Ministerio de Hacienda.

Chile. L.O.C. de Bases Generales de la Administración del Estado.

Chile. Ley General de Bancos.

Chile. Ley N º 19.223 que tipifica figuras penales relativas a la informática.

Chile. Ley Nº 19.628 sobre Protección de la Vida Privada.

Chile. Ley Nº 19.812.

Chile. Ley Orgánica del Servicio de Registro Civil e Identificación Nº 19.477, de 19 de Octubre de 1996.

Chile.Superintendencia de Bancos e Instituciones Financieras. Circular para Bancos Nº 2.544 de 8 de junio de 1990. [En línea] < http://www.sbif.cl/NormasSBIF/Bancos/C2544B.pdf > [consulta: 9 de Mayo 2003]

Colombia. Código Penal. [En línea] http://www.unifr.ch/derechopenal/legislacion/co/l2t3c1-9.htm#4 [consulta: 10 de Febrero 2003].

Colombia. Constitución Política. [En línea] < http://www.georgetown.edu/pdba/Constitutions/Colombia/col91.html > [consulta: 6 de Noviembre 2002].

Colombia. Ley General de Procedimiento Tributario. [En línea] < http://www.ciat.org/doc/docu/leg/cod/lal_colom_02_ley_procedimiento_tributario.doc >, [consulta: 3 de Enero 2003].

Colombia. Ley Nº 510 de 1999. [En línea] < http://www.secretariasenado.gov.co/leyes/L0510_99.HTM > [consulta: 7 de Enero 2003].

Colombia.Ley Nº 550-1999. [En línea] < http://www.supersociedades.gov.co/ss/drvisapi.dll?MIval=sec&dir=96 > [consulta: 3 de Febrero 2003].

Colombia. Proyecto de Ley Estatutaria Nº 75 de 2002. [En línea] < http://www.superbancaria.gov.co/gobierno/Proynorma/proyectosley.htm > [consulta: 14 de Enero 2003].

Nicaragua. Constitución Política. [En línea] < http://www.georgetown.edu/pdba/Constitutions/Nica/nica95.html > [consulta: 3 de Noviembre 2002]

Convención Americana Sobre Derechos Humanos. [En línea] < http://www.oas.org/juridico/spanish/firmas/b-32.html > [consulta: 20 de Marzo 2003].

Costa Rica. Código Civil. [En línea] < http://www.pgr.go.cr/leyes-usuales/Ley%20N%2063%20Codigo%20Civil.htm > [consulta: 3 de Febrero 2003].

Costa Rica. Código de Comercio [En línea] < http://www.pgr.go.cr/leyes-usuales/Ley%20N%203284%20Codigo%20de%20Comercio.htm > [consulta: 3 de Febrero 2003].

Costa Rica. Código Penal. [En línea] < http://www.pgr.go.cr/leyes-usuales/Ley%20N%204573%20Codigo%20de%20Penal.htm > [consulta: 2 de Febrero 2003].

Costa Rica. Código Tributario. [En línea] < http://www.nexos.co.cr/cesdepu/nbdp/cotri.htm > [consulta: 3 de Febrero 2003].

Costa Rica. Constitución Política. [En línea] < http://www.georgetown.edu/pdba/Constitutions/Costa/costa2.html > [consulta: 3 de Noviembre 2002].

Costa Rica. Ley de la Jurisdicción Constitucional. [En línea] < http://www.pgr.go.cr/scripts/TextoCompleto.dll,fecha > [consulta: 2 de Febrero 2003].

Cuba. Código Penal. [En línea] < http://www.unifr.ch/derechopenal/legislacion/cu/cpcuba7.htm > [consulta: 2 de Marzo 2003].

Cuba. Constitución Política. [En línea] < http://www.georgetown.edu/pdba/Constitutions/Cuba/cuba1992.html > [consulta: 3 de Febrero 2003].

Cuba. Decreto-Ley Nº 169 de 1997, sobre Normas Generales y Procedimientos Tributarios. [En línea] < http://www.ciat.org/doc/docu/leg/cod/cuba_dto_169_procedimientos_tributarios.DOC > [consulta: 2 de Marzo 2003].

Cuba. Decreto-Ley Nº 173 sobre Bancos e Instituciones Financieras no bancarias. [En línea] < http://www.bc.gov.cu/Espanol/regulaciones_bancarias/DL173.HTM > [consulta: 3 de Febrero 2003].

Cuba. Estatutos del Banco Central de Cuba. [En línea] < http://www.bc.gov.cu/Espanol/regulaciones_bancarias/EstatutosBCC.htm > [consulta: 3 de Febrero 2003].

Ecuador Código Tributario. [En línea] < http://webs.demasiado.com/eculegal/ecu1/011.htm > [consulta: 2 de Marzo 2003].

Ecuador. Codificación de la Ley General de Instituciones del Sistema Financiero. [En

línea] < http://www.superban.gov.ec/pages/e_leyes_sist-financiero_ley.htm > [consulta: 3 de Marzo 2003].

Ecuador. Código Civil. [En línea] < http://www.dlh.lahora.com.ec/paginas/judicial/paginas/CodcivilTP.html > [consulta: 2 de Marzo 2003].

Ecuador. Código Penal. [En línea] < http://www.dlh.lahora.com.ec/paginas/judicial/paginas/Codpenal.2.html#anchor1728504 > [consulta: 2 de Marzo 2003].

Ecuador. Constitución Política [En línea] < http://www.georgetown.edu/pdba/Constitutions/Ecuador/ecuador98.html > [consulta: 3 de Noviembre 2002].

Ecuador. Ley de Comercio Electrónico, Firmas y Mensajes de Datos. [En línea] < http://www.corpece.org.ec/documentos/ley/ley_ce.doc > [consulta: 2 de Marzo 2003].

Ecuador. Ley de Control Constitucional. [En línea] < http://www.cajpe.org.pe/rij/bases/legisla/ecuador/lh-25.HTMl > [consulta: 3 de Febrero 2003].

El artículo 29 de la Directiva, intitulado *"Grupo de protección de las personas en lo que respecta al tratamiento de datos personales* [En línea]< http://www.protecciondedatos.com.ar/dic42002.htm > [consulta: 12 de Mayo 2003].

Venezuela. Resolución Nº 001-06-98 de la Junta de Emergencia Financiera que establece normas relativas al funcionamiento del Sistema de Información Central de Riesgos (SICRI). [En línea] < http://www.iijusticia.edu.ar/privacidad/Paises.htm#VE > consulta: 10 de Abril 2003].

Nicaragua. Ley de Amparo. [En línea] < http://www.uc3m.es/uc3m/inst/MGP/JCI/02-nicaragua-leydeamparo.htm > [consulta: 19 de Enero 2003].

El Salvador. Código Penal. [En línea] < http://www.unifr.ch/derechopenal/legislacion/sv/cp_elsalvador15.htm > [consulta: 4 de Marzo 2003].

El Salvador. Código Tributario. [En línea] < http://www.ciat.org/doc/docu/leg/cod/lal_elsal_02_codigo_tributario.doc > [consulta: 4 de Marzo 2003].

El Salvador. Constitución Política. [En línea] < http://www.georgetown.edu/pdba/Constitutions/ElSal/ElSal83.html > [6 de Noviembre 2002].

El Salvador. Ley de Bancos. [En línea] < http://www.ssf.gob.sv/frm_marco/frm_marco.htm > [consulta: 4 de Marzo 2003].

El Salvador. Ley de Procedimientos Constitucionales. [En línea] < http://www.uc3m.es/uc3m/inst/MGP/JCI/02-elsalvador-leydeprocedimientosconstitucionalesl.htm > [consulta: 15 de Marzo 2003].

El Salvador. Ley Orgánica de la Superintendencia del Sistema Financiero. [En línea] < http://www.ssf.gob.sv/frm_marco/frm_marco.htm > [consulta: 15 de Marzo 2003].

España. Constitución Política. [En línea] <

http://www.congreso.es/funciones/constitucion/titulo_1_cap_2_sec1.htm > [consulta: 10 de Abril 2003].

España. Ley Orgánica de Protección de Datos Personales 15/1999.[En línea] < http://www.ua.es/oia/es/legisla/datos.html > [consulta: 10 de Mayo 2003].

Guatemala .Constitución Política. [En línea] < http://www.georgetown.edu/pdba/Constitutions/Guate/reforms99.html > [consulta: 17 de Enero 2003].

Guatemala. Código Penal. [En línea] < http://www.unifr.ch/derechopenal/legislacion/gt/cp_guatemala.htm > [consulta: 19 de Marzo 2003].

Guatemala. Código Tributario. [En línea] < http://www.ciat.org/doc/docu/leg/cod/lgt_02_codigo_tributario_guatemala.doc > [consulta: 18 de Marzo 2003].

Guatemala. Ley de Amparo, Exhibición Personal y Constitucionalidad. [En línea] < http://www.minugua.guate.net/derhum/CDROM/Normativa/Leyes%20Guate/leydeamparo.htm,fe > [consulta: 17 de Enero 2003].

Guatemala. Ley de Bancos y Grupos Financieros. [En línea] < http://www.banguat.gob.gt/leyes/2002/bancos.pdf > [consulta: 18 de Marzo 2003].

Guatemala. Ley Orgánica del Banco de Guatemala. [En línea] < http://www.sib.gob.gt/banguat/index_2.php > [consulta 19 de Marzo 2003].

Guatemala. Proyecto de Ley de Libre Acceso a la Información. [En línea] < http://www.congreso.gob.gt/Noticias/marzo/180303/11-2003.htm > [consulta: 19 de Marzo 2003].

Honduras. Código Tributario. [En línea] < http://www.ciat.org/doc/docu/leg/cod/lhn_02_codigo_tributario_honduras.doc > [consulta: 20 de Marzo 2003].

Honduras. Constitución Política [En línea] < http://www.georgetown.edu/pdba/Constitutions/Honduras/hond82.html > [consulta: 3 de Noviembre 2003].

Honduras. Ley de Instituciones del Sistema Financiero. [En línea] < http://www.hondurasri.com/business_honduras_spa/leyes/leysis.html > [consulta: 20 de Marzo 2003].

Honduras. Ley Orgánica del Comisionado Nacional de los Derechos Humanos. [En línea] < http://ns.rds.org.hn/participacion_ciudadana/legislacion/leyes_secundarias/ley_organica_del_co > [consulta: 20 de Marzo 2003].

México. Código Civil. [En línea] < http://www.solon.org/Statutes/Mexico/Spanish/codigo_civil.pdf > [consulta: 25 de Marzo 2003].

México. Código Fiscal de la Federación. [En línea] < http://www.ciat.org/doc/docu/leg/cod/lmx_02_codigo_fiscal_mexico.doc > [consulta: 26 de Diciembre 2002].

México. Código Penal. [En línea] <

http://www.unifr.ch/derechopenal/legislacion/mx/cp_mexico.htm > [consulta: 25 de Marzo 2003].

México. Constitución Política. [En línea] < http://www.georgetown.edu/pdba/Constitutions/Mexico/mexico1917.html > [consulta: 17 de Octubre 2002].

México. Ley de Amparo [En línea] < http://info4.juridicas.unam.mx/const/frames/ley.htm > [consulta: 6 de Febrero 2003].

México. Ley de Imprenta. [En línea] < http://www.cddhcu.gob.mx/leyinfo/pdf/40.pdf > [consulta: 22 de Noviembre 2002].

México. Ley de Instituciones de Crédito. [En línea] < http://www.shcp.gob.mx/servs/normativ/leyes/l_ic.html > [consulta: 22 de Noviembre 2002].

México. Ley de Protección y Defensa al Usuario de Servicios Financieros. [En línea] < http://www.condusef.gob.mx/marco_juridico/ley_proteccion_defensa.htm > [consulta: 22 de Noviembre 2002].

México. Ley Federal de Protección al Consumidor. [En línea] < http://www.cddhcu.gob.mx/leyinfo/113/ > [consulta: 26 de Diciembre 2002].

México. Ley para regular las Sociedades de Información Crediticia. [En línea] < http://www.shcp.gob.mx/servs/normativ/leyes/l_rsic.html > [consulta: 22 de Noviembre 2002].

México. Proyecto de Ley. Diputado Miguel Barbosa Huerta, Septiembre2001. [En línea] < http://www.cddhcu.gob.mx/servicios/datorele/cmprtvs/1po2/set/2.htm > [consulta: 22 de Noviembre 2002].

México. Proyecto de Ley. Senador Antonio García Torres, Febrero de 2001. [En línea] < http://telematica.cicese.mx/propuestaley/Leydatos/ > [consulta: 15 de Diciembre 2002].

Nicaragua. Código Penal. [En línea] < http://www.unifr.ch/derechopenal/legislacion/ni/cp_nicaragua.htm > [consulta: 26 de Marzo 2003].

Nicaragua. Legislación Tributaria Común.[En línea] < http://www.ciat.org/doc/docu/leg/cod/lni_02_legislacion_tributaria_comun_nicaragua.doc > [consulta: 26 de Marzo 2003].

Nicaragua. Ley General de Bancos, Instituciones Financieras no Bancarias y Grupos Financieros. [En línea] < http://www.siboif.gob.ni/DOCS/leyes/grales/LEY314.htm > [consulta: 26 de Marzo 2003].

Panamá. Código Fiscal.[En línea] < http://www.legalinfo-panama.com/legislacion/fiscal/isr_06.htm > [consulta: 17 de Enero 2003].

Panamá. Código Penal. [En línea] < http://www.unifr.ch/derechopenal/legislacion/pa/cp_panama6.pdf > [consulta: 17 de Enero 2003].

Panamá. Constitución Política. [En línea] < http://www.georgetown.edu/pdba/Constitutions/Panama/panama1994.html >

[consulta: 3 de Noviembre 2003].

Panamá. Ley Bancaria (Decreto-Ley Nº 9). [En línea] < http://www.shirleylaw.com/documents/Ley.Bancaria_1998_sp.htm,fecha > [consulta: 14 de Abril 2003].

Panamá. Ley de Transparencia en la Gestión Pública, establece la acción de Hábeas Data y dicta otras disposiciones (Ley Nº 6-2002). [En línea] < http://www.legalinfo-panama.com/legislacion/administrativo/00195.pdf > [consulta: 17 de Enero 2002].

Panamá. Ley que regula el Servicio de Información sobre el Historial de Crédito de los Consumidores o Clientes. [En línea] < http://www.legalinfo-panama.com/legislacion/00297.pdf > [consulta: 18 de Noviembre 2002].

Paraguay. Código Civil. [En línea] < http://comunidad.derecho.org/desvars/cc.html > [consulta: 31 de Marzo 2003.

Paraguay. Código Penal. [En línea] < http://www.itacom.com.py/ministerio_publico/codigo_penal/index.html > [consulta: 1 de Abril 2003].

Paraguay. Constitución Política. [En línea] < http://www.georgetown.edu/pdba/Constitutions/Paraguay/para1992.html > [consulta: 11 de Diciembre 2002].

Paraguay. Ley General de Bancos, Financieras y Otras Entidades de Crédito. [En línea] < http://www2.paraguaygobierno.gov.py/ley_861.html > [consulta: 5 de Febrero 2003].

Paraguay. Ley Nº 1.682. [En línea] < http://www.ulpiano.com/DataProtection-LA-links.htm > [consulta: 18 de Noviembre 2002].

Paraguay. Ley Nº 1969 [En línea] < http://www.informconf.com.py/informconf/site/downloads/Ley_1682.pdf > [consulta: 3 de Febrero 2003].

Paraguay. Ley que establece el Nuevo Régimen Tributario (Ley Nº 125/91). [En línea] < http://www.paraguaygobierno.gov.py/ley125.doc > [consulta: 18 de Noviembre 2002].

Perú. Código Civil. [En línea] < http://www.leyes.congreso.gob.pe/Imagenes/Codigos/1010807++.pdf > [consulta: 24 de Abril 2003].

Perú. Código Penal. [En línea] < http://www.unifr.ch/derechopenal/legislacion/pe/cpperuidx.htm > [consulta: 7 de Abril 2003].

Perú. Código Tributario. En línea] < http://www.congreso.gob.pe/out_of_domain.asp?URL=http%3A//www.leyes.congreso.gob.pe/ > [consulta: 5 de Febrero 2003].

Perú. Constitución Política. [En línea] < http://www.georgetown.edu/pdba/Constitutions/Peru/per93.html > [consulta: 11 de Diciembre 2002]

Perú. Ley de Amparo Nº 23.506. [En línea] < http://www.cajpe.org.pe/rij/bases/legisla/peru/23506c.htm > [consulta: 23 de Abril 2003].

Perú. Ley de Protección al Consumidor (Decreto Legislativo Nº 716-1991). [En línea] < http://www.indecopi.gob.pe/upload/cpc/tuo716.pdf > [consulta: 7 de Abril 2003].

Perú. Ley de Transparencia y Acceso a la Información Pública (Ley Nº 27.806). [En línea] < http://www.leyes.congreso.gob.pe/Imagenes/Leyes/27806.pdf > [consulta: 20 de Abril 2003].

Perú. Ley General de la Persona con Discapacidad. [En línea] < http://www.leyes.congreso.gob.pe/Imagenes/Leyes/27050.pdf > [consulta: 11 de Diciembre 2002].

Perú. Ley General del Sistema Financiero y del Sistema de Seguros. [En línea] < http://www.fsd.org.pe/normas/Ley.pdf > [consulta: 16 de Enero 2003].

Perú. Ley Nº 27.863. [En línea] < http://www.leyes.congreso.gob.pe/Imagenes/Leyes/27863.pdf > [consulta: 11 de Diciembre 2002].

Perú. Ley Orgánica de la Defensoría del Pueblo. [En línea] < http://www.cajpe.org.pe/rij/bases/legisla/peru/23506c.htm > [consulta: 7 de Abril 2003].

Perú. Ley que crea la Unidad de Inteligencia Financiera-Perú. [En línea] < http://www.leyes.congreso.gob.pe/Imagenes/Leyes/27693.pdf > [consulta: 12 de Diciembre 2002].

Perú. Ley que Regula las Centrales Privadas de Información de Riesgos y de Protección al Titular de la Información (Ley Nº 27.489). [En línea] < http://www.leyes.congreso.gob.pe/Imagenes/Leyes/27489.pdf > [consulta: 11 de Diciembre 2002].

Perú. Proyecto de Ley Nº 5233, Septiembre de 1999. [En línea] < http://200.37.159.7/pley/pley1995_2000.htm > [consulta: 21 de Enero 2003].

República Dominicana. Código para la Protección de Niños, Niñas y Adolescentes. [En línea] < http://www.iijusticia.edu.ar/privacidad/RD.htm#EDP > [consulta: 3 de Enero 2003].

República Dominicana. Código Penal. [En línea] < http://www.iijusticia.edu.ar/privacidad/RD.htm#EDP > [consulta: 3 de Enero 2003].

República Dominicana. Código Tributario. [En línea] < http://www.ciat.org/doc/docu/leg/cod/lal_domin_02_codigo_tributario.doc > [consulta: 8 de Abril 2003].

República Dominicana. Constitución Política [En línea] < http://www.georgetown.edu/pdba/Constitutions/DomRep/domrep02.html > [consulta: 6 de Noviembre 2002].

República Dominicana. Ley General de Bancos. [En línea] < http://cnnc.cancilleria.gov.do/bancos.doc > [consulta: 8 de Abril 2003].

República Dominicana. Ley sobre Expresión y Difusión del Pensamiento (Ley Nº 6.132-1962). [En línea] < http://www.iijusticia.edu.ar/privacidad/RD.htm#EDP >

[consulta: 3 de Enero 2003].

Uruguay. Código Civil. [En línea] < http://www.parlamento.gub.uy/Codigos/CodigoCivil/1996/l4P1T1.htm > [consulta: 10 de Abril 2003].

Uruguay. Código Penal. [En línea] < http://www.unifr.ch/derechopenal/legislacion/uy/cp_uruguay.htm > [consulta: 10 de Abril 2003].

Uruguay. Código Tributario. [En línea] < http://www.ciat.org/doc/docu/leg/cod/lal_urugu_02_codigo_tributario.doc > [consulta: 10 de Abril 2003].

Uruguay. Constitución Política. [En línea] < http://www.georgetown.edu/pdba/Constitutions/Uruguay/uruguay96.html > [consulta: 22 de Noviembre 2002].

Uruguay. Ley de Amparo Nº 16.011. [En línea] < http://www.parlamento.gub.uy/leyes/ley16011.htm > [consulta: 21 de Enero 2003].

Uruguay. Ley sobre el Sistema de Intermediación Financiera (Ley Nº 15.322). [En línea] < http://www.parlamento.gub.uy/Leyes/Ley15322.htm > [consulta: 9 de Abril 2003].

Uruguay. Proyecto de Ley que regula el Funcionamiento de los Bancos de Datos. Mayo de 2000. [En línea] < http://www.parlamento.gub.uy/Repartidos/Camara/D2000050141-00.htm > [consulta: 5 de Febrero 2003].

Uruguay. Proyecto de Ley que regula los Bancos de Datos de Información de Cumplimiento de Créditos o de Obligaciones de Tracto Sucesivo. Mayo de 2000. [En línea] < http://www.parlamento.gub.uy/Repartidos/Camara/D2000050112-00.htm > [consulta: 5 de Febrero 2003].

Uruguay. Proyecto de Ley sobre el Derecho a la Información y Acción de “Hábeas Data”. Mayo de 2000. [En línea] < http://www.parlamento.gub.uy/Repartidos/Camara/D2000050114-00.htm > [consulta: 5 de Febrero 2003]

Uruguay. Proyecto de Ley sobre la Creación de un Registro Nacional de Deudores Alimentarios. Abril de 2000. [En línea] < http://www.parlamento.gub.uy/Repartidos/Camara/D2000040062-00.htm > [consulta: 5 de Febrero 2003].

Uruguay. Proyecto de Ley sobre Personas Físicas o Jurídicas que Administren, Gestionen u Obtengan Información de cualquier Base de Datos. Octubre de 2000. [En línea] < http://www.parlamento.gub.uy/Repartidos/Camara/D2000100351-00.htm > [consulta: 5 de Febrero 2003].

Venezuela. Código Civil. [En línea] < http://comunidad.vlex.com/pantin/codigocivil.html > [consulta: 11 de Abril 2003].

Venezuela. Código Orgánico Tributario.[En línea] < http://comunidad.vlex.com/pantin/cot.html > [consulta: 20 de Abril 2003].

Venezuela. Código Penal. [En línea] < http://www.unifr.ch/derechopenal/legislacion/ve/cpveneidx.htm > [consulta: 20 de Abril 2003].

Venezuela. Constitución Política. [En línea] < http://www.tsj.gov.ve/legislacion/constitucion1999.htm > [consulta: 21 de Noviembre 2002].

Venezuela. Ley del Banco Central de Venezuela. [En línea] < http://comunidad.derecho.org/pantin/lbcentral.html > [consulta: 10 de Abril 2003].

Venezuela. Ley Especial Contra los Delitos Informáticos. [En línea] < http://www.tsj.gov.ve/legislacion/ledi.htm > [consulta: 21 de Noviembre de 2002].

Venezuela. Ley General de Bancos y Otras Instituciones Financieras. [En línea] < http://comunidad.derecho.org/pantin/bancos.html > consulta: 10 de Abril 2003].

Venezuela. Ley sobre Protección a la Privacidad de las Comunicaciones. [En línea] < http://www.iijusticia.edu.ar/privacidad/Paises.htm#VE > [consulta: 10 de Abril 2003].