Humberto Nogueira Alcalá (Chile) *

Autodeterminación informativa y hábeas data en Chile e información comparativa

1. La autodeterminación informativa forma parte del derecho al respeto de la vida privada

El registro de antecedentes y datos y su utilización adecuada han servido para la vigencia de diversos derechos fundamentales y para el desarrollo de la sociedad.

Sin embargo, el desarrollo de la telemática, que constituye la conjunción de las telecomunicaciones con la informática y que constituye el conjunto de servicios de naturaleza informática que pueden ser prestados a través de una red de comunicaciones,[1] presenta, junto con el progreso y sus aportes al desarrollo de las sociedades, riesgos importantes para el respeto de la vida privada e intimidad de las personas, por su capacidad de reunir datos, interrelacionarlos, ordenarlos, posibilitando el acceso a ellos y a transmitirlos, de manera de constituir importantes bases de datos con información de las personas tanto en manos del Estado como de particulares, con desconocimiento de los afectados.

El registro, procesamiento, entrecruzamiento, organización y transmisión de datos constituye una información valiosa para todo tipo de toma de decisiones económicas, políticas, sociales, empresariales; las bases o registros de datos personales implican la posibilidad de develar aspectos de la vida privada de las personas, haciendo ilusorio su derecho a la privacidad, lo que exige su regulación por el ordenamiento jurídico.

---

* Abogado; doctor en Derecho Constitucional por la Universidad Católica de Lovaina la Nueva (Bélgica). Profesor titular de Derecho Constitucional y director del Centro de Estudios Constitucionales de la Universidad de Talca. Vicepresidente del Instituto Iberoamericano de Derecho Procesal Constitucional. Director de la Asociación Chilena de Derecho Constitucional. ‹nogueira@utalca.cl›

[1] Olga Estadella Yuste: L*a protección de la intimidad frente a la transmisión internacional de datos personales*, Madrid, Tecnos, 1995, p. 13.

Como señala Losano, en el plano informático, el computador u ordenador, a través del "software aplicativo", se ha convertido para sus usuarios en el delator perfecto de informaciones sin que el titular de ellas llegue a enterarse, ya que el usuario se encuentra registrado, observado y puesto en un acuario de cristal, lo que se ha denominado *síndrome del pez rojo*.[2]

Así, los problemas desarrollados por la revolución informática y telemática encuentran su paralelismo con los provocados por la difusión de informaciones por los medios de comunicación tradicionales, que pueden afectar el derecho a la vida privada. Sin embargo, la primera adquiere características particulares, ya que no sólo se trata de controlar, reducir o anular la difusión de informaciones que afecten la privacidad de las personas, sino también de determinar quién se encuentra estructurando bases de datos personales accesibles a terceros, para qué fines han sido creadas, qué tipos de datos se registran, todo ello con objeto de controlarlos.

De esta forma, los Estados se han preocupado de determinar los límites legítimos dentro de los cuales puede concretarse la actividad de obtención, tratamiento y difusión o comunicación de datos personales y el derecho de acceso a la información pública que forma parte del derecho a la libertad de buscar y difundir información.

Se trata, por tanto, de conjugar armónicamente los derechos a la libertad de buscar y difundir información y el derecho al respeto de la vida privada en el contexto de la informática y la telemática.

El esfuerzo a realizar es el de compatibilizar y armonizar el derecho a la información y a la privacidad, autodeterminación informativa y buena reputación en la senda del desarrollo y bienestar de las personas.[3]

En este contexto, debe considerarse, por una parte, la *libertad de información* que incluye la búsqueda y difusión de informaciones sin límites arbitrarios y sin censura, como asimismo la *libertad informática*, constituida por el derecho de recolectar y almacenar toda la información cuyo conocimiento y registro no esté prohibido por el ordenamiento jurídico por motivos razonables, fundados en la protección de los derechos de las personas o en bienes jurídicos constitucionales.[4]

En el concepto de respeto de la vida privada se incluyen datos que a primera vista pueden ser irrelevantes desde la perspectiva de protección de la privacidad de la persona, pero que, en conexión con otros datos, considerados en su conjunto, pueden hacer totalmente transparente la personalidad de un individuo. Es lo que la doctrina ha denominado la *teoría del mosaico*: "al igual que ocurre con las pequeñas piedras

---

[2] Mario Losano: *Il diritto pubblico dell'informatica*, Einaudi, 1986, p. 13 (citado por Sentencia de Corte Constitucional Colombiana, T-414/92).

[3] Rodolfo Daniel Uicich: *Los bancos de datos y el derecho a la intimidad*, Buenos Aires, Ad-Hoc, p. 26.

[4] Ver Óscar Puccinelli: *El hábeas data en Indoiberoamérica*, Santafé de Bogotá, Temis, 1999, pp. 25-26.

que forman los mosaicos, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significado".[5]

El derecho al respeto de la vida privada de las personas tiene, además de su naturaleza de derecho de defensa, el de garantía institucional del *pluralismo y del sistema democrático*.

La democracia se desarrolla y justifica en el respeto de la privacidad de las personas que forman parte de ella, ya que sólo desde el ámbito de reconocimiento de la vida privada y autonomía de cada ciudadano puede construirse una sociedad democrática y libre.

El respeto de la vida privada o de la 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 de las personas adopta un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona; un derecho a la autodeterminación informativa, lo que requiere que las personas puedan conocer la existencia de los ficheros o archivos de registro de información, públicos o privados, sus finalidades y los responsables de ellos, de manera que las personas concernidas puedan conocer los datos contenidos en dichos archivos o ficheros sobre su propia persona, teniendo el derecho de autorizar su recolección, conservación, uso y circulación, como asimismo, el derecho a actualizarla, rectificarla o cancelarla.

La persona es la única que puede autorizar el uso de información respecto de su vida privada; el derecho de autodeterminación informática faculta a las personas a decidir básicamente por sí mismas cuándo y dentro de qué límites procede revelar situaciones o aspectos de su vida privada.

Ello exige que el Estado intervenga positivamente en la materia resguardando este derecho de autodeterminación informativa y estableciendo garantías jurisdiccionales que lo protejan, como ocurre, por ejemplo, con la acción de hábeas data en el derecho comparado.[6]

2. El derecho a la protección de datos de la vida privada de las personas o autodeterminación informativa

El derecho a la protección de datos puede ser definido como el conjunto de normas jurídicas destinadas a asegurar a las personas el respeto de sus derechos,

---

[5] Fulgencio Madrid, 1984, p. 45.

[6] Véase Humberto Nogueira Alcalá: "Reflexiones constitucionales sobre el establecimiento constitucional del hábeas data", en *Ius et Praxis*, año 3, nº 1, Facultad Ciencias Jurídicas y Sociales de la Universidad de Talca (Chile), 1997, p. 265.

especialmente del derecho a la vida privada e intimidad ante el tratamiento automatizado de los datos personales.

2.1. Los principios internacionales elaborados por las Naciones Unidas para proteger la vida privada y la intimidad de las personas de injerencias arbitrarias de carácter tecnológico

El documento del Consejo Económico y Social de las Naciones Unidas E/CN 4/1990/72, de 20 de febrero, recoge la versión revisada de los "Principios rectores para la reglamentación de los ficheros informatizados que contienen datos de carácter personal", elaborada por la Comisión de Derechos Humanos y preparada por Louis Joinet, relator especial. El documento lleva el título *Derechos humanos y desarrollos científico y técnico.*

El campo de aplicación de estos principios abarca *los ficheros públicos y privados,* con la posibilidad de extensión a los ficheros manuales.

Los principios que se proponen en ese proyecto son:

Principio de licitud y de lealtad. La utilización de los ficheros o bases de datos no puede ser contraria a los propósitos y principios de las Naciones Unidas (deportaciones, matanzas, genocidios). Los datos no pueden ser obtenidos o tratados por procedimientos ilícitos o desleales.

Principio de exactitud. Veracidad de los datos y que sean completos y puestos al día periódicamente.

Principio de finalidad. Datos pertinentes a la finalidad perseguida. Que no sean utilizados ni difundidos, salvo acuerdo, con fines incompatibles con el objeto del fichero. Que no se conserven los datos personales más allá del tiempo necesario para cumplir su finalidad.

Principio de acceso. El interesado tiene el derecho de saber si los datos que se refieren a él son conformes con el objeto del fichero. Debe tener acceso de forma inteligible, sin demora ni gastos excesivos. Tiene derecho a obtener las rectificaciones o destrucciones de los datos indebidos (ilícitos, injustificados, inexactos). Cuando se transmitan datos, tiene derecho a conocer los destinatarios.

Régimen de recursos. Debe preverse un régimen de recursos ante la autoridad de control. En caso de rectificación, los gastos serán de cargo del responsable del fichero.

Principio de no discriminación. Significa la prohibición de informaciones sensibles cuya utilización pueda engendrar una discriminación ilegítima o arbitraria.

Estos principios, salvo el de no discriminación, pueden ser derogados tan solo cuando así sea necesario para proteger la seguridad nacional, el orden público, la salud o la moralidad públicas y especialmente los derechos y libertades de los demás.

Pero tales derogaciones han de estar expresamente previstas por ley o por reglamentación equivalente.

Las derogaciones al principio de no discriminación deben hacerse con las mismas garantías y no podrán ser autorizadas más que dentro de los límites previstos por la Declaración Universal de los Derechos Humanos y demás instrumentos relativos a la protección de los derechos humanos y la lucha contra la discriminación.

*Principio de seguridad***.** Se refiere a la protección de los ficheros contra riesgos naturales y humanos (acceso no autorizado, utilización indebida de datos o contaminación por virus).

Control y sanciones. Debe existir una autoridad que, conforme con el sistema jurídico interno, controle el respeto a los principios señalados. Esta autoridad deberá ser imparcial e independiente respecto a las personas u organismos responsables del tratamiento de los datos y de su utilización y tener la adecuada competencia técnica.

Deben, también, preverse las sanciones penales o de otro tipo y los recursos individuales pertinentes.

Junto con los principios rectores, se encuentra la llamada *cláusula humanitaria,* que posibilita excluir la prohibición de registrar datos sensibles, con el objeto de permitir a las organizaciones no gubernamentales (ONG) especializadas en proteger a las personas perseguidas como consecuencia de un trato discriminatorio, basado en el origen racial, la religión, opiniones políticas, entre otras.

A su vez, la ONU estableció la resolución 45/95 de 14 de diciembre de 1990, "Principios rectores para la reglamentación de los ficheros computarizados en datos personales".

2.2. La legislación nacional en Estados Unidos de Norteamérica y en Europa

La mayor parte de los Estados democráticos, conscientes de este problema, han desarrollado leyes de protección de la información personal contenida en bases de datos o en ficheros informáticos de cualquier tipo.

En el ámbito norteamericano aparece el primer modelo sobre la materia, configurándose un conjunto sistemático de normas que regulan el manejo de bancos o registros de datos informatizados. Tales disposiciones son recogidas en dos leyes, el *Freedom of Information Act de 1966* y en la *Privacy Act de 1974.* En tales cuerpos normativos se regula la revelación y transmisión e informaciones y los derechos de acceso, rectificación o modificación de informaciones ya existentes a través de la jurisdicción ordinaria.

En Europa la primera legislación esta dada por la *Data Lag* de 1973 de Suecia; la ley n° 78-17, de 6 de enero de 1978, modificada por la ley 79-587 de 1979 sobre informática, ficheros y libertades, y la ley 79-18 de 1979 sobre archivos, donde se regula entre otras materias el acceso a los archivos públicos de Francia; la *Federal Data Protection Act* de 8/6/78 de Dinamarca; la ley 9/6/78 de Noruega; la *Data and Computer Processing Act* de 1979 de Luxemburgo; la ley de 12 de julio de 1984, sobre protección de datos, de Gran Bretaña; la ley 10/91 de protección de datos per-

sonales frente a la informática y promulgada el 9 de abril de 1991 de Portugal; la *Legge di tutela delle persone a di altri sogetti rispeto al trattamento dei dati personali de 1996* de Italia, la ley orgánica n° 1, de 5 de mayo de 1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, como asimismo, la ley sobre protección de datos de carácter personal 15/1999 de España; entre otros.

En líneas generales, toda la legislación sobre la materia responde a unos mismos principios, recogidos a su vez de la *Convención del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal,* de 1981.

Estos principios son susceptibles de ordenarse en tres grupos:

a) *Derechos de los individuos:* derecho a conocer la existencia de un fichero que contenga información sobre uno mismo; derecho de acceso al fichero; derecho a exigir la corrección de los datos erróneos.

b) *Responsabilidades de los titulares del fichero o base de datos:* recolección imparcial y legal de los datos; garantía de que la recopilación y el almacenamiento de los datos se realiza con una finalidad legítima y concreta, y que la información no se empleará con fines ajenos a los indicados; adecuación entre los objetivos a alcanzar con la configuración del fichero y el número y la calidad de los datos recopilados; exactitud de los datos y, cuando sea necesario, puesta al día de éstos.

c) *Deberes de los usuarios:* fácil identificación del responsable del fichero, gratuidad en el acceso a los ficheros por parte del particular afectado; notificación inmediata de cualquier modificación que se realice; instauración de un régimen de recursos y sanciones.

Junto con estos elementos comunes, las legislaciones nacionales presentan, sin embargo, ciertas diferencias; así, por ejemplo, algunas de ellas atienden no sólo a las bases de datos automatizados sino también a los ficheros manuales.

Otro factor de diferenciación importante está relacionado con el tema del *registro*. En atención a este aspecto, puede distinguirse entre el *modelo sueco* y el *modelo alemán.*

Las leyes inspiradas en la normativa sueca de 1973 establecían un registro central de todos los bancos de datos del país y creaban una Autoridad de Protección de Datos con amplísimas potestades de control sobre los responsables de cada fichero, como ocurre también en el caso español y en la mayoría de las legislaciones europeas.

La legislación alemana parte del principio de la autorregulación, de forma que basta que la ley permita la creación del fichero y que los particulares hayan dado su consentimiento para que el banco de datos quede constituido. Las compañías que los creen tienen la obligación de designar un contralor de datos de la propia compañía, y ésta será la única autoridad competente para supervisar las actuaciones del fichero en cuestión.

2.3. La normativa sudamericana

En el ámbito sudamericano, la regla general ha sido seguir un camino distinto del norteamericano y europeo, estableciendo para la defensa del derecho a la autodeterminación informativa y la protección de datos privados algunos medios procesales específicos, ya sea a través de la generación constitucional de la acción de hábeas data o la utilización de la acción constitucional de amparo o tutela como medio procesal idóneo para tal objetivo.

La excepción la constituye en esta materia el caso chileno, el que ha optado por establecer una ley de protección de datos y un procedimiento judicial específico.

En el constitucionalismo sudamericano, diversas Cartas Fundamentales de las últimas dos décadas del siglo XX incorporan en sus ordenamientos el derecho a la autodeterminación informativa o libertad informática y la institución del hábeas data; tal es el caso de Brasil, Colombia, Paraguay, Perú, Argentina, Ecuador, Venezuela.

En tales Constituciones el hábeas data es regulado junto con las acciones de hábeas corpus y de amparo o tutela, como garantías jurisdiccionales protectoras de la vida privada, intimidad, imagen y honra o buen nombre de las personas.

En Brasil, el artículo 5°, numeral LXXII de la *Constitución de 1988* determina:

> LXXII. Se concede hábeas data:
> a) para asegurar el conocimiento de informaciones relativas a la persona del solicitante contenida en registros o bancos de datos, de entidades gubernamentales o de carácter público;
> b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto o de carácter judicial o administrativo.

A su vez, es necesario tener presente en el mismo artículo 5°, el numeral LXVII, que establece la gratuidad de las acciones de hábeas corpus y hábeas data.

Luego, cronológicamente, será la *Constitución colombiana de 1991* la que en su artículo 15, junto con asegurar el derecho a la intimidad personal y familiar y al buen nombre, afirmará el derecho de hábeas data en los siguientes términos:

> De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en banco de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

Para la protección de este derecho fundamental se utiliza la acción de tutela, según dispone el artículo 42 del decreto 2591 de 1991, que constituye la acción constitucional protectora de los derechos fundamentales en el constitucionalismo colombiano, donde a su vez, la Corte Constitucional ha contribuido a delinear y desarrollar el hábeas data. La Corte Constitucional ha definido el *hábeas data* como:

> […] el derecho que asiste a todas las personas para "conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas", de modo que el individuo disfruta de la posibilidad jurídicamente garantizada de tener acceso a la información acopiada en los referidos

> bancos y archivos, y asimismo de la prerrogativa de solicitar y obtener la rectificación y actualización de informaciones inexactas, erróneas o ya no coincidentes con la realidad, mediante la introducción de las correcciones, aclaraciones o eliminaciones pertinentes.[7]

En *Paraguay, la Constitución de 1992*, en el artículo 135, precisa:

> Toda persona puede 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. Podrá solicitar ante el magistrado competente la actualización, rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos.

La *Constitución peruana de 1993*, en su artículo 2, referente a los derechos fundamentales de las personas, estipula en su numeral 5° el 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 afecten la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional"; a ello se agrega el numeral 6° que dispone el derecho de las personas "A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal o familiar". A su vez, el artículo 200, referente a garantías constitucionales, junto con regular en el numeral 1° la acción de hábeas corpus y en el 2° la acción de amparo, regula en el numeral 3° la acción de hábeas data en los siguientes términos:

> 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 2°, incisos 5 y 6° de la Constitución.

El *Código Procesal Constitucional* recientemente aprobado en 2004, en su título IV regula el proceso de hábeas data, señalando que el procedimiento será el mismo que el previsto en el Código para el proceso de amparo, salvo la exigencia de patrocinio de abogado, que es facultativa en este proceso. Además se faculta al juez para adaptar el procedimiento a las circunstancias del caso.

La *reforma constitucional argentina de 1994*, en el artículo 43, párrafo 3°, regula el hábeas data en conjunto con el hábeas corpus y la acción de amparo, como una subespecie de esta última, en los siguientes términos:

> 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 aquellos. No podrá afectarse el secreto de las fuentes de información periodística.

Para hacer operativo el hábeas data en Argentina se utiliza en términos generales y en principio el procedimiento de la acción de amparo previsto en la ley 16.986, en la medida en que esta institución se considera una variable de dicha acción cons-

---

[7] Sentencia de la Corte Constitucional colombiana T-354/1993.

titucional, sin perjuicio de las adaptaciones necesarias producto de las peculiaridades propias del hábeas data.

En *Ecuador*, la institución se introduce a través de la *reforma constitucional de 1996*, de acuerdo con el texto actual reformado en 1998, que es el texto actualmente vigente, el cual en su capítulo 6° ("de la garantía de los derechos"), regula el hábeas data en su artículo 94, el que señala lo siguiente:

> Art. 94. Toda persona tendrá derecho a acceder a los documentos, bancos e 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.

A su vez, la Ley de Control Constitucional, en su capítulo segundo titulado "Del hábeas data", regula la institución en sus artículos 34 a 45.

La *Constitución de Venezuela de 1999* se refiere al derecho y acción de hábeas data en su artículo 28, en los siguientes términos:

> Toda persona tiene derecho de acceder a la información y a los datos 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 a 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.

Finalmente, la *Constitución de Bolivia* de 1994, a través de la *reforma de febrero de 2004,* introduce en el artículo 23 el derecho a la autodeterminación informativa o libertad informática y el recurso de hábeas data, precisando:

> I. Toda persona que creyere estar indebida 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, a su imagen, a su honra y reputación reconocidos en esta Constitución, podrá interponer el recurso de Hábeas data ante la Corte Superior del Distrito o ante cualquier Juez de Partido a elección suya.
>
> II. Si el tribunal o 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 veinticuatro horas, sin que por ello se suspenda la ejecución del fallo.
>
> IV. El recurso de Hábeas data no procederá para levantar el secreto en materia de prensa.

V. El recurso de Hábeas data se tramitará conforme al procedimiento establecido para el recurso de Amparo Constitucional previsto en el artículo 19° de esta Constitución.

3. El hábeas data: concepto, naturaleza, sujetos activos y pasivos, tipos

3.1. El origen del concepto de hábeas data

La expresión *hábeas data* literalmente significa 'tengas los datos' y su objeto es asegurar el acceso a la información que de la persona afectada tengan registros o bancos de datos públicos o privados, con el objeto de proteger la vida privada, intimidad, imagen, buena reputación u honra de las personas.

3.2. Naturaleza del hábeas data

El hábeas data constituye una acción jurisdiccional protectora de la libertad informática o derecho de autodeterminación informativa (conocimiento y control de datos referidos a la persona) y protección de la vida privada, imagen, honra o reputación de la persona, frente a la recolección, transmisión y publicidad de información que forma parte de la vida privada o intimidad de la persona desarrollada por registros o bancos de datos públicos o privados.

En tal sentido, Pérez Luño señala:

> El *hábeas data* constituye, en suma, un cauce procesal para salvaguardar la libertad de la persona en la esfera informática, que cumple una función paralela, en el seno de los derechos humanos de la tercera generación, la que en la primera generación correspondió al *hábeas corpus* respecto de la libertad física o de movimiento de las personas.[8]

En diversos países de América del Sur, como es el caso de Argentina, Bolivia, Colombia, Paraguay, Perú y Venezuela, esta acción jurisdiccional forma parte de las acciones constitucionales protectoras de derechos fundamentales, como hemos reseñado en el punto 8.3. En algunos casos tal acción opera con un procedimiento autónomo y en otras oportunidades opera a través de la acción de amparo o tutela de derechos fundamentales.

Es necesario precisar que algunos textos constitucionales latinoamericanos, además de considerar el *hábeas data* como una *acción o proceso constitucional* (Argentina, Bolivia, Brasil, Ecuador, Paraguay, Perú), también la consideran como un *derecho fundamental* (Colombia y Venezuela).

---

[8] Antonio Pérez Luño: *Del "hábeas corpus" al "hábeas data"*, Madrid, Aranzadi, 1991, p. 174.

3.3. Sujetos activo y pasivo de hábeas data

El sujeto activo del hábeas data en el ámbito sudamericano es toda persona, nacional o extranjera, la que puede actuar personalmente o a través de su representante legal, según determinen las respectivas legislaciones.

Los sujetos pasivos son los bancos de datos y archivos de entidades tanto públicas como privadas, computarizados o no. En algunos casos, como los de Brasil y Paraguay, se limita el hábeas data en forma poco aconsejable solamente a entidades gubernamentales o de carácter público, dejando a las personas sin protección frente a las archivos y bancos de datos privados.

Debe señalarse que se excluyen como sujetos pasivos de hábeas data los registros privados de carácter personal que no estén destinados a proveer informes a terceros, ya que se encuentran protegidos por el derecho a la inviolabilidad de los documentos privados, protegido constitucionalmente.

Asimismo, parece importante explicitar en los respectivos ordenamientos jurídicos la exclusión del hábeas data en materia de archivos y fuentes de información periodísticas, como lo hacen las constituciones de Venezuela y Bolivia, con redacciones diferentes.

3.4. Los tipos de hábeas data

Puccinelli, utilizando la clasificación previa de Sagüés,[9] distingue diversos tipos de hábeas data,[10] atendiendo a las facultades que la normativa reconoce a los sujetos activos legitimados para interponer la acción o recurso:

a) El *hábeas data informativo.* Es aquel que busca lograr el acceso al registro o base de datos respectivo, con la finalidad de obtener la información contenida o tratada en él. Éste puede adoptar tres subtipos: 1) *exhibitorio,* el que se agota en el conocimiento de los datos contenidos en dicha base de datos; 2) *finalista*, que busca, además de conocer los datos contenidos en el registro o base de datos, determinar para qué y con que fin se realizó el registro de datos; 3) *autoral*, cuyo objetivo es determinar quién obtuvo los datos que se encuentran en el registro o banco de datos.

b) El *hábeas data aditivo.* Este tipo procura agregar más datos a los existentes en el registro o banco de datos respectivo, y puede adoptar dos subtipos: 1) *actualizador,* que es aquel que procura actualizar o renovar los datos vetustos o superados que existen en el registro o base de datos; 2) *inclusorio*, que tiene por objeto agregar o incluir en la base o registro datos que habían sido omitidos; 3) *aclaratorio,* cuyo objeto es precisar las circunstancias o calidad en que la persona se encuentra afectada

---

[9] Néstor Pedro Sagüés: "Subtipos de hábeas data", en *Jurisprudencia Argentina*, 20/12/1995, pp. 31 y ss.

[10] Puccinelli: o. cit., pp. 221-225.

por el dato; por ejemplo, clarificar, frente a un registro de deudores morosos, que no es la persona el deudor principal sino sólo un garante de la obligación contraída.

c) El *hábeas data rectificador o correctivo*. Su objeto o finalidad es el de enmendar informaciones o datos falsos, erróneos, inexactos o ambiguos, obteniendo su corrección.

d) El *hábeas data reservador.* Esta modalidad tiene por objeto asegurar que un dato legítima y correctamente registrado sólo pueda ser utilizado por quienes se encuentran autorizados para ello y con los fines especificados legalmente, impidiendo que dicha información sea transmitida a terceros no autorizados para su conocimiento.

e) El *hábeas data cancelatorio.* La finalidad de este tipo es eliminar la información almacenada en el registro o banco de datos por tratarse de información sensible, por corresponder a la intimidad de la persona o por no encontrarse autorizado su registro.

f) El *hábeas data disociador.* Busca separar el uso estadístico legítimo del dato, de la información sobre la persona a la cual el dato corresponde.

g) El *hábeas data asegurador*. Su fin es dotar de seguridad los datos contenidos en el registro o base de datos, exigiendo el desarrollo de procedimientos técnicos que eviten la fuga de datos o el acceso a la base de personas no autorizadas para ello.

h) El *hábeas data reparador.* Es aquel tipo en el que, comprobados los daños sufridos por la persona por registro de información sensible o de su vida íntima, o comprobada la transmisión de datos reservados o la transmisión de datos falsos o erróneos que han producido un daño en los derechos de la persona afectada, a través del hábeas data el tribunal ordena una indemnización por el daño causado a la persona por el responsable del banco o registro de datos.

4. La Ley de Protección de Datos Personales de Chile

En Chile, a diferencia de muchos países sudamericanos, no existe el derecho constitucional explícitamente contemplado referente a la libertad informática o autodeterminación informativa, como tampoco se ha articulado constitucionalmente una acción de hábeas data. El tema se incorporó a la agenda legislativa sólo en la segunda mitad de la última década del siglo XX, de donde surge la ley n° 19.628, que otorga una protección a los datos que pudieren afectar el derecho al respeto de la vida privada de las personas y su honra.

En la elaboración de la ley se tuvo presente un proyecto elaborado por una comisión designada por el Ministerio de Justicia durante el gobierno del presidente Aylwin (1990-1994), que contenía disposiciones tendentes a regular la recolección y el procesamiento de datos personales, los principios que deberían regular una efectiva protección de la intimidad y, respecto de la acción de hábeas data,[11] información

[11] "El hábeas data o protección de datos personales, establece las garantías mínimas de calidad y confiabilidad de los datos nominativos o personales que se recojan; el derecho de las personas a

complementaria de la comisión obtenida durante la tramitación del proyecto de ley que dio origen a la ley n° 19.223, que tipifica figuras penales relativas a la informática, y del proyecto de ley sobre libertades de opinión y de información. Además, se puso a disposición la legislación comparada existente sobre la materia.

La ley busca armonizar tres ámbitos de intereses:

El primer ámbito corresponde al *empresarial privado,* que es el formado por los consumidores de informática y por los productores de informática, que son quienes elaboran, distribuyen y comercializan productos informáticos.

El segundo ámbito corresponde al *público,* en el que los datos pueden proporcionarse a los particulares interesados o al público en general, debiendo protegerse el procesamiento de datos y la información de seguridad.

El tercer ámbito corresponde al de los *derechos del afectado* por la utilización de datos personales.

4.1. Principios generales que informan la materia

El texto legal armoniza y complementa el derecho que tiene toda persona de efectuar el tratamiento de datos, con el respeto al pleno ejercicio de los derechos de las personas sobre ellos.

En su artículo segundo, literal *o*, la ley señala que el tratamiento de datos comprende toda operación o procedimiento técnico que permita recolectar, almacenar, gravar, organizar, elaborar, seleccionar, confrontar, interconectar, disociar, procesar, comunicar, ceder, transferir, transmitir, cancelar o utilizar de cualquier forma datos personales.

A su vez, el artículo 2°, en su literal *f*, precisa que los datos personales son aquellos "relativos a cualquier información concerniente a personas naturales, identificadas o identificables".

No le pareció adecuado al legislador distinguir entre datos de carácter íntimo, de carácter privado y de carácter público. Se tuvo en cuenta, al efecto, que la Constitución Política diferencia solamente entre la vida privada y la vida pública de las

---

exigir que sus datos personales les sean exhibidos; el derecho a que sean rectificados, y el derecho a excluir los datos privados mantenidos sin autorización. Se le grafica de la forma siguiente: Dime qué sabes de mí; dime por qué lo sabes; dime para qué los tienes; si no sabes para qué los tienes, bórralos; si sabes para qué los tienes, dímelo y deja que yo te autorice; si esa información es errónea, déjame rectificarla.

"Muéstrame los datos que tienes de mí por lo menos una vez al año y mándame a mi domicilio toda la información que tienes recopilada sobre mí; si esa información es errónea déjame corregirla; si esa información ha sido alterada por el tiempo, porque mi situación cambió, pues de girador doloso de cheques me he convertido en un recto personaje de la sociedad, entonces déjame ahora mejorar mi estado; si tú no sabes para qué tienes la información sobre mí, bórrala, y si no la borras, por lo menos no podrás usarla en mi contra porque yo no te lo autorizo" (o. cit., pp. 103-104).

personas, y que la distinción entre lo íntimo y lo privado responde solamente a una determinada teoría o modelo analítico. En efecto, la *teoría de las esferas* diferencia entre lo íntimo, que correspondería a un círculo más interno, y lo privado, que equivaldría a un círculo concéntrico más amplio. Esta teoría ha sido reemplazada por la *teoría de los mosaicos*, cuyo presupuesto es que lo privado y lo público son relativos en función de quién sea el otro sujeto en la relación informativa, sin que haya informaciones o datos en sí privados o públicos.

El literal *g* del artículo 2º de la ley se refiere a los *datos sensibles*. Al respecto tuvo en consideración la legislación española, en cuyo artículo 7º los datos sensibles se consideran como datos especialmente protegidos. El legislador chileno asume tal conceptualización al incluir los datos sensibles como una especie dentro de la definición de los datos de carácter personal. Tales *datos sensibles* son aquellos datos personales que se refieren a las características físicas o morales de las personas, o a hechos o circunstancias de su vida privada tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias y convicciones religiosas, los estados de salud físicos y psíquicos y la vida sexual. Los antecedentes o hechos de la vida privada que corresponden a la denominada *información sensible* son reservados, por lo que su publicidad requiere del consentimiento del afectado o estar autorizada expresamente por una ley excepcional.

El tratamiento de datos que regula la ley es, como señala el artículo 2°, literal *m*, aquel que se hace en registros o bancos de datos, conceptualizados como conjuntos organizados de datos personales, manuales o automatizados, que permiten relacionar los datos entre sí y realizar todo tipo de tratamiento de ellos.

Tales bases de datos pueden ser desarrolladas por entes públicos o privados, sin establecerse diferencias entre ellos; todos quedan sujetos a las mismas regulaciones de la ley en análisis.

La ley dispone que la recolección, el procesamiento y la utilización de los datos personales se sujetarán a las disposiciones contenidas en la misma norma para proteger a las personas por el uso que terceros pueden hacer de sus datos personales. Establece que la información organizada es reservada y que *el que autoriza el registro de la información es el legislador o quien sea facultado por los interesados.*

La ley excluye de su regulación el tratamiento de datos personales que se concreta en ejercicio del derecho de libertad de opinión e información, lo que es regulado por la Ley n° 19.733 sobre Libertades de Opinión e Información y Ejercicio del Periodismo.

El objetivo de la ley es asegurar *el derecho de autodeterminación informativa de las personas* respecto de los datos personales tratados en bancos de datos o registrados en otros soportes, sea que se realice por particulares o por órganos del Estado, con el fin de garantizar el pleno respeto y ejercicio de los derechos fundamentales.

La ley reconoce la conveniencia social de las bases de datos, la utilidad de bancos de datos que den sustento al sistema crediticio (artículo 4°), al sistema previ-

sional y de salud (artículo 10), impositivo del Estado (artículos 15 y 20) y con información procesal y penal (artículo 21) y muchas otras actividades, entre las cuales se encuentran el Registro Civil y el Registro Electoral.

El tratamiento de los datos por parte del banco o registro de datos debe realizarse respetando los derechos fundamentales de las personas titulares de los datos y las facultades concedidas a estos últimos por la misma ley.

La ley posibilita el tratamiento de datos personales cuando la persona afectada lo autoriza o cuando tal autorización está determinada por los preceptos legales (artículo 4°).

La autorización que da la persona afectada debe ser por escrito e informada de la finalidad de la base de datos y de si ella es o no accesible al público. La autorización otorgada por el afectado puede ser revocada sin efecto retroactivo.

Puede sostenerse así la existencia de una *disponibilidad privada* del afectado o titular del dato, el que debe dar su consentimiento para la recogida y el tratamiento de los datos, como asimismo tiene el derecho a obtener información sobre sus datos incluidos en un archivo o fichero, así como la posibilidad de rectificar, completar o cancelar dichos datos en su caso, salvo disposición legal en contrario.

La ley puede autorizar el tratamiento de datos personales cuando ellos provienen de fuente públicas; cuando se trate de datos personales que procesen personas jurídicas privadas para uso de sí mismas o de sus asociados o afiliados y se traten sólo con fines estadísticos de tarificación o de beneficio general; cuando el tratamiento de datos personales lo realicen personas u organismos públicos respecto de materias de su competencia, o bien para el otorgamiento de servicios de salud que correspondan a sus titulares.

La ley busca proteger, respecto de las bases de datos personales, la vida privada, honra e imagen de la persona, además de la veracidad de los datos.

4.2. La protección de los derechos de los titulares de los datos

La ley reconoce a la persona un conjunto de facultades para cautelar tales derechos fundamentales y bienes constitucionales.

Los datos personales sólo pueden recolectarse, procesarse, transmitirse y difundirse para la finalidad para la que, lícitamente, se hubieren recogido.

El responsable del registro debe adoptar las medidas técnicas que garanticen la seguridad de los datos contenidos en su base de datos.

Asimismo, el responsable del archivo automatizado y quienes intervengan en las distintas fases del tratamiento de los datos deben guardar el secreto profesional o confidencialidad sobre ellos, según dispone la ley en su artículo 7°. A su vez, la ley obliga al responsable de la base de datos a actuar con la debida diligencia y determina su responsabilidad por los daños ocasionados al titular de los datos; éstos no pueden ser comunicados a personas no autorizadas, según dispone el artículo 11° de la ley.

Los datos registrados, una vez que se cumpla con el propósito para el cual fueron recolectados, deben ser cancelados.

La ley puede, excepcionalmente, autorizar la desviación del fin para el cual se recolectó el dato, sólo con el objeto de evitar una amenaza inminente al orden público o una violación grave de derechos de terceros.

Así, la legislación busca evitar que los datos de carácter personal existentes en bases informáticas, que reúnen antecedentes confidenciales sobre las personas recolectados con una finalidad determinada, sean utilizados con otros propósitos sin el permiso del sujeto de la información, como precisa el artículo 9° de la ley.

La persona tiene el derecho de conocer la información que haya sobre ella en estas bases de datos personales y el derecho de oponerse a que esos datos sean utilizados con otros fines diferentes de aquellos autorizados, así como el derecho de exigir que se corrijan los datos erróneos o inexactos.

La ley establece los límites hasta donde una persona puede aceptar que sus datos personales sean públicos y que una determinada parte de ellos, los datos sensibles, no puedan ser objeto de transacción ni de transferencia, bajo ningún título, a otra persona.

Así, el que procese legítimamente datos relativos a la vida privada de las personas sólo puede revelarlos o utilizarlos para aquellas finalidades que hayan sido autorizadas por la ley o consentidas por los afectados.

Los artículos 12 a 15 de la ley regulan las facultades de las personas en resguardo de sus datos personales.

Se establece el derecho de toda persona a que el usuario de datos procesados le suministre una copia de los antecedentes que tenga en su poder, con indicación de su fuente de origen, dentro de un plazo determinado por la ley, contado desde la solicitud. Se permite que el juez pueda apremiar al usuario de datos procesados a través de la informática, si se niega a entregar copia a la persona afectada.

El mismo derecho anterior tienen las personas respecto de los datos personales si éstos fueren inexactos, incompletos, equívocos o atrasados; en tal caso, la persona afectada tiene derecho a exigir que se rectifiquen, completen, aclaren o actualicen, debiendo proporcionársele copia del registro modificado.

La persona también tiene el derecho a exigir que se supriman tales antecedentes, si estuvieren caducos o hubieren sido obtenidos fuera de los casos autorizados por la ley. Lo mismo puede hacer si, habiendo proporcionado sus datos personales voluntariamente, no deseare continuar figurando en el registro respectivo.

La ley establece el derecho de la persona afectada por el uso de datos personales incorrectos, a ser indemnizada por quien los haya proporcionado.

El artículo 15 de la ley establece algunas excepciones al bloqueo, la eliminación o modificación de datos, cuando tales facultades impiden o dificultan el debido cumplimiento de funciones fiscalizadoras del organismo público pertinente, afectan la

reserva o el secreto previsto en leyes o reglamentos, o afectan la seguridad o el interés nacional, o cuando dichas facultades no hayan sido concedidas al titular en el precepto legal que determina el almacenamiento de los datos.

4.3. Algunas deficiencias de la ley en el resguardo de los derechos de los titulares de los datos y en la supervigilancia de las bases de datos

El legislador no reguló el establecimiento de un órgano de control independiente en el cual las bases de datos debieran registrar su existencia, órgano que cumple también en el derecho comparado europeo una función fiscalizadora y sancionadora, lo cual posibilita a los titulares de los datos conocer quiénes los están utilizando, con qué fines los están tratando y si ellos son o no comunicados a terceros. Al no establecerse la obligación de registro de los bancos de datos privados y al no generarse un órgano de supervisión y control encargado de velar por el cumplimiento de la ley, el sistema de protección estructurado es muy débil.

El control de legalidad establecido por la ley chilena es a posteriori por parte del titular de los datos, quien ejerce los derechos que concede la ley ante el responsable de la base o banco de datos público o privado, ante los tribunales de justicia de una acción legal prevista en el artículo 16 de la Ley de Protección a la Vida Privada, a diferencia de una gran parte de los países de América del Sur, entre ellos, Argentina, Brasil, Colombia, Perú, Paraguay, donde existe la consagración constitucional de una acción de hábeas data.

En todo caso, consideramos procedente en Chile el uso de la acción constitucional de protección establecida en el artículo 20 de la Carta Fundamental, en protección del derecho a la vida privada (artículo 19, nº 4) y el derecho de propiedad (artículo 19, nº 24) sobre los datos personales.

4.4. Las modalidades que reviste la acción jurisdiccional en resguardo de los derechos de los titulares de los datos personales

La ley asegura el derecho de las personas de solicitar judicial o extrajudicialmente la exhibición de bases o bancos de datos, sean públicos o privados, en los cuales estén registrados sus datos personales, con el objeto de verificar su exactitud y su veracidad o, en su caso, solicitar su rectificación, eliminación, complementación o reserva.

La acción puede tener un carácter preventivo o correctivo. En su dimensión preventiva tiene por objeto conocer la existencia de registros o bancos de datos que contengan informaciones de las que sea titular y acceder a ellas. La acción en su dimensión correctiva consiste en exigir que determinados datos personales del titular sean corregidos, rectificados, cancelados o bloqueados, por el hecho de que su tratamiento es ilegal y conculca derechos fundamentales.

4.4.1. Los bienes jurídicos protegidos

La acción resguarda como bien jurídico básico el derecho a la autodeterminación informativa, como asimismo, el derecho a la protección de la vida privada o privacidad y la honra de la persona, la igualdad ante la ley, la protección de la dignidad humana y la libertad, así como la veracidad y fidelidad de la información.

4.4.2. Tribunal competente

El tribunal competente para conocer de esta acción es el juez civil de turno correspondiente al domicilio del responsable del banco del registro o base de datos correspondiente, vale decir, el domicilio del demandado, que es la regla general en materia de competencia relativa en el ordenamiento jurídico chileno, de acuerdo con el artículo 134 del Código Orgánico de Tribunales.

4.4.3. Legitimación activa

El legitimado activamente para interponer la acción es el titular de los datos que ha visto vulnerado sus derechos reconocidos por la ley, y que solicita protección y amparo al tribunal competente.

4.4.4. Legitimación pasiva

El legitimado pasivo es el responsable del banco de datos, sea particular o público. Asimismo, la ley establece, en su artículo 14, una regla especial, la que determina que en el evento en que los datos personales se encuentren en una base de datos a la cual tienen acceso diversos organismos, el titular de los datos puede demandar la información a cualquiera de ellos, en cuyo caso, los sujetos pasivos pueden ser dos o más organismos privados o públicos.

4.4.5. El procedimiento judicial

El procedimiento judicial se desdobla en dos procedimientos diferentes, de acuerdo con el artículo 16 de la ley, dependiendo de la causal que da origen a la acción.

4.4.5.1. El procedimiento regular u ordinario

El primero se sitúa en la hipótesis de la falta de pronunciamiento del responsable del banco o registro de datos, dentro de los dos días hábiles siguientes a la solicitud presentada por el titular de los datos, o cuando el primero le niegue al segundo la información por una causal diferente de la de seguridad de la nación o de interés nacional. La segunda hipótesis ocurre cuando se vulneran los artículos 17 y 18 de la

ley 19.628, en cuyo caso la acción presentada ante el juez debe contener, por lo menos, una identificación clara de la infracción cometida por el responsable de la base de datos y los hechos que le dan forma, acompañándose los medios de prueba que los acrediten.

En ambas hipótesis se desarrolla el procedimiento que podemos denominar regular u ordinario.

La acción se notifica por cédula en el domicilio del banco de datos respectivo, el que debe contestar el traslado dentro de quinto día hábil, estableciendo sus descargos y adjuntando los medios de prueba en que se fundan. Si no tiene medios de prueba, deberá explicitarlo. Si el demandado ofrece prueba, el tribunal debe fijar una audiencia, para el quinto día hábil con la finalidad de recibir la prueba ofrecida que no ha acompañado.[12]

El tribunal puede adoptar todas las medidas cautelares que considere adecuadas para hacer efectiva la protección de los derechos que la ley asegura, de acuerdo con lo establecido en el artículo 23 de la ley.

La prueba rendida por las partes se aprecia en conciencia por el tribunal competente.

La sentencia definitiva se dicta dentro del tercer día de vencido el plazo para presentar los descargos, se hayan presentado éstos o no. Si el tribunal decretó una audiencia de prueba, el plazo se contará una vez vencido el plazo fijado para rendir la prueba.

La sentencia definitiva se notifica por cédula y es apelable en ambos efectos.

El recurso de apelación debe interponerse en el término fatal de cinco días, contado desde la notificación de la parte que lo entabla. El escrito de apelación debe contener los fundamentos de hecho y derecho en que se apoya y las peticiones concretas que se formulan.

Deducida la apelación, el tribunal debe elevar los autos a la Corte de Apelaciones respectiva; recibidos éstos en la secretaría de la Corte, el presidente ordenará dar cuenta preferente del recurso sin esperar la comparecencia de las partes, según determina el artículo 16, literal *g* de la ley.

Si la Corte lo estimase conveniente o se solicitase con fundamento plausible, podrá ordenar que los autos se traigan en relación y se oigan alegatos de los abogados de las partes, en cuyo caso la causa se agregará extraordinariamente a la tabla respectiva de la Sala.

Dicho fallo no es susceptible de casación; sin embargo, procede el recurso de queja, todo ello de acuerdo con el artículo 545 del Código Orgánico de Tribunales.

---

[12] Esta facultad otorgada al responsable de la base de datos y demandado, de determinar la existencia o no de una audiencia de prueba, que no tiene el ocurrente, rompe el principio de igualdad de armas procesales y de bilateralidad de la audiencia, lo que afecta centralmente el derecho constitucional a una racional y justa investigación y procedimiento determinado por el artículo 19, nº 3, de la Constitución.

4.4.5.2. El procedimiento especial en caso de considerarse afectada la seguridad o el interés nacional

Cuando el responsable de la base de datos se ha negado a entregar la información argumentando razones de seguridad o interés nacional, la reclamación es conocida directamente por la Corte Suprema de Justicia, la que pedirá informe al responsable de la base de datos de la manera más expedita posible, fijándole un plazo para la entrega de los antecedentes. Una vez vencido el plazo otorgado resolverá en cuenta.

En el caso de recibirse la causa a prueba, ella se consignará en un cuaderno separado y reservado.

La sala de la Corte Suprema que conoce de la acción puede, si lo estima pertinente o se le solicita con fundamento plausible, ordenar traer los autos en relación, en cuyo caso la causa se agrega extraordinariamente a la tabla y la audiencia no es pública.

4.4.5.3. Procedimiento residual

La ley prevé, en el caso de infracciones no contempladas en los artículos 12 y 19, la aplicación de un procedimiento sumario determinado en el artículo 23. Es el caso, entre otros, de cuando el responsable del registro o base de datos no cumple con avisar a terceros que los datos han sido cancelados o corregidos, o si un organismo público desarrolla una base e datos en ámbitos ajenos a su competencia.

4.4.6. Sanciones establecidas por la sentencia

En la sentencia que acoge la reclamación el tribunal fija un plazo prudencial para que el banco o registro de datos dé cumplimiento a lo ordenado. Puede adicionalmente sancionar al infractor con una multa de una a diez unidades tributarias mensuales, como asimismo determinar los perjuicios si le han sido solicitados, todo ello de acuerdo con los artículo 16, numeral 5°, y artículo 23 de la ley. En el caso de infracción a los artículos 17 y 18, referentes a datos personales de carácter económico, financiero, comercial o bancario, la multa asciende de 10 a 50 unidades tributarias mensuales, según lo dispuesto en la ley nº 19.812.

Si el responsable de la base de datos no cumple dentro del plazo otorgado por el tribunal, éste puede aplicar una multa de 2 a 50 unidades tributarias mensuales. A su vez, si se trata el requerido de un organismo público, el tribunal puede sancionar al jefe del servicio con suspensión de su cargo de 5 a 15 días.

Las sanciones, como puede observarse, son muy débiles y exiguas.

4.4.7. La indemnización de perjuicios

El monto de la indemnización de perjuicios será establecido prudencialmente por el tribunal atendiendo a la gravedad de los hechos y las circunstancias de cada caso.

La acción de indemnización de perjuicios que se contempla puede concretarse a través de tres vías diferentes. La primera es a través del procedimiento previsto en el artículo 23 del cuerpo legal que posibilita interponer la acción indemnizatoria conjuntamente con la reclamación destinada a solucionar la infracción reclamada.

El segundo procedimiento es mediante el juicio sumario referente a las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de perjuicios.

El tercer procedimiento es mediante una acción de indemnización de perjuicios en un procedimiento ordinario, de acuerdo con las reglas generales.

Bibliografía

BENDA, Ernst, y otros: *Manual de derecho constitucional*, Madrid, Marcial Pons, 1996.

BERTELSEN R., Raúl, y otros: *Tratamiento de datos personales y protección de la vida privada*, Cuadernos de Extensión Jurídica, n° 5, Facultad de Derecho, Universidad de los Andes, Santiago (Chile), 2001.

DAVARA RODRÍGUEZ, Miguel Ángel: *La protección de datos en Europa*, Madrid, Universidad de Comillas, 1998.

EKMEDKJIÁN, Miguel Ángel: *Tratado elemental de derecho constitucional*, tomo I, Buenos Aires, Depalma, 1993.

ESTADELLA YUSTE, Olga: *La protección de la intimidad frente a la transmisión internacional de datos personales*, Madrid, Tecnos, 1995.

DÍAZ, Francisco, y Luis Eugenio OLIVER: *Informática y derecho: derecho informático*, Madrid, UNED, 1998.

ESPINOSA SALDAÑA BARRERA, Eloy: *Jurisdicción constitucional, impartición de justicia y debido proceso*, Lima, ARA, 2003.

FERNÁNDEZ ESTEBAN, María Luisa: *Nuevas tecnologías, Internet y derechos fundamentales*, Madrid, Mc-Graw Hill, 1998.

GOZAÍNI, Osvaldo (coord.): *La defensa de la intimidad y los datos personales a través del hábeas data*, Buenos Aires, Ediar, 2001.

— *Derecho procesal constitucional: hábeas data*, Buenos Aires, Rubinzal-Culzoni.

LANDA, César: *Teoría del derecho procesal constitucional*, Lima, Palestra, 2004.

LETE DEL RÍO, J. M.: *Derechos de la persona*, Madrid, Tecnos, 1996.

LOSANO, Mario: *Il diritto pubblico dell'informatica*, Giulio Einaudi, 1986.

LUCAS MURILLO, Pablo: *El derecho a la autodeterminación informativa*, Madrid, Tecnos, 1990.

NOGUEIRA ALCALÁ, Humberto: *La libertad de información y sus límites. Honor y vida privada*, Santiago, Lexis Nexis, 2002.

NOVOA MONREAL: *Derecho a la vida privada y libertad de información. Un conflicto de derechos***,** Madrid, Siglo XXI, 1979.

ORTECHO VILLENA, Víctor Julio: *Jurisdicción y procesos constitucionales*, 7ª ed., Lima, Rodhas, 2003.

PECES-BARBA, Gregorio: *Curso de derechos fundamentales. Teoría general*, Madrid, Universidad Carlos III, 1995.

PÉREZ LUÑO, Antonio: *Libertad informática y leyes de protección de datos personales*, Madrid, Centro de Estudios Constitucionales, 1989.

— 1996: *Manual de informática y derecho*, Barcelona, Ariel Derecho.

PUCCINELLI, Óscar: *El hábeas data en Indoiberoamérica*, Santafé de Bogotá, Temis. 1999.

SAGÜÉS, Néstor Pedro: *Elementos de derecho constitucional*, Buenos Aires, Astrea, 1997.

— *Derecho procesal constitucional*, tomo III: Acción de amparo, Buenos Aires, Astrea, 2002.

SARAZA JIMENA, Rafael: *Libertad de expresión e información frente a honor, intimidad y propia imagen*, Pamplona, Aranzadi, 1995.

UICICH, Rodolfo Daniel: Los bancos de datos y el derecho a la intimidad, Buenos Aires, Ad-Hoc, 1999.

ULL PONT, Eugenio: *Derecho público de la informática (Protección de los datos de carácter personal)*, Madrid, UNED, 2000.

WARREN, E. D., y L. D. BRANDEIS: *El derecho a la intimidad* (traducción española de *The Right to privacy*), Introducción de Benigno Pendás, Madrid, Civitas, 1994.

WESTIN, Alan F.: *Privacy and Freedom*, 7ª ed., Nueva York, Atheneum, 1970.

Artículos y monografías

BAZÁN, Víctor: "Hábeas data y autodeterminación informativa", en *Revista Jurídica del Perú*, año XLVI, n°3, Trujillo, julio-septiembre de 1996.

GARCÍA BELAUNDE, Domingo: "Sobre el hábeas data y su tutela", en *Ius et Praxis. Derecho en la región*, año 3, n° 1, Talca, Universidad de Talca, 1997.

ESPÍN TEMPLADO, Eduardo: "Fundamento y alcance del derecho fundamental a la inviolabilidad del domicilio", en *Revista del centro de estudios Constitucionales*, n° 8, Madrid, 1991.

FERNÁNDEZ RODRÍGUEZ, José Julio: "¿Regular internet? Una reflexion sobre los límites del derecho y las funciones del Estado", en Víctor Bazán (coord.): *Defen-*

sa de la Constitución, garantismo y controles. Libro en reconocimiento al Dr. Germán Bidart Campos, Buenos Aires, Ediar, 2003, pp. 487-494.

HOFFMANN-REIN, Wolfgang, en Ernst Benda y otros: *Manual de derecho constitucional*, Madrid, Marcial Pons. 1996.

HERRERA BRAVO, Rodolfo: "La protección de datos personales como una garantía básica de los derechos fundamentales", en *Revista de Derecho Público, de la Agrupación de Abogados de la Contraloría General de la República***,** año 2, nº 5, mayo-agosto 2001.

— "Privacidad e internet: el problema del tratamiento invisible y automatizado de datos personales", en *Revista de Derecho Público, de la Agrupación de Abogados de la Contraloría General de la República,* año 2, nº 6, septiembre-diciembre 2002.

JERVIS ORTIZ, Paula: "Derechos del titular de datos y Hábeas data en la Ley 19.628", en *Revista Chilena de Derecho Informático*, Santiago, Facultad de Derecho, Universidad de Chile, 2003.

NOGUEIRA ALCALÁ, Humberto: "Reflexiones constitucionales sobre el establecimiento constitucional del hábeas data", en *Ius et Praxis*, año 3, n° 1, Talca, Facultad de Ciencias Jurídicas y Sociales, 1997, p. 265.

RIQUERT, Fabián Luis: "El derecho a la intimidad y su relación con las nuevas tecnologías", en Víctor Bazán (coord.): *Defensa de la Constitución, garantismo y controles. Libro en reconocimiento al Dr. Germán Bidart Campos*, Buenos Aires, Ediar, 2003, pp. 479-486**.**

SAGÜÉS, Néstor Pedro: "Subtipos de hábeas data", en *Jurisprudencia Argentina*, Buenos Aires, 20 de diciembre de 1995.