La protección de datos y el *habeas data* en Chile

Emilio Oñate Vera

Abogado, Lic. en Ciencias Jurídicas y Sociales de la Universidad Central de Chile. Magister en Gerencia y Políticas Públicas de la Universidad Adolfo Ibáñez. Magister en Derecho Administrativo de la Pontificia Universidad Católica de Valparaíso. Profesor asociado de Derecho Administrativo. Decano de la Facultad de Derecho y Humanidades de la Universidad Central de Chile.

Resumen

Este trabajo aborda el desarrollo de la protección de datos desde su regulación legislativa en Chile, con la Ley 19.628, hasta el reconocimiento constitucional de la protección de datos como derecho fundamental. También se analiza el procedimiento de garantía previsto en la señalada ley, denominado *habeas data* para tutelar este derecho, estudiando sus principales falencias, lo que pone en evidencia la urgente necesidad de una nueva ley que no solo mejore el procedimiento para el resguardo de tal derecho, sino que además sirva de sustento para la generación de una nueva institucionalidad en la materia.

Palabras clave: Protección de datos, *habeas data*, derechos fundamentales.

Abstract

*This work addresses the development of data protection from its legislative regulation in Chile, with Law 19,628, to the constitutional recognition of data protection as a fundamental right. The guaranteed procedure provided for in the aforementioned law to protect this right, called *habeas data*, is also analyzed, by highlighting its main shortcomings, which renders evidence of the urgent need for a new law that not only improves the procedure for the protection of such a right, but also serves as support for the generation of a new institutionalality in the matter.*

Key words: Data protection, *habeas data*, fundamental rights.

1. La protección de datos en Chile

El 28 de agosto de 1999, se publica en el Diario Oficial chileno la Ley N.º 19.628 sobre protección a la vida privada¹, también conocida como ley de protección de datos

¹ Como se puede apreciar, el título de la ley limita la protección de datos a la vida privada y no reconoce —a causa del legislador de la época, seguramente de manera involuntaria— la autonomía e independencia de

personales. Esta se estructura en un título preliminar, cinco títulos y un título final. El título preliminar se refiere a las disposiciones generales que determinan el objeto de la ley, sus límites, así como la definición de ciertas y determinadas palabras; el título primero se refiere a la utilización de los datos personales y, sustancialmente, aborda los principios en que se sustenta la protección de datos personales que tienen por finalidad resguardar su adecuado tratamiento; en el título segundo, se abordan los derechos de los titulares de datos, donde se distingue entre los derechos de acceso, rectificación, cancelación y bloqueo; el título tercero hace referencia a la utilización de datos personales relativos a obligaciones de carácter económico; el título cuarto se refiere al tratamiento de datos por los organismos públicos; el título quinto aborda la responsabilidades generadas por las infracciones a la ley, y por último, el título final se refiere, en un solo artículo, el 24, a introducir una modificación al Código Sanitario Chileno, otorgándole la calidad de reservados a las recetas médicas, exámenes de laboratorios y servicios relacionados con la salud en general².

La finalidad de esta ley es tutelar la información relativa a personas naturales, garantizando que, en definitiva, sean ellas las que decidan sobre su uso o tratamiento.

Se podría decir que la ley chilena, con casi tres décadas de diferencia, fue heredera de una serie de iniciativas legislativas provenientes, principalmente, de Europa, en la que diversos países, a finales de la década del sesenta y durante la década del setenta, empezaron a dictar leyes que regularon la protección de los datos personales, iniciativas legislativas que, evidentemente, fueron detrás del vertiginoso desarrollo informático y tecnológico. Lo que Pérez Luño denominó «la generación de leyes de protección de datos personales» (Pérez Luño, 1989, p 133).

El artículo segundo letra f) de la Ley N.º 19.628 conceptualiza los datos personales como datos de carácter personal a los relativos a cualquier información concerniente a personas naturales, identificadas o identificables. Es decir, aquellos datos que permiten individualizar a una persona y determinar quién es el titular de ellos, y que la propia ley se encarga de diferenciar de los datos estadísticos, que son aquellos que «en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable».

La ley chilena, al igual que otros ordenamientos jurídicos, consagra una serie de principios para la protección de datos personales y su adecuada tutela y tratamiento, los cuales son posibles de sistematizar de la siguiente manera:

este derecho.

² Artículo 24: «Agregase los siguientes incisos segundo y tercero, nuevos, al artículo 127 del Código Sanitario: "Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo. Lo dispuesto en este artículo 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. 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 expidieron, ni datos que sirvan para identificarlos».

a) El principio de licitud que se desprende de los artículos 2, 4 incisos 1³ y 6, según el cual el tratamiento solo cabe si existe autorización legal o de parte del titular, debiendo en este último caso tratarse de un consentimiento expreso, es decir que se manifieste en términos explícitos e inequívocos.

b) El principio de información al titular respecto del propósito del almacenamiento de sus datos personales, es decir, para qué se almacenarán los datos y su posible comunicación al público, establecido en el artículo 4, inc. 2⁴.

c) El principio de veracidad de los datos, que exige corregir los que sean erróneos, inexactos, equívocos o incompletos, según se colige del artículo 6, inc. 2⁵.

d) El principio de finalidad de los datos, que se desprende del artículo 9⁶, y en virtud del cual debe respetarse la finalidad para la que fueron recogidos los datos, de manera que exista una relación directa entre esa finalidad y el dato recabado.

e) El principio de seguridad de los datos, contemplado y cautelado en el artículo 11⁷ y, tratándose de los órganos de la Administración regulado por el D. S. N.º 83/2004, de la SEGPRES⁸.

f) El principio de confidencialidad que se aplica cuando se trata de datos obtenidos de fuentes no accesibles al público, según el artículo 7⁹.

Luego, el título segundo y, principalmente, el artículo 12¹⁰ de la ley hacen referencia a los derechos que se le confieren al titular, para salvaguardar el tratamiento de sus datos

³ Artículo 4: «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».

⁴ «La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público».

⁵ «Han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos».

⁶ Artículo 9 inciso 1: «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».

⁷ Artículo 11: «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».

⁸ Este decreto del Ministerio de Secretaría General de la Presidencia fue promulgado el 3 de junio del año 2004 y su título es «Aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos». Su objetivo es garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico; además de facilitar la relación electrónica entre los órganos del Estado, y entre estos y la ciudadanía.

⁹ Artículo 7: «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».

¹⁰ Artículo 12: «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.

En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen.

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.

personales: son los derechos de acceso, rectificación, cancelación y bloqueo¹¹. Estos constituyen la contrapartida a la habilitación legal para el tratamiento de datos personales, contenida en el artículo 1 de la Ley N.º 19.628. Por una parte, la ley permite a cualquiera realizar tratamiento de datos personales de un tercero, en la medida en que cumpla con ciertos requisitos, y, a su vez, otorga herramientas que buscan asegurar que dichos datos se correspondan con la realidad y que el tratamiento cumpla con todos los requisitos legales. Por lo mismo, ante el caso de dejar de cumplirse cualquiera de estas dos condiciones, la ley garantiza a las personas el derecho a solicitar la modificación, cancelación o bloqueo de sus datos.

Luego, el artículo 13¹² dispone que los derechos de información, modificación, cancelación y bloqueo son indisponibles; no pueden ser limitados por medio de ningún acto o convención.

La tutela de la protección de datos en Chile. El *habeas data*

En el contexto de tutelar la protección de datos de carácter personal y como uno de los mecanismos para asegurar la vigencia y eficacia de los derechos, la Ley N.º 19.628 también ha dispuesto un procedimiento para su resguardo. Eso sí, a diferencia de lo que ocurre en el ámbito europeo y también en otros países de Latinoamérica, este procedimiento no se sustancia ante una autoridad administrativa o entidad de control, la que hasta la fecha es inexistente; ello constata una de las mayores debilidades para el adecuado resguardo del titular de datos en el sistema chileno.

El recurso de *habeas data* puede revestir dos modalidades: una preventiva, cuando tenga por objeto permitir al titular de los datos personales ser informado sobre la existencia de bancos o registros de datos que contengan información que le concierne y, si así fuese, acceder a ellos; y una correctiva, cuando a través de él se exige que determinados datos personales sean corregidos, bloqueados, cancelados, pues el tratamiento que se hace de

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.

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.

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».

¹¹ Actualmente, son los denominados derechos ARCO, acceso, rectificación, cancelación y oposición.

¹² Artículo 13: «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».

ellos es indebido, en el sentido de que vulnera o conculca sus derechos. Así entonces, el *habeas data* se configura como el instrumento a través del cual los titulares de datos pueden ver protegidos sus derechos frente a acciones que resulten ilegales o arbitrarias o que importen un uso indebido de información de carácter personal que le concierne por parte del responsable del fichero o banco de datos.

Las causales de procedencia del *habeas data* están establecidas, principalmente, en el artículo 16 de la Ley N.º 19.628¹³, pero también algunas se encuentran en otras disposiciones. Sistematizándolas, se pueden distinguir las siguientes causales de procedencia:

1. Que el responsable del registro o banco de datos no se pronuncie sobre una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales dentro de dos días hábiles, contados desde la solicitud del requirente.

¹³ «Si el responsable del registro o banco de datos no se pronuncie sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, que se encuentre de turno según las reglas correspondientes, solicitando amparo a los derechos consagrados en el artículo precedente. El procedimiento se sujetará a las reglas siguientes: a) La reclamación señalará claramente la infracción cometida y los hechos que la configuran, y deberá acompañarse de los medios de prueba que los acrediten, en su caso. b) El tribunal dispondrá que la reclamación sea notificada por cédula, dejada en el domicilio del responsable del banco de datos correspondiente. En igual forma se notificará la sentencia que se dicte. c) El responsable del banco de datos deberá presentar sus descargos dentro de quinto día hábil y adjuntar los medios de prueba que acrediten los hechos en que los funda. De no disponer de ellos, expresará esta circunstancia y el tribunal fijará una audiencia, para dentro de quinto día hábil, a fin de recibir la prueba ofrecida y no acompañada. d) La sentencia definitiva se dictará dentro de tercero día de vencido el plazo a que se refiere la letra anterior, sea que se hayan o no presentados descargos. Si el tribunal decretó una audiencia de prueba, este plazo correrá una vez vencido el plazo fijado para ésta. e) Todas las resoluciones, con excepción de la indicada en la letra f) de este inciso, se dictarán en única instancia y se notificarán por el estado diario. f) La sentencia definitiva será apelable en ambos efectos. El recurso deberá interponerse en el término fatal de cinco días, contado desde la notificación de la parte que lo entabla, deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan. g) Deducida la apelación, el tribunal elevará de inmediato los autos a la Corte de Apelaciones respectiva. Recibidos los autos en la Secretaría de la Corte, el presidente ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes. h) El fallo que se pronuncie sobre la apelación no será susceptible de los recursos de casación. En caso de que la causal invocada para denegar la solicitud del requirente fuere la seguridad de la Nación o el interés nacional, 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. De recibirse prueba, se consignará en un cuaderno separado y reservado, que conservará ese carácter aun después de afinada la causa si por sentencia ejecutoriada se denegare la solicitud del requirente. La sala de la Corte Suprema que conozca la reclamación conforme al inciso anterior, o la sala de la Corte de Apelaciones que conozca la apelación, tratándose del procedimiento establecido en los incisos primero y segundo, 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 por las causales señaladas en el inciso precedente, el presidente del Tribunal dispondrá que la audiencia no sea pública. En caso de acogerse la reclamación, la misma sentencia fijará un plazo prudencial para dar cumplimiento a lo resuelto y podrá aplicar una multa de una a diez unidades tributarias mensuales, o de diez a cincuenta unidades tributarias mensuales si se tratare de una infracción a lo dispuesto en los artículos 17 y 18. La falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decreta el Tribunal, serán castigados con multa de dos a cincuenta unidades tributarias mensuales y, si el responsable del banco de datos requerido fuere un organismo público, el tribunal podrá sancionar al jefe del Servicio con la suspensión de su cargo, por un lapso de cinco a quince días».

2. Que el responsable del registro o banco de datos denegare una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales por una causa distinta de la seguridad de la nación o interés nacional.

3. Que el responsable del registro o banco de datos denegare una solicitud de información, modificación, bloqueo, cancelación o eliminación de datos personales por motivos de seguridad de la nación o el interés nacional.

4. Por infracciones a los artículos 17¹⁴ y 18¹⁵ de esta misma ley, que regulan los plazos y la forma en que pueden comunicarse a terceros por los responsables de los registros o bancos de datos de carácter económico, financiero, bancario o comercial.

¹⁴ «Los responsables de los registros o bancos de datos personales sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, cuando éstas consten en letras de cambio y pagarés protestados; cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa; como asimismo el incumplimiento de obligaciones derivadas 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. Se exceptúa la información relacionada con los créditos concedidos por el Instituto Nacional de Desarrollo Agropecuario a sus usuarios, y la información relacionada con obligaciones de carácter económico, financiero, bancario o comercial en cuanto hayan sido repactadas, renegociadas o novadas, o éstas se encuentren con alguna modalidad pendiente. También podrán comunicarse aquellas otras obligaciones de dinero que determine el Presidente de la República mediante decreto supremo, las que deberán estar sustentadas en instrumentos de pago o de crédito válidamente emitidos, en los cuales conste el consentimiento expreso del deudor u obligado al pago y su fecha de vencimiento. No podrá comunicarse la información relacionada con las deudas contraídas con empresas públicas o privadas que proporcionen servicios de electricidad, agua, teléfono y gas; tampoco podrán comunicarse las deudas contraídas con concesionarios de autopistas por el uso de su infraestructura. Las entidades responsables que administren bancos de datos personales no podrán publicar o comunicar la información referida en el presente artículo, en especial los protestos y morosidades contenidas en él, cuando éstas se hayan originado durante el período de cesantía que afecte al deudor. Para estos efectos, la Administradora de Fondos de Cesantía comunicará los datos de sus beneficiarios al Boletín de Informaciones Comerciales sólo mientras subsistan sus beneficios para los efectos de que éste bloquee la información concerniente a tales personas. Sin embargo, las personas que no estén incorporadas al seguro de cesantía deberán acreditar dicha condición ante el Boletín de Informaciones Comerciales, acompañando el finiquito extendido en forma legal o, si existiese controversia, con el acta de comparecencia ante la Inspección del Trabajo, para los efectos de impetrar este derecho por tres meses renovable hasta por una vez. Para que opere dicha renovación se deberá adjuntar una declaración jurada del deudor en la que manifieste que mantiene su condición de cesante. El bloqueo de datos será sin costo para el deudor. No procederá el bloqueo de datos respecto de quienes consignen anotaciones en el sistema de información comercial durante el año anterior a la fecha de término de su relación laboral. Las entidades responsables de la administración de bancos de datos personales no podrán señalar bajo ninguna circunstancia, signo o caracterización que la persona se encuentra beneficiada por esta ley».

¹⁵ «En ningún caso pueden comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible. Tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de haber sido pagada o haberse extinguido por otro modo legal. Con todo, se comunicará a los tribunales de Justicia la información que requieran con motivo de juicios pendientes».

5. Por infracciones no contempladas en los artículos 16 y 19¹⁶, según lo dispuesto en el inciso (apartado) 2 del artículo 23¹⁷ de la misma ley.

El órgano jurisdiccional competente para conocer de este recurso es el juez civil, correspondiente al domicilio del responsable del banco de datos (o fichero de datos en la denominación del RGPD), lo que sigue la regla general en el sistema chileno, en materia de competencia de los tribunales de justicia para conocer y juzgar los asuntos controvertidos sometidos a su conocimiento, en el sentido de que la demanda se presenta en el tribunal correspondiente al domicilio del demandado. Una alternativa a la determinación del tribunal competente para conocer del *habeas data* hubiese sido el juez del domicilio del afectado, o incluso entregar la posibilidad al titular del derecho de protección de datos, de elegir entre este y el del domicilio del demandado, ya que hay que considerar que, en el caso chileno, la regla general es que los domicilios de los responsables de bancos de datos se encuentran en la región metropolitana, lo que eventualmente dificulta la presentación del *habeas data* si el afectado tiene su domicilio o residencia en una región distinta del país¹⁸.

En relación con el procedimiento, la ley establece un proceso general principalmente contenido en el artículo 16, que dispone que el *habeas puede* sea sustentado sobre la base de lo siguiente:

1) La falta de pronunciamiento por parte del responsable del banco de datos dentro de los dos días hábiles siguientes al requerimiento presentado por el titular de los datos, o bien denegase la información por una causal distinta de la seguridad de la nación o el interés nacional.

¹⁶ «El pago o la extinción de estas obligaciones por cualquier otro modo no produce la caducidad o la pérdida de fundamento legal de los datos respectivos para los efectos del artículo 12, mientras estén pendientes los plazos que establece el artículo precedente. Al efectuarse el pago o extinguirse la obligación por otro modo en que intervenga directamente el acreedor, éste avisará tal hecho, a más tardar 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, a fin de que consigne el nuevo dato que corresponda, previo pago de la tarifa si fuere procedente, con cargo al deudor. El deudor podrá optar por requerir directamente la modificación al banco de datos y liberar del cumplimiento de esa obligación al acreedor que le entregue constancia suficiente del pago; decisiones que deberá expresar por escrito. Quienes efectúen el tratamiento de datos personales provenientes o recolectados de la aludida fuente accesible al público deberán modificar los datos en el mismo sentido tan pronto aquélla comunique el pago o la extinción de la obligación, o dentro de los tres días siguientes. Si no les fuera posible, bloquearán los datos del respectivo titular hasta que esté actualizada la información. La infracción de cualquiera de estas obligaciones se conocerá y sancionará de acuerdo a lo previsto en el artículo 16».

¹⁷ «La acción consiguiente podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil. En todo caso, 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».

¹⁸ Esto se abordó en la discusión legislativa de la ley, como da cuenta el Boletín N.º 896-07, «Informe de la Comisión Mixta» relativo al proyecto de ley sobre protección de datos de carácter personal.

2) La contravención a los artículos 17 y 18 de la Ley N.º 19.628.

Respecto de estas causales, se procede de la siguiente manera: se debe presentar una reclamación ante el Tribunal Civil, la que debe contener indicación clara de la infracción cometida y los hechos que la configuran, además de los medios de prueba que la acreditan. Este recurso se notifica por cédula en el domicilio del responsable del banco de datos correspondiente; por su parte, el responsable del banco de datos deberá contestar dentro del quinto día hábil, formulando sus descargos y adjuntando los medios de prueba respectivos.

Si no dispone de dichos medios de prueba, deberá así indicarlo. Ahora bien, si ofrece prueba, el tribunal fijará una audiencia, para dentro del quinto día hábil a fin de recibir la prueba ofrecida y no acompañada. Esta facultad que se le entrega al demandado, de la cual no goza el reclamante o afectado, constituye uno de los aspectos más cuestionables de este procedimiento, por cuanto vulnera el principio de la bilateralidad de la audiencia, al dejar en manos del responsable del banco de datos la posibilidad de que exista una audiencia de prueba, ya que, si no la ofrece, no existirá tal audiencia.

La sentencia definitiva se dictará dentro del tercero día de vencido el plazo para presentar descargos, se hayan o no presentado. Ahora bien, si el tribunal decretó una audiencia de prueba, este plazo correrá una vez vencido el plazo fijado para esta.

La sentencia definitiva se notifica por cédula y es apelable en ambos efectos. El recurso deberá interponerse en el término fatal de cinco días, contado desde la notificación de la parte que lo entabla; deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan.

Deducida la apelación, el tribunal elevará de inmediato los autos a la Corte de Apelaciones respectiva. Recibidos los autos en la Secretaría de la Corte, el presidente ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes. En todo caso, si la Corte 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. El fallo que se pronuncie sobre la apelación no será susceptible de los recursos de casación.

Todas las resoluciones, con excepción de la sentencia definitiva, se dictarán en única instancia y se notificarán por el estado diario.

La Ley N.º 19.628 consagra también otro procedimiento que tiene como única causal el sustento invocado para denegar la solicitud del requirente por parte del responsable del banco de datos, sea la seguridad de la nación o el interés nacional. Además, el sujeto o legitimado pasivo solo pueden ser organismos públicos, por cuanto son los únicos habilitados para invocar dicha causal. En este caso, el procedimiento es el siguiente:

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 este, resolverá la controversia. La explicación de por qué la competencia radica en el máximo Tribunal de Justicia chileno está en la importancia o entidad de

la causal invocada para el rechazo de la solicitud, teniendo en cuenta, además, que el requerido o demandado será un órgano del Estado.

De recibirse prueba, se consignará en un cuaderno separado y reservado, que conservará ese carácter aun después de terminada la causa si por sentencia ejecutoriada se denegare la solicitud del requirente.

La sala de la Corte Suprema que conozca la reclamación, 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. El presidente del Tribunal dispondrá que la audiencia no sea pública, ya que este procedimiento reviste las características de secreto, debido a las eventuales causales invocadas.

La Ley N.º 19.628 establece también un tercer procedimiento, previsto en el artículo 23, de naturaleza sumaria, que tiene lugar cuando las infracciones a la ley sean cualquiera de las que no están previstas en los artículos 16 y 19; por ejemplo, si una entidad pública realiza tratamiento de datos personales sin estar habilitada o tener competencia para ello, si el responsable de los datos no informa a terceros que dichos datos se han modificado o eliminado.

Las sanciones previstas en esta ley son pecuniarias y se harán efectivas en caso de acogerse la reclamación. La misma sentencia fijará un plazo prudencial para dar cumplimiento a lo resuelto y podrá aplicar una multa de 1 a 10 unidades tributarias mensuales o de 10 a 50 unidades tributarias mensuales. Finalmente, indica la ley que la falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decreta el Tribunal, serán castigados con multa de 2 a 50 unidades tributarias mensuales¹⁹ 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.

En lo procedimental, también hay que tener presente lo dispuesto en la parte final del artículo 23, en el sentido de que el juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece, que la prueba se apreciará en conciencia por el juez y que el monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos.

¹⁹ La Unidad Tributaria Mensual (UTM): Unidad definida en Chile que corresponde a un monto de dinero expresado en pesos y determinado por ley, el cual se actualiza en forma permanente por el Índice de Precios al Consumidor (IPC) y se utiliza como medida tributaria. 1 UTM equivale a poco menos de 55 euros; 10 UTM equivalen a 547 euros y 50 UTM equivalen a 2.735 euros.

2. El reconocimiento constitucional del derecho a la protección de datos en Chile

El 11 de junio del año 2014, se inició la tramitación legislativa, vía moción parlamentaria²⁰, con la finalidad de introducir la protección de datos en el Capítulo III de la Constitución, «De las Garantías Constitucionales», en el numeral cuarto del artículo 19. El texto de la moción original era el siguiente:

Artículo único: Modifíquese el artículo 19 n° 4 de la constitución política de la república, agregándose los siguientes incisos segundo y terceros nuevos:

Toda persona tiene derecho a la protección de sus datos personales y obtener su rectificación, complementación y cancelación, si éstos fueren erróneos o afectaren sus derechos, como asimismo a manifestar su oposición, de acuerdo a las disposiciones establecidas en la ley. Su tratamiento sólo podrá hacerse por ley o con el consentimiento expreso del titular.

Como se puede apreciar, el legislador chileno en esta primera etapa no solo pretendió consagrar constitucionalmente el derecho a la protección de datos como derecho fundamental reconocido expresamente en la Carta, sino además regular su contenido estableciendo los denominados derechos ARCO (acceso, rectificación, cancelación y oposición).

Más todavía, le imponía una limitación al legislador para la afectación del derecho de protección de datos, en términos en que esta solo podría hacerse por ley, lo que es coincidente con lo establecido en la Constitución chilena en el N.º 26 del art. 19, en orden a que las limitaciones a las garantías constitucionales solo pueden hacerse mediante preceptos legales. O, en su defecto, por consentimiento expreso de su titular; se impide con ello el tratamiento de los datos que se alojan en fuentes de acceso público.

Con el devenir del análisis y la discusión legislativa, finalmente el texto que se plasmó en el N.º 4 del artículo 19 fue el siguiente:

El respeto y protección a la vida privada y a la honra de la persona y su familia y asimismo la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley.

A partir de esta redacción, se equipará la protección de datos personales a los tradicionales derechos de protección y respeto a la vida privada y a la honra personal y familiar, en el sentido de investirlo de la misma tutela o resguardo del que gozan dichos derechos fundamentales reconocidos constitucionalmente, mediante el denominado

²⁰ La tramitación legislativa en Chile puede iniciarse por dos vías: moción parlamentaria, cuando la iniciativa es del Senado o de la Cámara de Diputados, o por mensaje presidencial, cuando la iniciativa la promueve el Ejecutivo (presidente de la República). De ello da cuenta el inciso primero de la Constitución chilena: «Las leyes pueden tener su origen en la Cámara de Diputados o en el Senado, por mensaje que dirija el Presidente de la República o por moción de cualquiera de sus miembros. Las mociones no pueden ser firmadas por más de diez diputados ni por más de cinco senadores».

«recurso de protección» (una especie de *habeas corpus*), que se encuentra consagrado en el artículo 20 de la Constitución Política de Chile, el cual dispone de esta manera:

El que por causa de actos u omisiones arbitrarios o ilegales sufra privación, perturbación o amenaza en el legítimo ejercicio de los derechos y garantías establecidos en el artículo 19, números 1º, 2º, 3º inciso quinto, 4º, 5º, 6º, 9º inciso final, 11º, 12º, 13º, 15º, 16º en lo relativo a la libertad de trabajo y al derecho a su libre elección y libre contratación, y a lo establecido en el inciso cuarto, 19º, 21º, 22º, 23º, 24º, y 25º podrá ocurrir por sí o por cualquiera a su nombre, a la Corte de Apelaciones respectiva, la que adoptará de inmediato las providencias que juzgue necesarias para restablecer el imperio del derecho y asegurar la debida protección del afectado, sin perjuicio de los demás derechos que pueda hacer valer ante la autoridad o los tribunales correspondientes. Procederá, también, el recurso de protección en el caso del N° 8 del artículo 19, cuando el derecho a vivir en un medio ambiente libre de contaminación sea afectado por un acto u omisión ilegal imputable a una autoridad o persona determinada.

Pero lo más importante es que esta redacción constitucional, a continuación de la expresión «asimismo», le reconoce a la protección de datos, tal como lo había hecho la doctrina y los ordenamientos jurídicos comparados, independencia y autonomía, dotándolo de un contenido y alcance propios. Lo reconoce no solo en su dimensión negativa, para que no se utilicen esos datos sin el consentimiento de su titular, sino también en su dimensión positiva, esto es, el derecho a disponer de ellos, consagrando así la libertad de los datos o la autodeterminación informativa.

Así, con fecha 16 de junio de 2018, se publicó en el Diario Oficial la Ley N.º 21.096, que consagra la protección de datos personales como garantía constitucional, en el numeral 4 del artículo 19 de la Constitución chilena.

Este significativo avance debe ir acompañado, necesariamente, de una nueva legislación que no solo dé cuenta de la nueva era digital y tecnológica por la que estamos atravesando, sino que además reconozca y les dé un adecuado tratamiento a los denominados derechos ARCO, cuestión que, como se ha expuesto, la actual legislación chilena no hace. Y, todavía más importante, debe estructurar una entidad o autoridad de control encargada no solo de proteger y fiscalizar tanto a instituciones públicas como privadas el cumplimiento efectivo del respeto a la protección de datos personales como derecho fundamental, sino además de la promoción y del desarrollo de acciones preventivas para su adecuado resguardo.

Consideraciones finales

De la revisión realizada, es posible advertir que la protección de datos en Chile requiere adaptarse al desarrollo de las nuevas tecnologías de la información y el *big data*, los que eran inexistentes o, al menos, muy incipientes cuando entró en vigencia la Ley N.º 19.628, por lo que se necesita una normativa que dé cuenta y se haga cargo del vertiginoso avance tecnológico y utilice la experiencia comparada de otros países latinoamericanos que han

tomado como referente el RGPD de la UE para perfeccionar y actualizar sus legislaciones en materia de protección de datos.

Del mismo modo, urge el establecimiento de una Autoridad de Control en Protección de Datos que no solo regule, sino también promueva este derecho y sea la instancia de reclamación administrativa ante la cual se presente el *habeas data*, el que también debe ser reconfigurado para que sirva como un mecanismo efectivo de tutela y protección de los titulares que han visto transgredido su derecho a la autodeterminación informativa. El proceso constituyente por el que atraviesa Chile es una oportunidad para reconfigurar los derechos fundamentales en su conjunto y, en especial, el de la protección de datos de carácter personal.

Referencias

Constitución Política de la República de Chile (Const). 21 de octubre de 1980 (Chile).

Ley N.º 19.628 de 1999. Sobre protección a la vida privada. 28 de agosto de 1999. Recuperado de: <https://www.bcn.cl/leychile/navegar?idNorma=141599>

Pérez Luño, A. (1989). *Los derechos humanos en la sociedad informática*. Madrid: Centro de Estudios Constitucionales.