UNIVERSIDAD FINIS TERRAE
FACULTAD DE DERECHO
MAGISTER EN DERECHO PÚBLICO

EL TRATAMIENTO DE LOS DATOS SENSIBLES QUE REALIZA EL PODER JUDICIAL EN CHILE Y SU IMPACTO EN EL EJERCICIO DE LA TUTELA JUDICIAL EFECTIVA

MACARENA ROCÍO VILLALOBOS MENA

Tesina presentada a la Facultad de Derecho de la Universidad Finis Terrae, para optar al grado de Magister en Derecho Público

Profesor Guía: Dr. Ignacio Covarrubias Cuevas

Santiago, Chile
2019

"EL TRATAMIENTO DE LOS DATOS SENSIBLES QUE REALIZA EL PODER JUDICIAL EN CHILE Y SU IMPACTO EN EL EJERCICIO DE LA TUTELA JUDICIAL EFECTIVA"

MACARENA ROCÍO VILLALOBOS MENA
Candidata a Magíster en Derecho Público – Universidad Finis Terrae
m.villalobos.m@gmail.com

RESUMEN

El dinamismo de la tecnología y la sociedad cada vez más interconectada, no sólo ha cambiado la vida de todas las personas, sino que además ha instado a generar cambios en el ámbito público. Así, los Estados y sus respectivos gobiernos han de adecuarse a la irrupción de estas nuevas tecnologías.
En el caso de Chile, dentro de las adecuaciones legislativas realizadas, se encuentra la ley de Tramitación Electrónica, N° 20.886 de 2015, que incorpora a los procesos judiciales el uso de tecnologías de la información y la comunicación.
Sin embargo, el texto y la aplicación de la referida ley no ha estado exenta de inconvenientes, en particular en lo relativo al tratamiento de los datos personales y sensibles que en las plataformas del Poder Judicial se exponen, dado que, pueden significar amenazas a derechos fundamentales de los justiciables.

Palabras clave: Datos sensibles, derecho a la vida privada, ley de Tramitación Electrónica, Poder Judicial.

Abstract:
The dynamism of technology and the increasingly interconnected society has not only changed the lives of all people, but has also urged to generate changes in the public sphere. Thus, the States and their respective governments must adapt to the emergence of these new technologies. In the case of Chile, within the legislative adjustments made, there is the "Tramitación Electrónica" Law, No. 20.886 of 2015, which incorporates the use of information and communication technologies into judicial processes. However, the text and application of the aforementioned law has not been exempt from inconveniences, in particular with regard to the processing of personal and sensitive

data that are exposed on the platforms of the Judiciary, since they can mean threats to rights fundamentals of the justiciables.
Key words: Personal data, sensitive data, right to privacy, “Tramitación Electrónica” law, “Poder Judicial”.

INTRODUCCIÓN

Los constantes avances tecnológicos y las nuevas formas de comunicación han hecho que cambie la forma en como interactuamos en sociedad. El Estado ha ido adecuando sus procesos a formas más modernas que permiten a los ciudadanos realizar una serie de gestiones y trámites a través de diversas plataformas digitales, simplemente con un dispositivo que le permita acceder a aquellos servicios.

El Poder Judicial ha avanzado en esa misma línea, y actualmente existe una Oficina Judicial Virtual y una plataforma de consulta jurisprudencial en línea.

Sin embargo, es válido cuestionarse si estos mecanismos digitales observan y respetan plenamente los derechos de los ciudadanos o usuarios de dichos sistemas.

Este trabajo por finalidad, a través del análisis de normas jurídicas vigentes dar respuesta a dicha inquietud, y de alguna forma, advertir algunas problemáticas que pueden generarse entre el libre acceso a toda la información disponible en dichas plataformas con los derechos fundamentales de los interesados o titulares de los derechos.

A través de dos breves capítulos se pretende hacer una revisión de las normas existentes y como éstas en la práctica pueden resultar insuficientes para el resguardo y protección de los derechos esenciales de las personas, alejándose además de los estándares sugeridos por la comunidad internacional.

CONTEXTO

Debido la revolución tecnológica, el Estado chileno ha debido adecuar sus procesos, impulsando diversos proyectos de innovación y modernización de plataformas digitales con la finalidad de facilitar la realización de trámites y de dar mayor acceso a la información pública. Prueba de ello es la implementación de la “Clave Única”, como una herramienta que permite a los usuarios a acceder a todos los servicios públicos.

En este contexto, el Poder Judicial, como una de las funciones del Estado, no podía quedarse atrás en esta materia.

Es indudable que la implementación y puesta en marcha de la ley de Tramitación Electrónica fue un gran avance tecnológico y procesal. El más grande que haya implementado el Poder Judicial en esta materia, sin embargo, tratándose de la protección de los datos personales que se exponen en las plataformas del Poder Judicial, principalmente en la Base Jurisprudencial disponible en la web, esta norma debe ser sistematizada con la ley N° 19.628, sobre Protección de Datos Personales.

1.1. CONCEPTO DE DATOS SENSIBLES

Con el fin de circunscribir el ámbito de estudio, es necesario señalar que abordaremos la problemática de exposición de datos sensibles en las plataformas disponibles en el Poder Judicial, principalmente la consulta abierta que se puede realizar en la Base Jurisprudencial disponible en la página web. [1]

Para estos efectos es necesario señalar que la ley N° 19.628, sobre Protección de Datos Personales, podemos advertir el reconocimiento de tres categorías de datos, que, por cierto, requerirán diferentes niveles de protección. El artículo 2, letra f) de la referida ley define lo que debemos entender por *datos de carácter personal* o *datos personales*, señalando que son "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables".

Por otro lado, se advierte el reconocimiento de los *datos públicos* o *de mera identificación* que son aquellos que se recolectan de una fuente accesible al público, entendiendo por aquéllas "los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes."[2]

Para Jervis (2002), la diferencia entre ambos radica principalmente en la protección tratándose de los datos personales les aplica una protección ordinaria, dado que se encuentran protegidos con las disposiciones propias de la ley, en tanto, los datos públicos o de mera identificación, poseen una limitación menor en cuanto a su tratamiento.

La tercera categoría de datos que reconoce la ley vigente corresponde a los *datos sensibles*, los cuales serán materia de nuestro estudio.

[1] http://basejurisprudencial.poderjudicial.cl/.
[2] Ley N° 19.628 (1999), artículo 2, letra i).

Se debe entender por datos sensibles "aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual."[3] En virtud de su contenido, los datos sensibles tendrían una mayor y especial protección en la ley.

Ahora bien, tratándose de aquellos datos pertenecientes a una causa judicial, denominados doctrinariamente "*datos judiciales*", "constituyen datos sensibles según la definición legal que el ordenamiento jurídico nacional hace de ellos. Basamos esta afirmación, en la característica esencial del dato sensible, cual es que a partir de su tratamiento automatizado (lo que faculta el *cruce de datos*[4]), pueden los tenedores de esa información tomar decisiones arbitrarias o discriminatorias respecto de los titulares de esos datos"[5], hecho que evidentemente los hace más propensos a afectar derechos fundamentales, no sólo del derecho a la vida privada y protección de datos personales, sino también a otros derechos, como igualdad ante la ley, la integridad física, síquica y moral de la persona humana, efectos indeseados de cualquier ordenamiento jurídico.

1.2. NORMATIVA NACIONAL E INTERNACIONAL APLICABLE EN CHILE EN MATERIA DE DATOS SENSIBLES.

Dentro de las normas jurídicas nacionales que se refieren a los datos sensibles advertimos la existencia de aquellas de orden constitucional y otras de orden legal.

Respecto de las primeras, se observa que la Constitución Política de la República no reconoce el derecho a la protección de los datos sensibles de manera explícita. Sin embargo, es dable aseverar que el artículo 19 N° 4 de la Carta Magna considera la protección de los datos personales. Este numeral reza lo que sigue: "La Constitución asegura a todas las personas el respeto y protección de la vida privada y a la honra de la

[3] Ley N° 19.628 (1999), artículo 2, letra g).

[4] Para efectos de este estudio, debe entenderse por *cruce de datos*, las actividades tales como el registro, procesamiento, análisis, entrecruzamiento y transmisión de datos, las cuales conformarán una información valiosa respecto de la toma de decisiones de toda índole (económicas, sociales, políticas, empresariales y laborales, entre otras) que develarán aspectos de la vida privada e incluso íntima de las personas.

[5] JERVIS (2002), p. 2.

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".

Con la dictación de la Ley N° 21.096, de 2018, se reformó el texto de la Constitución, adicionando la parte final del articulado, que hace expresa mención a la protección de los datos sensibles. Si dicho texto se interpreta de forma amplia, la protección de los datos sensibles estaría incluida en el cuerpo normativo más importante del ordenamiento jurídico chileno, lo cual tendría efectos en ámbitos procesales y judiciales.

La protección constitucional de este derecho considera también el contenido del numeral 26 del artículo 19 de la Constitución que impide que alguna ley complementaria, limitativa o reguladora de las garantías fundamentales las afecte en su esencia, les imponga condiciones, tributos o requisitos que impidan su libre ejercicio.

En cuanto a las normas legales que regulan el tratamiento de datos sensibles, encontramos la ya mencionada Ley N° 19.628, denominada "Protección de datos de carácter personal", de 1999, la que se analizará más adelante, particularmente respecto a las falencias que presenta en la protección de datos sensibles dentro del desarrollo de un proceso judicial, que, siendo tratados automatizadamente por particulares u organismos públicos, se transforman en datos sensibles, que, como ya se señalaba, se ha reconocido que deben contar con una especial protección.

Ciertamente existen otras normas legales que incorporan elementos de protección de datos personales, pero mucho más específicas o sectoriales, y, consecuentemente, no serán abordadas en el presente trabajo. [6]

Resulta imprescindible además considerar el artículo 5 inciso segundo de la Carta Fundamental chilena que obliga al Estado a respetar y promover los derechos esenciales de la persona humana, garantizados por la Constitución, así como por los tratados internacionales ratificados por Chile y que se encuentren vigentes, por lo cual los Tratados y Acuerdos Internacionales, que cumplan con dichas características, deben ser considerados como normas regulatorias plenamente aplicables en materia de protección de datos personales. Ahora bien, éstos hacen mención específicamente a la

[6] Por ejemplo: Ley N° 20.463 de 2010 que prohíbe a los administradores de bases de datos personales de carácter financiero hacer tratamiento de datos relativos a deudas de personas naturales, cuando éstas se encontraban sin empleo y Ley N° 20.521 de 2011, la cual prohíbe cualquier tipo de evaluación de riesgo comercial que no esté basada en información objetiva relacionada con la situación financiera de las personas, entre otras.

protección de datos personales, mas, ya hemos advertido que el reconocimiento de datos personales alberga también en concepto de datos sensibles.

Así, la doctrina internacional ha desarrollado progresivamente los lineamientos y requisitos mínimos para reconocer a cada Estado como una nación que posea un estándar idóneo de protección de datos personales.

En el caso de Chile, y por la adhesión a estas entidades internacionales, es especialmente relevante ajustarse a los fundamentos que provienen de la Organización para la Cooperación y el Desarrollo Económico (OCDE), la Organización de las Naciones Unidas (ONU) y el Foro de Cooperación Económica del Asia Pacífico (APEC), de los cuales se podrán observar la coherencia y similitud de los elementos que conforman el estándar internacional de protección de datos personales, y cuyos elementos más importantes serán expuestos sucintamente:

1.2.1. DIRECTRICES DE LA ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO (OCDE).

El 23 de septiembre del año 1980, la OCDE propone el primero de los documentos que establece recomendaciones para la circulación internacional de los datos personales para la protección de la intimidad. Esta intervención responde a la falta de uniformidad en la regulación de esta materia que poseían todos los países miembros, y dentro de sus objetivos podemos señalar los siguientes:

a. Garantizar la inexistencia de obstáculos a la libre transferencia internacional de datos.
b. Establecer los principios básicos que orientan el tratamiento de datos de carácter personal. Estos principios orientadores pueden ser resumidos de la siguiente forma:

   - Datos tratados de manera lícita, requiriendo el consentimiento del interesado.

   - El responsable del tratamiento de los datos debe especificar la finalidad para la cual se requieren los datos.

   - Los datos deben ser pertinentes de acuerdo a lo declarado.

   - El responsable del tratamiento de los datos debe adoptar medidas de seguridad para así resguardar la información y que no exista pérdida o acceso no autorizado a éstos.

   - Asimismo, el responsable debe informar a los titulares sobre el tratamiento dado a sus datos personales.

- Los titulares tendrán el derecho a conocer la existencia de sus datos personales y a solicitar la rectificación o cancelación de sus datos que han sido sujetos a tratamiento.

c. Regular medidas de implantación y de coordinación de los Estados miembros. Tratándose de las primeras, los deberes de los Estados miembros son el establecimiento de medidas legales, administrativas o de otro tipo que aseguren siempre la protección de la privacidad de las personas en cuanto a sus datos personales, fomentando de esta forma la autoregulación y la adopción de medidas garantes de dichos datos.

1.2.2. ASAMBLEA GENERAL DE LAS NACIONES UNIDAS.

La resolución 45/95 de fecha 14 de diciembre de 1990 de las Naciones Unidas estableció las directrices de protección de datos, en donde se informaron los principios mínimos de protección que los Estados debían contemplar en sus legislaciones internas. Estos principios podrían sistematizarse en los siguientes:

- Principio de recogida y tratamiento leal y lícito.
- Principio de exactitud y actualización de datos sometidos a tratamiento.
- Principio de especificación de la finalidad y proporcionalidad en el tratamiento.
- Principio de acceso a la persona interesada. Ello implica a su vez que los interesados no incurran en gastos o demoras excesivas para conocer de los datos personales que están siendo tratados y los destinatarios de los mismos. En caso de que exista un dato injustificado, ilícito o inexacto, se proceda a la rectificación o supresión de dichos datos.
- Limitación de las excepciones a los principios, ajustándolos a la protección de la seguridad ciudadana, el orden público y los derechos de terceros.
- Principio de seguridad, vale decir, que exista una protección de los datos contra aquellos riesgos de pérdidas naturales o accidentales.
- Supervisión e imposición de sanciones, ya sean penales, administrativas u otras, que sean aplicadas por una autoridad imparcial e independiente que tenga como fin la supervisión del cumplimiento de los principios informados por la Asamblea General.
- Transferencias internacionales, permitiendo el flujo de datos personales entre los Estados miembros, garantizando siempre la protección de la vida privada de los titulares del derecho.

1.2.3. FORO DE COMUNICACIÓN ECONÓMICA DEL ASIA-PACÍFICO (APEC)

En noviembre de 2004, durante el desarrollo de la décimo sexta reunión ministerial de la APEC se elaboró el acuerdo denominado "Asia - Pacific Economic Cooperation Privacy Framework", a través de la cual se establecen los principios de privacidad del APEC. Entre ellos se destacan:

- El principio de prevención de daño por el mal uso de la información.
- El principio de aviso a los titulares de los datos respecto de su información sujeta a tratamiento y los límites a la recolección que atiendan a la licitud y lealtad.
- El principio de uso o finalidad de la información.
- El principio de elección sobre el almacenamiento de sus datos y la integridad de la información de los titulares. Este principio precisa que los datos recolectados deben ser completos, exactos y actualizados.
- Medidas de seguridad sobre los datos recopilados.
- Un derecho de acceso junto a la posibilidad de corrección de los datos.
- El principio de la responsabilidad por infracciones de quien esté administrando los datos. Junto a estos principios, también se muestra una pauta de implementación tanto a un nivel interno como internacional.

1.2.4. ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA)

Chile como miembro fundador de la OEA, asume un compromiso de integración y cooperación con la comunidad americana. Eso por ello que con el progreso de la tecnología fue necesario establecer diálogos y discusiones sobre los problemas que surgían de forma temprana a propósito de la protección de datos personales.

En ese contexto, aparece el "Anteproyecto de Convención Americana sobre Autodeterminación Informativa", que es constituye como una guía internacional para nuestro país y que busca tutelar entre otros derechos: la honra, la reputación, la vida privada y familiar de las personas, reconocidos en la Convención Americana sobre Derechos Humanos de 1969.

Relevante es destacar que en el artículo 1 de este anteproyecto se busca de forma mucho más concreta la tutela del derecho a la autodeterminación informativa, a toda

persona física en relación a su privacidad, vida privada, derechos propios de la personalidad y la defensa su libertad e igualdad en el tratamiento automatizado o manual de sus datos.

En el artículo 3 no sólo se extiende a personas naturales, sino que también incluye a las personas jurídicas en cuanto le sean aplicables las normas por su naturaleza. También posee una serie de principios básicos para la protección de los datos, como el compromiso de los Estados partes del respeto de los derechos y libertades reconocidos en la Convención, el derecho de información en la recogida de los datos, el consentimiento del titular y la calidad de los datos.

Además, reconoce categorías especiales al señalar que existen datos más sensibles que otros, se habla de la seguridad de los datos de carácter personal, la cesión de los datos y una serie de derechos y garantías de las personas que les permitan de cierta forma conocer o medianamente controlar la información que le concierne en ficheros o sistemas de almacenamiento de información de terceros.

Junto a lo anterior, el anteproyecto se encarga de establecer un mecanismo de garantías judiciales y establecer el medio procesal idóneo para su consecución, a saber, el habeas data.

El referido Anteproyecto también obliga a los Estados partes a establecer sanciones y recursos frente a las infracciones, se regula el flujo transfronterizo o internacional de datos y se señala el deber de cooperación mutua entre los Estados Parte.

Por último, recomienda la creación de una agencia de protección de datos personales y la creación de un registro general de protección de datos.

De la revisión anteriormente realizada, se constata un lineamiento consistente y armonizado de aquellos elementos que son básicos para un adecuado tratamiento de los datos personales que deben adoptar los Estados miembros, y que lamentablemente Chile no ha cumplido a cabalidad.

2. LEY DE TRAMITACIÓN ELECTRÓNICA.

La ley de Tramitación Electrónica N° 20.886 de 2015 es una normativa cuyo objetivo principal es establecer una tramitación de las causas que deben conocer los tribunales de justicia[7] en un expediente digital, respecto del cual es posible encontrar una serie de ventajas, por ejemplo, economía procesal para las partes y para el propio tribunal, mayor contribución con el medio ambiente, mejoras en el sistema de notificaciones, mayor seguridad que un expediente físico, mayor facilidad en el acceso y consulta del expediente, etcétera.

Además de las ventajas señaladas, su promulgación e implementación es de gran importancia dado que, como ya mencionábamos, es la mayor modificación en orden tecnológico que implementa el Poder Judicial.

Esta ley fue antecedida por otras normas necesarias para su adecuada implementación, como lo fue la ley N° 19.799 de 2002 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma.

A pesar de los ajustes, nos parece necesario sostener que la técnica legislativa no fue la más adecuada, toda vez que el texto normativo señala expresamente la posibilidad de que la Corte Suprema regule y complemente a través de autos acordados problemas que pudieran generarse con la puesta en marcha de la ley, considerando el cambio radical en la forma de tramitación judicial de causas.[8]

Sin embargo, ese no es el único problema que posee esta norma. Advertimos problemáticas que dicen relación estrictamente con el tratamiento de datos personales y de datos sensibles, y también respecto a la titularidad de dichos datos, de conformidad a

[7] El artículo 1 de la ley N° 20.886 señala que el ámbito de aplicación de la ley corresponderá a los tribunales indicados en los incisos segundo y tercero del artículo 5 del Código Orgánico de Tribunales, con excepción de los tribunales militares en tiempo de paz. Con ello, se excluyen, por ejemplo, el Tribunal de la Libre Competencia, el Tribunal de Propiedad Industrial, los Tribunales Ambientales, los Juzgados de Policía Local, el Tribunal de la Contratación Pública, entre otros.

[8] Existen a la fecha 3 autos acordados dictados por la Excma. Corte Suprema que complementan el contenido de la ley N° 20.886. Éstos son: Acta 37-2016 "Auto Acordado para la aplicación en el Poder Judicial de la Ley N° 20.886 que modifica el Código de Procedimiento Civil, para establecer la tramitación digital de los procedimientos judiciales" (de 15 de abril de 2016); Acta 71-2016 "Auto Acordado que regula el funcionamiento de los tribunales que tramitan electrónicamente" (de 16 de junio de 2016) y finalmente el Acta 13-2017 "Auto Acordado que regula el funcionamiento de tribunales que tramitan electrónicamente".

los principios formativos de la Tramitación Electrónica, asuntos que abordaremos a continuación.

2.1 PROBLEMÁTICAS DE LA IMPLEMENTACIÓN DE LA TRAMITACIÓN ELECTRÓNICA EN TORNO A LA PROTECCIÓN DE LOS DATOS SENSIBLES.

Para abordar adecuadamente las problemáticas que se generan con la puesta en marcha de la Tramitación Electrónica, haremos la siguiente distinción: En primer lugar abordaremos la posibilidad de tratamiento que tiene el Poder Judicial de los datos que incorporan los justiciables a la plataforma y los respectivos límites, luego, la titularidad de dichos datos, al tenor de lo comprendido en la ley 20.886.

De acuerdo a lo anterior, necesariamente debemos remitirnos al texto legal que regulan por un lado la Tramitación Electrónica, y por otro, la Protección de Datos Personales.

El artículo 10 de la ley N° 19.628, contenido en el Título I, denominado "De la utilización de los datos personales" reza siguiente: No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares". Del análisis de la norma, se desprende que no se podrá realizar tratamiento de datos sensibles, salvo en las tres hipótesis que taxativamente menciona el referido articulado.

Ahora bien, si coordinamos dicho principio general con lo establecido en el artículo 20 de la misma norma legal, el cual establece que "El tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular". Por ello, es posible aseverar que el Poder Judicial efectivamente es un organismo público, y, en consecuencia, puede realizar el tratamiento de este tipo de datos, siempre con sujeción a las reglas que la propia ley consagra. En razón de ello, le es absolutamente aplicable el inciso segundo del artículo 1 de la misma ley, especialmente en lo referente a las limitaciones que reconoce la norma, la cual contempla ciertas limitaciones en el siguiente tenor: "Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento

jurídico. En todo caso deberá **respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos** y de las facultades que esta ley les reconoce." (El destacado es nuestro). Esto será especialmente relevante cuando abordemos algunos casos específicos en donde diversos derechos fundamentales se han visto vulnerados en la práctica por el tratamiento, pero, peor aún, la publicación de datos sensibles de justiciables.

De lo anterior, se concluye que el Poder Judicial, como órgano público, puede realizar el tratamiento de datos personales, siempre dentro de su competencia y con las limitaciones contempladas en la propia ley de Protección de Datos Personales.

Ahora bien, es menester abordar las normas atingentes que se encuentran en la propia ley de Tramitación Electrónica respecto a esta materia. El artículo 2, letra c) inciso tercero señala que "Se prohíbe el tratamiento masivo de los datos personales contenidos en el sistema de tramitación electrónica del Poder Judicial, sin su autorización previa. La infracción cometida por entes públicos y privados a lo dispuesto en este inciso será sancionada conforme a la ley Nº 19.628", remitiendo al sistema sancionatorio que contempla la ley de Protección de Datos Personales. Pero, y más importante aún, establece que no se podrá realizar el tratamiento masivo de datos personales sin autorización previa del titular. Es acá en donde nos enfrentamos al problema de la titularidad de los datos contenidos en la plataforma (datos judiciales/datos sensibles). Lo claro es quien debe entregar la autorización es el titular.

Pero ¿quién es el verdadero titular de los datos incorporados en la plataforma del Poder Judicial? La pregunta se formula a propósito del contenido de la Historia de la Ley N° 20.886, en foja 120, se señaló que "la redacción propuesta establece una excepción, en virtud de la cual el Poder Judicial está facultado para autorizar el tratamiento masivo de datos personales contenidos en el sistema de tramitación electrónica". En caso de "interpretar la norma a la luz de su historia, nos encontramos en un escenario en que el dueño de la base de datos es también el titular de los datos contenidos en ella, independiente de 'sobre quien' traten los datos"[9]. Ello constituiría en palabras de Sandra Bustos una "cesión forzosa" de los datos que entregan los justiciables al momento de incorporar una causa o entregar algún otro dato a la plataforma del Poder Judicial, y, la consecuencia de ello es que "los datos contenidos en ellas y toda decisión sobre su destino, uso o tratamiento no requerirá su autorización,

[9] BUSTOS (2018), p. 33

sino que quedaría a voluntad del cesionario, el flamante nuevo titular, el Poder Judicial"[10].

Las complicaciones y desventajas de los titulares originales de los datos es de consideración, no sólo en términos de información y económicos, sino que además, en la exposición de datos sensibles que podrán ser utilizados y publicados sin posibilidad efectiva de los justiciables para evitar dicho tratamiento indebido.

Es evidente que existe una colisión entre la protección de los datos personales y sensibles aportados en un proceso con la publicidad de los actos judiciales, sin embargo, consideramos que la limitación legal de respeto irrestricto a los derechos fundamentales del titular original de los datos y la consagración constitucional incorporada en nuestra Carta Fundamental en el año 2018, deberían conformar los límites al tratamiento de datos que realizar el Poder Judicial en sus diversas plataformas informáticas.

2.2. CASO CONCRETO DE VULNERACIÓN A LOS DERECHOS FUNDAMENTALES DE LOS JUSTICIABLES.

El conocimiento de un caso de vulneración de la protección de datos sensibles, generó especial interés para el desarrollo de esta breve investigación.

Un hombre, cuyos datos personales no serán entregados en esta oportunidad, inició un juicio civil en contra del Estado de Chile por falta de servicios, al no habérsele notificado en forma oportuna su resultado serológico positivo de VIH, juicio que llegó a ser conocido por la Excelentísima Corte Suprema en su última etapa procesal y que finalmente terminó estableciendo la responsabilidad del Estado y condenándole al pago de la indemnización de perjuicios demandados por aquel usuario afectado.

Sin embargo, al revisar la base jurisprudencial del Poder Judicial, el usuario advirtió que sus datos personales y sensibles, como lo son los estados de salud, de acuerdo a la norma expresa contemplada en la ley N° 19.628, habían sido divulgados por este órgano público. En concreto, sus antecedentes médicos se encontraban expuestos sin el resguardo apropiado a su identidad e identificación, puesto que los principales escritos y la sentencia se encontraban publicadas en dicha plataforma web.

[10] BUSTOS (2018), p. 33

El afectado, agobiado con el largo juicio, los costos asociados al pago de honorario de abogados y otras expensas relativas al juicio, acudió a la Oficina Regional de Maule del Instituto Nacional de Derecho Humanos, quién solicitó al Administrador Regional de la Corporación Administrativa del Poder Judicial (encargada de establecer las medidas para evitar el tratamiento automatizado de datos) en el mes de marzo del año en curso, que, con el fin de dar cabal cumplimiento al mandato institucional, colaboración para que en los antecedentes publicados se tarjen o borren los datos personales sensibles del interviniente afectado, entre ellos, nombre completo, cédula de identidad y domicilio, de modo de asegurar el resguardo efectivo, íntegro y oportuno de los derechos humanos afectados, otorgando argumentos legales y jurisprudenciales para ello.

En concreto, lo preceptuado en el artículo 2 letra g) de la ley N° 19.628 y el artículo 12 de la ley N° 20.584[11], la información relativa a la ficha clínica del paciente constituiría un dato sensible, cuya divulgación necesita el consentimiento expreso del interesado, hecho que en el caso en comento no ocurrió.

Con ello, la divulgación de dicha información sin el debido resguardo de la identidad del paciente y sin su consentimiento vendría a configurar una vulneración al ámbito de la privacidad, en donde deben quedar resguardados los antecedentes relativos a la intimidad de las personas.

Lamentablemente, a la fecha ni el Instituto Nacional de Derechos Humanos ni el interesado ha recibido respuesta alguna respecto a la solicitud realizada por esta vía, y peor aún, sus antecedentes médicos siguen publicados y exhibidos en la base jurisprudencial del Poder Judicial, afectando sus derechos de intimidad, vida privada y protección de sus datos sensibles.

CONCLUSIONES

Como reflexiones finales, nos permitimos realizar algunas sugerencias que creemos serán de utilidad para mejorar la legislación vigente, otorgar la debida

[11] Ley que regula los Derechos y Deberes que tienen las personas en relación con acciones vinculadas a su atención en salud. (2012)

protección a los derechos fundamentales de las personas y adecuarla para dar cumplimiento a los estándares internacionales sobre la materia.

En primer lugar, los derechos fundamentales en caso alguno revisten un carácter estático, sino por el contrario, están en permanente cambio y progresión, razón por la cual nos parece relevante que los datos sensibles tengan un reconocimiento constitucional, considerando como núcleo esencial del derecho la autodeterminación informativa, entendiéndola como el derecho de las personas a que se respete su derecho a la vida privada e intimidad ante el tratamiento automatizado de los datos personales y de datos sensibles, dentro de un contexto de privacidad informacional, que sea respetado por particulares y por los órganos del Estado, que debe considerar evidentemente al Poder Judicial.

Queda de manifiesto que las acciones constitucionales y legales existentes en la legislación obligan al afectado o afectada del derecho, que ya se encuentra en una situación de debilidad y desmejorada, a recurrir a tribunales de justicia ordinarios (en el caso de la acción de protección) y no especializados (en el caso del habeas data), resulta burocrático e ineficaz para la debida protección de este derecho fundamental.

En segundo lugar, se hace necesario adecuar el ordenamiento jurídico interno a las sugerencias de los órganos internacionales. Nos parece en este sentido que se hace imprescindible contar con un órgano imparcial, independiente y especializado que tenga como fin la supervisión del cumplimiento de los principios informados por los distintos órganos internacionales y que por la vía del artículo 5 inciso segundo de la Constitución Política de la República, se incorporan a nuestro ordenamiento jurídico interno.

Como tercer punto, nos parece relevante realizar modificaciones a las normas existentes, especialmente a la de Tramitación Electrónica, toda vez que no resulta adecuado que los justiciables se vean obligados a entregar datos personales para que los tribunales de justifica ejerzan jurisdicción, pero a la vez se ven expuestos a vulneraciones de otros derechos fundamentales por órganos del Estado.

Por último, y quizás la más sencilla de las recomendaciones. Mientras estos progresos legislativos no se concreten, es imprescindible que la Corporación Administrativa del Poder Judicial, al momento de alimentar la base jurisprudencial de la plataforma digital del Poder Judicial, revise, pondere y tarje todos aquellos datos son personales o sensibles y que pueden generar la afectación de los derechos a la intimidad, a la vida privada y a la no consagrada aún, autodeterminación digital.

BIBLIOGRAFÍA

1. APEC (2004). "Asia - Pacific Economic Cooperation Privacy Framework". Disponible en: https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework. [visitado el 31 de octubre de 2019].
2. ARRIETA CORTÉS, Raúl y REUSSER MONSÁLVEZ, Carlos. Coordinadores (2011): "Reflexiones sobre el uso y abuso de los datos personales en Chile. Ediciones Expansiva. Santiago, Chile. Disponible en: https://www.consejotransparencia.cl/wp-content/uploads/estudios/2018/01/reflexiones_sobre_el_uso_y_abuso_de_los_datos_personales_en_chile.pdf [visitado el 5 de noviembre de 2019].
3. ASOCIACIÓN POR LOS DERECHOS CIVILES (2014): "Acceso a la información y transparencia en el Poder Judicial: Guía de buenas prácticas en América Latina", ADC, Buenos Aires, Argentina.
4. BERTELSEN REPETTO, Raúl; CORRAL TALCIANI, Hernán; GONZÁLEZ HOCH, Francisco; JARA AMIGO, Rony; JIJENA LEIVA, Renato; MENDOZA ZÚÑIGA, Ramiro; VIAL CLARO, Felipe (2001); "Tratamiento de los datos personales y protección de la vida privada: estudios sobre la ley 19.628 sobre protección de datos de carácter personal", Cuadernos de Extensión Jurídica N° 5, Universidad de los Andes. Santiago, Chile.
5. BUSTOS ORELLANA, Sandra Sofía (2018). "Tratamiento de los datos personas en el Poder Judicial de Chile: ¿El Gran Hermano jurisdiccional?", en "Revista Chilena de Derecho y Tecnología", Volumen 7, Número 2. Páginas 27 a 44.
6. FIGUEROA GARCÍA-HUIDOBRO, Rodolfo (2013). "El derecho a la privacidad en la jurisdicción de protección", en Revista de Derecho, volumen 40 N° 3, páginas 859 a 889.
7. Historia de la Ley 20.886 (2015) "Nueva Ley de Tramitación Electrónica», Biblioteca del Congreso Nacional de Chile. Disponible en http://bit.ly/2R584in. [vistada el 1 de noviembre de 2019]
8. JERVIS ORTIZ, Paula (2002). "Comentario jurisprudencial. Intimidad y tratamiento de datos personales en el Poder Judicial", en Revista Chilena de Derecho Informático", Volumen 1, páginas 143 a 154.

9. JIJENA LEIVA, Renato (2013). “Tratamiento de datos personales en el Estado y acceso a la información pública”, en Revista Chilena de Derecho y Tecnología, Volumen 2, N° 2, páginas 50 a 90.
10. JUICA ARANCIBIA, Milton (2013). “Transparencia en el Poder Judicial de Chile: Diseño, políticas y estructuras para cumplir con este principio”, en Revista de Derecho Universidad Finis Terrae. Segunda época año I, N° 1, páginas 27 a 57.
11. NOGUEIRA ALCALÁ, Humberto (2005). “Autodeterminación informativa y hábeas data en Chile e información comparativa”, en Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México. Disponible en: http://www.biblio.dpp.cl/biblio/DataFiles/10626.pdf. [visitado el 3 de noviembre de 2019].
12. OEA. (1998) “Anteproyecto de Convención Americana sobre Autodeterminación Informativa”. Disponible en: http://akane.udenar.edu.co/derechopublico/DATOS_AMERICA.pdf [visitado el 30 de octubre de 2019].
13. OCDE (1980) “Directrices de la OCDE Sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales”. Disponible en: https://www.oecd.org/sti/ieconomy/15590267.pdf. [visitado el 30 de octubre de 2019].
14. ONG DERECHOS DIGITALES (1999). “Privacidad y nuevas tecnologías, regulación chilena y propuestas de política pública”. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/pp-02.pdf [visitado el 7 de septiembre de 2019].
15. ONG DERECHOS DIGITALES (2017). “El Estado de la Protección de Datos personales en Chile”. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf [visitado el 7 de septiembre de 2019].
16. ONU (1990). “Resolución 45/95 de la Asamblea General de las Naciones Unidas”. Disponible en: https://www.un.org/es/documents/ag/res/45/list45.htm. [visitado el 30 de octubre de 2019].
17. PARRA URIBE, Camila (2013). “Institucionalidad para la protección de datos personales en Chile”. Universidad de Valparaíso, Valparaíso, Chile.
18. PODESTÁ, Flavia (2010). “Tratamiento de datos personales en la Justicia digital. Panorama argentino y otras referencias”, disponible en:

http://www.redipd.es/actividades/seminario_2010/common/ponencias/Tratamiento_DP_en_PJ_F_Podesta.pdf. [visitado el 3 de septiembre de 2019].