EPU 2018

ONG Datos Protegidos en colaboración con Corporación Fundamental

Nombre: Fundación Datos Protegidos
Siglas: FDP
Correos electrónicos:
jessica@datosprotegidos.org
romina@datosprotegidos.org
Página web: www.datosprotegidos.org
Dirección: La Concepción 56, Providencia, Santiago de Chile.

Nombre: Corporación Fundamental
Siglas: CP
Correos electrónicos:
tbusch@cfundamental.cl
jalfaro@cfundamental.cl
ealvarado@cfundamental.cl
Página web:
https://corporacionfundamental.cl/
Dirección: O'Higgins 1082, oficina 102, Concepción, Chile.

I. INTRODUCCIÓN

Este Informe es presentado para la Revisión al Estado de Chile ante el Examen Periódico Universal en su 32° Período de Sesiones, de manera conjunta, por las organizaciones: **Fundación Datos Protegidos** y **Corporación Fundamental**. Las organizaciones ya mencionadas agradecen la oportunidad de presentar este informe que brinda la oportunidad al Estado de Chile de declarar qué acciones ha emprendido para mejorar las situaciones de derechos humanos en el país y superar los desafíos al disfrute de los derechos humanos, compartiendo las mejores prácticas de derechos humanos en todo el mundo.

a) FUNDACIÓN DATOS PROTEGIDOS

1. **FUNDACIÓN DATOS PROTEGIDOS (FDP)** es una organización independiente creada el 19 de junio de 2015, cuyas tareas son promover, defender y educar sobre el derecho a la privacidad y a la protección de los datos personales como derechos fundamentales. Favorecemos el debate público e influimos en las discusiones nacionales y regionales en fomento de una sociedad respetuosa de la dignidad, no discriminación y libertad de las personas.

2. Fundación Datos Protegidos posee ejes temáticos específicos de trabajo: *Litigación estratégica gratuita*, generando criterios jurisprudenciales y cambios sociales; *Influencia Global*, participando en congresos, seminarios, talleres y foros nacionales y extranjeros; *Incidencia en políticas públicas*, influyendo en las decisiones que impactan en la protección de datos apoyando el trabajo legislativo y la agenda gubernamental desde la mirada técnica; *Campañas públicas y de opinión*, difundiendo el debate sobre la protección de datos y privacidad en medios de comunicación y plataformas digitales; y *Asesorías y capacitación*, ofreciendo formación especializada a entes públicos y privados.

b) CORPORACIÓN FUNDAMENTAL Centro de Justicia y Derechos Humanos

3. **CORPORACIÓN FUNDAMENTAL**: Corporación de interés público, sin fines de lucro, que tiene como objetivo principal la promoción y protección de los Derechos Humanos, así como también, el empoderamiento y apoyo a Defensores y Defensoras de Derechos, a fin de robustecer el Estado de Derecho y la democracia en Chile. Para el cumplimiento de sus objetivos, FUNDAMENTAL despliega su actividad principalmente

asesorando y acompañando a instituciones públicas y privadas, con el fin de brindar acceso a herramientas jurídicas necesarias para la asegurar la vigencia de los Derechos Fundamentales; promoviendo la transparencia en el nombramiento, actuar y rendición de cuentas de los organismos públicos; y a través de la presentación de acciones de interés público ante cortes y órganos domésticos e internacionales.

4. Fundación Datos Protegidos y Corporación Fundamental desean manifestar algunas preocupaciones acerca de la protección y promoción del derecho a la protección de datos personales en Chile, en materia de legislación, políticas públicas, financiamiento, capacitación y sensibilización a la sociedad. El derecho a la protección de datos personales no ha sido considerado directamente en las revisiones anteriores realizadas al Estado chileno, y esperamos, en esta oportunidad, sean puestas a consideración en la sesión 32 del Grupo de Trabajo del Examen Periódico Universal (EPU) dada la relevancia actual e implicancias de la falta de regulación y protección de los datos personales, que afectan directamente el derecho a la privacidad y a la no injerencia de la vida privada de las personas.

II. EL DERECHO A LA PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

5. Con el desarrollo tecnológico de los últimos años, casi todos los aspectos de nuestra vida cotidiana están afectados por las nuevas tecnologías que crean un hiperflujo de información, como en Internet. Como un territorio libre y abierto, Internet debe mantenerse así, sin embargo, es necesario que el acceso y la libertad a la información se pondere con las garantías del control de la información personal, un derecho muy poco desarrollado en Chile. Pese a la penetración y uso de Internet, no somos siempre conscientes que hoy nuestra identidad se reduce a datos. Estos datos circulan en los grandes facilitadores de la web: los buscadores de información, las redes sociales y los medios. Estos datos revelan, lo queramos o no, todo o bastante de nosotros, no existiendo criterios de ponderación cuando esa información es proporcionada por terceros.

6. Constituyen datos personales información que pueden ser numérica, alfabética, fotográfica, etc., y que pueden identificarnos por la información personal que revelan. Según la Ley 19.628, sobre protección de la vida privada, dato personal es “cualquier información concerniente a personas naturales, identificadas o identificables.”, y entiende los 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[1]". Dada la capacidad de las nuevas tecnologías y la especificidad de los datos, el cruce de ellos permite y facilita la creación de perfiles detallados de individuos, los que están siendo cada vez más lucrativos e importantes para las industrias privadas[2]. No obstante, el almacenamiento, uso y regulación de estos datos en el mercado es una área que hoy en día en Chile se encuentra mal regulada y en opacidad.

III. SEGUIMIENTO DEL EPU ANTERIOR

7. Si bien en el párrafo 4 mencionamos que las recomendaciones realizadas en el EPU anterior al Estado de Chile no tratan directamente la regulación de los datos personales, sí se efectuaron recomendaciones **aceptadas** por el Estado de Chile vinculadas a las temáticas y áreas de preocupación que tratará este informe:

- Seguir promoviendo la armonización del ordenamiento jurídico nacional con los tratados internacionales (121.18)
- Lograr una amplia participación de los representantes de la sociedad civil en el proceso de preparación del plan nacional de derechos humanos (121.43)
- Continuar con los esfuerzos destinados a fortalecer su capacidad institucional de promover y proteger los derechos humanos, en particular para acelerar el establecimiento de la Subsecretaría de Derechos Humanos, y formular un plan de acción nacional en materia de derechos humanos integral (121.27; 121.28; 121.41)
- Aprobar una ley de protección integral para los niños, de conformidad con la Convención sobre los Derechos del Niño (121.36)
- Seguir promoviendo programas de educación y sensibilización acerca de los derechos humanos para los funcionarios del poder judicial (121.49)

IV. OBLIGACIONES INTERNACIONALES Y LEGISLACIÓN NACIONAL EN MATERIA DE LA PROTECCIÓN DE LOS DATOS PERSONALES EN CHILE

a) Obligaciones internacionales:

[1] Artículo 2 letras f) y g) de la Ley N° 19.628, sobre Protección de la vida privada. Disponible en: https://www.leychile.cl/Navegar?idNorma=141599

[2] Esto incluye no sólo las empresas de almacenamiento y procesamiento de datos, sino cualquier empresa que vende productos o servicios y también agencias de publicidad.

8. El Estado de Chile ha suscrito y ratificado diversos instrumentos internacionales de derechos humanos relativos a la protección de datos personales, si bien no existe un reconocimiento expreso a la protección de los datos personales en los instrumentos que mencionaremos, sí podemos afirmar que la no injerencia a la vida privada ha sido un derecho humano reconocido desde el comienzo de la cristalización de los derechos humanos en los tratados internacionales de derechos humanos.

9. Así, el Artículo 12 de la Declaración Universal de los Derechos Humanos declara: "*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques*".

10. El artículo 11 de la Convención Americana de Derechos Humanos indica que, *"Protección de la Honra y de la Dignidad. 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".*

11. El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos "*1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la Ley contra esas injerencias o esos ataques".*

12. Finalmente, el Comité de Derechos Económicos, Sociales y Culturales, en el Informe Final de la revisión efectuada a Chile en el año 2015, en su párrafo 10, relativo a la recopilación y almacenamiento de datos , indicó al Estado de Chile lo siguiente: *"El Comité recomienda al Estado parte que continúe promoviendo la recopilación sistemática de datos, así como la elaboración y utilización de estadísticas sobre los indicadores de los derechos humanos, incluidos los derechos económicos, sociales y culturales basadas en tales datos. A este respecto, remite al Estado parte al marco conceptual y metodológico de los indicadores de los derechos humanos elaborado por la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (véase HRI/MC/2008/3). El Comité insta al Estado parte que incluya en su siguiente informe periódico datos estadísticos anuales comparativos sobre el ejercicio de cada uno de los*

derechos consagrados en el Pacto, desglosados por edad, sexo, origen étnico, población urbana y rural y otros criterios pertinentes[3].

b) Leyes internas sobre Datos Personales y Privacidad:

13. La Constitución Política de la República, en su artículo 19 N° 4, reconoce a todas las personas *"el respeto y protección a la vida privada y a la honra de la persona y su familia."* Una reciente reforma -Ley 21.096[4]- consagra el derecho a protección de los datos personales, agregando al referido artículo 19 a continuación de esa frase lo siguiente: *"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,"* refiriéndose a la Ley N° 19.628, sobre protección de la vida privada.
Asimismo, el artículo 19 Nº 5 consagra el *derecho a la inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley*;

14. La Ley N° 19.628, dictada en 1999, regula el tratamiento de los datos de carácter personal de las personas naturales, contempla derechos para los titulares de los datos y deberes para quienes realizan tratamiento de la información de carácter personal, y determinados principios. No obstante, esta normativa no consideró la creación de una autoridad de control administrativa con potestades de intervención, fiscalización y sanción que vele por el cumplimiento de la ley frente a infracciones en el tratamiento de datos personales, y en su lugar, dispuso únicamente un mecanismo judicial para reclamar frente al tratamiento indebido e ilegal, en el que puede exigirse indemnizaciones civiles para el afectado en la medida que se pruebe un daño.

15. Por su parte, la Ley 20.285 sobre acceso a la información pública, y que crea el Consejo para la Transparencia, entregó a este organismo la facultad de "velar por el adecuado cumplimiento de la ley Nº 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado." Sin embargo, esta institución no tiene facultades para dictar instrucciones ni sancionar, y tampoco aplica a la totalidad de los organismos públicos, sino solo a un grupo específico de aquellos.

---

[3] Comité de Derechos Económicos, Sociales y Culturales E/C.12/CHL/CO/4. Observaciones finales sobre el Cuarto informe periódico de Chile, párrafo 10.

[4] Ley 21.096 que consagra el derecho a protección de datos personales. Disponible en: https://www.leychile.cl/Navegar?idNorma=1119730

16. El artículo 222 del Código Procesal Penal (CPP) regula la interceptación de comunicaciones telefónicas y cómo las empresas de comunicación deben cumplir con estas medidas. Específicamente, la norma dispone que las empresas deben mantener -en carácter reservado a disposición del Ministerio Público- un registro de los números de IP de las conexiones de sus abonados, y que el entorpecimiento de esta práctica será considerado un delito de desacato.

17. La Ley 19.496 establece normas sobre protección de los derechos de los consumidores. Específicamente, el artículo 13 de esta ley explica que "los proveedores no podrán negar injustificadamente la venta de bienes o la prestación de servicios comprendidos en sus respectivos giros en las condiciones ofrecidas," y es utilizado para defender la necesidad de no dar su Rut (número de identificación) para completar transacciones en farmacias, retail y supermercados. Pero, además, regula el sistema de marketing directo, basado en el modelo *opt out* que implica el envío masivo de comunicaciones comerciales sin necesidad de autorización del titular de los datos, entregando a éste solo el derecho a oponerse frente a esta actividad, a diferencia del sistema adoptado en Europa *opt in.*

V. ÁREAS DE PREOCUPACIÓN

a. <u>Videovigilancia: uso de cámaras en globos aerostáticos, drones, etc.</u>

18. Desde el año 2015 a la actualidad, existe una creciente expansión de métodos de vigilancia en calles de la ciudad, cada vez más sofisticados, de la mano con el crecimiento económico de nuestro país, lo que ha traído consigo la importación de nuevas tecnologías y desarrollo de múltiples industrias. Debido a los niveles de sensación de inseguridad que existen en la ciudad de Santiago; gobiernos locales y corporaciones han realizado fuertes inversiones para hacer frente impulsando una industria de tecnología y vigilancia que en Chile se ha manifestado en globos y drones. Los globos de vigilancia operan en dos comunas de la región Metropolitana de Santiago, Las Condes y Lo Barnechea. Los drones operan además en Las Condes. En particular, preocupa la falta de competencias específicas para videovigilancia, falta de regulación legal y nulo cumplimiento y fiscalización del tratamiento de datos personales que conlleva el uso de estos dispositivos.

19. Dos acciones constitucionales fueron presentadas en este sentido, bajo la reflexión que en un corto plazo la sociedad chilena se verá expuesta a la videovigilancia por parte de drones y globos aerostáticos, ambos dispuestos con cámaras de alta resolución.

20. Si bien bajar los índices de delincuencia es un objetivo que preocupa al Estado y a la ciudadanía, en una democracia resulta imperativo que debatamos sobre el tema y el costo que trae consigo obtener, eventualmente, mayor seguridad. Asimismo, cuáles serán las normas jurídicas que regirán esta actividad y que permitirán el efectivo ejercicio de derechos. En ambas acciones, incluida la Corte Suprema, la decisión fue su rechazo[56], reduciendo por nuestros tribunales la legítima expectativa de privacidad en lugares públicos. En el caso de los globos de vigilancia, el máximo tribunal fijó reglas de operación particulares para este caso que, dado nuestro sistema jurídico, no son aplicables a otros casos.

b. <u>Reconocimiento facial y otros sistemas biométricos en implementación de políticas públicas.</u>

21. Siguiendo la misma lógica anterior, crecimiento económico y mayores recursos para invertir en TIC, y ante la necesidad de construir muchas veces una cadena de identificación segura y unívoca, en Chile se ha masificado la identificación biométrica dactilar, para los más diversos usos: controles de acceso, verificación de identidad en comercios y sistemas de salud, autenticación a sistemas de uso crítico, etc. Sin embargo, esto se proyecta en el corto plazo a tecnologías de reconocimiento facial. En efecto, la misma Municipalidad de Las Condes conocida por sus globos y drones de vigilancia, ya ha anunciado la implementación de cámaras de seguridad con reconocimiento facial donde éstas identificarán a las personas registradas en una base de datos operada por el municipio cuyo acceso es compartido con las Policías.

22. Asimismo, para el control de la evasión en el transporte público el Ministerio también ha anunciado la implementación de estas cámaras faciales en buses para controlar a quienes no pagan su pasaje. Diversos cuestionamientos surgen respecto a cómo los registros serán usados y accedidos y cómo las tecnologías permiten no sólo construir "listas negras", sino que captar información sobre todas las personas, delincan o no, evadan o no. Nuevamente

[5] Caso globos, Sentencia Rol N° 18.481-2016, Corte Suprema. Acceso a la noticia y fallos judiciales en <https://datosprotegidos.org/corte-suprema-revoco-sentencia-que-ordeno-retirar-los-globos-de-televigilancia-en-las-condes-y-lo-barnechea-que-dice-el-fallo/>
<http://www.pjud.cl/documents/396543/0/PROTECCION+GLOBOAS+AEROSTATICOS.pdf/ecb2307b-0a6a-4145-8a8e-d39c6687270e>

[6] Caso drones, Sentencia Rol Nº 34.360-2017, Corte de Apelaciones Santiago. Disponible en <http://www.pjud.cl/documents/396729/0/DRONES+LAS+CONDES+CORTE.pdf/c12fb16c-8900-474f-a325-91fd58a42eea>

se demuestra que el Estado ha tenido poca capacidad para formular normas y criterios de tratamiento de la información, accesos, eliminación, seguridad, responsabilidades, transparencia, que acompañen la implementación de tecnología, que sin estas salvaguardas solo agrava sesgos raciales y sociales.

23. En materia de beneficios, recientemente la Corte de Apelaciones de Santiago[7] dispuso la ilegalidad de las cláusulas de las bases de licitación de un sistema biométrico para el control de raciones alimenticias de los niños y niñas beneficiarias de la Junta Nacional de Auxilio Escolar y Becas (JUNAEB). El tribunal determinó que, debido a la Ley de Protección de Datos Personales, para utilizar un mecanismo de control de este tipo en menores de edad—que son los beneficiarios del programa de raciones—se requeriría consentimiento de los padres. Sin embargo, más que aludir a una cuestión del tratamiento de los datos especialmente protegidos de los menores, el fallo versó en la carga que significaba conseguir esta autorización por parte de los postulantes a dicho servicio de tecnología.

c. <u>Interceptación de comunicaciones electrónicas y telefónicas, acceso no autorizado judicialmente. Procedimientos de inteligencia y vulneración de derechos.</u>

24. Durante agosto del año 2017 son dos los hechos relevantes relativos a la interceptación de comunicaciones en Chile. El primero de ellos es el intento de aprobación mediante el Decreto N° 866[8] de nuevas reglas de retención de datos de telecomunicaciones de los abonados a las compañías proveedoras de servicios de internet, a efectos que éstos pudieran ser usados en la investigación penal. La norma pretendía extender por un periodo de dos años todos los datos referidos a los antecedentes personales del suscriptor, antecedentes para identificar el origen de la comunicación, tales como, el número de teléfono, datos de identificación del suscriptor, direcciones IP, entre otros, antecedentes para identificar el destino de la comunicación, fecha, hora y duración, equipos terminales, ubicación geográfica y la información que sería definida en una norma técnica posterior. La norma sobrepasaba las potestades reglamentarias de la administración, pues la ley[9] solo autoriza esta retención por 12 meses, además carecía de especificidad, precisión y claridad sobre los datos que los ISP estarán obligados a almacenar. Preocupa particularmente las intenciones y capacidades de intrusión a metadatos, que hoy deben ser

[7] Guzmán, F. (08 de julio de 2017). Corte Suprema detecta cláusulas ilegales. La Tercera. Disponible en: <http://www2.latercera.com/noticia/corte-suprema-detecta-clausulas-ilegales-programa-alimentacion-la-junaeb>

[8] Disponible en: <https://www.leychile.cl/Navegar?idNorma=1046228>

[9] Artículo 222 del Código Procesal Penal. <https://www.leychile.cl/Navegar?idNorma=176595>

protegidos tal y como deben protegerse los datos, siendo por tanto necesaria la intervención legislativa para cualquier intrusión. Datos Protegidos, y otras organizaciones de la sociedad, académicos y parlamentarios, alegaron frente a la iniciativa ante la Contraloría General de la República, que declaró la ilegalidad de la medida.

25. En septiembre del año 2017, el Ministerio Público (órgano persecutor penal) inició una investigación por la presunta adulteración de pruebas entregadas por Carabineros en la denominada "Operación Huracán", un operativo policial iniciado al amparo de la Ley de Inteligencia[10], que condujo a la detención de ocho comuneros mapuches supuestamente involucrados en una asociación ilícita terrorista en el sur de Chile.

26. Las pruebas presentadas en este caso provenían de un software llamado Antorcha el cual permitía acceder a las conversaciones de WhatsApp y Telegram, aparentemente mediante la instalación de un malware en los teléfonos celulares. A esta fecha se encuentra establecido que el referido software nunca existió[11], por lo que las pruebas fueron fabricadas. Lo relevante es que, dentro del sistema de seguridad nacional, Policías, Inteligencia y Ministerio Público, se validó el uso de intervención ilícita de comunicaciones, vulnerando las garantías legales, que señalan que éstas sólo pueden realizarse cuando exista un triple filtro de proporcionalidad: delito grave, persona sindicada como autor y ser los únicos medios por los cuales se puede obtener una evidencia. Por otra parte, la Operación Huracán se trató de una operación de inteligencia, lo que implica que las normativas constitucionales que protegen los datos personales y el secreto de las comunicaciones quedan al margen, no aplicando el "triple filtro", sino los procedimientos especiales de obtención de información. Estos procedimientos especiales son la intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia; la intervención de sistemas y redes informáticos; la escucha y grabación electrónica, y la intervención de cualquier otro sistema tecnológico destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información. Estos métodos, cita la misma ley de inteligencia, sólo podrán usarse en actividades de inteligencia y contrainteligencia para resguardar la seguridad nacional y ante amenazas de terrorismo, el crimen organizado y el narcotráfico. La información obtenida servirá para apoyar decisiones estratégicas de la policía, pero no podrá utilizar estas pruebas en

[10] Ley 19.974 sobre el sistema de inteligencia del estado y crea la Agencia Nacional de Inteligencia. Disponible en: https://www.leychile.cl/Navegar?idNorma=230999

[11] Noticia de Diario La Tercera <http://www.latercera.com/reportajes/noticia/antorcha-nunca-existio-las-claves-del-ultimo-informe-la-operacion-huracan/154002/>; y Tele13 <http://www.t13.cl/noticia/nacional/operacion-huracan-alex-smith-admitio-software-antorcha-jamas-existio>

un juicio. Este caso aún no está cerrado, y si bien los comuneros fueron liberados, continúa el debate sobre el uso de pruebas de inteligencia en procesos judiciales.

d. <u>Registros de personas para consulta en Internet: deudores de transporte público, padrón electoral, etc.</u>

27. Corresponde señalar la idea instalada en Chile sobre los registros de carácter público, como aparente fuente de solución a diversos problemas de la sociedad. Si bien el Estado requiere información para tomar decisiones y los registros pueden ser una de esas fuentes, es menester que éstos se construyan siguiendo ciertas normativas básicas sobre tratamiento y garantías sobre la información personal. Una de esas garantías es la sujeción al principio de finalidad, esto es, que los datos registrados sólo puedan ser usados para los objetivos declarados en su almacenamiento. Un ejemplo de la vulneración a la que nos exponen los registros públicos son los "rutificadores", sitios web donde es posible encontrar y acceder, con la sola redacción del nombre o el RUT de una persona natural, en un formulario de búsqueda, a su información personal como el RUT, domicilio, sexo y otros datos privados. Estos sistemas se generan al alero de la publicación en Internet de datos electorales, los cuales son reprocesados y publicados en plataformas de búsqueda, sin la capacidad que los titulares de esos datos puedan conocer quiénes son las personas responsables de esos segundos registros de datos, no revelan ninguna información sobre origen de los mismos, cesiones, o manera de ejercer algún derecho de los consagrados en la ley: acceso, rectificación y cancelación o eliminación.

28. Estos sitios son el efecto práctico e indeseado de la publicación del padrón electoral dispuesta por la Ley 20.568[12] y anteriormente por el órgano chileno de transparencia, lo que termina por generar una base de datos de fuente accesible al público[13], un concepto que ha sido debatido por los expertos en cuanto a su origen e interpretación. Las normas electorales que autorizan la publicación del padrón atienden a la transparencia que debe rodear su confección frente a los intervinientes del proceso político, sin embargo, no considera el ordenamiento jurídico en su conjunto. En efecto, no avizora que la falta de una ley robusta en la protección de éstos, sumado a la realidad técnica actual, conduce a un acceso peligroso y descontrolado por parte de personas distintas a los titulares del RUT, lo que se traduce en términos concretos, en el acceso indebido a una esfera de resguardo

[12] Ley que regula la inscripción automática, modifica el servicio electoral y moderniza el sistema de votaciones. Disponible en: https://www.leychile.cl/Navegar?idNorma=1035420

[13] Artículo 2 letra I) Ley N° 19.628: i) Fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.

que muchas de las personas no exponen de una forma así de liviana y abierta. A lo anterior, agregamos que el número de identidad permite con mayor fluidez intercambiarse e ingresar en cualquier otro sistema que contenga la capacidad de abrirse bajo el mismo parámetro de identificación, tanto sistemas de bases de datos públicas como privadas, multiplicando las posibilidades de no solo atentar contra la privacidad si no contra la dignidad de las personas.

29. En segundo lugar, la creación del registro de evasores del transporte público y el registro de usuarios del transporte. Si bien ambos tienen finalidades distintas, en lo que importa, el Registro de Evasores del transporte, tiene por objeto anotar a las personas evasoras del pago del pasaje y que terceros puedan consultar este registro a efectos de verificar si una persona está incorporada en él o no. Si bien la ley[14] previó varias cuestiones relativas a la protección de los datos, e hizo previsiones tales como que ninguna consulta podrá afectar negativamente a quienes en él aparezcan en aspectos laborales, comerciales, inmobiliarios, crediticios o de acceso a diversos beneficios, esto resulta dudoso pues en Chile no existe un ente de control que permita verificar el cumplimiento de la norma y en segundo término, las autoridades han declarado públicamente que se espera que este registro tenga un uso disuasivo, en cuanto a que las personas sepan las connotaciones negativas de estar incorporados en él, puesto que podrá ser consultado por terceros. La ley que entró en vigencia el 04 de junio de 2018, delegó en un reglamento las cuestiones operativas del mismo, reglamento que aún no ha sido aprobado.

VI. RÉGIMEN DE PROTECCIÓN DE LOS DATOS PERSONALES EN CHILE

30. En este apartado identificamos tres áreas sumamente relacionadas con los datos personales—salud, banca, consumo y transparencia—y cómo las leyes protegen, o no, los datos de los ciudadanos en las áreas de salud y consumo y cómo la transparencia es esencial en asegurar la protección de datos en las otras áreas.

a. Salud:

31. En el caso del área salud, se permite que el tratamiento de la información pueda ser desarrollado por terceros; el artículo 3 DFL Nº1 de 2005[15] estipula que *"la labor de inspección o verificación del cumplimiento de las normas podrá ser encomendada a*

[14] Adopta medidas de seguridad y control en medios de pago del transporte público de pasajero. Disponible en: https://www.leychile.cl/Navegar?idNorma=1116754

[15] DFL Nº1 2005, Ministerio de salud. Disponible en: https://www.leychile.cl/Navegar?idNorma=249177

terceros idóneos debidamente certificados conforme al reglamento, sólo en aquellas materias que éste señale y siempre que falte personal para desarrollar esas tareas y que razones fundadas ameriten el encargo.". Sin embargo, no menciona la fiscalización respecto a estos "proveedores" por lo que infiere que los términos respecto al uso o almacenamiento de la información queda estipulado en los contratos.

32. Lo anterior resulta preocupante dada la facilidad con que los sistemas informáticos estatales han presentado brechas de seguridad de distinta índole. Uno de aquellos casos fue la filtración de la base de datos de salud de pacientes con VIH. Datos Protegidos solicitó al órgano fiscalizador su intervención[16].

33. Los datos de salud son datos sensibles y por lo tanto un mal uso de estos datos puede vulnerar los derechos de individuos con consecuencias graves. Por ende, requieren el estándar más alto de protección y una regulación más transparente, algo que no se encuentra con una dependencia en terceros. Aunque la ley dice que estos terceros contratados tienen que seguir los requisitos estipulados, no menciona detalladamente sobre cómo se fiscalizará estos terceros, dando mucho control a los proveedores.

b. <u>Banca:</u>

34. En noviembre de 2015, Datos Protegidos inició dos juicios contra el Banco Santander Chile, por abandono de miles de documentos en terrenos rurales, que contenían información personal de clientes del banco. En uno de los casos, se obtuvo una sentencia favorable[17], ordenándose el pago de una indemnización a los afectados. En cambio, el segundo caso, que se tramitaba en otro tribunal de primera instancia, se resolvió no dar lugar a la indemnización, caso que fue apelado y actualmente se encuentra en la Corte Suprema para su revisión.

c. <u>Consumo</u>:

35. La ley sobre protección de los derechos de los consumidores[18] no menciona normas respecto al tratamiento de uso de base de datos de sus clientes ya sea para fidelizar o hacer seguimiento de deudas.

---

[16] Disponible en <https://datosprotegidos.org/contraloria-se-pronuncia-acerca-de-filtracion-de-datos-sensibles-en-red-de-asistencia-publica-de-salud/>

[17] Disponible en: <https://datosprotegidos.org/datos-protegidos-gana-juicio-en-primera-instancia-contra-banco-santander/>

[18] Ley 19.496 que establece normas sobre protección de los derechos de los consumidores. Disponible en: https://www.leychile.cl/Navegar?idNorma=61438

36. Solo hace mención de que si se realiza una compra virtual el contrato y datos de este serán almacenados, no se especifica mediante qué medio pueden ser guardados, no indica por cuánto tiempo ni qué tipo de información puede ser almacenada en este documento contractual, tampoco indica si es solo para productos o también para servicios por lo que deja un vacío en cuanto a la interpretación de la ley y quien es responsable de la información recabada.

37. Sin embargo, en los últimos 20 años mucho ha cambiado acerca del tratamiento de los datos personales, especialmente con la comercialización de los datos de los consumidores: cada vez más, los datos están siendo recopilados con el fin de vender o usar estos datos en un ámbito comercial. Por consiguiente, la presente ley, cual fue escrita en 1997, no está actualizada en relación con la protección de los datos personales de los consumidores y no protege en manera clara y directa estos datos.

d. <u>Transparencia</u>:

38. Las disposiciones de Ley 20.285 sobre acceso a la información pública[19] son aplicables a los siguientes órganos del Estado: los ministerios, las intendencias, las gobernaciones, los gobiernos regionales, las municipalidades, las Fuerzas Armadas, los servicios públicos, y en menor medida a las empresas del Estado, la Contraloría General de la República, el Banco Central, el Congreso Nacional, los Tribunales que forman parte del Poder Judicial, el Ministerio Público, el Tribunal Constitucional y la Justicia Electoral.

39. El principio de transparencia de la función pública consiste en respetar y cautelar la publicidad de los actos, resoluciones, procedimientos y documentos de la Administración, así como las de sus fundamentos y en facilitar el acceso a esa información a cualquier persona.

40. Define como información pública a los actos y resoluciones del Estado, y la información elaborada con presupuesto público, salvo las excepciones que establece esta ley, cuando afecte: el debido cumplimiento de las funciones de un órgano del Estado; los derechos de las personas; la seguridad de la nación; el interés nacional y cuando una ley de quórum calificado haya declarado reservada o secreta cierta información.

[19] Ley 20.285 Sobre acceso a la información pública. Disponible en: https://www.leychile.cl/Navegar?idNorma=276363

41. Obliga a los órganos de la Administración del Estado a mantener en sus sitios web la información permanente y actualizada, al menos una vez al mes, de antecedentes tales como: estructura orgánica, facultades, personal, información sobre el presupuesto, resultados de auditorías, etc. Esto es lo que se denomina, transparencia activa. La fiscalización la realizan los controles internos de cada institución, el Consejo para la Transparencia y la Contraloría General de la República.

42. Además, establece que toda persona tiene derecho a solicitar y recibir información de cualquier órgano de la Administración del Estado. Es lo que se conoce como transparencia pasiva o derechos de acceso. El problema que surge y puede ser perjudicial, es el motivo de consulta de la información: no se hace seguimiento ni es regulado en el caso de difundir de manera excesiva tales datos obtenidos mediante la aplicación de la Ley de Transparencia.

43. Respecto a la regulación se especifica que la tarea recae en el Consejo para la Transparencia, que tiene por objeto promover la transparencia de la función pública, fiscalizar el cumplimiento de las normas sobre transparencia y publicidad de la información de los órganos de la Administración del Estado, y garantizar el derecho de acceso a la información.

44. Es relevante indicar que el Consejo debe velar por la debida reserva de los datos e informaciones que conforme a la Constitución y a la ley tengan carácter secreto o reservado, indicando que este Consejo es el responsable de la reserva y/o difusión de los datos, complementado con el velar por el adecuado cumplimiento de la ley Nº 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado. En este contexto existen bastantes casos en que el organismo ha resuelto la entrega de información personal, incluso sensible, casos en que los entes afectados han debido recurrir a la Corte de Apelaciones para evitar la entrega de datos que importa la vulneración al derecho a la privacidad, como aquel en que se pretendía la entrega del registro de condenados[20], y que fue declarado ilegal.

VII. RECOMENDACIONES

[20] Causa Rol N°1860-2017, de la Corte de Apelaciones de Santiago. Decisión de Amparo rol C-3721-16, del Consejo para la Transparencia.

45. Contar con una normativa de protección de datos actualizada en esta materia, tomando en cuenta las tecnologías nuevas y cambiantes. Esto incluye la regulación del uso de drones, globos de vigilancia y sistemas biométricos como tecnología de reconocimiento facial, limitando el alcance de estos sistemas y el uso de la información que es recolectada. Estas tecnologías pueden tener repercusiones negativas en la vida privada de los ciudadanos y, por lo tanto, requiere reglas y leyes actualizadas y aptas para asegurar un uso legítimo y proporcional al fin perseguido.

46. Crear una autoridad nueva, específica e independiente de protección de datos que pueda ejercer sus funciones sin influencia externa. Las agencias de datos deben ser organismos sumamente especializados, pues deben regular al sector privado en materia de tratamiento de datos, tales como el marketing, salud, crédito, educación, tecnología aplicada a los datos (internet de las cosas, big data, geolocalización, inteligencia artificial), televigilancia, biometría, entre otras; y al sector público en el tratamiento de datos propiamente tal, cesiones de datos, y además en la aplicación de las causales de reserva fundadas en datos personales cuando proceda. Esta autoridad debe fiscalizar las operaciones de tratamiento de datos personales, sancionar a los que infrinjan la ley de datos e interpretar las leyes de protección de datos. Por lo tanto, sus funciones deben ser únicas, no compartidas con otros entes públicos.

47. Contar con una normativa más clara y específica sobre la protección de datos de los titulares, especialmente regulando el almacenamiento de estos datos personales, detallando cuáles datos pueden ser recolectados, por cuánto tiempo pueden ser recolectados y a quien será otorgada la responsabilidad sobre los datos. Esta regulación es sumamente importante dado a que los datos personales de los ciudadanos están siendo cada vez más monetizados y utilizados para ganancia de las empresas privadas.

48. Fomentar la conciencia pública sobre la importancia del derecho a la privacidad y la necesidad de proteger los datos personales mediante campañas educativas, campañas comunicacionales y difusión. Es importante que la ciudadanía—quienes son los afectados directamente por las normativas, leyes, vulneraciones, y recopilaciones de los datos personales—sea más informada sobre lo que está ocurriendo con sus datos, no solo para tener más opciones en tomar decisiones sino también, para pronunciarse en contra de las violaciones de su derecho de la privacidad.

49. Apoyar y empoderar los gobiernos locales para enfocarse en el tema de protección de datos y derecho a la privacidad como derechos fundamentales. Con un enfoque en el nivel

comunitario y local, estos temas de datos y privacidad empiezan a ser más importantes en la conciencia ciudadana y, por lo tanto, parte del debate nacional.

50. Contar con normas en materia de movimientos transfronterizos de datos que estén acorde a los estándares internacionales, como el reciente Reglamento Europeo de Protección de Datos. Con la globalización de los mercados y empresas el tratamiento de los datos personales está ocurriendo más allá de las fronteras nacionales y resulta cada vez más importante regular el movimiento de los datos.