

Informe de las partes interesadas
Examen Periódico Universal
32º período de sesiones – Chile
Enero – 2019



El Derecho a la privacidad



**Comunicación conjunta de Derechos Digitales,
Ciudadano Inteligente, Fundación Pro Acceso,
y Privacy international**

Julio 2018

El Derecho a la privacidad

Julio 2018

I. Introducción

1. Este informe es presentado por Derechos Digitales, Ciudadano Inteligente, Fundación ProAcceso y Privacy International. Derechos Digitales es una organización no gubernamental de defensa, promoción y desarrollo de los derechos humanos en el entorno digital. Ciudadano Inteligente es una organización dedicada a fortalecer la democracia y reducir la desigualdad a través de la transparencia y la participación ciudadana. Fundación ProAcceso se dedica a la defensa del derecho de acceso a la información pública como un derecho fundamental. Privacy International es una organización de derechos humanos que trabaja en fomentar y promover el derecho a la privacidad y combatir la vigilancia alrededor del mundo.
2. Las organizaciones antes mencionadas desean manifestar sus preocupaciones sobre el derecho a la privacidad, y otros derechos fundamentales relacionados con éste. Estos temas no fueron abordados en revisiones anteriores del Estado chileno, y deseamos sean puestas a consideración en la sesión 32 del Grupo de Trabajo del Examen Periódico Universal (EPU).

II. Obligaciones de protección de la privacidad en Chile

a. Obligaciones internacionales

3. Chile ha suscrito y ratificado diversas convenciones y tratados internacionales, que se refieren a la protección de la privacidad y de datos personales. Ratificó el Pacto Internacional de Derechos Civiles y Políticos, cuyo artículo 17 protege la privacidad. Desde el 8 de octubre de 1990, Chile es signatario de la Convención Americana sobre Derechos Humanos, que en su artículo 11 también garantiza la privacidad. A todos los tratados de derechos humanos ratificados por Chile se les han concedido la misma jerarquía legal que la Constitución Política de acuerdo con el artículo quinto de la misma.

b. Leyes internas que impactan el ejercicio de la privacidad

4. La Constitución Política, 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, 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”*¹; mientras que el N°5 del mismo artículo, dispone *“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”*.
5. El Código Procesal Penal (CPP) regula el procedimiento de interceptación de comunicaciones telefónicas y de correspondencias en el contexto de una investigación criminal, y establece obligación de retención de datos por un

tiempo mínimo para los prestadores de servicios de acceso a Internet, en sus artículos 218 y 222.

6. La Ley N°19.974 Sobre el sistema de inteligencia del Estado y que Crea la Agencia Nacional de Inteligencia (Ley de Inteligencia) regula los organismos que desarrollan tales labores,² y establece controles con el objetivo de proteger las garantías constitucionales, incluyendo el secreto de la información recabada, y la necesidad de obtener una orden judicial para llevar adelante procedimientos especiales de obtención de información.
7. La Ley N°19.628 sobre protección de datos de carácter personal (LPD) regula el tratamiento de información referida a personas naturales identificadas o identificables, sistematiza los derechos y deberes involucrados en la recolección y tratamiento de datos personales; y, establece un mecanismo judicial para exigir indemnizaciones civiles en caso de incumplimiento. No contempla una autoridad administrativa con potestades de fiscalización y sanción por contravenciones.

III. Principales áreas de preocupación

a. Abusos en materia de vigilancia estatal

i) Vigilancia focalizada y descontrolada contra grupos específicos y comunidades indígenas

8. La implementación de tecnologías de vigilancia, ha tenido como principal consecuencia la vigilancia indiscriminada y constante a miembros de ciertos grupos sociales o étnicos, quienes se ven compelidos a dejar de actuar naturalmente por sentirse observados y perseguidos.³
9. En particular, la población Mapuche en sur del país es constantemente acosada y vigilada por las fuerzas militares y policiales en la zona sur del país, donde dichas comunidades han habitado desde antes de la creación del Estado. Algunos grupos se encuentran luchando por la recuperación de tierras ancestrales, mediante acciones que en ocasiones se han perseguido como actos terroristas por la autoridad. Esta vigilancia es llevada a cabo por medios presenciales tales como la implantación de puntos de control en caminos rurales, para control policial indiscriminado de la circulación de personas y vehículos; y también de manera remota, a través del uso y abuso de mecanismos de interceptación de telecomunicaciones, rastreo de geolocalización, y el empleo de drones - con sofisticadas capacidades de vigilancia.⁴
10. La Ley de Inteligencia regula el actuar de los organismos de inteligencia en el marco de una investigación que tenga por objeto el resguardo de la seguridad nacional y proteger al país de las amenazas del terrorismo, el crimen organizado

y el narcotráfico. También contempla procedimientos especiales de obtención de información para los organismos de inteligencia. El artículo 23 de ella señala que la información a recabar debe resultar *“estrictamente indispensable para el cumplimiento de los objetivos del Sistema y no pueda ser obtenida de fuentes abiertas”*, imponiendo un elevado estándar para la aplicación de tales procedimientos.

11. La exigencia estricta del artículo 23 se refuerza con lo dispuesto en el inciso segundo del artículo 28 de la misma ley, al imponer como requisitos esenciales de la autorización judicial otorgada por un Ministro de Corte de Apelaciones competente, que dicha resolución debe incluir *“especificación de los medios que se emplearán”*, además de la individualización de las personas a quienes se aplica la medida y las limitaciones temporales de su aplicación.
12. En 2017 se desarrolló la denominada “Operación Huracán”, la cual tenía por objetivo intentar interceptar y vulnerar el cifrado de las comunicaciones electrónicas de comuneros indígenas Mapuche. Esta operación de inteligencia puso en evidencia las insuficiencias de la Ley de Inteligencia para establecer un control efectivo que asegure el ejercicio sin exceso, por parte de estos organismos, de las facultades que le reconoce la Ley. La “Operación Huracán” Se inició como una operación de inteligencia, y terminó como un operativo policial con la detención de ocho dirigentes de comunidades Mapuche, imputados por su supuesta coordinación en ataques incendiarios en la zona sur del país.⁵
13. El Ministerio Público cerró más tarde el caso al llegar a la conclusión de que los teléfonos de los comuneros habían sido intervenidos en forma ilegal por parte de la Unidad de Inteligencia Operativa Especializada de Carabineros, con la intención de generar pruebas falsas e inculpativas contra los imputados. Carabineros habría insertado mensajes falsos en las aplicaciones Whatsapp y Telegram que se encontraban instaladas en los teléfonos celulares de los imputados después de su incautación. Información que se logró determinar tras el peritaje realizado por el Ministerio Público y organismos externos.⁶
14. La información inicial del caso apuntaba a que Carabineros contaba con un software de creación propia (denominado “Antorcha”) capaz de quebrar el cifrado de los mensajes de Whatsapp y Telegram. Y aunque a la fecha no ha sido posible acreditar la existencia de dicha tecnología, lo cierto es que, a través de una combinación de uso de phishing (fraude informático para acceder a información confidencial que permite suplantación de identidad) y uso de malwares públicamente disponibles, se intentó tomar control de la información contenida en dichos dispositivos, aparentemente sin éxito. Luego, perseverando en actividades focalizadas contra los comuneros mapuches, se intentó implantar mensajes falsos en los dispositivos.⁷ Todo lo anterior, amparado en una orden judicial excesivamente amplia, en cuanto a las actividades de vigilancia autorizadas y las personas alcanzadas con

ellas, obtenida al alero de la Ley de Inteligencia, pero sin un control de mérito sustantivo por el juez para cumplir con las limitaciones de dicha normativa.⁸

15. De lo anterior, sólo puede concluirse que los mecanismos contenidos en aquella normativa resultan insuficientes para cautelar que no se vulnere en su aplicación el respeto por la privacidad y la inviolabilidad de las comunicaciones de ciudadanos amparados por el principio de presunción de inocencia. La ley de inteligencia carece controles externos que permitan precaver los excesos de los organismos de inteligencia en su aplicación, y el poder judicial está fallando en aplicar un control sustantivo de las actividades de inteligencia al autorizarlas.
16. Por otra parte, se ha acreditado la compra del software de Forensic Oxygen, destinado a “recuperar todos los datos de las aplicaciones vitales del dispositivos móviles con iOS, el sistema Android, BlackBerry 10, Windows Phone 8”,⁹ por parte de los servicios de inteligencia a cargo de esta operación. La compra se rodea de circunstancias oscuras como el pago de altas sumas en efectivo, lo que dista de un proceso de adquisición y uso transparente.¹⁰ A esto se suma la adquisición en circunstancias similares de otras tecnologías de vigilancia, como expondremos más adelante.
17. Finalmente, y lo que resulta más relevante, la información obtenida de un procedimiento especial de inteligencia como el de este caso, carece totalmente de legalidad como prueba dentro de un proceso criminal si ha sido obtenida sin supervisión de parte del Ministerio Público, y sin una autorización previa de parte del Juez de Garantía competente.
18. Con ello, se infringen y exceden gravemente las salvaguardas a la privacidad contempladas en la Ley de Inteligencia, que fueron tenidos en cuenta la hora de aprobar las facultades excepcionales que en ella se contemplan. Estas facultades permiten la restricción proporcional y necesaria del derecho a la privacidad, no la conculcación de este derecho fundamental.

ii) Falta de salvaguardas legales para la obtención de evidencia en juicios criminales.

19. La Ley chilena no contiene suficientes protecciones relativas a la vigilancia de las comunicaciones ni incautación de informaciones privadas en juicios criminales, incluyendo casos donde la interceptación de comunicaciones no se notifican previamente al afectado, y una innecesaria distinción entre comunicaciones telefónicas y electrónicas.
20. El Código Procesal Penal regula el procedimiento de interceptación de correspondencia, incluyendo los correos electrónicos, y de comunicaciones telefónicas en los artículos 218 y 222, respectivamente. Sin embargo, como consecuencia de la evolución tecnológica, los requisitos exigidos para solicitar la incautación de correspondencia del artículo 218 -que se aplican en la práctica a documentos en formato digital y comunicaciones electrónicas-

son menos exigentes que los contenidos en el artículo 222 para intervenir comunicaciones telefónicas.

21. Así, en el artículo 218 sólo se requiere respecto a la medida de incautación que “por motivos fundados fuere previsible su utilidad para la investigación”, lo que resulta excesivamente amplio y ambiguo. En cambio, el artículo 222 regula de manera más detallada y exhaustiva los requisitos de procedencia de la interceptación telefónica, señalando como presupuesto mínimo que el hecho investigado pudiera merecer pena de crimen (superior a cinco años). Que tales exigencias no apliquen en el caso de comunicaciones electrónicas afecta directamente al debido proceso y al principio de proporcionalidad.
 22. Actualmente, los dispositivos electrónicos que son intervenidos en el marco de un proceso penal, contienen más de un mecanismo de comunicación. En consecuencia, la normativa actual asigna un estándar de exigencia más bajo para autorizar la intervención del correo electrónico o servicio de mensajería instantánea (como Whatsapp), que para intervenir un llamado telefónico. Lo anterior conduce al desarrollo de investigaciones que no satisfacen estándares de derechos en materia de privacidad y debido proceso, en cuanto a la recolección de evidencia de comunicaciones electrónicas.
 23. La diferencia de estándar aplicable entre comunicaciones telefónicas y electrónicas carece de justificación lógica, pues lo que el derecho a la privacidad protege es el contenido de las comunicaciones sin importar el soporte por el cual estas se llevan a cabo. Es necesario, en consecuencia, una reforma para que la ley chilena cumpla con el principio de proporcionalidad y las exigencias de un debido proceso, otorgando el mismo nivel de protección a las comunicaciones cualquiera sea su medio.
- iii) Régimen desproporcionado de retención de datos de comunicaciones.**
24. El artículo 222 del CPP regula la interceptación de las comunicaciones telefónicas, disponiendo cómo las empresas de comunicaciones deben cumplir con las órdenes de interceptación. Las empresas están obligadas a proporcionar a los funcionarios encargados de la diligencia las facilidades necesarias para que se realice. Sin embargo, el mismo artículo dispone además que los proveedores de servicios deben mantener -en carácter reservado- a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados. La norma no señala un límite máximo de tiempo para esta retención.
 25. Por su parte, el Decreto N°142 del año 2005,¹¹ regula en detalle el procedimiento que deben seguir los prestadores de servicios de telecomunicaciones frente a los requerimientos judiciales para proceder a la interceptación y a la grabación de las comunicaciones sostenidas por sus usuarios.

26. En 2017, el Gobierno trató de incrementar las obligaciones de retención de datos a través de la dictación del Decreto N°866, que intentó reforzar las habilidades de los organismos de persecución penal, otorgándoles amplias y desproporcionadas facultades de investigación, de un modo incompatible con el derecho a la privacidad y las disposiciones legales y constitucionales vigentes antes mencionadas.
27. El Decreto N°866 intentó modificar la obligación que tienen las compañías de telecomunicaciones de retener los datos de las comunicaciones efectuadas en Chile, extendiendo el período de almacenamiento de éstos de uno a dos años. Omitía además el requerimiento explícito de que en todos los casos se requiere de una orden judicial previa para acceder a los datos retenidos. Incluso buscaba poner trabas a la posibilidad de que los proveedores de servicios implementaran cifrado de sus comunicaciones por defecto. Aumentaba además el tipo y cantidad de datos sobre las comunicaciones que debían ser almacenados por los proveedores de servicios,¹² bajo el argumento de que estos datos no son datos personales, sino que solo datos comunicacionales o metadatos.
28. Diversos grupos de la sociedad civil reclamaron la ilegalidad de la norma propuesta ante la Contraloría General de la República, que es el órgano constitucionalmente encargado de revisar la legalidad de los actos ejecutados por la administración, y quien finalmente objetó la propuesta por no ajustarse a estándares de legalidad en la intromisión en derechos fundamentales.¹³
29. El nuevo gobierno ha venido anunciando el reforzamiento de las facultades de investigación de las policías y el uso de nuevas tecnologías para ello. Esto representa una clara amenaza de que se persevere en la ampliación de obligaciones de retención de datos, y se continúe debilitando la privacidad y la inviolabilidad de las comunicaciones.
30. La interceptación, recolección y uso de metadatos interfiere con el derecho a la privacidad, tal como lo han reconocido expertos en derechos humanos, incluyendo el Relator Especial de la ONU sobre libertad de expresión, el Relator Especial de la ONU sobre la lucha sobre la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo y el Alto Comisionado para los Derechos Humanos. El Tribunal de Justicia de la Unión Europea (TJUE) también señaló que los metadatos pueden permitir "extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han retenido" y concluyó que la retención de metadatos relativos a la vida privada y las comunicaciones de una persona es en sí misma, una injerencia en el derecho a la intimidad.¹⁴ El TJUE también sostuvo en un caso diferente que el derecho de los derechos humanos prohíbe a la "legislación nacional que, con el fin de combatir el delito, prevea la retención general e indiscriminada de todos los datos de tráfico y localización".¹⁵ Por su parte, el Comité de Derechos Humanos de la ONU ha confirmado que las políticas de

retención de datos constituyen una interferencia con el derecho a la privacidad y que, como regla general, los estados deben "abstenerse de imponer la retención obligatoria de datos por parte de terceros".¹⁶

iv) Adquisición y empleo desproporcionado de tecnologías de vigilancia.

31. Durante los últimos años, el Estado ha invertido grandes sumas de dinero en la adquisición de diversas tecnologías de vigilancia bajo el argumento de optimizar la investigación criminal. Sin embargo, no existen cifras ni datos oficiales sobre estos gastos, más allá de aquellos proactivamente solicitados por organizaciones de la sociedad civil y, en muchas ocasiones, negados bajo dudosos fundamentos de seguridad nacional. Además, tampoco existe en Chile una reglamentación específica que regule mecanismos de transparencia en la compra y uso de estas tecnologías por autoridades nacionales o locales.
32. Para el cumplimiento de las facultades de investigación criminal, o para el desarrollo de actividades de inteligencia, se adquieren por las diversas entidades estatales, tecnologías de vigilancia tales como softwares, malwares, IMSI catchers, entre otras, sin que dentro de las regulaciones que rigen a las policías y fuerzas armadas se contemplen garantías de control, supervisión y transparencia, que permitan constatar que el uso de estas tecnologías de vigilancia se registre en concordancia con el respeto de la privacidad y otros derechos fundamentales involucrados. Lo anterior es particularmente importante, dados los escándalos de corrupción y malversación de fondos que han involucrado a estas organizaciones en los últimos dos años.¹⁷
33. En el año 2015, la empresa Hacking Team (HT), una de las más importantes en el rubro del software de vigilancia a nivel mundial, fue hackeada y expuesta públicamente. La información revelada permitió descubrir que la Policía de Investigaciones de Chile (PDI) se contaba entre sus clientes. El malware adquirido es tan invasivo que no solamente puede intervenir conversaciones, sino que tiene capacidad para registrar todo tipo de información, incluyendo clics y datos del dispositivo infectado. Si bien en aquella oportunidad la PDI señaló que la vigilancia a través del malware adquirido se efectuaba considerando el pleno respeto a la ley y con orden judicial, en uno de los correos electrónicos filtrados, la PDI señaló a HT que el propósito del programa *"es usarlo como herramienta de apoyo para obtener los datos IP de los clientes y acceso a información que no obtendrán a través de una orden judicial"*.¹⁸
34. En relación con estas herramientas, los mecanismos de derechos humanos de la ONU han expresado su preocupación sobre el uso del hackeo con fines de vigilancia.¹⁹ El Relator Especial de la ONU sobre libertad de expresión señaló en su informe de 2013 que "los programas informáticos ilegales invasivos como los troyanos o los mecanismos de interceptación a gran escala atentan seriamente contra las nociones tradicionales de vigilancia que no pueden conciliarse con la legislación en vigor sobre vigilancia ni con el acceso a la información privada

(...) Desde una perspectiva de derechos humanos, el uso de estas tecnologías es sumamente perturbador. No solo permiten al Estado acceder a dispositivos, sino que también les permiten modificar, en forma inadvertida o deliberada, la información allí contenida. Esto atenta no solo contra el derecho a la intimidad y los derechos a la equidad procesal respecto del uso de estas pruebas en las actuaciones judiciales".²⁰

35. En el año 2008, la Policía de Investigaciones de Chile (PDI) utilizó simuladores de torres de celulares con el objetivo de intervenir teléfonos y retener sus datos.²¹ En muchos casos, estas vigilancias eran efectuadas sin orden previa del Ministerio Público, y sin autorización judicial que respaldara su ejecución. Estos dispositivos, además de vulnerar el debido proceso dentro de un proceso penal constituyen una verdadera vulneración a la privacidad de las personas que no están siendo investigadas. En efecto, cuando estas antenas son activadas, recolectan indiscriminadamente información y datos de todos los teléfonos que se conecten en esa zona, no existiendo garantía alguna del cumplimiento de la destrucción de los registros que fueran irrelevantes dentro de un procedimiento investigativo. En la actualidad, la PDI sigue utilizando estas antenas en la generalidad de las investigaciones, omitiendo en consecuencia, el carácter excepcional que debiese primar en su ejecución.^{22 23}

v) *Vigilancia masiva, desproporcionada y descontrolada en espacios públicos.*

36. Durante los últimos años autoridades locales han implementado el uso de naves no tripuladas -como globos de vigilancia y drones- dotadas de cámaras de alta resolución, con el argumento de incrementar los niveles de seguridad, ayudar en la persecución penal de los delitos y servir como un método de prevención de acciones delictuales. Ellas constituyen políticas de vigilancia masiva, arbitrarias y altamente intrusivas, que ponen en riesgo la privacidad y otros derechos fundamentales de las personas en forma constante y permanente.
37. A pesar de que la implementación de tales programas de vigilancia masiva a nivel local ha sido denunciada por diversas organizaciones de la sociedad civil, los tribunales de justicia nacional, incluyendo la Corte Suprema, no han reconocido que dichos programas implican una afectación desproporcionada al ejercicio de los derechos a la privacidad, la libertad de expresión, el derecho a la libertad de reunión y a la no discriminación.
38. Sin perjuicio del reconocimiento al derecho a la privacidad efectuado por la Corte Suprema en uno de los casos sobre vigilancia en espacios públicos,²⁴ a la fecha no existe una regulación general que vele por que las tecnologías y planes de vigilancia en materia de seguridad pública respeten los derechos humanos involucrados y los protejan de interferencias desproporcionadas, generando altos niveles de incertidumbre y arbitrariedad en la forma en que estos sistemas de vigilancia son implementados, atomizando en distintos organismos públicos la decisión de uso de tecnologías, sin que exista ningún

mecanismo de control o fiscalización que asegure el respeto efectivo de derechos humanos al momento de usar estas tecnologías.

39. Ejemplo de lo anterior, es el plan de vigilancia masivo que, en 2015, dos municipios de la Región Metropolitana implementaron a través de la utilización de globos aerostáticos dotados con cámaras de alta resolución posibilitando una amplia y detallada visión de todo lo que ocurre en el espacio público, e incluso el interior de las viviendas.²⁵
40. La implementación de este plan fue reclamada judicialmente a través de una acción de amparo constitucional destinada a proteger los derechos fundamentales. En primera instancia la Corte de Apelaciones se declaró la ilegalidad del plan fundado en su afectación a la vida privada, la falta regulación expresa para la videovigilancia en Chile, y la constatación de que el resguardo a la seguridad no justifica la intromisión a la privacidad.²⁶ Sin embargo, en segunda instancia la Corte Suprema revocó dicho criterio considerando que los compromisos de autorregulación adoptados por las autoridades involucradas resultaban efectivos para precaver la afectación del derecho a la privacidad, creando un irregular “régimen de autorización” sin ley, que descansa en el cumplimiento voluntario de las autoridades de una serie de condiciones, no sometidas a fiscalización de ninguna especie, y que no aseguran el respeto a la privacidad.
41. Otro plan de vigilancia masiva fue implementado en 2017 por la Municipalidad de Las Condes, esta vez con drones para vigilar espacios públicos y controlar la presencia de infractores a la ley. Nuevamente, varias organizaciones, incluyendo a Derechos Digitales, recurrieron a la justicia. Y nuevamente, la justicia rechazó las acciones legales, basados en la confianza en la capacidad de autorregulación de las autoridades a cargo de implementación del plan de vigilancia.²⁷
42. La recopilación de información públicamente disponible puede conducir a abusos a través de operaciones de vigilancia encubierta. Aunque los datos se obtengan de espacios públicos, los principios de legalidad, necesidad y proporcionalidad determinados por los estándares internacionales de derechos humanos siguen teniendo aplicación. El hecho de que estas prácticas no estén específicamente reguladas por la legislación chilena y se dejen a los códigos voluntarios no satisface los estándares de derechos humanos aplicables.
43. Los casos aquí ilustrados, sumados a los anuncios realizados por el Gobierno sobre la implementación de planes de seguridad pública que consideran el uso de tecnologías de vigilancia masiva tales como drones y cámaras de reconocimiento facial,²⁸ ponen en evidencia que el derecho a la privacidad en Chile se encuentra bajo severa amenaza por parte del Estado.

44. La situación aquí descrita representa un grave incumplimiento de las obligaciones en materia de privacidad y otros derechos humanos asumidas por el Estado chileno y debe ser objeto de representación en el presente EPU. La búsqueda de protección y seguridad de la población no puede usarse como excusa para desconocer la protección de otros derechos fundamentales.

b. Insuficiente protección de datos personales

45. Chile sufre de una paradoja: Reconoce estándares de protección de la privacidad basados en su Constitución, así como en tratados internacionales de derechos humanos, pero su ley interna es absolutamente deficiente para garantizar dicha protección.
46. Existe consenso entre los expertos en que la LPD que regula la materia resulta deficitaria por distintas razones: i) la ausencia de sanciones efectivas, ii) falta de una regulación de flujo transfronterizo de datos, iii) falta de un registro de banco de datos privados, iv) ausencia de una autoridad pública de control, v) amplias excepciones al consentimiento en el tratamiento de datos, y vi) falta de mecanismos procedimentales de resguardo efectivo de los derechos reconocidos en la ley. Como consecuencia, en la práctica la ley ha servido más para legitimar el tratamiento indiscriminado de datos personales, que para proteger a las personas.
47. La ley legitima el tratamiento indiscriminado de datos por la falta de conceptos claros y principios rectores que se apeguen al respeto de los derechos de las personas, lo que genera dificultades interpretativas. Si bien la ley exige el consentimiento expreso e informado del titular de los datos para efectos de llevar a cabo el tratamiento, contempla un número elevado de excepciones amplias a este principio, que en la práctica se transforman en la regla general.
48. Así, a grandes rasgos, la LPD señala que no será necesario requerir autorización para el tratamiento de datos personales cuando estos provengan o se recolecten de fuentes accesibles al público, o cuando dicho tratamiento sea realizado por las personas privadas para el uso exclusivo suyo.
49. La redacción de estas dos hipótesis no es para nada clara. El hecho de que solo deba cumplirse alguna de estas alternativas, hace que esta excepción sea sumamente amplia. Esto ha generado una gran cantidad de abusos en el tratamiento de datos personales, y que, debido a esta excepción, sean los titulares quienes se ven privados de la protección que la ley les debería brindar.
50. En marzo del 2017, se introdujo al Congreso una reforma a la LPD, que pretende subsanar en gran medida las deficiencias a la protección de datos personales aquí denunciada, y en particular, crear una autoridad con competencia para el control y fiscalización del adecuado uso de datos personales.

51. Es extremadamente importante que Chile tome las medidas necesarias para asegurar que el régimen de protección de datos personales que en definitiva adopte cumpla los más altos estándares y respete sus obligaciones domésticas e internacionales, dado algunos preocupantes incidentes de violación de la protección de datos ocurridos en los últimos años, y el despliegue cada vez mayor de sistemas públicos y privados basados en la inteligencia de datos. La falta de una ley que brinde protección adecuada ha tenido por principal consecuencia la sobreexposición de datos por parte del Estado y de privados, lo cual se ha manifestado en los casos que se describen a continuación.
52. La falta de conceptos y principios claros ha ocasionado la aparición de servicios de indexación de información personal asociada al número nacional de identificación (RUT) que se ponen a disposición del público a través de internet, sin que la publicación de dicha información cuente con la información y el consentimiento de sus titulares. Los datos son obtenidos desde otras fuentes no necesariamente de acceso público, a veces por erróneas interpretaciones de las obligaciones provenientes de la normativa electoral,²⁹ y en otras por mera negligencia de las entidades custodias de tal información.
53. Un episodio paradigmático de la negligencia pública en el manejo de datos personales es aquél en que un organismo de salud hizo accesible a través de internet las fichas clínicas de los pacientes infectados con VIH.³⁰ Y en el caso de entidades privadas, recientemente un banco abandonó al costado de una carretera carpetas con información financiera y personal de clientes.³¹ Ambos casos sólo pudieron ser perseguidos por los afectados para resarcir sus perjuicios, con las dificultades y costos excesivos de un proceso civil, y sin un mensaje claro de la responsabilidad a las entidades a cargo del mal manejo de los datos personales.
54. Otros ejemplos de la recolección y uso abusivo de datos personales es la implementación de tecnología biométrica por parte de entidades estatales como intento de solución a problemas de gestión. Así, una entidad del Estado ha anunciado que pretende fiscalizar la entrega de almuerzos a los niños en situación de vulnerabilidad social que reciben alimentación del Estado a través del registro de huellas dactilares de los menores de edad.³² Sumado a esto, el uso extendido e indiscriminado de tecnologías biométricas en el sector privado, incluyendo aseguradoras de salud, controles de asistencia laboral, sistemas de seguridad de acceso a edificios, que constituye también un ejemplo de uso indiscriminado de datos personales sensibles.
55. En una línea similar, el Ministerio de Transportes ha anunciado que podría implementar el reconocimiento facial en el proceso de fiscalización del pago del transporte público, sumado a la reciente creación de un registro de evasores del transporte público con “listas negras” de personas con multas impagas que facilitan la discriminación contra ellas en diversas situaciones como la búsqueda de empleo, como una forma de sanción social.³³ Todas medidas

ciertamente incompatibles con una legislación protectora de los derechos y la dignidad de las personas.

56. Este tratamiento abusivo de los datos personales por parte del Estado y los privados también ha originado discriminaciones arbitrarias en el área laboral e impactado sobre grupos específicos como mujeres y personas LGTBQI. Ya que el tratamiento de grandes bases de datos puede dar lugar a la implementación de programas que en base a variables algorítmicas se permite discriminar arbitrariamente en base a factores como la raza, género u orientación sexual, en áreas como la predicción de criminalidad, el acceso al crédito y a puestos de trabajos.³⁴

IV. Recomendaciones al Estado chileno

57. Revisar el marco jurídico que rige la vigilancia policial y de inteligencia en Chile, especialmente el Código Procesal Penal y la Ley de Inteligencia, para garantizar que cumplan con el Pacto Internacional de Derechos Civiles y Políticos, incluyendo el artículo 17, a fin de garantizar que cualquier injerencia en el derecho a la privacidad sea necesaria y proporcional al objetivo perseguido.
58. Adoptar reformas orgánicas de los servicios de inteligencia conducentes a asegurar que sus actividades de vigilancia se ajusten a sus obligaciones de acuerdo con el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana de Derechos Humanos. Entre ellas, implementar mecanismos de transparencia en la adquisición de tecnologías de vigilancia; imponer a los organismos de inteligencia una obligación de entregar informes sobre las actividades de vigilancia a un órgano supervisor fuerte e independiente; adoptar medidas para que el poder judicial aplique un control sustantivo de las actividades de inteligencia al autorizarlas; y, establecer un régimen de remedios efectivos con un enfoque en prevenir abusos de facultades de investigación.
59. Asegurarse de que las actividades de vigilancia estatal, y muy especialmente el uso de drones e interceptación de telecomunicaciones, sólo se realicen de maneras que cumplan los principios de legalidad, necesidad y proporcionalidad, y no sean aplicadas de manera discriminatoria contra grupos específicos de la población, como la población Mapuche.
60. Reformar la normativa de persecución criminal aplicable en materia de recolección de evidencia digital para asegurar que tales diligencias cumplan con requisitos que satisfagan el debido proceso y el principio de proporcionalidad, dando cumplimiento a las obligaciones del Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana de Derechos Humanos en materia protección de la privacidad y otros derechos.

61. Modificar las normas sobre la retención de datos para garantizar que no impongan obligaciones indiscriminadas de retener los datos de las comunicaciones, y disponer que cualquier solicitud de acceso a dichos datos esté sujeta a los principios de necesidad y proporcionalidad, y haya sido autorizada por los organismos judiciales pertinentes.
62. Adoptar una regulación general para el uso de tecnologías de vigilancia, en la cual se establezcan las salvaguardas que sean necesarias para que el resguardo a la seguridad pública no implique la renuncia a otros derechos como la privacidad, la libertad de expresión, el derecho a reunión y el derecho a no ser discriminado, dando cumplimiento a las obligaciones del Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana de Derechos Humanos.
63. Implementar obligaciones específicas de transparencia en la compra, uso y disposición de tecnologías de vigilancia por autoridades nacionales o locales, limitando estrictamente el secreto por causa de seguridad a casos calificados.
64. Garantizar que la implementación de normativa para el combate a los ciberdelitos y otras amenazas a la ciberseguridad no se usen como excusa para atropellar derechos humanos como la privacidad y la libertad de expresión, sino como un modo de garantizar plenamente estos derechos en el ciberespacio.
65. Asegurar que la reforma de la ley de datos personales aborde las principales deficiencias aquí expuestas, para garantizar el respeto y el cumplimiento de los principios de protección de datos internacionalmente reconocidos. En particular, asegurar el cumplimiento de esta ley mediante el establecimiento de una autoridad de control técnica e independiente.
66. Limitar la recolección y el uso de datos personales para la implementación de políticas públicas y la provisión de servicios públicos a aquellos datos que sean necesarios y proporcionales al fin legítimo perseguido, para asegurar el respeto al derecho a la privacidad y a los principios de protección de datos personales.

Referencias

- 1 La referencia a la protección de datos personales fue incorporada el 15 de mayo de 2018, mediante reforma constitucional introducida por el Boletín N°9384-07: Consagra el derecho a la protección de los datos personales., aprobado con dicha fecha. Disponible en: <https://www.camara.cl/pley/pley_detalle.aspx?prmID=9798&prmBoletin=9384-07>
- 2 La Agencia Nacional de Inteligencia de Chile, se estableció como un organismo sin carácter operativo. Las diligencias son efectuadas por los servicios de inteligencia de las policías y las fuerzas armadas facultadas en el marco de esta ley.
- 3 Flores, J. (18 de abril de 2018). Gobierno adelanta plan de acción en La Araucanía. Radio BioBio. Disponible en: <<http://rbb.cl/jxph>>
- 4 Barreno J. (24 de enero de 2014). Las comunidades mapuches denuncian el uso de drones espía en sus tierras. El Mundo. Disponible en: <<http://www.elmundo.es/internacional/2014/01/24/52e20330e2704e1f188b456b.html>>
- 5 Gutiérrez, Felipe. Dictan prisión preventiva a los ocho detenidos de la “Operación Huracán” basándose en conversaciones por Whatsapp. Mapuexpress. Disponible en: <<http://www.mapuexpress.org/?p=20717>>
- 6 Cifuentes, Gonzalo. (26 de enero de 2018). Fiscalía investiga montaje en Operación Huracán: ¿A qué le teme Carabineros? biobiochile.cl. Disponible en: <<https://www.biobiochile.cl/noticias/nacional/chile/2018/01/26/fiscalia-investiga-montaje-en-operacion-huracan-a-que-le-teme-carabineros.shtml>>
- 7 Ayala, Leslie. (6 de mayo de 2018). “‘Antorcha’ nunca existió”: Las claves del último informe sobre la Operación Huracán. Diario La Tercera. disponible en: <<http://www.latercera.com/reportajes/noticia/antorcha-nunca-existio-las-claves-del-ultimo-informe-la-operacion-huracan/154002/>>
- 8 Toro, P. y Rivera, V. (11 de abril de 2018). Caso Huracán: Carabineros pidió intervenir más de 60 teléfonos en indagatoria. Diario La Tercera. disponible en: <<http://www.latercera.com/nacional/noticia/caso-huracan-carabineros-pidio-intervenir-mas-60-telefonos-indagatoria/129660/>>
- 9 <https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective/analyst/applications>
- 10 Toro I. y Toro P. (7 de junio de 2018). El software espía que Carabineros compró para el “profesor” Smith: \$21 millones en billetes. La Tercera. Disponible en: <<http://www.latercera.com/la-tercera-pm/noticia/software-espia-carabineros-compro-efectivo-usado-profesor-smith-21-millones-billetes/196428/>>
- 11 Reglamento Sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de telecomunicación: Disponible en: <<https://www.leychile.cl/Navegar?idNorma=242261>>

- 12 Datos del titular, llamadas enviadas y recibidas, sitios web visitados, tráfico de voz y datos de las comunicaciones, datos de comunicaciones a través de sistema de mensajería y ubicación georeferencial de todos los clientes.
- 13 Sólo la ley es está autorizada para restringir el ejercicio de los derechos fundamentales conforme al principio de reserva establecido en el artículo 19 N°26 de la Constitución Política de la República.
- 14 Sentencia del 8 de abril de 2014, Digital Rights Ireland Ltd, C-293/12 y Kärntner Landesregierung, C-594/12, EU:C:2014:238, párrafo 27. Disponible en: <http://curia.europa.eu/juris/document/document>.
- 15 Tele2 Sverige AB vs. Telestyrelsen post-Och (C-203/15); Secretary of State for the Home Department vs. Tom Watson et. al. (C-698/16), Joined Cases, Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 21 de diciembre de 2016.
- 16 UN Human Rights Committee, Concluding Observations of the Fourth Periodic Report of the United States of America, UN Doc. CCPR/C/USA/CO/4, 23 April 2014, para. 22.
- 17 ADN Radio (31 de mayo de 2017). Comisión Investigadora Pacogate: "La cifra del fraude seguirá aumentando". Disponible en: <http://www.adnradio.cl/noticias/nacional/comision-investigadora-pacogate-la-cifra-del-fraude-seguira-aumentando/20170531/nota/3479645.aspx>
- 18 Partarrieu. B y Jara. M. (10 de julio de 2015). Los correos que alertaron sobre la compra del poderoso programa espía de la PDI. CIPER. Disponible en: <http://ciperchile.cl/2015/07/10/los-correos-que-alertaron-sobre-la-compra-del-poderoso-programa-espia-de-la-pdi>
- 19 En 2017, el Comité de Derechos Humanos expresó su preocupación por el uso del hackeo con fines de vigilancia en Italia. Ver: Observaciones finales sobre el sexto informe periódico de Italia, Comité de Derechos Humanos, UN Doc. CCPR/C/ITA/CO/6 (28 de marzo de 2017)
- 20 Informe del Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, UN Doc. A/HRC/23/40, párr. 62 (17 de abril de 2013).
- 21 Peña, C. y Minay, S. (29 de octubre de 2008). Así se hacen los cuestionados "pinchazos" telefónicos legales. Ciper. Disponible en: <http://ciperchile.cl/ciper-radar/bmnpuy256>
- 22 Villarrubia, Gustavo. (6 de septiembre de 2011). Las tretas de los policías para "pinchar" teléfonos sin autorización judicial. Ciper. Disponible en: <https://ciperchile.cl/2011/09/26/las-tretas-de-las-policias-para-%E2%80%9Cpinchar%E2%80%9D-telefonos-sin-autorizacion-judicial/>
- 23 Sepúlveda, Nicolás. (5 de abril de 2018) "Operación Huracán": la secreta casa donde se hacían centenares de escuchas telefónicas ilegales. Ciper. Disponible en: <https://ciperchile.cl/2018/04/05/operacion-huracan-la-secreta-casa-donde-se-hacian-centenares-de-escuchas-telefonicas-ilegales/>

- 24 Sentencia de la Corte de Apelaciones de Santiago, 21 de agosto de 2017, Rol N°34360-17. Considerando Vigésimo Séptimo.
- 25 Vecinos de Lo Barnechea y Las Condes contra globos de vigilancia. 24Horas. Disponible en: <<http://www.24horas.cl/nacional/vecinos-de-lo-barnechea-y-las-condes-contraglobos-de-vigilancia-1783243>>
- 26 Sentencia de la Corte de Apelaciones de Santiago, 04 de marzo de 2016, Rol N°82289-15. Disponible en: <<http://www.pjud.cl/documents/396543/0/PROTECCION+GLOBOAS+AEROSTATICOS.pdf/ecb2307b-0a6a-4145-8a8e-d39c6687270e>>
- 27 Sentencia de la Corte de Apelaciones de Santiago, 21 de agosto de 2017, Rol N°34360-17. Disponible en: <<http://www.pjud.cl/documents/396729/0/DRONES+LAS+CONDES+CORTE.pdf/c12fb16c-8900-474f-a325-91fd58a42eea>>
- 28 Bastarrica, D. (01 de junio de 2018). Cuenta pública de Piñera. FayerWayer. Disponible en: <<https://www.fayerwayer.com/2018/06/cuenta-publica-pinera/>>
- 29 Cornejo, F. (19 de agosto de 2012). Servel revela padrón electoral incluyendo datos personales de los electores. Radio Biobio. Disponible en: <<http://rbb.cl/3e5e>>
- 30 Carvajal, V. y Jara. M. (05 de marzo de 2016). Grave falla en la red Minsal dejó expuesta información confidencial de pacientes. CIPER. Disponible en: <<http://ciperchile.cl/2016/03/05/grave-falla-en-la-red-del-minsal-dejo-expuesta-informacion-confidencial-de-pacientes/>> <http://ciperchile.cl/2016/03/05/grave-falla-en-la-red-del-minsal-dejo-expuesta-informacion-confidencial-de-pacientes/>>
- 31 (13 de octubre de 2015). Clientes de Banco Santander tomarán acciones por documentos botados. 24Horas. Disponible en: <<http://www.24horas.cl/nacional/clientes-de-banco-santander-tomaran-acciones-legales-por-documentos-botados-1814035>>
- 32 Gúzman, 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/>>
- 33 Liencura, J. (4 de junio de 2018). Transantiago. Publimetro. Disponible en: <<https://www.publimetro.cl/cl/noticias/2018/06/04/transantiago-este-martes-empieza-el-registro-de-evasores-que-promete-multas-de-hasta-70-mil-para-quienes-no-validen.html>>
- 34 Derechos Digitales. (2016). Información financiera y discriminación laboral en Chile: Un caso de estudio sobre Big Data. Disponible en: <<https://www.derechosdigitales.org/wp-content/uploads/big-data-informe.pdf>>