INFORME

MATERIA	El derecho a la privacidad en la era digital
AUTORES	Romina Garrido y Jessica Matus Fundación Datos Protegidos (FDP)
DESTINATARIO	Alto Comisionado de Derechos Humanos. Naciones Unidas.
FECHA	Abril 2018.

I. ANTECEDENTES DE LA ORGANIZACIÓN.

Datos Protegidos es una organización independiente sin fines lucrativos que promueve, defiende y educa sobre el derecho a la privacidad y a la protección de los datos personales como derechos fundamentales. https://datosprotegidos.org/

II. INFORMACIÓN RELEVANTE ACERCA DE CHILE.

El presente documento entrega un panorama sobre los desafíos, brechas y avances con respecto a la promoción y protección del derecho a la privacidad en Chile.

1. Avances normativos 2017.

a) Proyecto de ley de datos personales.

Ley 19.628. Chile cuenta con una ley de protección a la vida privada desde 1999. Esta ley contiene procedimientos anacrónicos de ejercicio de derechos en tribunales civiles frente a los procesadores y responsables, donde la carga de la prueba recae en los usuarios. Su ejercicio es casi nulo debido los costos e inciertos resultados sancionatorios.

Enero 2017. Chile lleva al menos 10 años debatiendo sobre el cambio a la norma de protección a la vida privada. No existen opciones reales de control sobre nuestra información personal ni la posibilidad de impugnar los tratamientos indebidos no consentidos y desinformados. La ley no contempla requisitos básicos: seguridad, sanciones ni control a través de un ente especializado y autónomo. También pugna con los principios y buenas prácticas promovidas por la OCDE, Naciones Unidas y la Unión Europea. Actualmente, se tramita un tercer proyecto de ley que dispone garantías procesales e institucionales, mecanismos de supervisión y recursos disponibles para las personas expuestas al tratamiento de sus datos en el territorio nacional o extraterritorialmente. Puede verse comentarios al proyecto en informe de FDP[1].

b) Política Nacional de Ciberseguridad.

Abril de 2017. Publicación de la Política Nacional de Ciberseguridad, documento construido entre el sector público y el privado, cuyo objeto es promover un ciberespacio libre, abierto, seguro y

[1] Reporte ley de datos para Chile. https://datosprotegidos.org/projectos/reporte-ley-de-datos-para-chile/

resiliente. La política busca ser un marco de acción que permita acompañar la discusión de seguridad pública, infraestructuras críticas, gobierno digital, entre otros. La Política enfatiza que el combate a los ciberdelitos y amenazas en Internet no pueden ser excusa para atropellar la privacidad y la libertad de expresión, sino un modo de garantizar estos derechos en el ciberespacio. Además, propone la implementación de mecanismos eficaces de protección de la vida privada y la inviolabilidad de las comunicaciones en el ciberespacio, protecciones contra la recolección, procesamiento y publicación no autorizada de sus datos personales; la transparencia en el manejo de esos datos por privados y públicos. El documento tiene como eje los usuarios y la necesidad de actualización de la normativa relacionada con el ciberespacio seguro.

c) Adopción de Convenio de Budapest.

Abril de 2017. El Congreso aprobó la principal herramienta internacional para fijar estándares de protección jurídica en materia penal, procesal penal y de cooperación internacional para delitos cometidos a través de Internet o medios informáticos. Importa en esta materia, adoptar medidas legislativas nacionales de protección a la privacidad en redes informáticas que permitan abordar la violencia en línea, difusión no consentida de imágenes, doxing de datos y otros flagelos que, en general, afectan a las mujeres y minorías sexuales.

2. Jurisprudencia sobre el derecho a la privacidad.

a) Baja de fotografías de Internet por afectación a privacidad, memoria y honra:

Año 2017. FDP interpuso acción constitucional de protección a la privacidad en la última arista del caso de Sergio Landskron, joven fallecido en 2014 en una explosión. La acción se motiva debido a la exposición en la web de fotografías del cuerpo fallecido y calcinado de Sergio, filtradas por Carabineros y personal de salud, hecho por el cual en 2016 la familia recibió una indemnización. Sin embargo, el daño se seguía produciendo ya que las imágenes continuaban en la web. El caso debatió entre la libertad de información, el honor y la privacidad. La Corte dio prevalencia a la libertad de información contra nuestro planteamiento de falta de interés público en la difusión de las imágenes, rechazando la acción. Los requeridos, Google y dos sitios web, sin embargo eliminaron los contenidos.

b) Drones de vigilancia:

Mayo 2017. Esta acción judicial por infracción al derecho a la privacidad buscó detener el uso de drones como medio de vigilancia. La acción fue rechazada por la Corte de Apelaciones y Suprema, estimándose que existe competencia por parte de los municipios (la ley señala que son colaboradores en materia de seguridad) y que "*al acceder a un lugar público cada persona aspira, entre otros aspectos, que sus conversaciones no sean de acceso público, como también que en su desplazamiento no sea objeto de registro (…) a menos que incurra en conductas ilegales o se vea involucrado en situaciones de emergencia, pues en tales casos, normal es que tales expectativas de privacidad se desvanecen".* Se estimó que la vigilancia no resulta atentatoria pues en los espacios públicos (…) "*el anonimato de los transeúntes decrece en pro de otros fines legítimos de seguridad."*

3. Intercepción de comunicaciones:

Agosto 2017. En la Contraloría General de la República se tramitó una modificación al reglamento sobre interceptación y retención de las comunicaciones, exigiendo a las ISP mantener almacenadas por dos años todos los datos referidos a antecedentes personales de usuarios, número de teléfono, direcciones IP, y todo dato para identificar el destino de la comunicación, fecha, hora y duración, equipos terminales, ubicación geográfica y otros que serían definidos en una norma posterior. La Contraloría escuchó posiciones, incluida la nuestra, y declaró la ilegalidad de la propuesta. Entre nuestros argumentos[2] acogidos, la norma sobrepasaba las potestades legislativas para el almacenamiento de metadatos, careciendo de especificidad, precisión y claridad sobre los datos, entre otros.

4. La industria de drones de vigilancia en Chile.

Un reporte publicado por FDP reveló que las autoridades de América Latina no han dado cuenta de la implicancia del uso de drones de vigilancia en los derechos de las personas existiendo un vacío regulatorio sin límites respecto de los datos y privacidad[3]. Algunas empresas mencionadas en el reporte son:

a) **Dajiang Innovation Technology Co (DJI)** proveedor de drones en comuna Las Condes. El modelo implementado corresponde DJI Matrice 600 Pro, con una cámara Z30 DJI con un zoom óptico de 30x y zoom digital de 6x4. Este zoom es lo suficientemente poderoso para reconocer objetos pequeños (como un lápiz rojo) a 150 metros de distancia[5].

b) **Dronestore** facturó USD $63.000 en los últimos 5 años sólo en contratos públicos. De acuerdo con su CEO, sólo desde 2014 a 2015 aumentaron sus ventas en un 300%. Esta compañía fue la primera en vender drones DJI en Chile. Actualmente, son seis compañías las distribuidoras de esta marca[6]. Chile ha gastado sólo en drones desde 2016 USD $350.292. Específicamente, para vigilancia, el monto es de USD $124.118.

c) **Petric Companie**[7] facturó USD $11 millones de dólares en los últimos 10 años, proveyendo cámaras de vigilancia y CCTV sólo en contratos públicos[8]. Suma a su negocio la identificación biométrica, globos de vigilancia y otros dispositivos similares. En Chile, las compañías de seguridad han crecido un 46% entre 2010 y 2015. Las comunas más ricas de Santiago (Las Condes, Vitacura, Lo Barnechea, Providencia y Santiago) han gastado en este ítem, el año 2015, unos USD $30 millones en seguridad pública, según un medio local[9].

---

[2] Presentación a Contraloría por ilegalidad del Decreto Espía. https://datosprotegidos.org/presentacion-a-contraloria-por-ilegalidad-del-decreto-espia/

[3] Drones en Chile: Un análisis de los discursos, industria y los derechos humanos. https://datosprotegidos.org/wp-content/uploads/2018/02/Informe-Drones-espa%C3%B1ol.pdf

[4] Para más datos técnicos véase en: http://www.dji.com/zenmuse-z30/info#specs

[5] Para ver una demostración, véase: https://www.youtube.com/watch?v=roxgQh73ye8

[6] A pesar de las insistencias de la ONG Datos Protegidos, no se pudo obtener una respuesta ni de Rodrigo Salcedo, CEO de DJI en Chile, ni de Jorge Zalaquett CEO de Dronestore.

[7] http://www.comercialpetric.cl/televigilancia/index.php/es/empresa3

[8] Pino, Patricio. "Los empresarios tras el negocio de la vigilancia electrónica de los municipios", La Segunda, May 12th, 2017. Disponible en: http://impresa.lasegunda.com/2017/05/12/A/fullpage#slider-23

[9] Orellana, Antonia. "Drones y Globos: Cómo se expande el negocio de vigilar en Santiago desde el barrio alto", El Desconcierto, 24th february, 2017. Disponible en: http://www.eldesconcierto.cl/2017/02/24/drones-globos-se-expande-desde-barrio-alto-

Luego del rechazo de la acción judicial, se ha anunciado la implementación de drones en las comunas de Peñalolén[10], Cabrero[11], Curicó[12] y en la zona del conflicto de la Araucanía[13].

5. Mecanismos correctivos de las empresas comerciales.

a) Código de Autorregulación Asociación de Marketing Directo Digital (AMDD).

Septiembre 2017. Lanzamiento del Código de Autorregulación de AMDD que reúne a 47 empresas nacionales. Este reglamento, sin fuerza normativa formal, busca sincronizar los procedimientos de las empresas en favor de la privacidad de las personas. La industria busca mediante la adopción voluntaria, adelantarse a las nuevas regulaciones de datos personales. Se incorporan regulaciones a medios y herramientas de marketing digital como cookies, banners y redes sociales, y sanciones por infracciones al Código[14]. Cabe señalar que la discusión actual del proyecto de ley de datos personales no contempla la autorregulación como un mecanismo normativo válido, lo que debería ser corregido durante la tramitación del proyecto.

b) Normativa para la gestión de ciberseguridad en la banca.

Enero 2018. Publicación de marco normativo de ciberseguridad aplicable a bancos, cooperativas de ahorro y crédito, sociedades de apoyo y emisores de tarjetas de pago, que será fiscalizada por la Superintendencia de Bancos. La norma define las infraestructuras físicas, hardware y sistemas tecnológicos que almacenan, administran y soportan estos activos de información bancarios y que, de no operar adecuadamente, exponen a la entidad a riesgos de integridad, disponibilidad y confidencialidad de la información. Obliga a las entidades a contar con una base de incidentes de ciberseguridad, entre otras novedades[15].

6. Creciente dependencia de la tecnología basada en datos biométricos:

Actualmente, diversos procesos gubernamentales y privados integran sistemas de identificación biométricos. Un informe de CMSpeople.com presentado en SINACOFI[16] proyecta que la biometría es junto a la vigilancia una industria al alza, para diversos usos: control de acceso, autenticación a sistemas de uso crítico, etc. En Chile, existe masivamente la tecnología dactilar, sin embargo, se pueden proyectar el reconocimiento facial, el patrón de mapa de venas, ocular entre los de mayor crecimiento.

Junio 2017: La Municipalidad de Las Condes anuncia marcha blanca de **cámaras de seguridad con reconocimiento facial**[17]. En marzo de 2018, se firmó convenio con la Policía de Investigaciones que permitirá cruce de datos policiales con transeúntes, a efectos de identificar personas con antecedentes penales. Surgen cuestionamientos, respecto a la creación de "listas negras" y criterios

---

negocio-vigilar-santiago-desde-cielo/

[10] http://www.cnnchile.com/noticia/2018/02/04/municipalidad-de-penalolen-refuerza-televigilancia-con-drones

[11] http://www.latribuna.cl/noticia.php?id=MTk3NjE=

[12] http://www.diarioelcentro.cl/noticias/cronica/municipio-y-carabineros-afinan-incorporacion-de-dron-para-vigilancia-aerea

[13] https://www.araucanianoticias.cl/tag/drones

[14] Código AMDD http://amddchile.com/codigo-amdd/

[15] SBIF emite norma sobre Ciberseguridad https://www.sbif.cl/sbifweb/servlet/Noticia?indice=2.1&idContenido=11965

[16] Biometría Aplicada: Proyecciones y Tendencias. https://www.sinacofi.cl/eventos/training_biometria_aplicada_2013/docs/Tendencias_V4_0_EMC_SIN_VIDEOS.pdf

[17] Fuente: Emol.com - http://www.emol.com/noticias/Nacional/2017/06/23/863987/Las-Condes-implementa-camaras-con-reconocimiento-facial-para-detectar-a-delincuentes.html

de tratamiento de la información, accesos, eliminación, seguridad, responsabilidades ulteriores bajo una legislación laxa de protección a la privacidad, agravando sesgos raciales y sociales.

Julio 2017. Corte Suprema declara ilegales cláusulas de licitación de la Junta Nacional de Auxilio Escolar y Becas (JUNAEB) quien para la entrega de raciones alimenticias en colegios exigía **la implementación de un control biométrico a los estudiantes** beneficiarios. La acción judicial fue interpuesta por nueve empresas proveedoras del Programa de Alimentación Escolar (PAE). La Corte señaló que para utilizar un mecanismo de control de este tipo en menores de edad -beneficiarios del PAE- se requiere permiso del tutor adulto, lo que en opinión de los recurrentes dificultaba la asignación de los alimentos

Mayo 2017. Se anuncia instalación de **cámaras de reconocimiento facial** para identificar a quienes evadan el pago del transporte público. La cámara se activaría al pasar la tarjeta por el punto de pago captando 500 puntos del rostro para la identificación biométrica, comparando la imagen con la que aparece en la tarjeta de pago. En caso de no pagar, la imagen revelará la evasión y se creará un registro oficial de personas que no pagan su pasaje. La base de datos es, posteriormente, enviada a las empresas de transporte y a la autoridad para que se cursen multas[18]. Cabe señalar que el proyecto de ley de datos personales en actual discusión en el Congreso dispone que la biometría sólo podrá implementarse con autorización legal expresa.

7. Nuevos desafíos sobre el derecho a la privacidad.

a) Registro de evasores y usuarios del transporte público.

Abril 2018. Publicación de la Ley 21.083[19] que crea un registro de evasores y de usuarios del transporte. Ambos registros están a cargo del Ministerio de Transportes.

Registro de usuarios: Sus finalidades son, entre otros, verificar el uso del transporte público, generar estadísticas y desarrollo de políticas públicas asociadas al transporte. Los órganos del Estado podrán acceder a los datos del registro según sus competencias. Respecto a los documentos del transporte usados por menores, la información deberá ser especialmente protegida extremando las medidas de seguridad. La información de usuarios se declara reservada pero accesible a terceros competentes. Los titulares de los datos podrán acceder a sus datos y ejercer los derechos de la ley N° 19.628. Desde la tramitación de este proyecto, nuestras aprensiones se relacionan con la baja exigencia de protección de datos existente en la norma general, ambigüedad de las normas de competencias estatales de acceso a los datos, y lo cuestionable de un registro masivo de todos los usuarios como condición de acceso al transporte. Esta medida sólo a los habitantes de la ciudad de Santiago.

Registro de evasores: Será de consulta abierta a efectos de conocer si una persona está anotada o no. La ley delegó en un reglamento el procedimiento de transferencia, seguridad, tratamiento, ejercicio de derechos vinculados a datos personales. La información no podrá afectar negativamente a las personas en aspectos laborales, comerciales, inmobiliarios, crediticios o de acceso a beneficios. Los desafíos se encuentran en el reglamento y en los posibles efectos negativos de la anotación, generación de "listas negras" paralelas de la población más vulnerable, entre otros[20].

[18] https://www.eldinamo.cl/nacional/2017/05/25/transantiago-camaras-reconocimiento-facial/
[19] Ley 21.083 https://www.leychile.cl/Navegar?idNorma=1116754
[20] Rechace el DICOM del Transantiago. https://datosprotegidos.org/rechace-el-dicom-del-transantiago-diputad/

b) Operación Huracán.

Septiembre 2017. El Ministerio Público inició una investigación por presunta adulteración de pruebas entregadas por Carabineros en la denominada Operación Huracán. Este es un operativo policial amparado en la Ley de Inteligencia, que condujo a la detención de ocho comuneros mapuches supuestamente involucrados en una asociación ilícita terrorista en el sur de Chile. Este caso tiene diversas aristas, una de las más relevantes es el uso por parte de la Policía del software **Antorcha,** para acceder a las conversaciones de WhatsApp y Telegram de los comuneros mapuches. Sin entrar en los sendos debates de este caso, importa relevar dos asuntos:

- El uso de un procedimiento de inteligencia, reglado y de finalidades estratégicas contra la lucha terrorista, narcotráfico y otros, en un contexto de investigación penal específico, con el sólo objeto de evadir la autorización judicial para la intervención de comunicaciones privadas.

- La elaboración y uso de un software por encargo del Estado, instalado ilegalmente en dispositivos, para intervenir las comunicaciones privadas sin orden judicial y en condiciones de dudosa legalidad.