07/

Innovación tecnológica, protección de datos personales y derechos humanos

Innovación tecnológica, protección de datos personales y derechos humanos

ANTECEDENTES

En este capítulo se abordará la protección de los datos personales[1] desde una perspectiva de derechos humanos, considerando que el desarrollo de la tecnología y de las plataformas digitales plantea nuevos desafíos al Estado a fin de resguardar eficazmente el derecho a la privacidad y otros que puedan verse afectados cuando no se establecen las medidas necesarias para evitar la captura maliciosa de datos o para que no sean objeto de transferencia o tratamiento ilícitos. Para estos efectos, fueron analizadas fuentes secundarias, legislación comparada, jurisprudencia nacional, y se desarrolló una discusión grupal con expertas en las materias mencionadas.[2]

El 17 de marzo de este año, fue publicada una investigación conjunta de varios medios de prensa sobre el mal uso de datos personales de más de 50 millones de usuarias y usuarios de Facebook. De acuerdo a la publicación, una de las responsables de esta controversia era la consultora londinense *Cambridge Analytica* —dedicada al análisis de datos para fines electorales— que tuvo participación en la campaña a favor del *Brexit* (referéndum sobre la salida de Gran Bretaña de la UE que se ganó por menos del 2% de los votos y donde se gastó gran cantidad de dinero en publicidad a medida basada en datos personales[3]) y en la candidatura de Donald Trump.[4]

La operación efectuada por *Cambridge Analytica* utilizó Facebook como su base de recolección de datos. Mediante el desarrollo de una aplicación que presentaba un cuestionario de personalidad, que contaba con una licencia de fines meramente académicos, se extrajeron datos sensibles de las usuarias y usuarios, tales como la orientación sexual, etnia, género, incluso inteligencia y traumas infantiles. Estos datos fueron combinados y analizados

1 Los datos personales son aquellos que identifican a una persona o, al menos, la vuelven identificable. Algunos ejemplos de datos personales son el nombre, fecha y lugar de nacimiento, domicilio, el rol único nacional, y otros datos de carácter biométrico que se analizarán detalladamente más adelante.

2 Es importante considerar que este capítulo no aborda la cuestión central desde la perspectiva de los derechos civiles y políticos, en relación al impacto que pueda tener el uso de Big Data o Data Mining en nuestras democracias. Desde una perspectiva optimista se sostiene que tales usos podrían reducir la brecha entre los representados y sus representantes, pues estos podrían saber de mejor modo los pensamientos e intereses de aquellos. Sin embargo, desde una perspectiva pesimista, se teme que la existencia de una inteligencia artificial centralizada, que controle lo que sabemos, pensamos y cómo actuamos, tendría características totalitarias.

3 *El País*. "El Brexit no habría sucedido sin Cambridge Analytica", Pablo Guimón, 27 marzo 2018, https://elpais.com/internacional/2018/03/26/actualidad/1522058765_703094.html

4 *The New York Times*, "How Trump Consultants Exploited the Facebook Data of Millions", Matthew Rosenberg, Nicholas Confessore y Carole Cadwalladr, 17 marzo 2018, https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

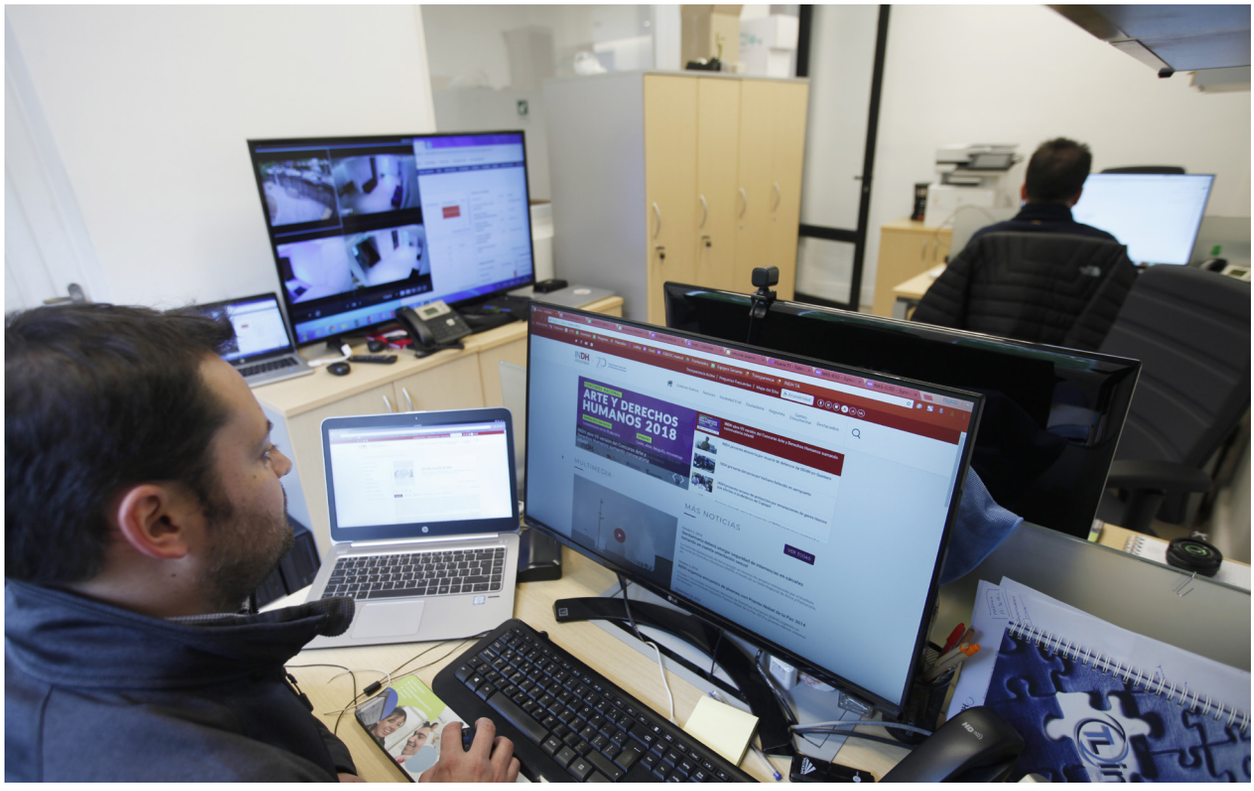
para buscar patrones y construir un algoritmo[5] que permitía identificar las tendencias políticas y comportamientos electorales de las personas que pasaron a integrar esta base de datos, lo que permitía al comando de Trump formular mensajes específicos para un perfil de votante determinado. En este escándalo también hubo una importante participación de la propia plataforma Facebook, ya que —al menos— fue negligente en adoptar todas las medidas necesarias para proteger los datos de sus usuarias y usuarios.[6]

Ya en el ámbito nacional, durante 2018 se han producido dos episodios de filtraciones de datos bancarios, afectando a miles de clientes cuya información comenzó a circular a través de internet;[7] hecho que, además, pone en relieve el nivel de responsabilidad de las empresas privadas que acumulan y manejan datos personales, a fin de

5 De acuerdo a ECIJA, "los algoritmos predictivos son una técnica estadística que, por medio de la modelización, aprendizaje automático y minería de datos, permiten identificar tanto posibles riesgos como oportunidades, siendo la base de su uso el manejo de datos masivos, tanto históricos como transaccionales. El diseño y utilización de algoritmos predictivos es una realidad presente hoy en día más que nunca, teniendo como base para su funcionamiento el uso de una gran cantidad de datos. Sus finalidades pueden ir desde la predicción de muertes repentinas por episodios cardiorrespiratorios, hasta combatir el crimen a través de la asignación de puntuación a diversas actividades delictivas determinando la predisposición a la comisión de futuros delitos". ECIJA. La aplicación de protección de datos personales a los algoritmos predictivos. Disponible en: https://ecija.com/la-aplicacion-la-proteccion-datos-los-algoritmos-predictivos/ [Último acceso: 30 agosto 2018.]

6 Lawfare, "The Cambridge Analytica-Facebook Debacle: A Legal Primer", 20 marzo 2018, https://www.lawfareblog.com/cambridge-analytica-facebook-debacle-legal-primer

7 Conforme a los datos reportados por la Superintendencia de Bancos e Instituciones Financieras (SBIF), la filtración de datos que se produjo en julio de 2018 afectó a 14.071 tarjetas de créditos emitidas por distintos bancos. SBIF. Segundo comunicado acerca del incidente de seguridad de tarjetas de crédito. Disponible en: https://www.sbif.cl/sbifweb/servlet/Noticia?indice=2.1&idContenido=12161 [Último acceso: 6 septiembre 2018.] La filtración ocurrida en agosto de 2018 afectó a 924 tarjetas de crédito, de las cuales 210 estaban activas. SBIF. SBIF informa sobre filtración de datos de tarjetas de crédito. Disponible en: https://www.sbif.cl/sbifweb/servlet/Noticia?indice=2.1&idContenido=12199 [Último acceso: 6 septiembre 2018.]



asegurar que estos no sean objeto de tráfico ilícito.[8] También se han reportado casos de plataformas que recopilan y procesan información que las personas publican en sus propias redes sociales, con información que contiene datos privados. Se trata de *Instagis*, una empresa que utiliza un software de predicción territorial, según se anuncia en su sitio web. De acuerdo a un reporte de Centro de Investigación e Información Periodística (CIPER), la actividad de *Instagis* consiste en:

> *Cruzar distintas bases de datos con información de usuarios en redes sociales para predecir patrones de comportamiento, de consumo e incluso preferencias políticas. Así, cada vez que usted interactúa en su cuenta de Facebook, Twitter o Instagram, uno de los "robots" de Instagis puede monitorear ese contenido para luego cruzar la información con su RUT y domicilio, aunque estos últimos son datos personales que debiesen estar protegidos, pero los vacíos legales hacen que en la práctica no sea así.*[9]

De acuerdo a la opinión de Pablo Viollier, miembro de la Fundación Derechos Digitales consultado por CIPER, la actividad desarrollada por *Instagis* "transita por una delgada línea que aprovecha los forados de Ley 19.628 sobre protección de la vida privada, que desde su promulgación en 1999 estuvo más orientada a regular el negocio del tráfico de los datos personales, antes que proteger los derechos fundamentales de las personas".[10] Este aspecto es particularmente preocupante, ya que esta empresa trabaja con las bases de datos que son aportadas por sus mismos clientes, entre los que se encuentran más de una docena de municipios, el SERVEL,[11] Chile Compra y el Servicio Nacional para Prevención y Rehabilitación del Consumo de Drogas y Alcohol (SENDA).

8 Cooperativa, "Reportan nueva filtración de datos desde entidades bancarias", 27 agosto 2018, https://www.cooperativa.cl/noticias/pais/consumidores/reportan-nueva-filtracion-de-datos-desde-entidades-bancarias/2018-08-27/160414.html

9 CIPER, "Instagis: el 'gran hermano' de las campañas políticas financiado por CORFO", 3 enero 2018, https://ciperchile.cl/2018/01/03/instagis-el-gran-hermano-de-las-campanas-politicas-financiado-por-corfo/

10 Ibídem.

11 Existen antecedentes de un laxo tratamiento de datos personales por parte del SERVEL. El 1 de octubre de 2009, fue solicitada a esa entidad copia del padrón electoral computacional de inscripciones electorales vigentes. Con fecha 2 de octubre del mismo año, mediante el Oficio Ord. 10.305, el director nacional de la época contestó que lo solicitado por el requirente se encontraba a la venta como un producto electoral del órgano y que podía ser adquirido por cualquier persona. El 14 de octubre de 2009, el requirente formuló amparo ante el Consejo para la Transparencia, ya que estimó que la exigencia de un pago trasgredía a las obligaciones dispuestas en la ley en cuanto al acceso a la información pública. El Consejo, por mayoría, acogió el amparo, ya que el pretendido cobro del SERVEL hubiese impedido el acceso a la información. En voto de minoría, el entonces presidente del Consejo, fue de la opinión de que se entregara parcialmente la información requerida, eliminando de la copia del padrón a entregar al solicitante la profesión, fecha de nacimiento, domicilio, número de cédula de identidad e indicación de discapacidad de las personas inscritas en el registro.

Así, cada vez que usted interactúa en su cuenta de Facebook, Twitter o Instagram, uno de los "robots" de Instagis puede monitorear ese contenido para luego cruzar la información con su RUT y domicilio, aunque estos últimos son datos personales que debiesen estar protegidos, pero los vacíos legales hacen que en la práctica no sea así (CIPER).

Las afectaciones al derecho a la intimidad y el tratamiento ilegal de datos personales no solo se producen en plataformas virtuales. En 2009, cobró gran relevancia mediática el caso de una abogada que acusaba traspaso de información, sin que se le informara o solicitara su consentimiento, entre su doctora tratante, la ISAPRE a la cual estaba afiliada y la cadena de farmacia con la cual la institución de salud mantenía convenio; de modo tal que cuando se acercaba a cualquier sucursal de la cadena de farmacia, los dependientes tenían acceso a su historial de diagnósticos clínicos.[12]

Más recientemente, en agosto de 2015, las municipalidades de Las Condes y Lo Barnechea instalaron globos con cámaras de videovigilancia, capaces de identificar a una persona en movimiento a 1,6 kilómetros de distancia. Frente a este hecho, fueron presentadas dos acciones constitucionales de protección ante la Corte de Apelaciones de Santiago por considerar la instalación de los globos de vigilancia arbitraria e ilegal, pues atentaba en contra de los derechos fundamentales de protección de la privacidad, de inviolabilidad del hogar e incumplir con las prescripciones de la Ley 19.628 sobre Protección de la vida privada (en adelante, LPVP).[13]

La Corte de Apelaciones de Santiago concluyó que las cámaras eran capaces de registrar imágenes tanto en espacios públicos como privados; además, entendió que las bases administrativas de licitación, por las cuales las municipalidades adjudicaron a una empresa la instalación y operación de las cámaras, no consideraban los resguardos necesarios para evitar la captación de imágenes en lugares privados. Aun cuando en atención al artículo 20 de la LPVP los órganos públicos pueden prescindir de la autorización de los titulares para el tratamiento de datos personales —cuestión que, sin embargo, debe realizarse con pleno respeto a los derechos fundamentales—, la Corte entendió que dicha excepción no concurría en la especie, pues la captación y tratamiento de las imágenes estaba delegada en un privado. Conforme a estos argumentos, la Corte de Apelaciones de Santiago ordenó cesar de inmediato la captación, almacenamiento y procesamiento de las imágenes que se realizan por medio de los globos de videovigilancia.

La Corte Suprema, conociendo en apelación las acciones constitucionales previamente citadas, revocó las sentencias, lo que implicaba mantener en funcionamiento los globos.[14] El máximo tribunal desechó el argumento de la Corte de Santiago en cuanto a que, en la especie, al ser las cámaras operadas por privados, no concurrían los supuestos del artículo 20 de la LPVP, ya que tal delegación estaría amparada por la normativa administrativa y en todo caso las municipalidades aludidas mantendrían su responsabilidad ante los ciudadanos. La Corte precisó que la captación de las imágenes solo cabe realizarla en espacios, lugares o recintos públicos, pero no en domicilios o espacios privados.[15]

Como puede observarse, el derecho a la vida privada y la protección de datos personales pueden ser afectados de diversos modos e intensidades; y los nuevos escenarios configurados por los avances digitales y tecnológicos obligan a reformular ciertos conceptos tradicionales para que el Estado cumpla con su obligación de proteger los derechos humanos de las personas. Por estos motivos son

12 Verónica Sánchez G. con N.N., 7° Juzgado de Garantía de Santiago, RIT 9869-2009. Verónica Sánchez G. con N.N., Juzgado de Garantía de Rancagua, RIT 5280-2010. A pesar de que la afectada presentó querellas por estos hechos, las dos fiscalías que intervinieron en su investigación decidieron no perseverar en el procedimiento, ya que no reunieron antecedentes suficientes para fundar la acusación.

13 Soffge Guemes, Stephanie y otros con Ilustre Municipalidad de Las Condes y otro, Ilustre Corte de Apelaciones de Santiago, Rol 82289-2015. Costa Cordella, Ezio con Ilustre Municipalidad de Las Condes, Ilustre Corte de Apelaciones de Santiago, Rol 81627-2015. En el primer caso mencionado, el INDH presentó un informe en derecho apoyando las alegaciones de las personas afectadas por la instalación de los globos de videovigilancia. Al respecto, consultar: http://bibliotecadigital.indh.cl/handle/123456789/858 [Último acceso: 1 octubre 2018.]

14 Soffge Guemes, Stephanie y otros con Ilustre Municipalidad de Las Condes y otro, Corte Suprema, Rol 18.481-2016. Costa Cordella, Ezio con Ilustre Municipalidad de Las Condes, Corte Suprema, Rol N° 18458-2016.

15 Además, la Corte Suprema ordenó el siguiente régimen de operación de las cámaras: 1. El ámbito físico a grabar se delimita a los lugares públicos, y de los espacios privados abiertos cuando se trate del seguimiento de un hecho que pueda constituir la comisión de un ilícito. 2. Un inspector o delegado municipal deberá certificar, al menos una vez al mes, que no se hayan captado imágenes desde espacios de naturaleza privada como el interior de viviendas, de establecimientos comerciales o de servicios, jardines, patios o balcones. 3. La destrucción de las grabaciones se hará efectiva por parte del responsable de su custodia después de 30 días, salvo si la grabación ha captado un ilícito penal u otra falta, caso en el cual las municipalidades recurridas adoptarán las medidas para su pronta entrega a los órganos competentes. 4. Todo ciudadano tendrá derecho de acceso a las grabaciones, para lo cual deberá dirigir una solicitud al funcionario municipal que designe la autoridad edilicia, debiendo indicar el día en que presumiblemente fue grabado, debiendo las municipalidades recurridas establecer un procedimiento que permita el efectivo ejercicio de esta atribución.

Globo con cámara de videovigilancia en Lo Barnechea.

relevantes algunas iniciativas estatales como la Creación del Comité Interministerial sobre Ciberseguridad,[16] la publicación de la Ley 21.096[17] mediante la cual se incorporó la protección de datos personales en el artículo 19 N° 4 de la CPR y la tramitación del proyecto de ley que regula la protección y el tratamiento de los datos personales[18] y crea la agencia de protección de datos personales y la presentación, a fines de octubre de 2018, del proyecto de ley de delitos informáticos y la publicación de un instructivo presencial que, entre otras medidas, dispone que cada servicio público debe designar un encargado de ciberseguridad de alto nivel, que será responsable de implementar las normas y estándares que aseguren la seguridad informática en su repartición.[19]

16 Creado por el Decreto 533 del Ministerio del Interior y Seguridad Pública, publicado en el *Diario Oficial*, 17 junio 2018.

17 *Diario Oficial,* 16 junio 2018.

18 Boletines 11.092-07 y 11.144-07, refundidos.

19 Es conveniente señalar que es distinto el concepto de privacidad y el de intimidad, pues la vida privada es distinta la vida íntima; sin embargo, conscientes de esta distinción, en el derecho anglosajón se traduce el derecho a la intimidad como "right to privacy" (Álvarez Caro, 2015, p. 27).

INTIMIDAD, VIDA PRIVADA Y DATOS PERSONALES

Desde un análisis de las concepciones clásicas, la intimidad[20] puede ser entendida como una "garantía que tiene el individuo de no sufrir intromisiones o investigaciones no deseadas en su vida privada y que éstas no pueden ser divulgadas" (Matus y Montecinos, 2006, p. 9). La intimidad ha sido entendida por la doctrina como la presunción de que el individuo debe tener una esfera de desarrollo autónomo y de libertad; una "esfera privada" con o sin relación con otros y libre de la intervención del Estado y de la injerencia excesiva no solicitada de individuos no autorizados.

Para determinados autores, la privacidad se trata de un concepto intenso que incluye a la intimidad, por tanto, se trataría de ámbitos distintos, pero consecuentes: "lo íntimo sería un concepto estricto de dimensiones propiamente individuales; y lo privado sería un ámbito que, abarcando lo íntimo, lo supera" (Álvarez Caro, 2015, p. 29), pues el concepto de privacidad también abarca la interacción con terceros. Modernamente, el derecho a la intimidad ha sido entendido como la capacidad de las personas

20 Es conveniente señalar que es distinto el concepto de privacidad y el de intimidad, pues la vida privada es distinta a la vida íntima; sin embargo, conscientes de esta distinción, en el derecho anglosajón se traduce el derecho a la intimidad como *right to privacy* (Álvarez Caro, 2015, p. 27).

para determinar quién posee información acerca de ellos y cómo se utiliza dicha información (La Rue, 2013).

La protección de la vida privada es un derecho reconocido en una serie de instrumentos internacionales, como se verá más adelante, pero a pesar de esta amplia recepción, no ha sido desarrollado plenamente el contenido de este derecho, lo que ha provocado inconvenientes al momento de su aplicación y cumplimiento. Tal como lo ha planteado el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión:

El derecho a la vida privada es un derecho condicionado, su interpretación plantea desafíos respecto de qué constituye la esfera privada y el establecimiento de nociones sobre qué constituye el interés público. Los cambios rápidos y trascendentales en las tecnologías de la información y las comunicaciones registrados en los últimos decenios también han afectado de manera irreversible a nuestra comprensión de los límites entre las esferas pública y privada (La Rue, 2013).

Más recientemente, el Relator Especial sobre el derecho a la privacidad ha manifestado que el derecho a la privacidad es de carácter habilitante, y no un fin en sí mismo, para el ejercicio del derecho al desarrollo de la personalidad de manera libre y sin trabas; en este sentido, el derecho a la privacidad se relaciona estrechamente con otros derechos fundamentales, como la libertad de expresión y la libertad de acceso a la información de dominio público (Cannataci, 2016). Ha agregado que "el derecho a la privacidad es particularmente difícil de ejercer, pues el veloz desarrollo de la tecnología de la información no solo ofrece nuevas oportunidades de interacción social, sino que también suscita inquietudes sobre cómo elaborar adicionalmente ese derecho para hacer frente a los nuevos problemas" (Cannataci, 2016, p. 3).

Efectivamente, los vertiginosos avances tecnológicos han trastocado las nociones clásicas de la intimidad y la vida privada, pues frecuentemente estas pueden resultar afectadas por manejos u operaciones que se pueden ejecutar a distancia y sin que el titular de estos derechos se entere (Matus y Montecinos, 2006). En este sentido, irrumpe el concepto de derecho a la intimidad informática, cuya fundamentación arranca desde los conceptos clásicos de la intimidad, pero que ha cobrado autonomía en lo que respecta al control de la información personal, pues plantea perfiles nuevos con la penetración de nuevas tecnologías (Matus y Montecinos, 2006).

Tal como ha sido mencionado, lo privado engloba a lo íntimo, ya que todo lo íntimo es privado, pero no todo lo privado es íntimo; asimismo, los datos personales pertenecen a la esfera de lo privado y, aunque en ocasiones podrían pertenecer a la esfera de lo íntimo, no necesariamente siempre es así. Justamente, es la posibilidad del tratamiento masivo de datos, con independencia de si estos son de naturaleza íntima o no, y la posibilidad cierta de formular perfiles de personalidad —como en el caso de *Cambridge Analytica* o *Instagis*—, lo que termina afectando el derecho a la intimidad y la privacidad, poniendo de manifiesto la necesidad de proteger los datos personales (Álvarez Caro, 2015).

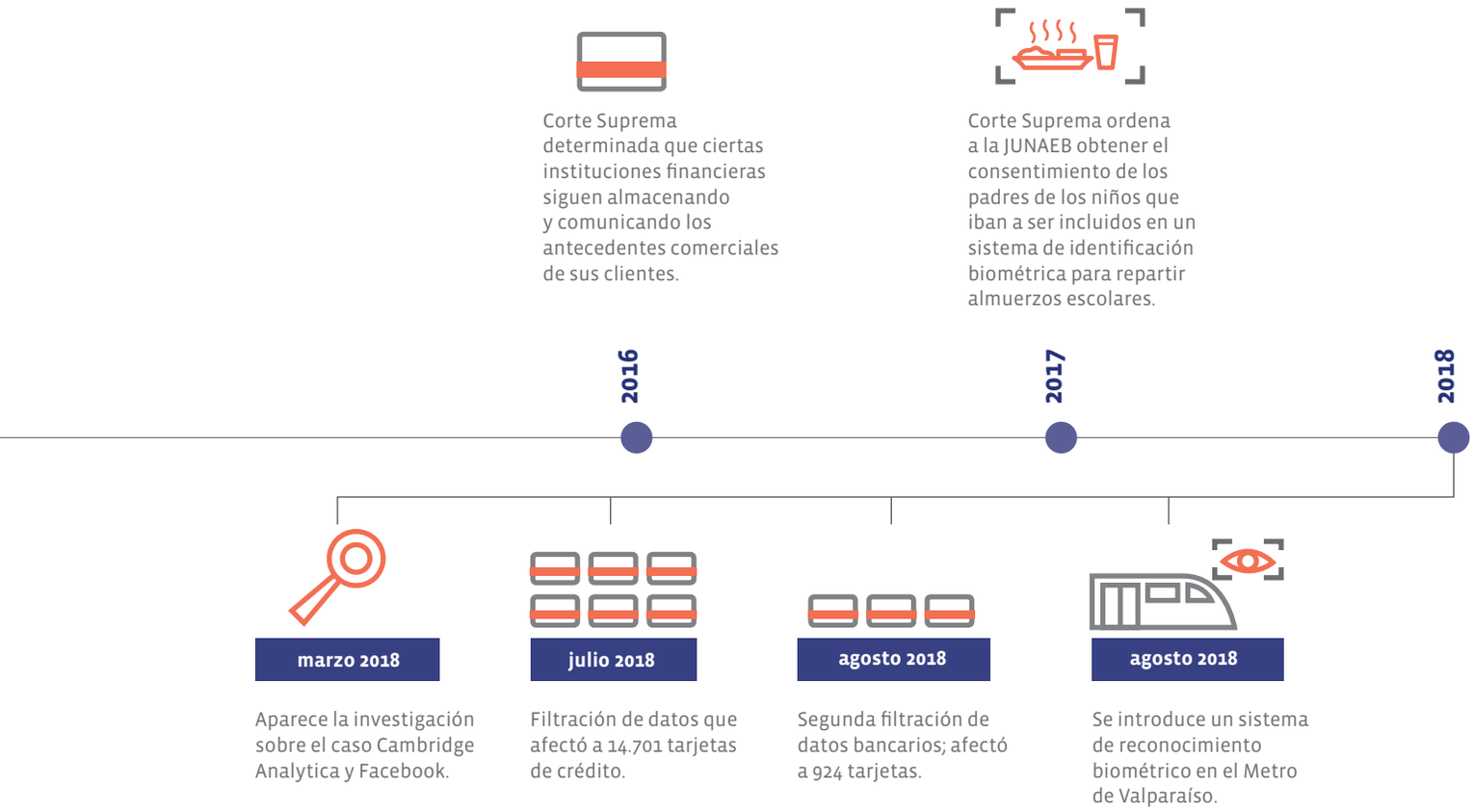
Los vertiginosos avances tecnológicos han trastocado las nociones clásicas de la intimidad y la vida privada, pues pueden resultar afectadas por manejos u operaciones que se pueden ejecutar a distancia y sin que el titular de estos derechos se entere. En este sentido, irrumpe el concepto de derecho a la intimidad informática, cuya fundamentación arranca desde los conceptos clásicos de la intimidad, pero que ha cobrado autonomía en lo que respecta al control de la información personal.

HITOS SOBRE DATOS PERSONALES EN CHILE

Conforme a lo expuesto, la protección de datos personales puede ser entendida como "el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado o no, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad" (Davara, 1999, p. 15).

Además de las distinciones ya precisadas, es necesario delimitar ciertos conceptos a fin de establecer hasta dónde debería extenderse la obligación del Estado de proteger los datos personales y, más estrictamente, los datos de carácter sensible. En general, se ha afirmado que los *datos* describen hechos empíricos, sucesos y entidades; el *dato* es susceptible de ser examinado conforme a un enfoque a fin de apreciar la información contenida en ellos. Cuando el *dato* porta *información* relativa a una persona determinada o susceptible de serlo, se denomina *dato personal* o *dato nominativo*, es decir, una unidad de información que se predica de una persona determinada o determinable (Cerda, 2012). Esta noción es concordante con los conceptos de la LPVP, cuyo artículo 2°, letra f), dispone que "dato de carácter personal o datos personales, son los relativos a cualquier información concerniente a personas naturales, identificado o identificable"; por su parte, en la letra g) del mismo artículo, dispone que los datos sensibles son "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".

El Reglamento General de Protección de Datos de la Unión Europea (GDPR por sus siglas en inglés), que está en vigor desde el 25 de mayo de 2018, dispone en su artículo 4° que los datos personales corresponden a "toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona". La definición sobre datos personales que provee el GDPR es más amplia que la actualmente establecida por nuestra legislación doméstica, pues incluye datos de carácter sensible que se relacionan con aspectos íntimos de la persona, como información sobre su condición de salud.



PROTECCIÓN DE LA PRIVACIDAD

Obligaciones internacionales de derechos humanos

Tal como fue mencionado, el derecho a la vida privada ha sido reconocido en diversos tratados universales de derechos humanos. La DUDH (artículo 12), el PIDCP (artículo 17), la la CDN (artículo 16), la CMW (artículo 14) y la Convención sobre los Derechos de las Personas con Discapacidad (artículo 22), de modo similar disponen que ninguna persona 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; y que cualquiera tiene derecho a la protección de la ley contra tales injerencias o ataques.

En el ámbito interamericano, el derecho a la vida privada se encuentra reconocido, en términos análogos a los mencionados anteriormente, en la Declaración Americana de Derechos y Deberes del Hombre (artículo 5°), en la CADH (artículo 11) y en la CIPM (artículo 16).

De este modo, tal como lo recuerda la Asamblea General de la ONU, en su Resolución 68/167, de 18 de diciembre de 2013, relativa al derecho a la privacidad en la era digital, el derecho internacional de los derechos humanos proporciona un marco universal para evaluar toda injerencia en los derechos individuales a la privacidad, sobre todo si se considera el rápido ritmo del desarrollo tecnológico que permite a las personas utilizar las nuevas tecnologías de la información y las comunicaciones y, al mismo tiempo, incrementa la capacidad de los gobiernos, las empresas y las personas de llevar a cabo actividades de vigilancia, interceptación y recopilación de datos, lo que podría constituir una violación o una transgresión de los derechos humanos, en general, y en particular al derecho a la privacidad.

El Relator Especial sobre el derecho a la privacidad, en su último informe de febrero de 2018, ha reconocido la gravedad de la vigilancia como una amenaza para el disfrute del derecho a la intimidad y ha promovido que los Estados desarrollen un marco jurídico internacional exhaustivo destinado a regular la vigilancia en el ciberespacio (Cannataci, 2018, p. 21).

En este mismo sentido, en el proyecto de Resolución 38/L.10 del Consejo de Derechos Humanos, de 2 de julio de 2018, sobre Promoción, protección y disfrute de los derechos humanos en internet, los Estados que la han suscrito, entre ellos Chile, han afirmado que “los mismos derechos que tienen fuera de línea las personas también deben protegerse en línea” (párr. 1) y que los Estados deben “adoptar, aplicar y, de ser necesario, reformar leyes,

reglamentos, políticas y medidas relativas a la protección en línea de los datos personales y la privacidad, para prevenir, mitigar y remediar la recolección, la retención, el procesamiento, el uso o la revelación arbitrarios o ilícitos de datos personales en Internet que pudieran violar los derechos humanos" (párr. 17).

Por su parte, la CIDH ha señalado que el derecho a la privacidad protege al menos cuatro bienes jurídicos, a saber: a) el derecho a contar con una esfera de cada individuo resistente a las injerencias arbitrarias del Estado o de terceras personas; b) el derecho a gobernarse por reglas propias según el proyecto individual de vida de cada uno; c) el derecho al secreto respecto de lo que se produzcan en ese espacio reservado con la consiguiente prohibición de divulgación o circulación de la información capturada, sin consentimiento del titular, en ese espacio de protección reservado a la persona; y d) el derecho a la propia imagen (RELE-CIDH, 2017, p. 78).

La CIDH ha precisado que los Estados deben "respetar y proteger el derecho a la privacidad en la era digital y adoptar o adaptar su legislación y sus prácticas al efecto, protegiendo a todas las personas bajo su jurisdicción —incluyendo conforme al derecho internacional, aquellas personas sobre las cuales tenga control efectivo— sin discriminación por origen nacional, nacionalidad, sexo, raza, religión o cualquier otro motivo" (RELE-CIDH, 2017, p. 79); y que, en tanto, "la protección de la privacidad en internet requiere que se garantice la confidencialidad de los datos personales en línea" (RELE-CIDH, 2017, p. 81).

En ese sentido, los alcances de la clásica formulación del derecho a la protección de la vida privada, a fin de alcanzar cierto estatuto de protección de los datos personales y sensibles, deben reinterpretarse conforme a las necesidades y problemáticas que plantea el desarrollo de las nuevas tecnologías.

Regulación nacional

En 1995, fue publicada la Ley 19.423 que agrega disposiciones al Código Penal en lo relativo a delitos contra el respeto y la protección a la vida privada y pública de la persona y su familia. El artículo 161-A introducido por esta ley plantea que "se castigará con la pena de reclusión menor en cualquiera de sus grados y multa de 50 a 500 Unidades Tributarias Mensuales al que, en recintos particulares o lugares que no sean de libre acceso al público, sin auto-

Los alcances de la clásica formulación del derecho a la protección de la vida privada, a fin de alcanzar cierto estatuto de protección de los datos personales y sensibles, deben reinterpretarse conforme a las necesidades y problemáticas que plantea el desarrollo de las nuevas tecnologías.

rización del afectado y por cualquier medio, capte, intercepte, grabe o reproduzca conversaciones o comunicaciones de carácter privado; sustraiga, fotografíe, fotocopie o reproduzca documentos o instrumentos de carácter privado; o capte, grabe, filme o fotografíe imágenes o hechos de carácter privado que se produzcan, realicen, ocurran o existan en recintos particulares o lugares que no sean de libre acceso al público".

Posteriormente, en consideración a la redacción original del artículo 19 N° 4 de la CPR, en 1999 fue promulgada la LPVP.[21] El artículo 1° de esta ley dispone que "el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones" que en ella se establecen y que "toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con la ley y para las finalidades permitidas por el ordenamiento jurídico".

El artículo 4° de la LPVP dispone que "el tratamiento de los datos personales sólo puede efectuarse cuando esta ley y otras disposiciones legales lo autoricen o el titular consienta expresamente en ello". Algunos de los casos en que la ley autoriza expresamente el tratamiento de estos datos son: i) cuando el tratamiento de datos personales provenga o se recolecten de fuentes accesibles al público; ii) cuando sean de carácter económico, financiero, bancario o comercial; iii) cuando se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia de la persona a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios; y iv) cuando el tratamiento de datos personales lo realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquellos.

Las condiciones que se establecen para que el consentimiento dado por el titular para el tratamiento de datos sea válido, son: i) la persona autorizante debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y probable comunicación al público; ii) la autorización debe constar por escrito; iii) la autorización puede ser revocada, aunque sin efecto retroactivo, lo que también debe hacerse por escrito.

El artículo 9° de la ley dispone que los datos personales deben utilizarse solo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hubieren recolectado de fuentes accesibles al público.

En el artículo 12, establece que todas las personas tienen derecho a exigir a quien se dedique al tratamiento de datos personales, de forma pública o privada, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus

21 En la moción original que dio inicio a la tramitación de la LPVP se expresó que para su formulación se tomaban como "parámetros orientadores los principales criterios esbozados por el derecho comparado de las naciones más avanzadas; los diversos convenios, pactos y trabajos suscritos por la comunidad internacional en materia de derechos humanos, civiles y políticos, tales como la Declaración Universal de Derechos Humanos, de 1948; la Declaración Americana de los Derechos y Deberes del Hombre, de 1949, el Pacto Internacional de Derechos Civiles y Políticos, de 1966 y, la Convención Americana Sobre Derechos humanos, de 1969, y, el mandato constitucional establecido en los artículos 5° y 19 números 4 y 5, de nuestra Ley Fundamental".

datos sean transmitidos regularmente. Además, la misma norma indica que en caso de que los datos sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tiene derecho a que se modifiquen, eliminen o bloqueen. En caso de que el responsable del registro o banco de datos no se pronuncie sobre la solicitud del requirente dentro de dos días hábiles o la deniegue por razones distintas a la seguridad o interés de la Nación, el titular de los datos tendrá derecho a recurrir al juez de letras en lo Civil, solicitando amparo de los derechos mencionados.

Recientemente, mediante la publicación de la Ley 21.096,[22] se modificó el artículo 19 N° 4 de la CPR, que reconoce como derecho fundamental el respeto y protección de la vida privada y a la honra de la persona y su familia, para incluir la protección de los datos personales:

> *Artículo 19. La Constitución asegura a todas las personas:*
>
> *4°.- 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.*

Mediante esta modificación, la CPR ofrece una mayor protección que los tratados internacionales en materia de protección explícita de los datos personales.

La conceptualización de la protección de datos personales como una cuestión de derechos fundamentales ha sido entendida por algunos como una derivación del derecho a la privacidad.[23] Sin embargo, mientras la interpretación clásica del derecho a la privacidad se ha traducido en el aforismo "ser dejado solo o en paz" (*the right to be let alone*),[24] la protección de datos personales se estructura sobre una prerrogativa positiva, es decir, se trata del derecho de las personas a controlar sus datos personales incluso si estos se refieren a aspectos íntimos.

El derecho fundamental de protección de los datos personales, conforme a lo dispuesto en el artículo 20 de la CPR, está protegido por la acción constitucional de protección. Además, también quedaría cubierto por el procedimiento de tutela de derechos fundamentales, según lo establecido el artículo 485 del Código del Trabajo. Conforme a la opinión de Gálvez:

> *Será menester que los empleadores tomen las medidas necesarias a fin de dar la debida protección a los datos personales de sus trabajadores que deban manejar en razón de la relación laboral que tienen con éstos, debiendo en primer lugar revisar que cuenten con la correspondiente autorización escrita de cada uno de sus trabajadores y que éstos estén en conocimiento del propósito del almacenamiento de sus datos personales por parte del empleador.*[25]

Según lo expuesto hasta el momento, a pesar de que la puerta de entrada a la protección de los datos personales tradicionalmente ha sido el derecho a la privacidad, no debe perderse de vista que la materia en análisis se relaciona estrechamente con otros derechos humanos y fundamentales, pues la captación de datos personales, su procesamiento y transferencia puede impactar en el ejercicio de otros derechos, tal como ha tratado de ejemplificarse mediante los ejemplos consignados en los antecedentes de este capítulo. En este sentido, Jessica Matus, presidenta de la Fundación Datos Protegidos, ha precisado que *"la protección de los datos personales como derecho fundamental es considerado un derecho instrumental, que no sólo viene a proteger el derecho a la privacidad,*

22 *Diario Oficial,* 16 junio 2018.

23 Reconoce su origen en el Tribunal Constitucional Federal Alemán a través de la protección jurisprudencial que otorgó a la libertad informativa basado en el derecho general de la personalidad y que ofrece protección frente a la captación, el almacenamiento, la utilización y la transmisión ilimitada de los datos de carácter personal y garantiza la facultad del individuo de decidir básicamente por sí mismo sobre la difusión y la utilización de sus datos personales.

24 Al respecto, la jurisprudencia del Tribunal Constitucional chileno ha entendido predominantemente el derecho a la protección de los datos personales en su fase negativa y no de modo positivo, es decir, en el sentido de que la persona tiene derecho a no ser perturbada en su privacidad y no en el sentido del derecho que las personas tienen a poder controlar sus datos personales y, en tanto, autorizar y denegar su uso, almacenamiento, procesamiento y comunicación. Sobre esta materia revisar Quezada Rodríguez (2012), *La protección de datos personales en la jurisprudencia del Tribunal Constitucional de Chile*.

25 Gálvez, Romina, "La protección de los datos personales del trabajador se eleva a derecho fundamental", 5 julio 2018, http://www.az.cl/la-proteccion-de-los-datos-personales-del-trabajador-se-elevan-a-derecho-fundamental/

sino que además otros derechos".[26] La naturaleza instrumental del derecho a la protección de los datos personales significa que en su virtud *"se puede garantizar el ejercicio de otros derechos, como el derecho al trabajo, el derecho a la no discriminación, el derecho a la igualdad, a la salud, porque la gran cantidad de información que se maneja de las personas, tanto por organismos públicos y empresas, ha devenido en el último tiempo en crear lo que se llama la datificación, que se traduce en capturar gran cantidad de información, generar infraestructura de datos y generar perfiles de las personas muy detallados, con todas sus características*". Jessica Matus precisa que este proceso de *datificación* no sólo se produce en el *"entorno digital mediante la información que nosotros mismos entregamos en internet, sino también en los espacios físicos mediante el desarrollo de técnicas de vigilancia y biometría"*.

María Paz Canales, directora ejecutiva de la ONG Derechos Digitales, refrenda la idea anterior, *"ya que tradicionalmente ha habido una mirada muy limitada acerca del impacto del uso de la tecnología y solo se piensa en el impacto que tiene en la privacidad, cuando en realidad hay muchos derechos civiles y políticos afectados, como la libertad de expresión o el derecho a reunión*".[27] Agrega que

> *"lo mismo aplica respecto de los derechos económicos sociales y culturales, porque en el fondo todo este tipo de tecnología de vigilancia posibilita la discriminación. […] [La] posibilidad efectiva de ejercer nuestros derechos, nuestro acceso a la educación, al trabajo, a la cultura, el derecho a recibir beneficios sociales; todo está condicionado por la posibilidad de discriminación perfecta que entregan estas tecnologías que permiten recopilar información acerca de nosotros, en donde el ciudadano está en una situación de completa disparidad y desventaja respecto ya sea del aparato público o de las empresas privadas, que son las que deciden qué es lo que se recopila y para qué se usa, sin que nosotros podamos tener ningún control al respecto"*.

26 Discusión de grupo realizada el 31 de mayo de 2018.

27 Discusión de grupo realizada el 31 de mayo de 2018.

PRINCIPALES PROBLEMÁTICAS EN RELACIÓN A PROTECCIÓN DE LOS DATOS PERSONALES

Deficiencias de la LPVP

Tempranamente, el contenido de la LPVP fue calificado de insuficiente en lo que se refiere a una efectiva protección de datos personales, posición que se ha mantenido en el tiempo a pesar de las múltiples modificaciones que ha experimentado esta ley.[28] Existe consenso entre la doctrina, que los marcos legales sobre protección de datos personales es débil (Jijena, 2001; Viollier, 2017). Se ha mencionado que la insuficiencia de la LPVP responde "al hecho de que su contenido fue condicionado por ciertos intereses durante la discusión legislativa. Este diagnóstico se ve ejemplificado en el nivel de protección otorgado por la ley, que se caracteriza por ofrecer un marco regulatorio para el mercado de las bases de datos personales, más que por garantizar protección a los derechos de las personas titulares de estos" (Viollier, 2017, p. 4).

28 La LVPV ha sido modifica en cuatro oportunidades, en virtud de los siguientes cuerpos legales: 1. Ley 19.812 (D.O. 17.02.02); 2. Ley 20.463 (D.O. 25.10.10); 3. Ley 20.521 (D.O. 23.07.11) y 4. Ley N° 20.575 (D.O. 17.02.12).

También debe considerarse que a pesar de que la LPVP es del año 1999, *"nació desfasada, porque toma en consideración precedentes legales comparados de los años 70; entonces, ni siquiera cuando llegó en su momento, en el 1999 o en el 2000, fue una ley actualizada"*, declara María Paz Canales. También agrega que esta normativa *"en ninguna parte se refiere a los desarrollos de internet y tecnologías relacionadas"*.

Se ha planteado que las principales problemáticas de la LPVP son "la ausencia de sanciones efectivas, la falta de regulación del flujo transfronterizo de datos personales, la autorización del uso de datos para marketing directo sin consentimiento del titular, la falta de registro de bancos de datos privados, la ausencia de una autoridad pública de control, excepciones amplias al consentimiento para el tratamiento de datos, y la falta de mecanismos procedimentales de resguardo efectivo" (Viollier, 2017, p. 4).

Una de las problemáticas más relevantes de esta ley es que formalmente declara que el tratamiento de datos personales solo puede hacerse en virtud de autorización legal o del titular de los datos, "pero del contexto de las normas se desprende que la mayoría de los datos provienen de "fuentes de acceso público" (por lo cual no se requiere de autorización para su tratamiento) y se consagran im-

La LPVP no establece estándares para que los organismos públicos y las empresas privadas que se dedican al manejo de datos personales resguarden que esa información no sea objeto de tráfico ilícito y usos que no hayan sido autorizados por las personas. A modo de ejemplo, este 2018 se ha producido una sucesión de denuncias respecto al robo por internet de dinero desde cuentas corrientes, robo a fondos de los propios bancos por hackers, extracción de información sensible de los clientes de empresas y sustracción de información por los propios empleados.

portantes y amplias excepciones sobre todo en materia de datos "personales-patrimoniales", lo cual transforma a la regla general en una mera "declaración de principios" (Jijena, 2001).

Otra deficiencia de la LPVP guarda relación con aspectos orgánicos, ya que no establece un órgano que fiscalice su cumplimiento. El artículo 22 de la ley dispone que el Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos. Esta disposición es limitada, pues en sí no contempla facultades ni mecanismos de control o fiscalización ni sanciones en caso de incumplimiento (Jijena, 2001).

Junto a lo anterior, el tratamiento de datos personales también se efectúa en directa contravención a las obligaciones y limitantes que impone actualmente la LPVP. Los tribunales de justicia han conocido casos donde se han acreditado conductas contrarias a lo dispuesto en el artículo 18 de la LVPV, que prohíbe la comunicación y utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial "luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible". Este mismo artículo agrega que "tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de haber sido pagada o haberse extinguido por otro modo legal".

En 2012, la Corte de Apelaciones de Santiago, conociendo una acción constitucional de protección, falló en contra del Banco BBVA por "mantener y consultar un registro que debe ser calificado como 'clandestino' o al margen de la ley, [y que, en tanto, incurrió] en una conducta ilegal y arbitraria que afectó la garantía constitucional contemplada en el N° 4 del artículo 19 de la CPR, que se refiere a la protección de la vida privada de las personas".[29]

Una práctica similar ha sido sancionada por la Corte Suprema, ya que determinadas instituciones financieras siguen almacenando y comunicando los antecedentes comerciales de sus clientes, a pesar de haber pagado o extinguido sus deudas, situación que entra en directo conflicto con el artículo 18, inciso segundo, de la LPVP que dispone "tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de haber sido pagada o haberse extinguido por otro modo legal".[30] También, la Corte Suprema ha corregido conforme a derecho, casos donde, a pesar de que las deudas han sido declaras prescritas, la institución acreedora ha insistido en mantener su registro.[31]

Otro problema se produce en la captación y uso de información y datos personales para fines comerciales sin el consentimiento expreso del titular, práctica muy utilizada en los servicios del *retail* y salud, por ejemplo, que solicitan el RUT del cliente al momento del pago, vinculando así a la persona con necesidades y gustos personales. Al respecto el presidente del Consejo para la Transparencia (CPLT) ha manifestado que ninguna compraventa en tiendas comerciales puede condicionarse a la entrega del RUT. Respecto de la entrega de un dato personal como el mencionado y eventuales usos indebidos o transferencia a terceros sin consentimiento del titular, el presidente del Consejo afirmó que desde ahora *"las empresas chilenas tienen que empezar a transparentar políticas de privacidad claras, donde estas cosas no se permitan"*. Además, insistió en que no es posible que las entidades piensen que el solo hecho de levantar los datos les permite usarlos con fines distintos para los cuales fueron recolectados. Recordó que *"quien los recibe (los datos) solo puede utilizarlos para el fin para el cual los obtuvo"*.[32]

Las prácticas previamente mencionadas, guardan relación con los bajos niveles de seguridad en la gestión de la información. La LPVP no establece estándares para que los organismos públicos y las empresas privadas que se dedican al manejo de datos personales resguarden que esa información no sea objeto de tráfico ilícito y usos que no hayan sido autorizados por las personas. A modo de ejemplo, este 2018 se ha producido una sucesión de denuncias respecto al robo por internet de dinero desde cuentas corrientes,[33] robo a fondos de los propios bancos por hackers, extracción de información sensible de los

29 Corte de Apelaciones de Santiago, causa ROL 5072-2011, sentencia del 18 de enero de 2012.

30 Corte Suprema, causa Rol 4903-2015, sentencia del 11 de octubre de 2016.

31 Corte Suprema, causa Rol 9078-2014, sentencia del 31 de diciembre de 2014.

32 CPLT. Consejo para la Transparencia afirma que ninguna compraventa en tiendas comerciales puede condicionarse a la entrega del RUT. Disponible en: https://www.consejotransparencia.cl/consejo-para-la-transparencia-afirma-que-ninguna-compraventa-puede-asociarse-a-la-entrega-del-rut/ [Último acceso: 26 septiembre 2018.]

33 Bio-Bío, "Denuncian a Banco Itaú por no responsabilizarse en caso de presunto fraude por internet", Sebastián Asencio, 5 junio 2018, https://www.biobiochile.cl/noticias/economia/negocios-y-empresas/2018/06/05/denuncian-a-banco-itau-por-no-responsabilizarse-en-caso-de-presunto-fraude-por-internet.shtml

clientes de empresas[34] y sustracción de información por los propios empleados.[35]

Como puedo concluirse, tanto los exámenes doctrinarios como la jurisprudencia de los casos analizados ponen de manifiesto que la LPVP no establece adecuados niveles de protección.

Biometría y vigilancia

En los antecedentes de este capítulo se citaba el caso de los globos de videovigilancia de Las Condes y Lo Barnechea. Sobre la base de una legítima pretensión de prevenir la comisión de hechos delictivos, se ha estimado que la instalación de cámaras en espacios públicos es una medida que contribuiría a conseguir dicho objetivo. La videovigilancia se torna más compleja cuando mediante sus características tecnológicas es posible captar datos biométricos, procesarlos y almacenarlos.

La biometría, conforme a lo indicado por la OCDE, consiste en "características únicas y medibles de rasgos en los seres humanos que sirven para automáticamente reconocer o verificar una identidad" (OCDE, 2004a). El GDPR, en su artículo 1°, número 14, dispone que los datos biométricos son "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos". Algunos ejemplos de datos biométricos son las huellas dactilares o palmares, la forma y pigmentación del iris o las medidas faciales. En general, cualquier rasgo físico o de comportamiento es susceptible de ser capturado por medios tecnológicos y, posteriormente, ser procesados como un dato en la medida que se cumpla con cuatro requisitos: coleccionabilidad o posibilidad de ser medido; universalidad, es decir, la existencia del elemento en todas las personas; unicidad, que el elemento sea distintivo en cada persona; y la permanencia del elemento en el tiempo (Díaz, 2018, p. 6).

Los usos principales de los datos biométricos son la verificación y la identificación. Mediante la verificación se pretende validar una identidad por medio de la comparación con los datos biométricos que la propia persona ha entregado; este uso también ha sido denominado modelo biométrico de uno contra uno, "pues consiste en comparar uno o más rasgos de un individuo con una plantilla

34 Cooperativa, "Hackeo masivo de tarjetas: Correos de Chile confirmó filtración desde su casilla en Miami", 10 septiembre 2018, https://www. cooperativa.cl/noticias/pais/consumidores/hackeo-masivo-de-tarje- tas-correoschile-confirmo-filtracion-desde-su/2018-09-10/204026.html

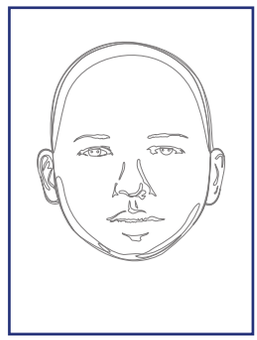
35 CEPYME, "Un 69% de las empresas ha experimentado el robo de datos por parte de empleados", 16 junio 2017, https://cepymenews.es/69-las-empresas-ha-experimentado-robo-datos-parte-empleados/

TIPOS DE DATOS

DATOS PERSONALES

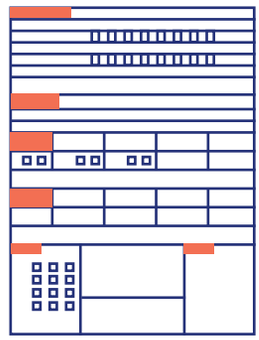
Nombres
Apellidos
Rut
Fecha de nacimiento

DATOS BIOMÉTRICOS



Características faciales
Huellas digitales
Retina

DATOS SENSIBLES



Orientación sexual
Identidad de género
Ascendencia étnica
Filiación política

correspondiente a la identidad de ese mismo individuo, es decir, es un proceso mediante el cual se verifica la declaración de identidad hecho por una persona en cuyo poder reside, por ejemplo, un carnet de identidad" (Díaz, 2018, p. 6). Por su parte, la identificación de una persona se refiere a un procedimiento mediante el cual los datos biométricos son contrastados con otros que están sistematizados en una base de datos; se trata de una "comparación de uno a muchos, lo que significa que requiere una base que contiene los datos biométricos de un grupo determinado de individuos, almacenados centralizadamente con la finalidad de: a) determinar si el individuo en cuestión se encuentra en esa base de datos (por ejemplo, en un modelo de entrega de servicios asistenciales), o b) identificar quién es el individuo dentro del rango de esa base de datos (por ejemplo, el caso de la búsqueda de un sospechoso en una base de datos de antecedentes penales)" (Díaz, 2018, p. 6).

Se ha manifestado que el uso de la biometría para fines de identificación es mucho más compleja que la utilizada para validación de una identidad, ya que la creación de una base de datos centralizada con información biométrica crea riesgos de seguridad y privacidad, puesto que tales datos no se encuentran bajo el poder de la persona, sino que la administración de la base de datos se encuentra a cargo de un organismo estatal o empresa privada (Díaz, 2018).

La videovigilancia y la captación de datos biométricos han generado polémica en la región, donde han sido presentadas como una solución a una serie de problemáticas históricas, como la seguridad ciudadana, la adecuada distribución de beneficios sociales y la mejora de los procedimientos de registro de la identidad de los ciudadanos (Díaz, 2018, p. 22). En 2017 intentó instalarse un sistema de videovigilancia con captación biométrica en el sistema de transporte público Transmilenio de Bogotá (Colombia), lo que generó alerta entre organizaciones y defensores de derechos humanos por las potenciales afectaciones al derecho a la privacidad y el inadecuado tratamiento de datos de carácter sensible (Spanger y Sáenz, 2018). Una situación similar se experimentó hacia mediados de 2018 ante la instalación de cámaras capaces de captar datos biométricos en el área metropolitana de Asunción (Paraguay), sin que se establecieran marcos normativos efectivos para resguardar los datos de carácter sensible (Fulchi, Carrillo, y Sequera, 2018).

A partir de agosto de 2018, en el Metro de Valparaíso opera un sistema de reconocimiento facial:

Durante el recorrido, se verificó la operación del sistema de reconocimiento facial destinado a fiscalizar el correcto uso de las tarjetas con beneficios, como las de los estudiantes. Gracias a la incorporación de inteligencia artificial en el análisis de las imágenes que capta el circuito cerrado de televisión, cada vez que una persona pasa por el torniquete con una tarjeta con beneficios, el sistema compara sus datos biométricos con los del usuario registrado en la base de datos. Así, se efectúa un proceso de verificación que determina si se trata del pasajero titular de la tarjeta. Esta fiscalización remota permite asegurar un buen uso de los recursos asignados a las rebajas tarifarias.[36]

El uso de tecnologías biométricas requiere de marcos legales exhaustivos que se orienten de modo estricto a regular su funcionamiento y resguardar los derechos fundamentales de las personas. La LPVP debería establecer estándares más estrictos que aquellos dispuestos para el tratamiento de datos personales e, incluso, sensibles, pues los datos biométricos no solo pertenecen a la persona (como su nombre, RUT o domicilio) sino que son la persona misma.

Son varios los riesgos asociados al uso de datos biométricos: son fáciles de captar, sobre todo considerando que son las mismas personas quienes suben fotografías de sus rostros a sus redes sociales sin activar suficientes medidas de seguridad y privacidad; las huellas dactilares pueden ser obtenidas de objetos que tocamos; la voz puede ser grabada y modificada (Garrido y Becker, 2017, p. 82). En fin, todos estos aspectos facilitan la falsificación de datos biométricos, lo que crea el problema de falsas identificaciones: ¿cómo una persona podría solicitar que sus datos biométricos falsificados dejen de estar asociados a un historial penal que no le pertenece?

La OCDE ha manifestado que el uso de biometría no es en sí mismo un aspecto que lesione el derecho a la privacidad, no obstante pasa a ser relevante la regulación de sus usos, para lo cual debe considerarse desde un comienzo el resguardo de la intimidad de las personas, a fin de evitar o disminuir ciertos riesgos asociados a su uso (OCDE, 2004b, p. 12). A modo de ejemplo, el artículo 9° del GDPR prohíbe el tratamiento de datos que revelen el origen étnico o racial, datos genéticos y datos biométricos dirigidos a identificar de manera unívoca a una persona física.

Un riesgo asociado al uso de datos personales, en general, pero que es particularmente complejo en el uso de biometría, es el denominado *function creep* o *purpose creep*; esto es un comportamiento indebido de quienes recolectan datos para un uso específico pero que posteriormente lo emplean o transfieren para finalidades que no han sido autorizadas por el titular de los datos. Por ejemplo, puede ser que el prestador de un determinado servicio social requiera que el beneficiario enrole su huella digital solo con la finalidad de evitar que reciba un subsidio dos veces, pero si la imagen dactilar capturada es ocupada posteriormente con otro propósito no informado inicialmente se configura un caso de *function creep* (OCDE, 2004b, p. 12).

Otra problemática de la biometría guarda relación con el consentimiento y la transparencia, pues ciertos datos de esta naturaleza se pueden capturar sin la autorización o la participación activa (o incluso sin el conocimiento) del individuo. Tal como lo señala la OCDE en su informe, desde hace varios años se utilizan métodos de reconocimiento en casinos para detectar a tramposos y contadores de cartas, o la práctica de ciertas compañías que rastrean hábitos de compra a través de tecnología que permite el reconocimiento facial; también existen reportes que detallan que la exploración del iris puede realizarse sin problemas desde distancias considerables (OCDE, 2004b, pp. 12-13). Desde una perspectiva de privacidad, estas situaciones pueden entrar en conflicto con los principios de limitación de la recopilación, apertura y especificación de objetivos.

Los sistemas biométricos también son complejos, ya que son susceptibles a diversos tipos de ataques, pues el iris de una persona puede ser suplantado mediante impresiones de alta resolución o las huellas de una persona también pueden ser duplicadas mediante procedimientos sencillos (OCDE, 2004b, p. 13).

Respecto a las complejidades del uso de la biometría, María Paz Canales, de Datos Protegidos, recuerda la licitación pública de la Junta Nacional de Auxilio Escolar y Becas (JUNAEB), mediante la cual se buscaba incorporar biometría para la entrega de almuerzos escolares y otros beneficios de alimentación: *"Se planteaba hacer un enrolamiento de todos los datos biométricos de los niños, para mejorar la distribución de la alimentación de la JUNAEB, porque efectivamente tienen un problema con ese aspecto; pero en vez de pensar en una solución que esté orientada a solucionar el problema sin un impacto negativo, se*

36 Metro de Valparaíso, "Subsecretario de transporte supervisa sistema de reconocimiento facial y novedades tecnológicas de pago implementadas en Metro Valparaíso", 1 agosto 2018, https://www.metro-valparaiso.cl/subsecretario-de-trasnportes-supervisa-sistema-de-reconocimiento-facial-y-novedades-tecnologicas-de-pago-implementadas-en-metro-valparaiso/

Un riesgo asociado al uso de datos personales, en general, pero que es particularmente complejo en el uso de biometría, es el denominado function creep o purpose creep; esto es un comportamiento indebido de quienes recolectan datos para un uso específico pero que posteriormente lo emplean o transfieren para finalidades que no han sido autorizadas por el titular de los datos.

quiere enrolar en un sistema biométrico, poner esa data de los niños más vulnerables de todo Chile. Este caso se judicializó y la Corte Suprema en el fallo que emitió acerca de las características de la licitación, le dio la orden a la JUNAEB de asegurarse de que se les exigiera a las empresas que pudieran obtener el consentimiento de los padres de esos niños", pero el problema es que las personas no conocen las implicancias del almacenamiento de datos biométricos ni las empresas informan adecuadamente el uso que se hace de ellos.[37]

Uso de Big Data y Data Mining en políticas públicas: posibles tensiones con la protección de datos personales

En los últimos años, el término Big Data ha irrumpido con gran fuerza. Según Diebold (2012), citado por Velasco y Viollier (2016), este término proviene de las ciencias computacionales, las estadísticas y la econometría. Una de las definiciones de Big Data lo caracteriza como "bases de datos cuyo tamaño está más allá de la habilidad de un software corriente para capturar, administrar y analizar dicha base de datos" (Mayinka et al., 2011, citado en Velasco y Viollier, 2016). Por su parte, la minería de datos o *Data Mining* "es el conjunto de técnicas y tecnologías que permiten explorar grandes bases de datos, de manera automática o semiautomática, con el objetivo de encontrar patrones repetitivos, tendencias o reglas que expliquen el comportamiento de los datos en un determinado contexto".[38] De acuerdo a María Paz Hermosilla, directora del GobLab de la Universidad Adolfo Ibáñez (UAI), la utilización de Big Data para formular políticas públicas sirve para

> *[...] aumentar la eficiencia y disminuir los costos, puede mejorar la toma de decisiones, porque apura algo que se demoraba mucho antes; por ejemplo, el Servicio de Impuestos Internos ahora ejecuta en una hora procesos que antes se demoraban dos semanas. El Big Data permite generar nuevos productos y servicios, o mejorar productos y servicios basados en el análisis de las personas o las necesidades y preferencias, en este caso, de los ciudadanos.*[39]

Según detalla la directora del GobLab UAI, en Estados Unidos se creó un algoritmo para detectar cuándo un niño o niña estaba en mayor riesgo de ser vulnerado en sus derechos.

> *De hecho, se hizo una revisión ética de la implementación del algoritmo por expertos independientes, y dijeron que era ético implementarlo porque con el algoritmo podían, por un lado, no ir a visitar a los niños que no tenían riesgo, y por otro lado captar a los niños que sí iban a ser vulnerados.*

37 Salud y Vida S.A., Sociedad Alimenticia Departamental Ltda., Coan Chile Ltda., Sociedad de Servicios de Alimentación S.A., contra Junta Nacional de Auxilio Escolar y Becas, Corte Suprema, Rol 6.080-2017.

38 Business Intelligence. Dataminig (minería de datos). Disponible en: https://www.sinnexus.com/business_intelligence/datamining.aspx [Último acceso: 1 de octubre de 2018.]

39 Discusión de grupo realizada el 31 de mayo de 2018.

Otra experiencia, detallada por Mansell (2018), es la de la Agencia de Infancia, Juventud y Familia (CYF por sus siglas en inglés) de Nueva Zelanda, la que compiló una lista de 2 mil niños y niñas de entre 6 y 7 años, la mitad de los cuales se estimaba estaría en una institución penal adulta cuando fuesen mayores:

> *Lo anterior fue posible gracias a que el equipo recién formado de análisis avanzado unió datos de CYF, los servicios de Justicia Juvenil y el sistema correccional de adultos. Esto proveyó una historia longitudinal de personas que habían conocido el sistema correccional y habían estado también en el sistema de protección de niños, niñas y adolescentes a edades tempranas, usando más de 20 años de historia. Empleando esta información longitudinal, se podían identificar con relativa claridad las variables predictivas para los jóvenes que tendrían más probablemente la tendencia a reincidir durante sus vidas (Mansell, 2018).*

María Paz Hermosilla detalla que el Big Data y el Data Mining también puede servir para la prevención de epidemias: "Por ejemplo, en Pakistán hubo una epidemia de dengue y armaron un call center para derivar a la gente a distintos hospitales, pero se dieron cuenta que, con esos datos, más otra información de clima, podían hacer un modelo predictivo para ver dónde iba a haber un brote de dengue y resulta que lo podían predecir dos a tres semanas antes". Al predecir la zona geográfica específica donde habría un brote de dengue, se podían adoptar medidas preventivas para evitar su proliferación efectiva.

El ejemplo señalado sirve para distinguir la utilización de *data* en políticas públicas, incluso de gran volumen, a la utilización de datos personales. Sobre este punto María Paz Canales, precisa que:

> *Es importante tener clara la distinción entre lo que es data en general y lo que es dato personal, porque son conceptos que se mezclan mucho cuando se está hablando de Big Data; por ejemplo, la finalidad de la política adoptada en Pakistán para evitar la proliferación del dengue, pudo hacerse mediante datos climáticos o geográficos, cuestión que no implica usar datos personales. O también se pudo haber utilizado data anonimizada, es decir, recogida inicialmente de datos personales, pero a la cual se le aplica una medida de mitigación para desconectar esa información del dato personal y se conserva como información estadística y es igualmente útil para la política pública que se quiere aplicar.*

Según lo comentado por María Paz Canales, hay muchos beneficios de la utilización de la Big Data para la formulación de políticas públicas que pueden ser extraídos al nivel de data anonimizada y categorizada, no se pierde el beneficio del dato y no se ponen en riesgo datos de carácter personal, lo que implica una mayor protección de los derechos de las personas y a la vez se puede conseguir el objetivo de la política pública.

La directora ejecutiva de Derechos Digitales también señala que uno de los déficits más relevantes en la utilización de Big Data, a través de minería de datos para políticas públicas, es que no se realiza una *"evaluación de impacto respecto de las otras materias o derechos que no son los directamente implicados en el problema que se quiere solucionar con esa política pública; entonces hay una visión muy parcializada, en donde generalmente se busca enfrentar un problema específico que puede ser real y para el cual la tecnología puede ser una de las herramientas útiles para poder solucionarlos, pero al tomar esa decisión de qué tipo de tecnología implementar o en qué forma implementarla, no se hace un análisis de espectro más amplio acerca de cuáles son los otros derechos que van a ser impactados de manera negativa",* a fin de evitar la difusión de datos personales, la estigmatización y la discriminación sobre ciertos grupos sociales.

Un nuevo paradigma en la protección de datos personales

La protección de datos personales alcanza diversos niveles, desde la adopción de leyes hasta políticas y otras medidas que sean capaces de responder a los múltiples riesgos, que, en virtud del desarrollo tecnológico, están expuestos los datos personales, sensibles y biométricos. La cuestión fundamental a dilucidar es cómo se protegen los datos personales. El modo de responder a esta pregunta no es unívoco, pues será necesario que confluyan diversas circunstancias a fin de generar un verdadero derecho de protección de datos personales.

En primer lugar, el Estado debe adoptar las medidas necesarias para garantizar el derecho de protección de datos personales consagrado en virtud de la nueva redacción del artículo 19 N° 4 de la CPR. También será necesario que se adopten medidas de educación y concienciación para que las personas individualmente consideradas comprendan que la información que comparten o entregan es utilizada para diversos fines, que no necesariamente son informados. En tercer término, en atención a las obligaciones de la debida diligencia, el Estado debe establecer marcos claros orientados a que en la captación, procesamiento, utilización y transferencia de datos personales,

tanto por agentes públicos como por empresas privadas, se respeten principios mínimos para no lesionar los derechos de las personas.

De acuerdo a la opinión de Jessica Matus, el control del Estado sobre la materia en discusión se relaciona primordialmente con dos aspectos: *"Una ley que realmente resguarde los derechos de las personas y por otro lado una autoridad que pueda aplicar esa ley"*. Ante la dificultad de que una ley que establezca y regule de modo específico la protección de datos personales pueda abarcar todas las posibilidades y riesgos que el vertiginoso desarrollo tecnológico produce, María Paz Canales sostiene que existen *"modelos de diseño regulatorio que permiten expresar los conceptos con una neutralidad suficiente, como para dar espacio para el desarrollo tecnológico entrante"*.

En este sentido, es relevante que el proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la agencia de protección de datos personales (boletines 11.092-07 y 11.144-07, refundidos), incorpore ciertos principios básicos según se detallará.

Conforme a lo comentado por María Paz Canales, estos principios son los de legalidad, finalidad, proporcionalidad y transparencia. Según señala, el principio de legalidad guarda relación con que debe existir una fuente que autorice el tratamiento de datos, ya sea el consentimiento del titular o la ley misma. El principio de la finalidad se refiere a que el dato solamente puede ser utilizado para aquellas finalidades que fueron específicamente autorizadas por el consentimiento otorgado o en el marco legal respectivo. Conforme al principio de la proporcionalidad, los datos deben ser suficientes y no excesivos para el objetivo que se tenga que cumplir. Agrega que es en relación a este principio donde se producen más tensiones respecto al manejo de datos que realiza el Estado para la adopción de políticas públicas, pues *"se recaba mucha data inicialmente, sin tener claro para qué se quiere usar, y se recaba preventivamente de manera masiva generando un riesgo para las personas, que no se justifica en ninguna finalidad actual, sino que simplemente con la eventualidad de que podría ser útil para el futuro*". Por último, el principio de transparencia en esta materia se refiere a que quienes re-

Los avances tecnológicos que se expresan mediante nuevos medios de videovigilancia, el desarrollo de algoritmos predictivos, la utilización de dispositivos que son activados mediante biometría, por una parte, y la necesidad de los agentes públicos y privados de mejorar sus propios procesos a través del análisis de información sobre sus usuarios, por otra, plantea la necesidad de consagrar la protección de los datos de carácter personal como un derecho fundamental.

colectan y manejan datos deben estar permanentemente informando su utilización.

Estos principios han sido recogidos en el artículo 5° del GDPR, donde se expresa que los datos personales deben ser tratados de "manera lícita, leal y transparente"; "recogidos con fines determinados, explícitos y legítimos"; "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados"; "exactos y actualizados".

En los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, aprobados en 2016 por la Red Iberoamericana de Protección de Datos (foro integrador de los actores públicos y privados que desarrollan iniciativas en materia de protección de datos), también se establece una serie de principios para el tratamiento de datos personales, tales son los principios de legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad.

Una ley de protección de datos personales debería establecer ciertas obligaciones mínimas sobre el manejo de datos personales, denominadas medidas técnicas y organizativas, cuya finalidad es garantizar la seguridad del dato. María Paz Canales detalla que *"cuando se llega a la conclusión de que es necesario recoger un dato, que es pertinente para la finalidad buscada y que no es excesivo, quien maneja la base de datos donde esa información va a ser almacenada tiene la obligación de brindar los mejores estándares para la protección de esa información"*.

Otro aspecto esencial de un nuevo marco regulatorio guarda relación con la creación de una agencia pública de carácter independiente y técnico, con los recursos económicos y capacidades humanas necesarias para fiscalizar el cumplimiento de una ley de protección de datos personales, estableciendo vías efectivas de reclamo.

Un nuevo paradigma en materia de protección de derechos personales supera la sola adopción de una nueva ley que complemente al derecho fundamental establecido en el artículo 19 N° 4 de la Constitución. Jessica Matus considera que es importante promover entre la ciudadanía una adecuada valoración del concepto de datos personales *"que va más allá de la información puramente identificativa, sino que se extiende hasta otros aspectos como gustos, hábitos, expresiones en línea, los estados de salud, establecimiento educacional y otros datos que tienen que ver con la personalidad"*. Agrega que es muy relevante concienciar sobre *"la existencia de esta huella digital, pues toda la información que se encuentra en internet no se borra, hecho que nos deja expuestos a varios riesgos"*. Sobre los aspectos relacionados con los operadores privados, sostiene que se les debe exigir *"políticas, reglas y condiciones claras respecto de lo que se hace con la información, porque hasta el momento esto ha estado cubierto por un oscurantismo total"*, cuestión que también afecta al Estado.

Sin perjuicio de lo anterior, se ha visto que el tratamiento de datos por parte de los agentes públicos no requiere del consentimiento de los titulares, cuya información de carácter personal podría ser utilizada para la formulación de políticas públicas. No obstante, aclara Jessica Matus, el Estado:

> *[…] "sí está obligado a cumplir las otras obligaciones que tiene cualquier entidad o responsable de una base de datos que son: mantener la información actualizada, o sea, cumplir con los principios de calidad de los datos, pero además las obligaciones que dicen relación con la confidencialidad y con seguridad y ahí es donde está el problema, pues los sistemas de seguridad que ha utilizado el Estado han sido insuficientes, por eso se han filtrado desde el Ministerio de Salud, por ejemplo, los datos de las personas que viven con VIH y de las jóvenes que habían accedido a la pastilla del día después".*[40]

Un nuevo paradigma de protección de derechos personales también debe contemplar de modo sustantivo regulaciones para que las empresas respeten los derechos humanos, porque en muchos casos en que se pretende solucionar problemáticas en las prestaciones de servicios públicos mediante aplicaciones tecnológicas, estas son externalizadas en empresas privadas, *"sin que esas empresas hayan hecho un verdadero análisis respecto de cuál es el impacto que la implementación de esas tecnologías tiene para el ejercicio de otros derechos de esos mismos ciudadanos, a los cuales la tecnología pretende servir, entonces también hay una responsabilidad de parte de las empresas privadas, en términos de los compromisos que implican los Principios Rectores de Empresas y Derechos Humanos, establecidos por las Naciones Unidas",* señala Jessica Matus.

CONCLUSIONES

Mediante este capítulo se ha buscado abordar la problemática de la protección de los datos personales desde una perspectiva de derechos humanos, cuya fundamentación tradicional ha sido planteada desde los derechos a la privacidad y protección de la vida privada, ampliamente reconocidos en el DIDH, pero que modernamente ha cobrado autonomía por medio de la doctrina jurisprudencial de la autonomía informática, en virtud de la cual la persona tiene la potestad de decidir quién y bajo qué condiciones puede tener acceso a sus datos de carácter personal.

Los avances tecnológicos que se expresan, por ejemplo, mediante nuevos y mejores medios de videovigilancia, el desarrollo de algoritmos predictivos, la utilización de dispositivos que son activados mediante biometría, por una parte, y la necesidad de los agentes públicos y privados de mejorar sus propios procesos a través del análisis de información sobre sus usuarios, por otra, plantea la necesidad de consagrar la protección de los datos de carácter personal como un derecho fundamental, a fin de evitar riesgos, como eventuales discriminaciones, y vulneraciones a otros derechos, como el acceso a la salud o la educación.

El Estado de Chile ha avanzado en lo que se refiere a la protección de los datos personales, puesto que ha incorporado esta materia en el numeral 4° del artículo 19 de la Constitución, de modo que este derecho está, además, garantizado por la acción constitucional de protección y por el procedimiento de tutela de derechos fundamentales regulado en el Código del Trabajo. Sin perjuicio de esto, la actual regulación sobre protección de datos personales y sensibles no establece marcos de protección adecuados a los riesgos que el desarrollo tecnológico ha creado.

Por tales motivos, es fundamental que el proyecto de ley que actualmente se discute en el Congreso Nacional considere los principios de legalidad, finalidad, proporcionalidad y transparencia; establezca obligaciones mínimas sobre el manejo de datos personales que garanticen su seguridad, denominadas medidas técnicas y organizativas; y que se cree una agencia rectora en la materia, de carácter independiente y técnico que pueda fiscalizar la aplicación de este nuevo marco regulatorio.

Junto a lo anterior, también es necesario que se adopten medidas de educación y concienciación para que las personas tengan conocimiento de la importancia de resguardar la difusión de datos de carácter personal, y ejercer control sobre la información que brindan los responsables de las bases de datos respecto de los fines y la necesidad de la recolección de los datos personales de que se trate.

También será necesario que el Estado establezca obligaciones claras para que los propios agentes públicos y también los privados cumplan con los estándares mínimos que la nueva legislación sobre protección de datos personales debería contemplar, de modo que la recolección de datos personales esté siempre reconocida por una fuente válida y responda a una necesidad actual y no meramente potencial.

40 *La Tercera*, "Filtración de datos del Minsal", Editorial, 11 marzo 2018, http:// www2.latercera.com/noticia/filtracion-de-datos-del-minsal/

RECOMENDACIONES

1. Se recomienda a los órganos colegisladores concluir la tramitación del proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la agencia de protección de datos personales (boletines 11.092-07 y 11.144-07, refundidos) y que este proyecto incluya los principios de legalidad, finalidad, proporcionalidad y transparencia; y establezca obligaciones mínimas sobre el manejo de datos personales que garanticen su seguridad.
2. Se recomienda al Poder Ejecutivo que, mediante el proyecto de ley ya indicado, se cree una institucionalidad independiente, técnica y con recursos asociados para fiscalizar el cumplimiento de la futura ley de protección de datos personales tanto respecto de agentes públicos como privados.
3. Se recomienda a los órganos del Estado que respeten y garanticen, en todo momento, los derechos humanos afectados en el manejo de bases de datos que contengan datos personales, para el ejercicio de sus competencias o en el mejoramiento de sus procesos internos.
4. Asimismo, se insta a las empresas que trabajan con datos personales a impulsar procesos de debida diligencia, de modo que puedan prevenir la afectación del derecho a la intimidad y vida privada que se puedan provocar en sus operaciones.

BIBLIOGRAFÍA

Álvarez Caro, M. (2015). *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital*. Madrid: Reus.

Cannataci, J. (2016). *Informe del Relator Especial sobre el derecho a la privacidad*.

Cannataci, J. (2018). *Report of the Special Rapporteur on the right to privacy*.

Cerda, A. (2012). *Legislación sobre protección de las personas frente al tratamiento de datos personales*. Santiago: Centro de Estudios en Derecho Informático, Universidad de Chile.

Davara, M. (1999). *Guía práctica de Protección de Datos, desde la óptica del titular del fichero*. Madrid: Asociación Nacional de Establecimientos Financieros de Crédito, Universidad Pontificia Comillas.

Díaz, M. (2018). *El cuerpo como dato*. Santiago de Chile.

Fulchi, L. A., Carrillo, E., y Sequera, M. (2018). La enajenación continua de nuestros derechos. Asunción. Recuperado de https://www.tedic.org/wp-content/uploads/sites/4/2018/07/La-enajenación-continua-de-nuestros-derechos_TEDIC_2018.pdf

Garrido, R., y Becker, S. (2017). La biometría en Chile y sus riesgos. *Revista Chilena de Derecho y Tecnología, 6*(1), 67-91.

Jijena, R. (2001). Sobre la no protección de la intimidad en Chile. Análisis de la Ley 19.628, de agosto de 1999. *Revista Electrónica de Derecho Informático* (39).

La Rue, F. (2013). *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión*. ONU.

Mansell, J. (2018). Construyendo bases sólidas de información para invertir en resultados. En I. Aninat y S. Razmilic (Eds.), *Un Estado para la ciudadanía. Estudios para su modernización* (pp. 575-642). Santiago: Centro de Estudios Públicos.

Matus, J., y Montecinos, A. (2006). *La cesión de datos personales*. Santiago: Lexis Nexis.

OCDE (2004a). Background material on biometrics and enhanced network systems for the security of international travel. Paris. Recuperado de www.oecd.org/sti/security-privacy

OCDE (2004b). Biometric-based Technologies. *OECD Digital Economy Papers* (101).

Quezada Rodríguez, F. (2012). La protección de datos personales en la jurisprudencia del Tribunal Constitucional de Chile. *Revista Chilena de Derecho y Tecnología, 1*(1), 125-147.

RELE-CIDH. (2017). *Estándares para una Internet libre, abierta e incluyente.*

Riofrío Martínez-Villalba, J. C. (2014). La cuarta ola de derechos humanos: los derechos digitales. *Revista Latinoamericana de Derechos Humanos, 25*(1), 15-45.

Spanger, A., y Sáenz, P. (2018). *Cámaras indiscretas. Análisis del fallido sistema de videovigilancia inteligente para Transmilenio*. Bogotá.

Velasco, P., y Viollier, P. (2016). Big Data. Información financiera y discriminación laboral en Chile, un caso de estudio. Santiago. Recuperado de https://www.derechosdigitales.org/wp-content/uploads/big-data-informe.pdf

Viollier, P. (2017). El estado de la protección de datos personales en Chile. Santiago. Recuperado de https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf

Cámara de vigilancia en Santiago.