CUADERNO DE TRABAJO N°3 / DICIEMBRE 2015

Protección de Datos Personales

EN EL MANEJO DE DATOS DE INVESTIGACIÓN REALIZADO POR ORGANISMOS PÚBLICOS

UNIDAD DE ESTUDIOS Y PUBLICACIONES / DIRECCIÓN DE ESTUDIOS / CONSEJO PARA LA TRANSPARENCIA

consejo para la Transparencia

CUADERNO DE TRABAJO N°3 / DICIEMBRE 2015

Protección de Datos Personales

EN EL MANEJO DE DATOS DE INVESTIGACIÓN REALIZADO POR ORGANISMOS PÚBLICOS

UNIDAD DE ESTUDIOS Y PUBLICACIONES / DIRECCIÓN DE ESTUDIOS / CONSEJO PARA LA TRANSPARENCIA

Ediciones Consejo para la
Transparencia, Santiago Chile
Diciembre 2015

Diseño y Composición: Natalia Royer
ISSN 0719-4609

Índice de Contenidos

I. Presentación

El presente trabajo busca dar cuenta de las limitaciones que existen actualmente para dar adecuada protección a los datos personales de los sujetos de estudio en las investigaciones que realizan las instituciones del sector público en el país. Este es un tema de gran relevancia para la comunidad de investigadores que trabajan en el sector público y para quienes prestan servicios de esta naturaleza al Estado en calidad de proveedores.

El documento se estructura en cinco capítulos, comenzando por una sección de antecedentes donde se presentan los principales conceptos relacionados a la protección de datos personales, la relevancia del tema en la sociedad actual y los principios fundamentales y elementos institucionales sobre los cuales se establecen las prácticas más comunes en la materia a nivel internacional.

El segundo capítulo presenta información relativa a la falta de conciencia sobre el tema en nuestro país, a través de la presentación de algunos datos que se han venido recolectando en el Estudio Nacional de Transparencia del Consejo para la Transparencia desde el año 2012.

El tercer capítulo da cuenta de las limitaciones actuales de la normativa que regula el tema en el país desde el año 1999, para luego llegar al análisis de las limitaciones que enfrentan las instituciones públicas para dar adecuado cumplimiento a los principios asociados a la protección de datos personales y privacidad de las personas, ya sea por el desconocimiento general del tema, o bien, por la falta de especificidad de la normativa vigente.

Finalmente, se presentan algunas consideraciones a tener en cuenta en la discusión de la materia.

II. Antecedentes

Es importante reconocer que vivimos en la sociedad de la información y cada día se tratan millones de **datos personales**. Pero, ¿de qué información hablamos cuando nos referimos a "datos personales"? Esencialmente, cosas tan simples como nuestro nombre y apellidos, nuestra fecha de nacimiento, nuestra dirección postal o de correo electrónico, el número de teléfono, el RUT, la patente de nuestro automóvil y muchos otros datos que constituyen información que podría permitir identificar a una persona, ya sea directa o indirectamente. Además, dentro de los datos personales, existe una categoría de información que requiere de protección adicional: los **datos sensibles**, que corresponden a datos personales que se refieren a características físicas o morales de las personas o a hechos o circunstancias de su vida privada o íntima, tales como 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.

Los datos personales pueden ser recogidos en ficheros que dependen de las administraciones públicas, de empresas y organizaciones privadas que los utilizan para desarrollar su actividad. Es relevante tener claridad que toda esta información revela aspectos de la personalidad, de los bienes que una persona consume y dónde lo hace, su historia clínica, imágenes y videos que se cargan en la web o los perfiles de las redes sociales y que, por lo tanto, constituyen información que dice todo —o mucho— sobre nosotros (AGPD, 2011).

Los ejemplos sobre cómo puede tratarse la información en la sociedad digital y los resultados que ofrece son muy numerosos: En nuestro perfil en una red social, contamos desde la fecha de nacimiento y el colegio en el que estudiamos, hasta cuándo salimos de vacaciones; nuestra dirección de correo electrónico del trabajo suele indicar en qué trabajamos y con ello, brinda una primera aproximación a nuestro perfil económico y nuestros intereses profesionales; aparecer en un fichero como DICOM u otro referido a nuestra solvencia, puede afectar a nuestra capacidad de compra, o bien para recibir una ayuda o subvención estatal, dependemos de la comprobación de múltiples datos personales.

En este escenario, uno de los desafíos de la sociedad actual es la Protección de Datos Personales y la privacidad de las personas. De acuerdo al trabajo de OCDE (2013), al comparar la situación presente en la materia con lo que sucedía hace 30 años, ha habido un profundo cambio de escala en el rol de los datos personales en nuestra sociedad y nuestra vida cotidiana. Algunos de estos cambios son: el incremento del volumen de datos personales recolectados, usados y almacenados; la expansión de los análisis estadísticos y de mercado que involucran datos personales que reflejan gustos, preferencias, patrones de consumo, entre otros elementos que sirven a empresas, gobiernos y actores sociales para la toma de decisiones; el aumento del valor comercial y estratégico de la información; la expansión de las tecnologías de información para el acopio y análisis de los datos y finalmente; la globalización de la información a través de las redes sociales. Todos estos cambios han traído consigo una expansión de los riesgos a la privacidad de las personas, un aumento en el número y variedad de actores capaces de poner la privacidad de otros en riesgo, y la presencia de múltiples contextos en los cuales debemos interactuar usando nuestros datos personales, como por ejemplo, al abrir cuentas en redes sociales (OCDE, 2013).

En este contexto, la protección de datos personales ha sido entendida como un **derecho fundamental, y se asocia a la capacidad que tiene el ciudadano para disponer y decidir sobre todas las informaciones que se refieran a él**. En este sentido, se han identificado una serie de principios comunes a distintas regulaciones y modelos institucionales en el mundo, que permiten regular el uso de los datos personales por parte de las empresas, las instituciones públicas y todos aquellos que manejan este tipo de información. De acuerdo a OCDE (1980), estos principios son:

1. Principio de limitación de la recogida: Indica que debería haber límites en la recolección de datos personales, los cuales deben recabarse mediante medios lícitos y justos y, en su caso, con el conocimiento o consentimiento informado del sujeto de los datos.

2. Principio de calidad de los datos, los cuales deberían ser exactos, completos y mantenerse actualizados.

3. Principio de especificación de la finalidad: Las razones por las cuales se recojan los datos personales deberían especificarse en el momento de la recolección y, su uso posterior, debería quedar limitado al cumplimiento de tales efectos o de otros que no sean incompatibles y que se especifiquen en cada ocasión en que se cambie la finalidad.

4. Principio de limitación de uso: Los datos personales no deberían revelarse, hacerse disponibles o utilizarse de otro modo que no sean los especificados, salvo: a) con el consentimiento del sujeto de los datos, o b) por imperativo legal.

5. Principio de salvaguardas de seguridad: Los datos personales deberían protegerse, mediante salvaguardas de seguridad, frente a riesgos como pérdida, acceso, destrucción, uso, modificación o revelación no autorizados.

6. Principio de apertura: Debería haber una política general de apertura respecto a avances, prácticas y políticas relativas a datos personales. A su vez, deberían existir medios fácilmente disponibles para establecer la existencia y características de los datos personales, y de las principales finalidades para su uso, así como la identidad y domicilio del controlador de los mismos.

7. Principio de participación individual: La persona debería tener derecho a: a) recabar, del controlador de los datos o de otro modo, confirmación de si tiene o no, datos correspondientes a la misma; b) hacer que se le comuniquen los datos correspondientes dentro de un plazo razonable y de una forma que le resulte fácilmente inteligible; c) que se le den los motivos para denegar la solicitud y la posibilidad de impugnar tal denegación, y; d) impugnar los datos personales y, si ella prospera, hacer que se supriman, rectifiquen, completen o modifiquen.

8. Principio de responsabilidad: El controlador de datos debería ser responsable del cumplimiento de las medidas que den efecto a los principios expuestos más arriba.

Para la correcta aplicación de estos principios, múltiples países han desarrollado normativas específicas que definen las prácticas, estándares y responsables del acopio, resguardo y actualización de los datos personales. En América Latina, los países que cuentan con este tipo de regulación son: Argentina, Chile, Colombia, Costa Rica, México, Nicaragua, Perú, República Dominicana y Uruguay (López et. al., 2014). Pero no todas las legislaciones se encuentran actualizadas a los desafíos actuales, ni tampoco incluyen de manera explícita los principios recomendados por OCDE, como ocurre en el caso chileno.

Adicionalmente, **existe cierto consenso a nivel internacional sobre la necesidad de contar con una institución que vele por el adecuado resguardo del Derecho a la Protección de los Datos Personales.** Las características de estas instituciones varía en distintos contextos sociales y, en muchos casos, la autoridad ligada a la protección de datos personales es también la encargada de velar por el acceso a la información pública (López et. al., 2014; Liang, 2015; Graham, 2015).

En un proceso de revisión de los modelos institucionales que se han desarrollado para la protección de los datos personales de 6 países —Alemania, Francia, Australia, Reino Unido, España y México—, es posible observar al menos tres elementos comunes: estas instituciones tienen autonomía respecto del gobierno, cuentan con atribuciones de fiscalización del cumplimiento de la normativa y además, atienden y tramitan reclamos de personas que consideren que su derecho ha sido vulnerado por alguna institución pública o privada (CPLT, 2015).

Como se mencionó anteriormente, Chile cuenta desde el año 1999 con una normativa en la materia, contenida en la Ley N° 19.628 sobre Protección de la Vida Privada. Sin embargo, la discusión sobre el alcance y las características de esta norma ha suscitado mayor interés en el último tiempo en el ámbito nacional. Uno de los elementos que ha contribuido a esta discusión es su interrelación con la Ley de Transparencia (N°20.285), dado el alto volumen de datos personales y datos sensibles que han sido requeridos bajo el amparo del Derecho de Acceso a la Información Pública y que son tratados por los órganos de la Administración del Estado con el objeto de desarrollar e implementar políticas públicas, tales como la entrega de beneficios, las actividades de planificación y la prestación de servicios sociales. Así, múltiples casos presentados al Consejo para la Transparencia han debido ser analizados bajo la lógica de la ponderación entre el Derecho de Acceso a la Información y el Derecho a la Protección de Datos Personales (CPLT, 2011; Jaraquemada, 2015).

Otro elemento relevante en la discusión guarda relación con el contexto internacional y la expansión del uso de tecnologías de información que han fortalecido el Derecho a la Autodeterminación Informativa, la protección de los datos en Internet y la regulación del flujo transfronterizo de datos como elementos esenciales que deben atenderse normativamente. De hecho, la OCDE ha realizado recomendaciones a Chile para mejorar la normativa actual en la materia, ya que no responde de manera adecuada a los desafíos de nuestro tiempo, especialmente por deficiencias en su aplicación. Así, la norma no ha sido objeto de modificaciones sustanciales y los intentos por efectuar adecuaciones que se ajusten a la situación actual y los parámetros internacionales, hasta ahora, no han sido concretados.

Finalmente, es posible constatar que en nuestro país, pese a la relevancia de la protección de datos personales, existe un gran desconocimiento de los derechos y obligaciones de los titulares de datos personales, así como también de los responsables del tratamiento de los mismos (CPLT, 2014).

III. El contexto social de la protección de datos personales en Chile

Si bien el tema de la protección de datos personales está presente en la discusión normativa y en temas de política pública, en nuestro país existe un bajo nivel de claridad y conciencia sobre este tema entre los ciudadanos. Desde el año 2012, el Estudio Nacional de Transparencia del Consejo para la Transparencia[1], ha indagado sobre algunos temas relacionados con la protección de datos personales entre los ciudadanos (CPLT, 2012; CPLT, 2013; CPLT, 2014).

Los primeros resultados del año 2012 mostraron que el 87% de las personas consideraron muy importante la protección de los datos personales pero, al mismo tiempo, las prácticas cotidianas, como por ejemplo, la entrega del RUT en diversos comercios para acumulación de puntos, se reconocían como prácticas habituales.

Dentro de esta preocupación por los datos personales, los elementos que suscitan mayor preocupación al entregar información a los órganos públicos son:

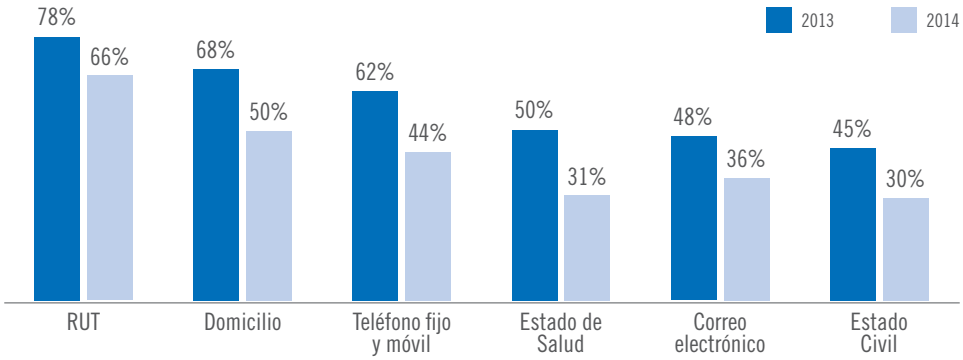
- Que sean entregados a terceros, sin su consentimiento, para que obtengan información sobre su situación financiera, bancaria o económica (33%).

- Que sean robados del organismo públicos por falta de seguridad en su almacenamiento, pudiendo utilizarlo terceros ajenos a éste (26%).

- Que sean entregados a privados para ser utilizados con fines comerciales, como por ejemplo, enviarle publicidad u ofertas de productos (23%).

En los años 2013 y 2014, dando cuenta de las prácticas más comunes de las personas en la materia, se preguntó por el cuidado que las personas declaran tener respecto de la información personal. En este caso, se observa una disminución del cuidado de la información el año 2014, pero también algunas declaraciones que podrían interpretarse fundamentalmente marcadas por deseabilidad social, ya que se contradicen con las prácticas habituales que se pueden observar. Por ejemplo, es más difícil que las personas den su dirección o teléfono que su RUT para acceder a beneficios de carácter comercial.

¿Ud. diría que cuida la información de su...?

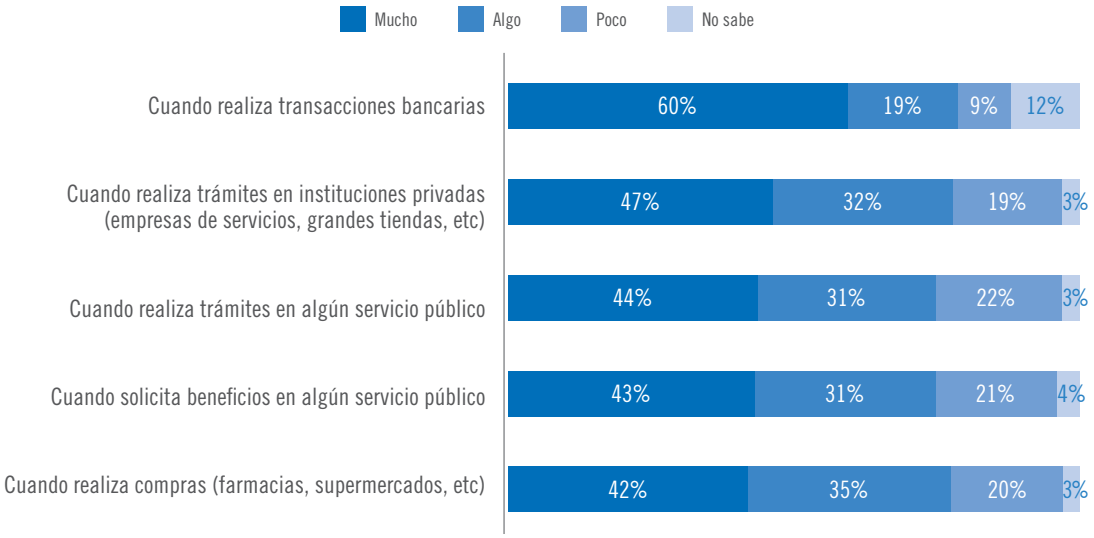


Fuente: Elaboración Propia en base al Estudio Nacional de Transparencia CPLT 2013 y 2014

[1] Todos los informes disponibles en http://www.cplt.cl/estudios-nacionales-de-transparencia/consejo/2012-12-13/155411.html

Finalmente, el año 2014 se indagó en las situaciones en las cuales las personas manifestaban mayor preocupación por el mal uso de su información personal. En este caso, se observó que las transacciones bancarias y trámites en instituciones privadas son las que generan mayor preocupación. Por otra parte, si bien los trámites o solicitudes de beneficios al Estado, producen algún nivel de preocupación por el uso de la información, ésta es menor que en el caso de las operaciones bancarias. Finalmente, el uso de datos personales en situaciones de compra en farmacias, supermercados, grandes tiendas, etc. es el aspecto que genera menores niveles de preocupación.

¿Cuánto se preocupa por el mal uso de información general?



Fuente: Elaboración Propia en base al Estudio Nacional de Transparencia CPLT 2014

Con estos datos es posible observar que las personas reconocen, más bien a nivel intuitivo, la relevancia de la información personal y la necesidad de su protección, pero no se ha logrado avanzar de manera clara y consistente en la instalación del tema y la difusión de los mecanismos de la protección de los datos personales y de identificación.

IV. Situación de la normativa de protección de datos personales en Chile

La discusión sobre la protección de datos personales en Chile ha estado marcada por distintos aspectos tanto del cumplimiento del Derecho, como de la economía asociada a la materia. En efecto, pese a que la actual legislación (Ley Nº 19.628) ha establecido una serie de principios en favor de la protección de datos, no ha sido capaz de proporcionar una seguridad apropiada a la información personal, entre otros factores, por la carencia de una institucionalidad a cargo del buen cumplimiento de la normativa.

En este contexto, el Consejo para la Transparencia ha cumplido un rol relevante en el tema de la protección de datos personales, ya que no sólo ha sido creado para promover la transparencia en el sector público, fiscalizar y garantizar el Derecho de Acceso a la Información Pública, sino que también, de acuerdo al Artículo 33 de la Ley 20.285, se le ha asignado la función de *velar por el adecuado cumplimiento de la ley Nº 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado.* Cumpliendo con dicha misión, desde el año 2010 ha realizado una serie de actividades de diagnóstico y orientación en la materia.

Una de las primeras actividades fue una encuesta en la que participaron 261 instituciones públicas. En este ejercicio se detectó un bajo conocimiento de la normativa y las obligaciones que la Ley establece, por lo cual el nivel de cumplimiento y de registro de las bases de datos (ficheros de datos) por parte de las instituciones públicas en el Registro Civil también era bastante bajo. Por ello, en agosto del año 2011, el Consejo lanzó el documento "Recomendaciones del Consejo para la Transparencia sobre Protección de Datos Personales por parte de los órganos de la administración del Estado", cuyo objetivo fue establecer orientaciones respecto de los criterios jurídicos aplicables por las instituciones públicas en el tratamiento de datos de carácter personal que obren en su poder, a fin de garantizar a las personas el Derecho a la Protección de los Datos de Carácter Personal y asegurar el debido manejo de los registros o bancos de datos personales que sean necesarios para el ejercicio de sus competencias[2].

Al margen de los avances que generó la Recomendación, los vacíos legales se han mantenido, dejando amplios ámbitos de la aplicación de la normativa sin cubrir. Por ello, el Consejo para la Transparencia ha identificado una serie de ámbitos específicos donde nuestra legislación podría perfeccionarse para dar adecuado resguardo a este Derecho Fundamental. De hecho, se ha identificado la necesidad de que la norma converse con lo propuesto en el Boletín Nº 9.384-07, Proyecto de Reforma Constitucional que consagra el Derecho a la Protección de Datos Personales.

Un segundo elemento relevante es la creación de un órgano garante, recomendación que surge de la revisión de la experiencia internacional y la dificultad real y práctica de resguardar este Derecho a través de los Tribunales de Justicia donde, además, la carga de la prueba recae sobre el titular de datos personales que ha visto vulnerado su Derecho. Este órgano garante debiese tener facultades de promoción, de resolución de casos, además de facultades normativas y fiscalizadoras, a modo de responder eficientemente a las necesidades actuales, marcadas por el desconocimiento y la falta de protección efectiva de los datos personales.

Otro elemento relevante a considerar en la revisión de la normativa actual, es la incorporación de mayores especificaciones en temas tales como:

a) el catálogo de definiciones que tenemos sobre los conceptos relevantes en la materia como "datos personales", "datos sensibles", "fuentes accesibles al público", "tratamiento de datos" y verificar la conveniencia de incorporar otros conceptos;

b) el consentimiento del titular de los datos, definiendo la forma en que debe prestarse, su alcance, oportunidad y si habrá situaciones de excepción;

c) la incorporación expresa de la regulación de los principios en materia de protección de datos promovidos a nivel internacional[3];

[2] El texto completo de la Recomendación se encuentra disponible en http://www.cplt.cl/consejo/site/artic/20121224/asocfile/20121224003258/recomendacion_pd.pdf

[3] Principios de legitimidad, finalidad, proporcionalidad, transparencia, responsabilidad y seguridad.

d) el reforzamiento de los Derechos de los titulares de los datos;

e) la definición de las obligaciones de los sujetos responsables en el tratamiento de los datos;

f) el establecimiento de un Registro Nacional de bases de datos permanente en el que se deberán inscribir y registrar las bases de datos de los organismos públicos y las entidades privadas;

g) la regulación de "datos especialmente protegidos" como, por ejemplo, los datos relativos a salud, telecomunicaciones, datos biométricos, datos sobre niños, niñas y adolescentes y de actividad comercial o crediticia;

h) procedimientos de reclamo para los titulares de datos respecto de los responsables y encargados del tratamiento de datos;

i) la generación de un marco de referencia para tratamiento de datos personales por organismos públicos, que incorpore la forma, los medios y condiciones bajo las cuales éstos podrán transferir y compartir sus datos con otras entidades públicas o privadas, sus obligaciones y las medidas de seguridad necesarias;

j) la incorporación de un régimen de infracciones y de sanciones;

k) el tratamiento de los datos personales cuando éstos cruzan los límites territoriales del país.

Como se ha mencionado, las limitaciones de la normativa actual redundan en una deficitaria protección de los datos personales en nuestro país, donde tanto los titulares de los datos, como quienes están en posesión de los mismos, no cuentan con lineamientos claros y específicos sobre cuáles son sus obligaciones y Derechos en la materia, ni tampoco sobre cuáles serían los mecanismos más adecuados para darles aplicación concreta. Si bien esta situación aplica a múltiples áreas del quehacer nacional, queremos centrar el foco en una de ellas: el desarrollo de estudios en el sector público que, al ser una actividad donde se recaban datos personales de manera regular, se ve regulada por la normativa de protección de datos personales, pero en un escenario donde existe una limitada capacidad para aplicarla de manera efectiva.

V. El tratamiento de los datos personales en la investigación del sector público

Tal como se enunció anteriormente, dentro del escenario actual, una de las áreas específicas donde se han detectado falencias para el adecuado resguardo de los datos personales —pero no la única—, es la **investigación o los estudios que se realizan por parte de instituciones del sector público.** En este caso, junto con las limitaciones normativas de nuestra regulación en la materia —especialmente en temas como el consentimiento del titular de los datos y el respeto a los principios de finalidad, responsabilidad y seguridad, que son temas a resolver directamente por los organismos públicos—, esta actividad tiene un riesgo adicional: la externalización de los servicios de recolección de información —y por ende, de captura y registro de datos personales—, que habitualmente se adjudica vía licitación pública a empresas, consultoras, centros de estudios o universidades, que **muchas veces no cuentan con estándares regulares, claros y sistemáticos de resguardo de la información** que permitan dar adecuado cumplimiento al Artículo 3 de la Ley Nº 19.628. La norma establece que: *"En toda recolección de datos personales que se realice a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, sin perjuicio de los demás derechos y obligaciones que esta ley regula, se deberá informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información. La comunicación de sus resultados debe omitir las señas que puedan permitir la identificación de las personas consultadas. El titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión".*

Así, en el caso chileno, estas debilidades normativas y prácticas en la instalación de los principios de protección de datos personales no permiten consensuar estándares explícitos y obligatorios para el resguardo de la información a nivel general, pero esta situación se agudiza en las actividades de investigación, donde también se puede constatar una **falta de guías e instituciones que regulen de manera clara la aplicación de los principios éticos de la investigación en el país.**

Estas falencias resultan especialmente delicadas ya que, en muchos casos, la acción del Estado está orientada hacia sectores de la población que presentan algún tipo de vulnerabilidad social. En ellos, la divulgación de la información personal resulta más complejapues, junto con los riesgos de exposición de la identidad de las personas, se pone en riesgo la divulgación de datos sensibles.

En países anglosajones, como Estados Unidos, Inglaterra, Australia y Canadá[4], existen instancias formales e independientes que velan por el riguroso cumplimiento de estándares éticos de investigación. Entre los estándares protegidos, está presente la protección de los datos personales, pero también se consideran otros aspectos del proceso, especialmente en los casos de investigación de tipo experimental. Uno de los principales aportes de este tipo de instancias es que, a pesar de su diversidad institucional —que va desde la autorregulaciónhasta normas legales transversales—, se instalan de manera muy potente en los espacios de formación de investigadores en las Universidades y Centros de Estudios. Por ende, los estándares éticos de la investigación que deben cumplirse, se aplican de manera transversal en todos los ámbitos de la investigación, lo cual evita diferencias en la manera en la cual se realizan las actividades por los diversos actores.

Por otra parte, es interesante constatar que, al margen de los estándares éticos de investigación que se promueven y fiscalizan a nivel académico, también existen estándares generados por la industria de la investigación social y de mercados a nivel internacional, bajo principios de autorregulación. En el caso de nuestro país, solamente algunos proveedores declaran formal y abiertamente su adhesión a este tipo de principios y estándares que son bastantes conocidos. Uno de los más comunes y expandidos son los de ESOMAR, que exige a sus consultoras y empresas afiliadas el respeto de sus normativas (ESOMAR, 2008), así como los lineamientos IRB (académico USA) los que, a modo de ejemplificar, se presentan brevemente a continuación:

[4] Las instituciones son: Estados Unidos, Institutional Review Board; Inglaterra, Data Protection Act 1998, Guidelines for social research; Australia, Privacy Market and Social Research Code; Canadá, Panel on Research Ethics.

RESGUARDOS	IRB (Washington University in St. Louis, 2015)	ESOMAR (Art. 7. Protección de Datos y Privacidad)
Políticas de privacidad	Se debe establecer con claridad el estándar de confidencialidad en el tratamiento de los datos personales o si el estudio cumple estándares para considerarse anónimo, dando cuenta en ambos casos, de los mecanismos que lo garantizan.	Públicas y accesibles para todos quienes participan en los estudios.
Recolección de datos	Se define el lugar, contexto y tiempo de recolección de información de manera anticipada a través del consentimiento. La información recabada es solamente aquella que es adecuada, relevante y no excesiva para alcanzar los objetivos del estudio.	Clarificación del propósito y de las posibilidades de ser contactados para el control de calidad del estudio. La información recabada es solamente aquella que es adecuada, relevante y no excesiva para alcanzar los objetivos del estudio.
Uso de los datos	Hay un consentimiento explícito que define los objetivos de la investigación y el uso que se dará a los datos. El consentimiento se presenta de manera verbal y escrita, en el caso de los menores de edad y otros casos especiales, con un testigo.	La información recolectada solamente se usa para los propósitos que fue definida. Sólo se preserva la información por el período que es requerida. La identidad de los participantes no es accesible para el cliente que encarga la investigación. Hay un consentimiento explícito del participante y sus datos no se usarán para otras actividades comerciales.
Seguridad de los datos	Deben establecerse medidas de seguridad específicas para la protección de la información personal, tales como: acceso restringido a las carpetas y archivos digitales y físicos, determinación del tiempo que se mantendrán los archivos, etc.	Definición de autorizaciones para quienes usen la información personal y medidas de protección y seguridad para evitar el uso incorrecto de los datos.
Derechos de los participantes	Asegurar que los participantes: puedan decidir si participar o no de manera libre, sin coerción o influencia. Especificar los costos, riesgos y compromisos que implica para la persona participar del estudio. Mostrar las consecuencias que podría tener dejar de participar en el estudio (especialmente en investigaciones que implican acceso a recursos o servicios de manera experimental).	Asegurar que los participantes: participen de manera voluntaria sin ningún tipo de consecuencia, puedan abandonar su participación en cualquier momento, solicitar privacidad en el uso de sus datos personales, pedir que se elimine o corrija información personal que la empresa tenga en su poder.
Transacciones Transfronterizas	Quedan regulados por la normativa de cada Estado de USA y las normativas de la FDA.	Protecciones especiales de seguridad deben considerarse cuando la información se transfiere a otro país, deben asegurarse todos los pasos necesarios para proteger los principios precedentes en materia de protección de datos.

De esta forma, en el escenario nacional, la falta de claridad en la regulación, sumada a la falta de principios estandarizados en la industria lleva a que, frente a requerimientos formales de las instituciones públicas que solicitan explícitamente protocolos de tratamiento de protección de datos personales, muchas organizaciones proveedoras de servicios vayan generando modelos ad-hoc, con el riesgo de que estas soluciones, al no estar arraigadas en las prácticas permanentes, no permitan una trazabilidad completa de la información, y al mismo tiempo, no favorezcan la instalación de capacidades y competencias permanentes para abordar estos desafíos.

A modo de identificar con mayor claridad las prácticas que se aplican para el resguardo del Artículo 3 en las actividades del sector público, la Unidad de Estudios y Publicaciones de la Dirección de Estudios del Consejo para la Transparencia, revisó al azar un total de 20 Términos de Referencia asociados a estudios y encuestas publicados en el portal Mercado Público entre los años 2012 y 2015. Se seleccionaron estudios vinculados a encuestas de opinión y evaluación de programas donde existen datos sensibles, como estudios del Ministerio de Desarrollo Social en materia de infancia, protección de población penal, servicios de atención a población vulnerable; estudios en materia de educación; de evaluación de los servicios de salud; y de consumo de drogas, entre otros.

Los resultados de este ejercicio permitieron constatar que:

- De los 20 casos analizados, solamente 6 mencionaban explícitamente la Ley 19.628, aunque en ninguno de ellos había una especificación sobre las obligaciones que recaen sobre el proveedor.

- En 10 casos, se solicita al proveedor proponer o establecer el estándar de tratamiento y protección de los datos.

Para complementar los hallazgos de este diagnóstico inicial, en agosto de2015, el CPLT realizó un taller con distintos organismos públicos, con el objetivo de conocer prácticas sobre protección de datos personales en la realización de estudios que se realizan de manera periódica en las instituciones públicas, indagando sobre los mecanismos y protocolos utilizados para asegurar el cumplimiento de la Ley 19.628.

Al taller asistieron representantes de 5 instituciones que realizan investigación de manera regular[5]. Las reflexiones y discusiones del taller permitieron detectar y confirmar elementos que ya habían sido identificados en la etapa previa:

1. Ausencia de prácticas y protocolos específicos para la protección de datos personales desde la perspectiva normativa, lo que incluye falencias en su incorporación tanto en términos de referencia, como en los contratos de los proveedores.

2. No hay especificaciones respecto de este tratamiento, ni lineamientos claros que se entreguen a los proveedores externos para asegurar las condiciones de protección, resguardo y consentimiento de los sujetos de estudio.

3. Cada institución ha ido definiendo prácticas y estándares propios que, al no estar estandarizados, no son necesariamente compartidos para este tipo de tratamiento de datos.

Por otra parte, el taller permitió identificar algunas buenas prácticas, consistentes con la protección de datos, que se realizan más bien sustentadas en principios éticos de la investigación social. Éstas son:

En la relación con el proveedor externo:

- Los estudios cuentan con cláusulas de uso exclusivo de la información por parte de la institución.

- Muchas veces se establece el uso del consentimiento informado, especialmente en estudios de carácter cualitativo.

En relación a la difusión de información que puede contener datos personales:

- Se establecen ciertas bases que regulan la relación con centros de investigación, investigadores y usuarios de los datos, donde hay estándares de resguardo.

- Las bases de datos que se entregan por solicitudes de acceso a la información, no permiten individualizar a los usuarios del Servicio[6].

A pesar de la identificación de algunas buenas prácticas, se visualizan importantes desafíos en materia de difusión de los principios y obligaciones que se derivan de la normativa vigente en materia de protección de datos en el área de la investigación. En este sentido, se constató el interés de las distintas instituciones por contar con mayor claridad sobre estos estándares, y también surgió un tema nuevo vinculado a los protocolos de traspaso de información entre instituciones del sector público.

[5] Las instituciones participantes fueron: SENDA, FOSIS, INDH, INJUV, SENCE.

[6] Un tema vinculado a la Protección de Datos Personales, es el resguardo de la propiedad y la disponibilidad de los resultados de investigación y bases de datos completas que debe quedar en manos de las instituciones que encargan los estudios. Esto, porque toda esa información, incluidas las bases de datos, al realizarse con fondos vinculados al gasto público, forman parte del acervo de información pública del país y queda bajo el amparo de la Ley N°20.285, por ende, las instituciones tienen al mismo tiempo la obligación de proteger la información personal de los sujetos de estudio y de garantizar el acceso a esa información de acuerdo a las disposiciones de la Ley de Transparencia.

VI. Consideraciones Finales

Existen múltiples desafíos para el desarrollo de un adecuado tratamiento de los datos personales en Chile. Como se discutió previamente, existen deficiencias desde el punto de vista normativo, pero también, desde la instalación del tema como un Derecho Fundamental que es susceptible de ser vulnerado en múltiples contextos de la vida cotidiana actual, la que se desarrolla crecientemente sobre la base de tecnologías de información y traspaso de datos.

Las limitaciones actuales de la normativa para una adecuada protección de los datos personales, afecta múltiples áreas de la actividad comercial, productiva y social de las personas. Una de ella es el desarrollo de la investigación que se realiza al alero de las instituciones públicas, donde se ha podido constatar que no existe claridad sobre las obligaciones específicas que establece la normativa en la materia, especialmente en aquellos casos en los cuales, tanto la recolección de los datos, como su procesamiento y almacenamiento, queda en manos de consultoras, centros de estudios o universidades que prestan los servicios. Esta falta de claridad puede redundar en una potencial vulneración de los datos personales de los sujetos de estudio lo que, en el caso de temas específicos de política pública, puede además afectar la divulgación de datos sensibles. Este riesgo es bastante claro, especialmente si se considera que dados los objetivos de focalización de múltiples políticas públicas, los esfuerzos de intervención y evaluación se concentran en población vulnerable, donde sus características socioeconómicas, de salud, de género, de etnicidad u otras, les hacen acreedores de los beneficios o la participación en los programas estatales.

La mitigación de este riesgo no es clara y no se cuenta con estándares comunes que permitan asegurar el resguardo de los datos de las personas, esto debido a que no existen criterios transversales que se usen por todos los actores de la industria, ni tampoco que sean exigidos por parte de las instituciones públicas como contraparte de los servicios. Esta falta de estandarización de criterios adecuados al tratamiento de datos personales, deviene de 3 fuentes:

a) No existe claridad, consenso y coherencia en los estándares a seguir o resguardar por parte de las instituciones públicas;

b) no existen instancias académicas formales que fomenten, eduquen y divulguen los estándares éticos de la investigación entre estudiantes, investigadores y la comunidad en general, que puedan ser usados como referencia para estos fines;

c) si bien existen algunos estándares exigentes que se aplican en la industria de la investigación social —especialmente en la investigación de mercados, por ejemplo, ESOMAR—, éstos son de adhesión voluntaria y pocas empresas y proveedores de investigación adhieren sistemática y públicamente a ellos.

Finalmente, es posible indicar que sería de utilidad contar con orientaciones concretas que permitan o faciliten, la adopción de estándares comunes para las instituciones públicas, especialmente en su relación contractual con proveedores externos a fin de asegurar el adecuado resguardo de los Derechos de las personas en materia de protección de datos personales. Idealmente estas orientaciones podrían abordarse en la discusión legislativa de las modificaciones a la Ley Nº 19.628 pero, mientras esa discusión avanza en la esfera parlamentaria, sería de gran utilidad contar con una guía común que establezca los mínimos necesarios para el desarrollo de la investigación en el Estado.

Bibliografía

AGPD (2011). *El derecho fundamental a la protección de datos: Guía para el Ciudadano.* Descargado de Internet el 03 de diciembre de 2015 desde http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO.pdf

CPLT (2011). *Protección de Datos Personales.* Descargado de Internet el 03 de diciembre de 2015 desde http://www.cplt.cl/consejo/site/artic/20121213/asocfile/20121213160518/proteccion_de_datos_web.pdf

CPLT (2012). *Estudio Nacional de Transparencia 2012.* Descargado de Internet el 03 de diciembre de 2015 desde http://www.cplt.cl/consejo/site/artic/20121213/asocfile/20121213155411/estudio_nacional_de_transparencia_2012.pdf

CPLT (2013). *Estudio Nacional de Transparencia 2013.* Descargado de Internet el 03 de diciembre de 2015 desde http://www.cplt.cl/consejo/site/artic/20121213/asocfile/20121213155411/estudio_nacional_de_transparencia_2013.pdf

CPLT (2014). *Estudio Nacional de Transparencia 2014.* Descargado de Internet el 02 de noviembre de 2015 desde http://www.cplt.cl/consejo/site/artic/20121213/asocfile/20121213155411/informe_final_de_resultados_ent_2014__2_.pdf

ESOMAR (2008). *Directory 2008: Research Organizations.* Amsterdam: ESOMAR.

Graham, C. (2015). *Entrevista para la Revista Transparencia y Sociedad.* Revista Transparencia y Sociedad (3), p.121-130. Descargado de Internet el 10 de diciembre de 2015 desde http://www.cplt.cl/transparenciaysociedad

Jaraquemada, J. (2015). *La afectación de la vida privada como límite al acceso a la información.* Revista Transparencia y Sociedad (3), p.29-53.

Liang, S. (2015). *Entrevista para la Revista Transparencia y Sociedad.* Revista Transparencia y Sociedad (3), p.111-120. Descargado de Internet el 10 de diciembre de 2015 desde http://www.cplt.cl/transparenciaysociedad

López, D. et. al. (2014). *Protección de datos y habeas data: Una visión desde Iberoamérica.* Madrid: Imprenta Nacional de la Agencia Estatal Boletín Oficial del Estado. Descargado de Internet el 10 de noviembre de 2015 desde http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/premios_2015/Proteccion_de_datos_y_habeas_data.pdf

OECD (1980). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Descargado de Internet el 03 de diciembre de 2015 desde http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

OECD (2013). *The OECD Privacy Framework*. Descargado de Internet el 03 de diciembre de 2015 desde http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Washington University in St. Louis (2015). Washington University Institutional Review Board: Policies and Procedures. Descargado de Internet el 20 de noviembre de 2015 desde http://hrpo.wustl.edu/wp-content/uploads/2015/04/2015-04-20-WU-IRB-policies-and-procedures.pdf

PROTECCIÓN DE DATOS PERSONALES EN EL MANEJO
DE DATOS DE INVESTIGACIÓN REALIZADO POR
ORGANISMOS PÚBLICOS