

Chile y la protección de datos personales: Compromisos internacionales

Raúl Arrieta

Introducción

Desde sus orígenes, la protección de los datos personales ha estado vinculada al derecho a la privacidad. Un ejemplo de ello es el desarrollo legislativo que ha tenido la materia en nuestro país, cuyo tratamiento lo podemos encontrar fundamentalmente en la ley 19.628 sobre protección de la vida privada. Así, la protección de datos nace concebida como parte del derecho de las personas a ser dejadas solas.

Sobre la base de esta idea es posible afirmar que en una sociedad democrática el juego pareciera tener lugar entre la protección de datos, como forma de privacidad, y la publicidad, de manera que la primera aparece configurándose como un elemento que restringe el anhelado derecho a que la democracia sea concebida, utilizando las palabras de Stefano Rodotà, como el “gobierno en público”,¹ donde la transparencia es un elemento fundamental de la corrección de la vida pública en su conjunto. En ese marco, el esfuerzo principal de la normativa asociada a dichas materias debería concentrarse en establecer los criterios que permitan ponderar cuál valor democrático debería prevalecer, básicamente teniendo en consideración el interés público que pueda generar la información de que se trata y el hecho de que en ambos casos nos encontramos frente a derechos consagrados constitucionalmente.

Sin embargo, una aproximación actual de la relación existente entre democracia y protección de datos nos obliga a tener presente los cambios que ha producido la incorporación masiva de la tecnología en la vida cotidiana de las personas. En efecto, las telecomunicaciones y el desarrollo de avanzados sistemas computacionales permiten tratar en milésimas de segundos gran cantidad de información y, dependiendo del manejo que se haga de ésta en todos los niveles, mayor o menor será la posibilidad de que ella pueda afectar no sólo el derecho a la privacidad, sino también cualquier otro derecho.

De esta forma, la protección de los datos personales deja de tener una correspondencia unívoca con el derecho a la vida privada y a la intimidad,

(...) una aproximación actual de la relación existente entre democracia y protección de datos nos obliga a tener presente los cambios que ha producido la incorporación masiva de la tecnología en la vida cotidiana de las personas.

(1) Rodotà, S., “Democracia y protección de datos”, *Cuadernos de Derecho Público*, INAP, Madrid, 2003, p. 15.

para pasar más bien a configurarse como un derecho autónomo relacionado con la posibilidad de cada persona de tutelar la circulación de la información que le incumbe. Así, la protección de datos se convierte en un elemento central de la forma en que el ciudadano vive y se relaciona en la sociedad de la información y comunicación.

En tal sentido, el cambio de paradigma es sustantivo, sobre todo si se tiene en consideración que en el derecho a la vida privada los mecanismos de tutela del mismo parten de la premisa de que la persona tiene derecho a excluir interferencias ajenas sobre su vida; así, la tutela es estática y negativa. Sin embargo, en la protección de datos personales la cuestión es sustancialmente diferente, ya que su ejercicio se concreta en poderes de intervención; la tutela es dinámica y sigue a los datos durante su circulación. Adicionalmente, se confía no sólo a la iniciativa de las personas interesadas, sino que también requiere la instalación de autoridades independientes que contribuyan a proteger a las personas, lo que implica una permanente y específica responsabilidad pública.²

Dicho esto, consideramos indispensable resaltar que los derechos fundamentales deben crear y mantener las condiciones elementales para asegurar una vida en libertad y digna. Esto sólo se consigue cuando la libertad de la vida en sociedad resulta garantizada en igual medida que la libertad individual. Ambas se encuentran inseparablemente unidas.³

Si lo anterior se vincula al hecho de que en un mundo cada vez más integrado, queda en evidencia la crisis de autosuficiencia de los ordenamientos nacionales. Ello se advierte sobre todo en materia de derechos fundamentales, debido a la tensión universalística que anima la protección de la persona humana.⁴ Así, la internacionalización de los derechos fundamentales nos conduce inexorablemente hacia la búsqueda de instituciones y técnicas de codificación que permitan garantizar y tutelar en forma adecuada el derecho a la protección de datos personales.

Ello es de tal magnitud, que los países y asociaciones que forman parte de nuestro entorno de referencia habitual, o de aquellos a los que como país nos deseamos integrar, nos exigen resolver las cuestiones que permitan in-

(2) Ibid.

(3) Hesse, C., *Manual de derecho constitucional*, Marcial Pons, Barcelona, 2001, p. 89.

(4) Rolla, G., “La concepción de los derechos fundamentales en el constitucionalismo latinoamericano”, p. 9, www.costituzionale.unige.it/crdc/docs/articles/Rolla3.pdf (consulta: 05.07.08).

crementar y asegurar el adecuado respeto a los derechos de las personas en lo que se relaciona con el tratamiento de datos personales.

De este modo, estimamos que el verdadero desafío que se nos presenta es determinar cuál es el estándar internacional de protección de datos que se le exige al país para ser parte de una sociedad globalmente relacionada.

(...) estimamos que el verdadero desafío que se nos presenta es determinar cuál es el estándar internacional de protección de datos que se le exige al país para ser parte de una sociedad globalmente relacionada.

El estándar internacional y la protección adecuada

Definir el estándar que debe cumplir nuestro país en materia de protección de datos pasa por establecer cuál es el parámetro que los Estados y asociaciones que forman parte de nuestra esfera de influencia nos exigen para poder integrarnos realmente con ellos, sea simplemente porque se lo mire bajo un prisma de utilitarismo comercial o porque nos interese realmente incrementar los niveles de protección de los derechos humanos. Y mucho más si consideramos que Huntington nos recuerda que el sentido político más importante de la democracia es la capacidad que poseen sus instituciones para proteger los derechos y libertades de los individuos.⁵

Para el análisis de este punto resulta necesario tener a la vista los principales instrumentos normativos de nuestro entorno de referencia habitual y de las asociaciones a las que pertenecemos o deseamos incorporarnos. Así, resulta necesario considerar los fundamentos que provienen de la Organización para la Cooperación y el Desarrollo Económico (OCDE), la Unión Europea, la Organización de las Naciones Unidas (ONU) y el Foro de Cooperación Económica del Asia Pacífico (APEC).

De la revisión de dichos instrumentos es posible advertir que existe una significativa coherencia y consistencia respecto de los elementos que han de configurar el estándar de protección de datos que debiera satisfacer nuestro país. Con todo, estimamos que para la conformación de ese estándar es útil considerar un principio que es de habitual incorporación en los convenios de derechos humanos, el de *pro homine*, según el cual no puede restringirse o

(5) Huntington, S., “El sobrio significado de la democracia”, *Revista Estudios Públicos*, Centro de Estudios Públicos, Santiago, 33, 1989, p. 2.

menoscabarse ninguno de los derechos reconocidos en un Estado en virtud de su legislación interna o de otros tratados internacionales, invocando como pretexto que el convenio en cuestión no lo reconoce o lo reconoce en menor grado. Se ha entendido, entonces, que conforme a ese principio se debe acudir a la norma más amplia o a la interpretación más extensiva cuando se trata de reconocer derechos protegidos.⁶

Con ello –no obstante no ser plenamente homologable la situación– nos parece que la mirada subyacente es enteramente aplicable y, de este modo,

En el presente trabajo sostendremos que para fijar el estándar de protección de datos que deberá cumplir Chile debe considerarse la normativa proveniente de la Unión Europea y especialmente la directiva 95/45/CE (...)

el instrumento internacional que habremos de tener en cuenta es aquel que permita “atrincherar” en nuestro ordenamiento jurídico el derecho, brindando la protección más extensiva para las personas, ya que con ello nuestro país quedará en condiciones de satisfacer las exigencias que todos

los Estados y asociaciones de nuestro entorno habitual nos demandan.

En el presente trabajo sostendremos que para fijar el estándar de protección de datos que deberá cumplir Chile debe considerarse la normativa proveniente de la Unión Europea y especialmente la directiva 95/45/CE, relativa a la protección de las personas, en lo que respecta al tratamiento de datos personales y su circulación, de manera de determinar cuáles son las condiciones que nos impone la Unión Europea para considerar que Chile tiene una “protección adecuada” en la materia.

En consecuencia, lo primero que es necesario determinar es qué se entiende por “protección adecuada” y, en segundo lugar, cuál es la importancia que tiene dicha calificación.

La protección adecuada es una calificación que exige la Unión Europea para permitir que los datos de sus nacionales circulen libremente por un país que la integra, por considerar que el conocimiento de ellos por parte de ese tercer Estado es capaz de ofrecer protección a las personas. Por esta razón, el G-29⁷ ha sostenido que las normas de protección de datos sólo contribuyen a

(6) Uprymni, R., “Bloque de constitucionalidad, derechos humanos y proceso penal”, p. 64. www.wcl.american.edu/humright/hracademy/2008/documents/RodrigoUprimny- BloquedeConstitucionalidad.pdf (consulta: 05.07.08).

(7) Grupo de trabajo de la Unión Europea sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales de la Unión Europea.

la protección de las personas si efectivamente se cumplen en la práctica, por lo que resulta necesario considerar no sólo el contenido de las normas aplicables a los datos personales transferidos a un tercer país, sino también el sistema utilizado para asegurar la eficacia de esas normas.⁸

Así, es claro que la primera exigencia para lograr una adecuada protección es tener en cuenta que no basta con “atrincherar” derechos, sino que resulta igualmente importante y necesario contar con los mecanismos y estructuras judiciales y/o administrativas que aseguren que esos derechos van a ser debidamente amparados. De este modo, cualquier análisis que busque pronunciarse sobre los requerimientos que debe satisfacer Chile para garantizar una adecuada protección según las exigencias que impone la Unión Europea supone analizar dualmente la materia. Por una parte, respecto del contenido de las normas aplicables y, por la otra, en cuanto a los medios que permiten asegurar que su aplicación realmente logre brindar protección a las personas cuyos datos son objeto de tratamiento.

La protección adecuada es una calificación que exige la Unión Europea para permitir que los datos de sus nacionales circulen libremente por un país que la integra, por considerar que el conocimiento de ellos por parte de ese tercer Estado es capaz de ofrecer protección a las personas.

1. Principios de contenido de la protección de datos personales

Se trata de una serie de principios informadores, con pretensión de carácter universal, que han de inspirar la forma y la oportunidad en las que se desarrolla el tratamiento de datos personales por parte de los responsables del mismo y de los bancos de datos. Así, se trata de ciertas consideraciones mínimas que deberán estar incorporadas en las reglamentaciones sobre la materia. Los principios básicos reconocidos por el G-29 son:

- a. Principio de limitación de objetivos.
- b. Principio de proporcionalidad y calidad de los datos.
- c. Principio de transparencia.
- d. Principio de seguridad.
- e. Derechos de acceso, rectificación y oposición.

(8) G-29, “Documento de trabajo. Transferencia de datos personales a terceros países: aplicación de los artículos 25 y 26 de la directiva sobre protección de datos de la UE”, Comisión Europea, 1998, p. 5.

f. Restricciones respecto de transferencias sucesivas a otros terceros países.

2. Normas de ejecución

Norberto Bobbio, en el *Diálogo en torno a la república*⁹, que mantiene con Mauricio Virola, nos plantea la idea de que la exigencia de los derechos nace de la necesidad de defenderse de la prepotencia y la opresión, de todas las formas de poder despótico que hemos experimentado durante nuestra vida. Sin duda, esta reflexión nos ayuda a profundizar la idea de que no basta con que los derechos sean incorporados en la legislación, sino que también se hace necesario configurar un sistema complejo de protección de las personas que, junto con establecer y plasmar principios, implante mecanismos que permiten tutelar la efectividad de su cumplimiento.

Por ende, al pensar en la protección de datos personales, la idea es –una vez atrincherados los derechos– implementar un sistema que sea capaz de articular la concurrencia de ciertos elementos esenciales que contribuyan a ofrecer un nivel satisfactorio de cumplimiento de las normas, conocimiento de los derechos y obligaciones de los actores del tratamiento de datos personales y de las vías y/o recursos que posibiliten amparar los derechos una vez que han sido amenazados o privados. De este modo, advertiremos que los objetivos de un sistema de protección de datos son básicamente tres, en opinión del G-29:

a) Ofrecer un nivel satisfactorio de cumplimiento de las normas. Para ello la atención debe centrarse en que los responsables del tratamiento de datos personales conozcan clara y precisamente cuáles son sus obligaciones. Por otra parte, los titulares de datos deben tener claridad respecto de sus derechos y de los medios disponibles para asegurar su cumplimiento. Finalmente, es necesario que el sistema de protección considere sanciones efectivas que permitan disuadir las malas prácticas e ilícitos en la materia.

b) Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos. Esto está orientado a que los interesados deben tener la capacidad de hacer valer sus derechos con rapidez, eficacia y sin que los costos asociados aparezcan como un desincentivo para actuar. En este punto la Unión Europea considera indispensable la existencia de un mecanismo institucional que

(9) Bobbio, N. y Virola, M., *Diálogo en torno a la república*, Tusquets, Barcelona, 2002, p. 41.

permita investigar las denuncias de manera independiente.

c) Ofrecer vías adecuadas de recurso a quienes resulten perjudicados por la no observancia del cumplimiento de las normas. Esto se centra en que el afectado debe poder obtener una resolución judicial o un equivalente jurisdiccional que reconozca la infracción y que eventualmente ordene el pago de las indemnizaciones e imponga las sanciones.

Por último, es necesario señalar que la importancia de que Chile sea reconocido como un país que tiene un nivel de protección adecuado gira fundamentalmente en torno a la posibilidad de que los datos personales circulen libremente entre nuestro país y Europa sin mayor burocracia, de manera de agilizar el flujo de información transfronterizo. Estas facilidades incidirían en la pretensión nacional de convertir a Chile en un país plataforma para la provisión de servicios con valor agregado. Además, por cierto, en habernos incorporado al selecto grupo de países que hoy considera que no es posible un verdadero desarrollo sustentable en la sociedad de la información y el conocimiento sin que se resguarden debidamente los derechos fundamentales, sobre todos aquellos que se hacen más vulnerables como consecuencia de la masiva incorporación de tecnología al quehacer cotidiano.

La importancia de que Chile sea reconocido como un país que tiene un nivel de protección adecuado gira fundamentalmente en torno a la posibilidad de que los datos personales circulen libremente entre nuestro país y Europa sin mayor burocracia (...)

Estado de la legislación nacional

El cuerpo normativo principal asociado a la protección de datos personales es –como se dijo– la ley 19.628, titulada de protección a la vida privada.

No obstante su nombre, la causa de su dictación se origina en la necesidad de establecer un marco legislativo que permitiera el tratamiento de datos personales para efectos de disminuir nuestro “riesgo país”. Ello hizo que no se considerara adecuadamente que se estaba hablando de una actividad que podía afectar los derechos fundamentales de las personas, lo que, a su vez, trajo consigo que, si bien la finalidad de la ley era absolutamente válida y legítima, ella terminara teniendo graves defectos y falencias para garantizar

el estándar internacional que Chile debe satisfacer. Esto, además, impide que nuestro país sea considerado como uno de aquellos que tienen un “nivel de protección adecuado”.

Del mismo modo, la ley permite e incentiva, en abierta contradicción con su espíritu, ciertas estrategias que posibilitan la vulneración de los derechos supuestamente amparados por la misma, sin considerar sanciones para los responsables del tratamiento de datos personales que infringen la ley; igualmente, la acción judicial prevista para la protección del derecho no cumple estándares de aseguramiento del principio del debido proceso que debe

(...) la legislación nacional sobre la materia tiene dificultades en lo que se refiere al estándar internacional que debe satisfacer, tanto en la dimensión de los principios de contenido de la protección de datos personales como de las normas de ejecución.

regir a los procedimientos judiciales. A ello se suma que el sistema de información a los ciudadanos es insuficiente y que no se cuenta con una autoridad de control, lo que redundando en que las personas, que diariamente se ven afectadas por la forma en que se tratan sus datos personales, muchas veces abusivamente, tanto por parte

de organismos públicos como privados, ni siquiera conocen o dimensionan cuáles son sus derechos ni cómo se ejercen. Y, cuando lo hacen, la barrera del acceso a la justicia termina –a causa de los costos de tramitación– echando por la borda la voluntad de exigir el respecto de los derechos vulnerados por la forma en que se tratan los datos personales.

Por tanto, es posible afirmar categóricamente que la legislación nacional sobre la materia tiene dificultades en lo que se refiere al estándar internacional que debe satisfacer, tanto en la dimensión de los principios de contenido de la protección de datos personales como de las normas de ejecución.

Chile no cumple con las exigencias que su entorno de referencia le demanda; en consecuencia, debe incorporar una serie de modificaciones a la legislación con miras a lograr el cumplimiento del estándar internacional requerido.

Las principales dificultades de la ley 19.628 se encuentran, entre otras materias, en las siguientes:

a) Ausencia de consagración del principio de finalidad en el tratamiento de datos personales. Se trata de uno de los principios esenciales que permiten salvaguardar que los datos personales sean realmente utilizados sólo para los

objetivos para los cuales fueron recolectados, y que por lo demás es la causa en cuya virtud el titular de éstos libremente consintió en su entrega. Junto a este vacío normativo el artículo 4º, inciso final, de la ley permite que las personas jurídicas privadas podrán tratar datos personales sin autorización del titular 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. Esta norma acarrea uno de los mayores riesgos del tratamiento de datos, pues permite que por la vía de la asociación se vulneren todas las normas y principios que pretendidamente protege la ley¹⁰.

b) Existencia de conceptos que generan dificultades interpretativas y que han servido para vulnerar la protección de datos personales. Por ejemplo, lo que ocurre con el concepto de fuente accesible al público, el que adolece de un defecto sustancial: radicar en el titular del registro o banco de datos la facultad de dejar o no abierto a público un registro, con el consecuente riesgo cierto de fraude al espíritu de la ley, especialmente en lo que dice relación con la posibilidad de realizar tratamiento de datos sin autorización del titular de los datos en aquellos casos en que la fuente es de esta naturaleza¹¹.

c) Falta de claridad respecto de quién es el responsable del tratamiento de datos personales. La ley define al responsable del registro o banco de datos como la persona natural o jurídica privada, o el respectivo organismo público, a quien competen las decisiones relacionadas con el tratamiento de los datos de carácter personal. Sin embargo, no se hace cargo de definir al responsable del tratamiento de datos, que es la persona que toma las decisiones operativas respecto del banco de datos y en quien debiera radicar la responsabilidad directa por el uso indebido de los datos personales¹².

d) Deber de información en el tratamiento de datos personales. Éste persigue que los titulares de datos personales sean informados de los posibles tratamientos de datos que puedan afectarles para los efectos de que puedan ejercer los derechos que les otorga la ley. La legislación nacional no regula esta materia, lo que es un elemento básico y esencial de la protección de datos personales.

e) Falta de registro de banco de datos privados. Se trata de una forma

(10) Donoso, L., y Reusser, C., “Chile y el derecho a la protección de datos. Propuesta de adecuación de la normativa nacional a los estándares internacionales”, documento de trabajo, p. 5. www.subtel.cl/prontus_subtel/site/edic/base/port/p_estt_proyectos.html (consulta: 05.07.08).

(11) *Ibid.*, p. 10.

(12) *Ibid.*, p. 8.

de materialización del deber de información en el tratamiento de datos personales, donde por intermedio de un registro de carácter universal cualquier persona puede consultar sobre los tratamientos de datos que se hacen de ella. En nuestro país, no obstante que las bases de datos del sector público deben estar inscritas en un registro que mantiene el Registro Civil, no han sido incorporadas al mismo la gran mayoría de las bases de los obligados, careciendo aquél, en consecuencia, de validez y confianza. Adicionalmente, no existe el mandato de registro de las bases de datos privadas.

f) Ausencia de sanciones por infracción a la normativa. La ley carece de un régimen sancionatorio por el incumplimiento de las obligaciones que impone, lo que redundo en que las vulneraciones a la misma quedan impunes y, consecuentemente, no hay presencia de mecanismos disuasivos ni correctivos por no tratar los datos de acuerdo a las exigencias mínimas que se imponen para asegurar la vida privada. También resulta gratuito, por ejemplo, no cumplir con la obligación de registro de las bases de datos públicas en el Registro Civil.

g) Recurso de *habeas data* atrofiado. La forma que ha tomado este recurso en la ley ha traído como consecuencia que, pese a la existencia de un recurso especial para garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y bloqueo de los datos personales, aquel no haya sido utilizado, prefiriendo los operadores jurídicos recurrir por intermedio del recurso de protección a los tribunales de justicia invocando la vulneración de un derecho fundamental, normalmente la privacidad. Las dificultades que presenta el recurso de *habeas data* son muchas, pero sólo con fines enunciativos podemos aseverar que tiene problemas para el titular de los datos personales en lo que significa la determinación del tribunal competente, el desigual tratamiento procesal que tienen las partes en el proceso lo que trae implícita la vulneración del debido proceso y la bilateralidad de la audiencia; finalmente, no se establece un plazo de prescripción de la acción con lo que se afecta la seguridad jurídica.

h) Ausencia de una autoridad de control. El hecho de no contar con una autoridad independiente que se encuentre permanentemente velando por el cumplimiento de la ley tanto por parte de los organismos públicos como privados, que tenga la posibilidad de aplicar sanciones por el incumplimiento y que tenga un fuerte rol de promoción de la protección de datos personales, es un vacío que quizás formalmente aparece como la mayor dificultad de Chile

de cumplir el estándar internacional exigido.

i) Recogida y tratamiento de datos para marketing directo. La ley considera que para los efectos de realizar marketing directo es posible tratar datos personales sin autorización del titular, otorgándole a éste el derecho de oponerse cuando sea con fines de publicidad. Ello ha conducido a que en nuestro país nos encontremos desbordados por el *spam* o correo electrónico no deseado.

Conclusiones

Si consideramos que la protección de datos personales es el amparo de los ciudadanos contra la posible utilización por parte de terceros, en forma no autorizada, de sus datos personales con el fin de confeccionar información que, identificable con él, afecte su entorno personal, social o profesional, en los límites de su intimidad¹³, claramente el análisis expuesto en las páginas precedentes nos conduce inexorablemente a la conclusión de que la legislación sobre protección de datos personales existente en nuestro país ha debilitado el sistema de derechos y garantías consagrados en la Constitución.

La inadecuada forma en que los organismos públicos y privados, como consecuencia de la tolerancia legal normativa, tratan los datos personales lleva a que los ciudadanos vean hasta con naturalidad que se pueda hacer cualquier cosa con la información de las personas, sin considerar que se afectan, o se puede afectar con ello, derechos fundamentales, como el derecho a la vida privada, al trabajo, a la educación, a la salud, etcétera.

Por otra parte, el no cumplimiento del estándar que internacionalmente se le exige a Chile trae consigo que la integración o incorporación al entorno de referencia habitual se vea entorpecido y se pierdan ventajas comparativas con los países con los cuales competimos para convertirnos en aliados estratégicos. Así, a modo de ejemplo, una transferencia de datos personales de ciudadanos europeos hacia Argentina se demora un día, mientras que a Chile tarda siete meses aproximadamente, lo que ha hecho que los inversionistas europeos que desean prestar servicios como los *call center* evalúen positivamente a nuestros vecinos en esta materia y no a Chile. Otra dificultad concreta con la OCDE es que mientras no cumplamos el estándar exigido no

(13) Garriga, A., *Tratamiento de datos personales y derechos fundamentales*, Editorial Dykinson, Madrid 2004, p. 29.

podremos incorporarnos a tan anhelado club de países desarrollados.

Así, los desafíos que tenemos por delante son muchos. Por una parte, actualizar nuestra normativa de manera de resolver los déficit institucionales, mejorar el tratamiento que se hace de los principios del tratamiento de datos personales, asegurar que los derechos consagrados en la legislación sean exigibles, y que quienes no respeten la ley sean sancionados y reparadas aquellas víctimas del tratamiento ilegal y/o abusivo de datos personales. Por otra parte, resulta indispensable que la normativa se infunda a todo el ordenamiento jurídico y se eduque a la población respecto del derecho a la protección de datos, de manera que sea el principal custodio de su información personal.

Autor



Raúl Arrieta

Abogado de la Universidad Central. Magíster (c) en Derecho Público, Universidad de Chile.

© 2009 Expansiva UDP

La serie **en foco** recoge las investigaciones del Instituto de Políticas Públicas Expansiva UDP las que tienen por objeto promover un debate amplio y riguroso sobre los temas de la sociedad actual, con el fin de hacer propuestas que contribuyan a mejorar las políticas públicas del país.

Este documento forma parte de un proyecto del Instituto en conjunto con la Escuela de Derecho de la Universidad de Chile, el que tuvo como objetivo analizar el marco legal necesario para el funcionamiento de los actuales sistemas de tratamiento de datos personales, además de trazar ciertas directrices sobre las soluciones urgentes que el país tiene que adoptar en materia de derechos fundamentales.

El documento forma parte del libro “Chile y la Protección de Datos Personales: ¿Están en Crisis nuestros derechos fundamentales?” publicado por la Serie de Políticas Públicas de Ediciones Universidad Diego Portales.

Se autoriza su reproducción total o parcial siempre que su fuente sea citada.