

Protección de datos y servicios globales:
¿Regulación o incentivo?

Francisco J. Cruz Fuenzalida

I. Introducción

Los servicios globales, también conocidos como *offshoring*, significan un modelo de negocios por el cual una empresa decide trasladar una de sus funciones o procesos internos hacia el exterior, ya sea mediante su traspaso a una subsidiaria en otro país o bien a través de la subcontratación de un tercero que ejecutará dicho proceso o función en una locación geográfica distinta. Este modelo de negocios permite reducir costos, liberar flujos e incrementar la eficiencia operativa, privilegiando enfoques basados en la innovación empresarial, al aprovechar ventajas laborales, tributarias y tecnológicas de plazas diversas.

Este modelo de negocios permite reducir costos, liberar flujos e incrementar la eficiencia operativa, privilegiando enfoques basados en la innovación empresarial, al aprovechar ventajas laborales, tributarias y tecnológicas de plazas diversas.

Los procesos más comunes que pueden identificarse en la industria del *offshoring* se vinculan a las tecnologías de la información (ITO), los procesos empresariales (BPO) y los procesos de conocimiento (KPO).⁽¹⁾ Los primeros cubren funciones asociadas a tecnologías en infraestructura o aplicación, como puede ser el soporte técnico de negocios, desarrollo de software, captura y procesamiento de bases de datos y mantención de redes. Los BPO se identifican con procesos administrativos (*back office*), procesamiento de *telemarketing*, *callcenters* y, en general, administración de recursos humanos y compras corporativas. A su vez, los KPO se vinculan con flujos de alto valor agregado en investigación, ingeniería, biotecnología y, frecuentemente, con sectores profesionales específicos como medicina o derecho.

La operación del negocio descansa, mayoritariamente, sobre centros de producción y despacho de conocimiento o procesos (*delivery centers*), preferentemente ubicados en Europa y Asia, siendo deslocalizados desde la matriz al país extranjero en donde se ejecuta la función.

En la actualidad la tasa de crecimiento de esta industria bordea el 15% anual y moviliza más de US\$ 192.000 millones. En el caso de Chile existe un grupo aproximado de 60 firmas extranjeras cuyos flujos de exportación representan cerca de US\$ 1.000, generando 20.000 plazas de empleo.⁽²⁾

(1) ITO: Information Technology Outsourcing. BPO: Business Process Outsourcing. KPO: Knowledge Process Outsourcing.

(2) Cifras de la Corporación de Fomento de la Producción (CORFO) dadas a conocer por El Mercurio, Economía y Negocios; Crónica del 27 de septiembre de 2010.

A nivel mundial los márgenes de crecimiento del *offshoring* están en plena expansión, considerando el progresivo proceso de globalización económica, la creciente aplicación de tecnologías de la información en la industria y el surgimiento de nuevos modelos de negocios.

India e Irlanda son algunos de los principales proveedores que deslocalizan operaciones en América Latina, aprovechando ventajas de huso horario, proximidad geográfica y bajos costos de operación para prestar servicios hacia Estados Unidos, uno de los consumidores más importantes del sector.

Es en este escenario que las economías emergentes, dotadas de buen ambiente institucional, tienen una oportunidad privilegiada para capturar esta industria, la que desafía a competir en costos y también en el desarrollo de segmentos que generen un valor agregado en aspectos como: Capital Humano, Investigación y Desarrollo (I+D), Nuevas Tecnologías y Protección de Datos. Cabe destacar que esta última es clave para todos los segmentos en los que se desarrolla el *offshoring*, ya que mientras en ITO y BPO la protección de la información permite que los procesos se desenvuelvan dentro de marcos jurídicos y estándares de seguridad que habiliten un tratamiento de datos responsable, en KPO la información personal constituye la “*materia prima*” para el desarrollo del rubro, muy especialmente cuando se trata de servicios que transitan varios

(...) en lo que respecta a los procesos de conocimiento, los servicios globales demandan marcos regulatorios sofisticados y definidos, que brinden protección al “corazón” del negocio y que se sumen al incentivo permanente que mueve la industria (...)

destinos (como lugar de origen, plaza de procesamiento y locación final en donde se entrega el servicio).

En síntesis, en lo que respecta a los procesos de conocimiento, los servicios globales demandan marcos regulatorios sofisticados y definidos, que brinden protección al “*corazón*” del negocio y

que se sumen al incentivo permanente que mueve la industria, el de relocalizarse en lugares con costos de operación bajos y altas oportunidades de proyección.

II. Tutela de la protección de datos a propósito de los servicios globales

La justificación de la protección jurídica en la industria de los servicios globales surge de la ineficiente regulación que existe en materia de transferencias internacionales y de la necesidad de armonizar marcos normativos regidos

por estándares desiguales. Lo anterior genera una insuficiencia o asimetría que puede encontrarse en el origen del dato, el lugar de su tratamiento o el destino final del mismo.⁽³⁾

La literatura comparada identifica dos sistemas principales para entender el soporte de estándares que deben tener las legislaciones que interactúan en las transferencias de información. Estos sistemas son conocidos como Nivel Adecuado de Protección y Puerto Seguro.

El Nivel Adecuado de Protección, vigente en la Unión Europea (UE), descansa sobre un complejo conjunto de normas y principios que definen y orientan la decisión de la autoridad⁽⁴⁾ llamada a evaluar si el país receptor de la transferencia califica con un escenario institucional que dé garantías a los datos que serán objeto de flujo. Este complejo sistema de normas está compuesto, preeminentemente, por el Convenio 108 del Consejo de Europa; la Directiva 95/46 de la CE;⁽⁵⁾ el Grupo de Trabajo del Artículo 29 de dicho instrumento (GT29)⁽⁶⁾ y las directrices de la OCDE⁽⁷⁾ en la materia, que en

La literatura comparada identifica dos sistemas principales para entender el soporte de estándares que deben tener las legislaciones que interactúan en las transferencias de información. Estos sistemas son conocidos como Nivel Adecuado de Protección y Puerto Seguro.

(3) Cuando se transfieran datos de una agencia (exportador de los datos) a la entidad matriz de un grupo (importador de los datos), ubicada en un tercer país, con la finalidad de centralizar una gestión, se entenderá que el importador de los datos es responsable de su posterior tratamiento, es decir, decidirá sobre la finalidad, contenido y uso del tratamiento de la información. A su vez, cuando una entidad (exportador de los datos) transfiera información a otra entidad (importador de los datos), ubicada en un tercer país, cuya finalidad es la prestación de un servicio, el importador de los datos será el encargado del tratamiento que recibirán los datos para su posterior uso en nombre del exportador de los datos, de conformidad con sus instrucciones.

(4) Respecto de la agencia llamada a efectuar esta evaluación, la UE exhibe fórmulas con arreglos diversos. De esta forma en países como Reino Unido la primera evaluación es efectuada por el propio responsable de exportar los datos, mientras que en España y los Países Bajos dicha decisión radica directamente en la autoridad de control, que podría ser el propio órgano regulador (caso español) o bien en el órgano del Ejecutivo vinculado al rubro, como el Ministerio de Justicia en el caso de los Países Bajos.

(5) El considerando quinto de dicha directiva, atinente en esta materia, señala: “La integración económica y social resultante del establecimiento y funcionamiento del mercado interior (...), va a implicar necesariamente un aumento notable de los flujos transfronterizos de datos personales entre todos los agentes de la vida económica y social de los Estados miembros, ya se trate de agentes públicos o privados; que el intercambio de datos personales entre empresas establecidas en los diferentes Estados Miembros experimentará un desarrollo; que las administraciones nacionales de los diferentes Estados miembros, en aplicación del derecho comunitario, están destinadas a colaborar y a intercambiar datos personales a fin de cumplir su cometido o ejercer funciones por cuenta de las administraciones de otros Estados miembros, en el marco del espacio sin fronteras que constituye el mercado interior”.

(6) Vid http://ec.europa.eu/justice/policies/privacy/index_en.htm

(7) Vid OECD’s “Guidelines governing the Protection of Privacy and Transborder Data Flow of Personal Data” en www.oecd.org

su conjunto permiten inferir un núcleo de principios con contenido,⁽⁸⁾ que fija las pautas de cumplimiento mínimo para el Nivel Adecuado.⁽⁹⁾

Por cierto, bajo determinados contextos en los que se consideren elementos como las empresas involucradas en la transferencia, el volumen y nivel de seguridad de los datos sujetos a la operación, y otras circunstancias que incidan en la evaluación de riesgos, esta línea de partida podría ampliarse o bien tener ciertas indulgencias restrictivas para su aplicación. En definitiva, deben evaluarse todas las circunstancias que concurran en una transferencia.

(...) el sistema de Puerto Seguro es aún más complejo ya que significa una serie de regulaciones parciales, estructuradas sobre normas específicas y conductas sectoriales, con un fuerte énfasis en la autorregulación (...)

Por su parte, el sistema de Puerto Seguro es aún más complejo ya que significa una serie de regulaciones parciales, estructuradas sobre normas específicas y conductas sectoriales, con un fuerte énfasis en la autorregulación, pero sin un contenido de estándares básicos de apli-

cación general. Este es el sistema vigente en Estados Unidos y que para algunos genera vacíos y riesgos al depender excesivamente del autocumplimiento.

(8) En este contexto es posible destacar como principios de contenido centrales los siguientes:

- Principio de Finalidad: Los datos deben tratarse con un objetivo específico, debiendo haber armonía entre dicho objetivo y el que motiva la transferencia.
- Principio de Proporcionalidad y Calidad: Los datos deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren.
- Principio de Transparencia: Debe informarse en todo momento a los titulares acerca del objetivo del tratamiento y la identidad del responsable en el tercer país.
- Principio de Seguridad: El responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento.
- Principio de Acceso, Rectificación y Oposición: El titular o interesado debe tener derecho a obtener una copia de todos los datos relativos a su persona, rectificar datos inexactos y a oponerse a su tratamiento.
- Principio de restricción respecto a transferencias sucesivas a terceros países: Las transferencias sucesivas de datos personales del tercer país de destino a otro tercer país deben considerar, en el caso de este último, un nivel de protección adecuado.

(9) Existen otros marcos atendibles que no detallamos en el eje central de este trabajo, pero que es importante considerar si se desea profundizar en el tema, como es el caso Foro de Cooperación Económica Asia Pacífico (APEC) con su Marco de Privacidad (2004) que vigoriza la protección de la privacidad y los flujos de información, y con el Privacy Pathfinder (2007) que impulsa la aprobación de normativas que establezcan responsabilidades en los flujos internacionales de datos derivados de las necesidades empresariales, reduce costes de cumplimiento con la normativa y facilita a los consumidores instrumentos efectivos de protección de sus derechos, fortaleciendo la acción de reguladores y minimizando cargas administrativas. Para acometer estos fines el Privacy Pathfinder desarrolla un sistema que permite al sector privado crear sus propias reglas transfronterizas para la protección de la privacidad y los datos personales, apoyándose en el uso de sellos de confianza para el consumidor y de una plataforma tecnológica multilingüe que facilita la interacción de los consumidores de cualquier economía de la APEC con las distintas instancias nacionales que se encuentren a cargo de la instrumentación de mecanismos alternativos de resolución de conflictos.

En este contexto, puede considerarse que la complejidad de dicho sistema radica en que produce soluciones aisladas y con un enfoque casuístico, las que, sin embargo, podrían generar los incentivos correctos respecto de ir avanzando en crear respuestas universales a partir de los casos específicos que se vayan resolviendo. Esto no sólo permitiría acrecentar buenas prácticas sectoriales, sino que además entregaría soluciones regulatorias flexibles y dinámicas.

(...) la complejidad de dicho sistema radica en que produce soluciones aisladas y con un enfoque casuístico, las que, sin embargo, podrían generar los incentivos correctos respecto de ir avanzando en crear respuestas universales a partir de los casos específicos que se vayan resolviendo.

En síntesis, existen aproximaciones diversas a un mismo tema, en donde el Puerto Seguro presenta más las cualidades de un buen sistema registral y certificadorio que de control y normativo.

III. Protección de datos y servicios globales

Tras haber realizado una descripción general de los servicios globales, habiendo justificado la necesidad de su tutela jurídica y evidenciado cómo en ella se identifica la protección de datos, volvemos a nuestra interrogante original, la que refiere a si la protección de datos constituye una regulación indispensable para el desarrollo de la industria de los servicios globales o es más bien un incentivo para la misma; si es una carga necesaria o si constituye una oportunidad aprovechable, en otras palabras, ¿las normas de protección requeridas son para justificar el negocio o para potenciarlo?

Para responder a lo anterior no son precisas explicaciones muy elaboradas, pues basta apreciar la experiencia internacional que permite entender la protección de datos como un activo corporativo y no sólo como una carga regulatoria.

A continuación se desarrollan algunas razones que permiten justificar esta posición:

- 1. Al ser una industria altamente expuesta al flujo transfronterizo de datos, la protección de éstos se convierte en un “ancla de certezas” para los servicios globales, que permite fijar reglas claras y estándares, añadiendo predictibilidad a las decisiones en los negocios.**

En efecto, las empresas que operan en la industria de servicios globales, particularmente las que hemos denominado como BPO, transfieren grandes volúmenes de información, deslocalizando centros de operación de dimensiones acotadas hacia plazas de negocios que exhiban garantías institucionales para el tratamiento de datos. En síntesis, buscan países en donde los costos de instalación y operación sean bajos, pero que posean un sólido marco legal que les garantice el “*corazón del negocio*”, es decir, el tratamiento de la información y el procesamiento de los datos.

2. Las medidas tendientes al resguardo de los datos ayudan a uniformar las políticas de *Privacy by Design*⁽¹⁰⁾ (PbD), denominación que apunta a la protección de la información desde el origen de las operaciones y no sólo cuando éstas puedan constituir un riesgo, promoviendo también la autorregulación.

Las empresas internacionales consolidadas están dotadas en su gran mayoría de políticas internas que protegen sus flujos corporativos entre las filiales y entre éstas y su matriz. En la literatura especializada esto es conocido

Las empresas internacionales consolidadas están dotadas en su gran mayoría de políticas internas que protegen sus flujos corporativos entre las filiales y entre éstas y su matriz.

como *Privacy by Design*, adelantando mapas de riesgo y levantando procesos que den confianza a los consumidores, socios, accionistas y, en general, a los titulares de datos.⁽¹¹⁾

Un segundo elemento destacable es que fomentan el surgimiento de códigos tipo o normas de autorregulación, como ocurre en el caso de las denominadas BCR (*Binding Corporate Rules*).⁽¹²⁾ Las BCR’s son reglas de conducta vinculantes, que fijan estándares para transferencias internacionales dentro

(10) “El término “*Privacy by Design*” (PbD) refiere en general a la incorporación de la privacidad y la protección de datos dentro del ciclo de vida del sistema de tecnología de la información, desde sus inicios hasta el cese de su actividad”. (AEPD y Fundación CEDDET; “El Derecho a la Protección de Datos”; Módulo 3º: Seguridad, Confidencialidad, Transferencias Internacionales y Autorregulación, Primera Edición; página 69.

(11) “PbD puede suponer diferentes acciones, dependiendo del caso concreto donde se implante, ya sea eliminando o reduciendo datos de carácter personal, previniendo o eliminando tratamientos no deseados. También puede suponer el empleo de herramientas que mejoren el control del interesado sobre sus datos personales. Además pueden ser incorporadas dentro de la arquitectura de los sistemas de información y las comunicaciones y/o en la estructura de las organizaciones que traten datos de carácter personal”. *Ibidem* página 67.

(12) Reglas Corporativas Vinculantes.

de grupos multinacionales de empresas y que gozan de mayor flexibilidad para la exportación e importación de datos. Cabe entonces preguntarse cuál debiera ser el incentivo que tienen las grandes multinacionales para contar con escenarios que contemplen un nivel adecuado de protección, si ellas mismas ya han internalizado el costo de este estándar.

La respuesta tiene al menos dos expresiones elocuentes. La primera se relaciona precisamente con los costos de operación, mientras más sofisticadas y precisas sean las regulaciones para el tratamiento de datos mayores externalidades positivas reportará ese contexto al negocio, sin tener que asumir las brechas de la legislación como desafíos propios.

En segundo lugar, el hecho de que dos empresas de volúmenes y rubro similares cuenten con estándares distintos —en una misma plaza y al mismo tiempo— nos arroja al menos la duda razonable de que alguna falla de mercado podría originarse por la vía de que no existirían las mismas reglas de juego para que la competencia despliegue su negocio.

(...) mientras más sofisticadas y precisas sean las regulaciones para el tratamiento de datos mayores externalidades positivas reportará ese contexto al negocio (...)

3. La protección de datos comparte similares gratitudes de mercado como las políticas de responsabilidad social empresarial, impactando en este caso directamente en los titulares de datos (la mayoría de las veces el cliente), que siempre esperan información adecuada y proporcional a la entregada.

No se debe perder de vista que la protección de datos es un derecho fundamental, aquel definido como de “autodeterminación informativa” y que en esa virtud permite al titular del dato controlar su información de manera que ésta sea genuina y circule respetando estándares como calidad y adecuación. Es importante hacer énfasis en este punto ya que por lustros la protección de datos —quizás por una tradición “americanista”— ha estado a ratos fuertemente influenciada por la libertad de expresión, siendo vista como contradictoria de esta última. Se trata de un sesgo errado ya que la protección de datos busca precisamente llenar una dimensión de la libertad de expresión que apunta a la entrega de información referida a personas individuales.

Así, el respeto por la circulación de datos responsables no puede sino contribuir a que el mercado de la información, pública y privada, encuentre su centro de equilibrio y no arriesgue distorsiones que vayan en desmedro del interés general o lesionen derechos fundamentales.

(...) el respeto por la circulación de datos responsables no puede sino contribuir a que el mercado de la información, pública y privada, encuentre su centro de equilibrio y no arriesgue distorsiones que vayan en desmedro del interés general o lesionen derechos fundamentales.

Quizás hay aquí un punto de convergencia que vale la pena resaltar en el sentido de que en la protección de datos “*todos ganan*” por igual: los consumidores al controlar su información, las empresas al prevenir los riesgos de que la información de sus clientes sea vulne-

rada y los países al vigorizar sus políticas públicas de atracción de inversiones, mejorando su posición comparativa y cumpliendo con los niveles internacionales en esta materia.

- 4. La protección de datos no es sólo un requisito del negocio de los servicios globales, sino que es un activo agregado del mismo, por lo cual estamos convencidos de que ésta es a la vez regulación e incentivo, apostando a que en este ámbito el costo de contar con marcos regulatorios adecuados⁽¹³⁾ sólo puede generar retornos al país que invierte en ellos, convirtiéndolos en verdaderas plataformas de servicios.**

Como se ha sostenido, la deslocalización de funciones o procesos, propia de la industria de servicios globales, conlleva la lógica de instalarse en países en donde el ambiente público, institucional y legal otorgue garantías a sus operaciones, a través de regulaciones certeras y recogidas en los instrumentos internacionales descritos. Estas regulaciones no constituyen un mayor costo de transacción para sus operaciones sino que, por el contrario, son una ventaja comparativa para desenvolverse en los mercados.

En el caso de Chile esto adquiere una importancia creciente por el impacto de los servicios globales en el mercado nacional, y el crecimiento evidenciado en países como Colombia, Perú, Uruguay y Argentina (este último con

(13) Es evidente que para aproximarnos al concepto de marcos regulatorios adecuados es necesario revisar lo que apuntamos con ocasión de “Nivel Adecuado de Protección” y “Puerto Seguro”, en la sección anterior.

nivel adecuado de protección), los que han avanzado hacia políticas de protección de datos más audaces, transformándose en plazas altamente atractivas para el desarrollo de servicios globales.⁽¹⁴⁾

Importante es destacar que el sector privado comparte esta necesidad y la ha manifestado en instancias como el Consejo Estratégico de la Industria de Servicios Globales, alianza público-privada que lidera la Corporación de Fomento de la Producción (CORFO), lo cual demuestra que esta preocupación no es un monopolio estatal de posibles regulaciones emergentes, sino una necesidad de competitividad de los propios destinatarios de la regulación.

IV. Conclusiones y desafíos futuros

La protección de datos implica no sólo avanzar en la tutela de las garantías fundamentales —transitando de un modelo binario de resguardo de la intimidad a uno de autodeterminación informativa—, sino que además trae consigo una serie de impactos positivos en áreas extrajurídicas, como ocurre en los servicios globales.

Esto refuerza nuestra tesis de aunar alianzas institucionales bien constituidas, en donde consumidores, empresas, agencias públicas y ciudadanos titulares de datos personales entiendan lo importante de una normativa informada y en la cual todos los intereses en juego se develen con organización y transparencia en el mercado, contribuyendo así a concentrar costos de regulación.

Para lograrlo es indispensable promover liderazgos responsables y diversos que procedan de todos los sectores involucrados, de manera de no polarizar el debate en grupos específicos.

En el caso de la industria de servicios globales resulta crítico tener una discusión sensible al interés privado y que incluya a todos los rubros y

Esto refuerza nuestra tesis de aunar alianzas institucionales bien constituidas, en donde consumidores, empresas, agencias públicas y ciudadanos titulares de datos personales entiendan lo importante de una normativa informada (...)

(14) Cifras de la Agencia Española de Protección de Datos (AEPD) exhiben que, entre enero y septiembre de 2010, México ha recibido 18 autorizaciones de transferencia de datos, Perú 11, Uruguay 9, Colombia 9 y Chile 4. Esto evidencia el impacto de las políticas a favor de la protección de datos en el estímulo comercial. Por cierto que Argentina no figura en este listado, ya que al tener “nivel adecuado de protección” no requiere de autorización para estas transacciones.

empresas potencialmente involucradas, más allá de su tamaño. En esta lógica es perfectamente posible pensar en los nuevos mercados que van surgiendo, por ejemplo, en las empresas emergentes que se abren a la oferta de tratamiento de información por encargo.

Un segundo orden de materias que consideramos importante, más allá del arreglo institucional por el cual se opte para albergar una regulación de protección de datos, es la provisión de una normativa que promueva “*externalidades posicionales*”. Éstas deberán ser entendidas como aquellas recompensas colectivas que el comportamiento individual de los obligados es capaz de entregar al sistema. En términos simples: que todos, en alguna medida, ganen con la protección de datos.⁽¹⁵⁾

¿Cómo avanzar en esa dirección? Creemos que a partir de la generación de un *accountability* sustantivo⁽¹⁶⁾ que priorice la aplicación de políticas transparentes, justificadas desde el interés público y desde el punto de vista económico (eficiencia y redistribución).

¿Cómo avanzar en esa dirección? Creemos que a partir de la generación de un *accountability* sustantivo que priorice la aplicación de políticas transparentes, justificadas desde el interés público y desde el punto de vista económico (...)

Esto último no es una novedad cuando se entra en mercados regulados y de fuerte competencia, pero es especialmente relevante considerarlo si en esos mercados habrá en juego actores muy diversos, por su identidad, tamaño, interés y ubicación geográfica. Es así que cabe

sostener que la rendición de cuentas es un concepto relacional, que cobra particular vigencia en la protección de datos y en su vinculación con la industria de servicios globales, en donde las bondades o defectos de una buena política cruzarán fronteras.

En tercer lugar la protección de datos debiera ser un terreno fértil para la autoregulación y las políticas de normalización en materia de flujos de información. Esto no significa promover alternativas sustitutivas a ciertos parámetros normativos básicos que hemos venido revisando, pero sí alentar una cultura responsable de tratamiento de la información que pueda colaborar con disminuir costes regulatorios y vigorizar el *enforcement* de la legislación.

(15) En materia regulatoria esto podría simplificarse a través de un “Pareto Superior”, en virtud del cual al menos un individuo gana y ninguno pierde.

(16) Vid “Accountability y Transparencia en el Estado Regulador”; Juan José Romero Guzmán, Apuntes Inéditos.

En esta línea los sellos de calidad o confianza en comercio electrónico y mecanismos de resolución de conflicto alternativos, en soporte *online*, son un ejemplo de buenas prácticas que permiten avanzar en la dirección correcta y sobre la cual el énfasis del estándar de APEC en el Proyecto Pathfinder (al cual aludimos anteriormente) ha puesto especial atención.

Por último, un llamado a mirar las cosas desde una perspectiva diferente: la protección de datos no debe ser asumida como una exquisitez jurídica que interese a sesudos estudiosos de un área del Derecho o beneficie a mercados elitistas y desconectados de la necesidad económica local. La protección de datos es, al mismo tiempo, tutela ciudadana, garantía de consumidor y un muy buen negocio, ya que sólo puede proveer bienes públicos al mercado de la información, corrigiendo asimetrías, mejorando la calidad y adecuación de los datos que circulan y sincerando la responsabilidad de quienes intervienen en su tratamiento. Significa entonces un esfuerzo de Estado, colectivo y democrático, que redundará en iguales beneficios para todo el país.

La protección de datos es, al mismo tiempo, tutela ciudadana, garantía de consumidor y un muy buen negocio, ya que sólo puede proveer bienes públicos al mercado de la información, corrigiendo asimetrías, mejorando la calidad y adecuación de los datos que circulan y sincerando la responsabilidad de quienes intervienen en su tratamiento.

Autor



Francisco J. Cruz Fuenzalida

Abogado de la Pontificia Universidad Católica de Chile, postulado en Derecho Constitucional y egresado del Programa de Magíster en Derecho Público de esa misma Universidad. Miembro de la Red Iberoamericana de Protección de Datos (RIPD).

© 2011 Expansiva

La serie **en foco** recoge las investigaciones de la **Corporación Expansiva**, las que tienen por objeto promover un análisis interdisciplinario y riguroso sobre los temas fundamentales de la sociedad actual, con el fin de hacer propuestas que contribuyan a mejorar las políticas públicas del país.

Se agradece la participación de Raúl Arrieta como coordinador del proyecto que dio origen a este documento, así como el apoyo otorgado por el Comité de Retail Financiero. La presente versión fue editada por Daniela Crovetto y tanto ésta como todo el quehacer de Expansiva se encuentran disponibles en www.expansiva.cl

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