RED ACADÉMICA INTERNACIONAL DE

PROTECCIÓN DE DATOS PERSONALES

Revista Internacional de Protección de Datos Personales

La protección inteligente de los datos personales: *Privacy by design* (PbD)

Ana Brian Nougrères

Universidad de los Andes. Facultad de Derecho (Bogotá, Colombia)

No. 1 Julio - Diciembre de 2012. ISSN: 2322-9705

La protección inteligente de los datos personales: *Privacy by design* (PbD)

Ana Brian Nougrères*

"Here´s to privacy and freedom – living well into the future" [1]

Resumen

El presente artículo analiza las particularidades de la doctrina del *Privacy by Design* (PbD), los fundamentos basales de la teoría y sus características, y concluye analizando brevemente algunos ejemplos de su aplicación práctica.

Palabras claves: Privacidad inteligente, privacidad por diseño, PbD.

Abstract

This paper analizes the peculiarities of the Privacy by Design doctrine, the fundamentals of the theory of SmartPrivacy and Privacy by Design as well as its characteristics, and concludes with a short reference to some practical examples.

Keywords: SmartPrivacy, Privacy by Design, PbD.

Sumario

* Doctora en Derecho y Ciencias Sociales por la Facultad de Derecho, Universidad de la República Oriental del Uruguay (1985). Docente en la Cátedra de Informática Jurídica, Facultad de Derecho, Universidad de la República (desde 2001). Cofundadora del Instituto de Derecho Informático, Facultad de Derecho, Universidad de la República (2000). Asesor letrado en el Parlamento de la República, Cámara de Senadores y Cámara de Representantes (desde 1992). Consultante en el Colegio de Abogados del Uruguay (2003 en adelante). Integrante de la Red Iberoamericana de Protección de Datos Personales desde su creación (2003) y del Capítulo Uruguay de FIADI (desde 2006). Miembro del IWGDPT (Grupo de Berlín, desde 2004) y de la International Association of Privacy Professionals (desde 2007). Recientemente designada embajadora de Privacy by Design (2011) y miembro de la Mesa Directiva de la Red Académica Internacional de Protección de Datos de Nuevo León (2011). Dirección electrónica: abrian@netgate.com.uy.

1 "Privacy by Design… Take the challenge", Ann Cavoukian, Ph.D., Information and Privacy Commissioner of Ontario, Canada, Introduction, pág. v.

minada - C. Privacidad integrada en el diseño - D. Funcionalidad plena - E. Protección del dato en todo su ciclo vital - F. Visibilidad y transparencia - G. Respeto por la privacidad del usuario - IV. EJEMPLOS DE APLICACIÓN PRÁCTICA DE PbD - *A. PbD en el uso de la energía eléctrica - B. PbD para encarar los problemas de seguridad y privacidad asociados con los sistemas biométricos* - V. CONCLUSIONES - Bibliografía.

Introducción

El concepto *Privacy by Design* (PbD), que puede traducirse como privacidad por diseño o privacidad a la medida del cliente, fue acuñado en la década de los noventa por Ann Cavoukian, Comisionada de Información y Privacidad de Ontario, Canadá. En esa época, el enfoque otorgado a los temas de privacidad era tendiente a fomentar la regulación normativa, pero esto ha ido cambiando al son de los nuevos desafíos que se van planteando. El mundo en el que vivimos hoy es un mundo en que la vigilancia se considera un insumo imprescindible para una vida armónica en sociedad, en que se procura información acerca de los individuos por todos los medios, en que se producen perfiles de las personas según sus comportamientos, acciones que pueden llevarnos a asumir conductas discriminatorias. La ubicuidad, los nuevos paradigmas que nos inducen a compartir información, las redes sociales, la computación en la nube, son factores que han ido delineando con nuevos visos la privacidad.

En este contexto, si pretendemos preservar la privacidad (y nuestros derechos fundamentales), debemos enfrentar la situación con una nueva filosofía, desde una perspectiva integradora de la privacidad en la tecnología, y debemos hacerlo ya. ¿De qué forma lograrlo? Introduciendo los fundamentos de la protección de datos en el sistema tecnológico de procesamiento de la información. Este fue el enfoque inicial del PbD, que posteriormente se expandió hacia un total de tres áreas de aplicación: la tecnología, las prácticas del negocio, el diseño físico.

En esta coyuntura, el concepto de *Privacy by Design* ha ido adquiriendo reconocimiento, aceptación y notoriedad, hecho este del cual nos ilustran especialmente los eventos a los que nos referiremos a continuación.

Mencionaremos en primer lugar que, en el ámbito de la 32ª Conferencia Internacional de Protección de Datos, llevada a cabo en Jerusalem, Israel, en octubre del 2010, se otorgó un reconocimiento especial al *Privacy by Design*, que consistió en aprobar una resolución histórica declarando que este concepto de privacidad introducido en el seno mismo del diseño del negocio y de la arquitectura del sistema desde el momento de su concepción, será fundamental a efectos de preservar el futuro de la privacidad. Esta resolución de las autoridades de la Conferencia, que fue apoyada por la comisionada canadiense Jennifer Stoddart y por los comisionados de Berlín, Nueva Zelanda, República Checa y Estonia, invita, asimismo, a la adopción de los principios de *Privacy by Design* como una parte de la organización de las empresas y propone el concepto como una forma de operar en pos de los principios protectores de los datos personales, a la vez que insta a los comisionados a abrir líneas de investigación acerca de todo lo que *Privacy by Design* implica.

Como consecuencia de ello, la concepción de *Privacy by Design* fue objeto de consideración por el comisionado europeo de Protección de Datos, quien realizó un llamamiento a los gobiernos a dictar leyes que rijan las nuevas tecnologías, y motivo de mención por la CNIL, autoridad francesa de protección de datos en sus guías para la protección de datos personales. El térmi-

no también apareció en la legislatura federal de los Estados Unidos de Norteamérica en abril del 2011, cuando se presentó el Commercial Privacy Bill of Rights en el Senado por los señores legisladores John Kerry (D-Mass) y John McCain (R-Ariz).

Mencionaremos, a su vez, como un nuevo hito para la doctrina de *Privacy by Design*, el que refiere a la International Federation for Information Processing (IFFIP), una organización que representa sociedades dedicadas a las tecnologías de la información en más de cincuenta países, y que otorgó a la comisionada Cavoukian el Premio 2011 Kristian Beckman, por su pionera labor creativa del PbD, por cuanto cumple un rol importante como generador de un puente de conocimientos en la protección de la privacidad en el medio internacional moderno. Este reconocimiento le fue entregado en el marco de la 26ª Conferencia Internacional de Seguridad de la Información que se llevó a cabo en Lucerna, Suiza, entre el 7 y el 9 de junio de 2011.

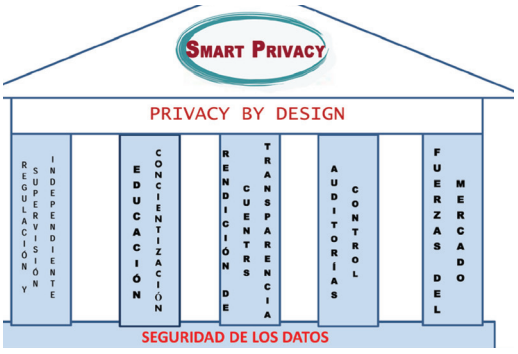
Al entender de la comisionada Cavoukian, puede suceder que en Silicon Valley tanto los que invierten en capital de riesgo como los empresarios estén convencidos de que el concepto de privacidad está obsoleto, pero eso no es así; por el contrario, las reacciones de los consumidores vienen a probar que, tanto el concepto privacidad como el de protección de datos personales siguen vigentes. Si bien hace unos años se llegó a considerar a la privacidad como un obstáculo para la innovación y el progreso, eso ya es historia y obviar la privacidad es un grave error. La realidad es que, sin la confianza de los consumidores, las tecnologías no pueden avanzar; la privacidad está en la esencia de la democracia y se presenta como la libertad de escoger y controlar nuestra información.

I. LA PRIVACIDAD INTELIGENTE (*SMARTPRIVACY*)

Cuando hablamos de privacidad nos referimos a la facultad de cada individuo para controlar la forma en que sus datos personales son objeto de recolección, de almacenamiento y de uso.

El término *SmartPrivacy*, que puede traducirse como privacidad inteligente, hace referencia a un concepto que abarca un amplio espectro de medidas de protección de datos, comprensivo de todo lo necesario para asegurar que los datos personales que están en manos de las organizaciones públicas y privadas son administrados en forma adecuada. Normalmente el *SmartPrivacy* se representa por el siguiente gráfico:

Fig. 1. Ann Cavoukian, Commissioner Ontario, 2009.



(Traducción realizada por la autora)

En la base del *SmartPrivacy* pueden apreciarse las prácticas justas para el tratamiento de la información, lo que implica que la información personal debe ser recabada siguiendo rutinas de uso adecuadas. También el término hace re-

ferencia a que se tomen las medidas necesarias para la protección de datos personales.

En un segundo escalón aparece la seguridad de los datos, como una exigencia justa que merece especial atención cuando refiere a asegurar la privacidad. Privacidad no implica seguridad. La seguridad tiene que ver con las prácticas de gerenciamiento de la información, desde el punto de vista del control. Aluden a proteger la privacidad contra ataques de terceros, pero el hecho de que exista seguridad no trae ínsita la existencia de privacidad. La privacidad no queda garantizada por el hecho de que los datos se preserven confidencialmente. En realidad, la seguridad es necesaria pero no es garantía suficiente de la existencia de una adecuada protección para los datos personales.

A continuación pasamos a mirar las columnas que sostienen la sombrilla de la *SmartPrivacy,* que son condición *sine qua non* de la PbD.

La primera columna corresponde a leyes, normativa y supervisión independiente. Los tres elementos funcionan de manera reactiva, describiendo las consecuencias de cualquier falla en la protección de los datos personales. Tienden a actuar por detrás de la tecnología y por detrás de la sociedad.

A continuación está la columna educación y concientización. Como bien lo decía el filósofo griego Epictetus: "solo los educados son libres". En materia de privacidad tanto la educación como la concientización son claves para las empresas, para las organizaciones, para los consumidores.

La tercera columna predica la transparencia y rendición de cuentas como buenas prácticas que son consideradas elementos de higiene organizacional.

La cuarta columna, auditorías y control, describe los procesos necesarios para asegurar la ejecución de la protección de datos personales en todo su ciclo. Si bien se fomenta que la privacidad esté presente desde el inicio, como una forma de anticipar y prevenir riesgos futuros, se entiende de importancia que los distintos procesos sean testeados a efectos de asegurar resultados adecuados. De ahí surge la importancia de ejercitar el control, de minimizar el número de personas que tienen acceso a datos personales y de limitar en el tiempo la conservación de los datos.

La última columna trae a colación las fuerzas del mercado. Así se trate de empresas que hagan negocios por Internet, o no, es innegable que los consumidores cada vez se vuelcan más hacia el comercio electrónico. Aquellas empresas con contingencias que afectan los datos personales de sus clientes, con seguridad verán disminuir el valor de su marca y sufrirán una desventaja con respecto a las demás.

Por encima de estas columnas está el concepto PbD que asegura la protección de los datos personales, integrado con las especificaciones del diseño de las tecnologías de la información del medio físico y de las prácticas del negocio.

II. FUNDAMENTOS DE LA PROTECCIÓN DE DATOS

A continuación analizaremos las buenas prácticas en materia de protección de datos en la versión del Grupo de Trabajo de Comisionados Internacionales de Protección de Datos (2006).

Los fundamentos de la protección de datos se pueden apreciar en:

A. Consentimiento

B. Rendición de cuentas

C. Finalidad

D. Limitaciones en la recolección

E. Limitaciones en el uso, la retención y la divulgación

F. Precisión

G. Seguridad

H. Apertura

I. Acceso

J. Cumplimiento

A. *Consentimiento*. Para el acopio, el uso y la exposición de la información personal es necesario que se recabe el consentimiento libre y específico del titular del dato. De este principio general solo se exceptúan aquellos casos que la ley indica. Cuanto más sensible es el dato, el consentimiento requerido deberá ser más claro y más específico. El consentimiento puede ser revocado.

B. *Rendición de cuentas.* Toda recolección de información personal trae aparejada una obligación de protección de los datos. La responsabilidad por el cumplimiento de las políticas de privacidad, así como por los procedimientos que se realicen al efecto, debe ser documentada y comunicada y debe estar a cargo de personas específicas dentro de la empresa. Cuando transferimos información personal a terceras partes, estas deben disponer de una protección de datos equivalente, que puede lograrse ya sea por contratos o por otros medios. Siempre la rendición de cuentas habrá de estar presente.

C. *Finalidad*. Es necesario especificar el propósito para el cual la información es acopiada, usada, retenida, exhibida, y comunicar esta finalidad al titular del dato en el momento en que esta es recolectada. La finalidad debe ser clara, delimitada y proporcional a las circunstancias.

D. *Limitaciones a la recolección.* La colecta de información personal debe ser realizada de buena fe, conforme lo indican las normas, y debe estar limitada a los datos necesarios para la finalidad específica.

Los datos personales que se colectan deben ser los estrictamente necesarios. En principio, el diseño de programas, la participación de las tecnologías de la información y la arquitectura de los sistemas deben encauzarse por medio de interacciones y transacciones que no permitan asociar los datos con sus titulares, atendiendo a su anonimización. Deben agotarse los esfuer-

zos tendientes a evitar la asociación, identificación y exposición del titular del dato.

E. *Limitaciones en el uso, la retención y la divulgación.* Es necesario que el uso, la retención y la divulgación de los datos se vean limitados a la finalidad que fuera explicitada al titular del dato, con las únicas excepciones previstas por la ley.

Los datos personales debe ser retenidos sólo durante el lapso necesario para la finalidad y *a posteriori* esa información debe ser totalmente destruida.

F. *Precisión.* Los datos personales deben ser conservados en forma completa, precisa y actualizada a efectos de cumplir con la finalidad.

G. *Seguridad.* Es necesario que el responsable de la base de datos asuma su obligación de brindar seguridad a los datos personales en todo su ciclo de conservación.

Esta seguridad debe ser consistente con los estándares internacionales. Los datos personales deben ser protegidos por medios razonables, que podrán ser físicos, técnicos y administrativos y deberán ser apropiados al grado de sensibilidad del dato.

H. *Apertura*. La apertura y la transparencia son claves para la rendición de cuentas. De ahí que es preciso proveer a los titulares del dato de información acerca de las políticas de privacidad y de las prácticas que tienen relación con el manejo de sus datos personales.

I. *Acceso*. Debe suministrarse a todo titular del dato acceso a su información personal e informársele, asimismo, del uso y la exposición que se dará a su dato.

Todo titular del dato debe poder verificar la precisión del mismo y exigir su corrección si fuera necesario.

J. *Cumplimiento*. Es necesario establecer mecanismos de queja y comunicarlos abiertamente. En la comunicación deben incluirse todas las instancias y los pasos a los que se puede recurrir para obtener la corrección o actualización del dato. Es de importancia, asimismo, que se tomen las medidas necesarias para monitorear, evaluar y verificar el cabal cumplimiento de las políticas de privacidad y los procedimientos.

III. ¿EN QUÉ CONSISTE LA TEORÍA DEL *PRIVACY BY DESIGN*?

La noción de PbD refiere tanto a una filosofía como a un enfoque por el cual la privacidad se encuentra integrada en el diseño tecnológico mismo, consistente con la arquitectura del sistema de información y con el modelo de negocios. Se presenta como una forma de asegurar que la privacidad va a estar garantizada ante los cambios tecnológicos, que hoy por hoy se van sucediendo de manera cada vez más vertiginosa.

El concepto procura comprender el futuro de la privacidad. De ahí que, más allá del cumplimiento de marcos regulatorios, la privacidad se entiende como un modo de operar de las organizaciones y de las empresas públicas y privadas.

La PbD comprende una trilogía de aplicaciones: los sistemas de tecnologías de la información,

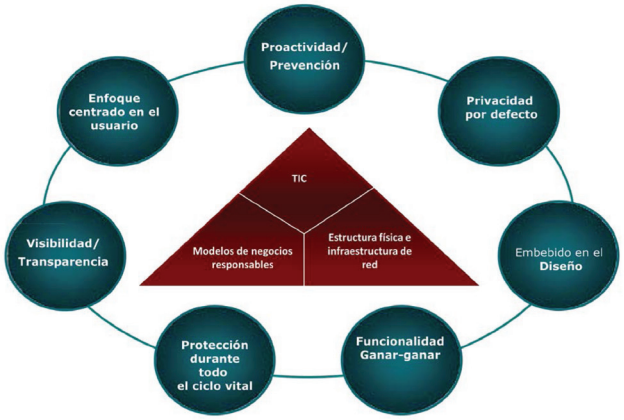
las prácticas de transparencia y rendición de cuentas, y el diseño físico de las infraestructuras en red.

Toda la idea surge alrededor de siete principios que informan la PbD y que son marcos referenciales que pueden ser utilizados para el desarrollo de criterios de aplicación del sistema y para su verificación.

Son principios que se aplican a las tecnologías, a la operación de negocios, a las arquitecturas físicas y a las infraestructuras de red, que en suma configuran los sistemas de información. A su vez, constituyen la clave para la consecución práctica de las ventajas estratégicas de los programas de privacidad por diseño. Con ellos se trata de promover la privacidad de los consumidores dentro de las organizaciones y de las empresas, en cada etapa del desarrollo de los productos y servicios ofrecidos. Los principios caracterizan la PbD y delimitan este nuevo paradigma diferenciándolo de los esquemas utilizados anteriormente para encarar la protección de datos. Sólo aplicando los siete principios se puede alcanzar el modelo de privacidad por diseño (PbD).

En la figura 2 pueden apreciarse los siete principios fundacionales de la PbD.

Fig. 2. Ann Cavoukian, Commissioner, *The Curriculum.*



(Traducción realizada por la autora)

A. Proactividad y no reacción, prevención y no corrección

Este principio fundacional hace referencia a que los intereses y preocupaciones que tienen que ver con la privacidad deben ser encarados proactivamente, es decir, deben ser anticipados antes de que sucedan.

En la teoría del PbD no se espera que los riesgos se materialicen ni se ofrecen soluciones para casos de infracción o daños, de lo que se trata es de prevenirlos.

Esto implica:

- Un compromiso claro al mayor nivel, de establecer altos estándares de protección de datos (generalmente superiores a los que establecen las leyes y la regulación global) y compeler a su cumplimiento.

- Un compromiso de privacidad compartido por la comunidad en una cultura de mejora continua.

- El establecimiento de métodos para reconocer diseños que no protegen adecuadamente los datos personales, anticipar prácticas en tal sentido y corregir sus impactos negativos antes de que ocurran, aplicando fórmulas proactivas, sistemáticas e innovadoras.

B. Privacidad como configuración predeterminada

Partimos de la base de que lo primero que se genera son las configuraciones que han sido predeterminadas teniendo en cuenta la especial valoración del elemento privacidad.

El sistema se genera con total certidumbre, previendo desde el inicio la privacidad, razón por la cual no hay opción posible de que la configuración no preste a los elementos de protección del dato la debida atención y consideración ni es posible que el usuario del sistema pueda actuar con error aplicando un parámetro que contradiga los elementos básicos de la protección del dato personal.

De ahí que el PbD otorga el nivel máximo de privacidad asegurando que los datos personales van a estar protegidos en todo el sistema de tecnologías de la información, y también en el sistema de prácticas del negocio.

No existe ningún elemento relacionado con privacidad que quede librado a la acción individual: todo el sistema de PbD es concebido por dentro de la arquitectura de la red, reconociendo y valorando los principios básicos de respeto a la privacidad por defecto.

Dentro de esta configuración predeterminada, como parte del sistema de buenas prácticas que se sugiere implementar, habrá de tenerse en consideración:

- La finalidad específica de la recolección, uso, retención y divulgación del dato, y la información de dicha finalidad al titular del dato.

- La limitación de la recolección a la finalidad específica.

- La minimización de los datos recogidos y su anonimización.

- Las limitaciones en el uso, retención y divulgación de los datos personales, que se configuran en atención a la finalidad, al consentimiento y a lo que indica la ley.

Siempre que no estén claramente identificados los usos de los datos personales debe presumirse que estos deben ser protegidos. La configuración por defecto debe tender a proteger la privacidad.

C. Privacidad integrada en el diseño

El concepto de PbD se presenta integrado en el diseño y la arquitectura de los sistemas de tecnologías de la información y en las prácticas de negocios.

Lo referente a la protección de datos no está agregado al sistema, no está superpuesto al sistema ni es un anexo al mismo. Es un componente esencial del sistema: su núcleo funcional.

Se presenta holísticamente, esto es, abierto a los nuevos contextos que puedan surgir, como factor de integración e interacción de los distintos intereses involucrados y, además, en una forma por demás creativa, por cuanto se prevé la necesidad de autoinventarse a sí misma cuando no existan otras alternativas viables.

La privacidad concebida con integración al sistema no disminuye su funcionalidad.

D. Funcionalidad plena

Todos los intereses y objetivos se presentan en forma de ganar-ganar. No se trata de sacrificar protección de datos en pos de seguridad, pues lo que se procura es evitar falsas dicotomías, demostrando que es posible y deseable honrar la protección de datos y también la seguridad.

En el caso, no se trata de plantear expectativas ni de hacer declaraciones ni compromisos, sino de satisfacer los legítimos objetivos de la organización, además de las metas sobre protección de datos personales.

La PbD se presenta con una naturaleza que habilita la funcionalidad plena de la organización, de manera que los resultados reales, prácticos, sean logrados por todas las partes involucradas.

E. Protección del dato en todo el ciclo vital

La PbD ha sido integrada al sistema antes de que el primer elemento de información se haya recolectado, extendiendo la seguridad a través de todo el ciclo de vida del dato: seguridad de extremo a extremo.

Las medidas de seguridad son esenciales para la privacidad, del inicio al fin.

Esto asegura que todos los datos serán retenidos adecuadamente, y que también serán destruidos de manera apropiada al final del proceso, conforme corresponda. De ahí la referencia a que la seguridad se prevé para todo el ciclo vital del dato.

La especial relevancia del principio de la seguridad en la instancia, está en el hecho de que no es posible concebir la privacidad sin fuertes medidas de seguridad.

Los estándares de seguridad aplicados deben garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales en todo su ciclo y deben incluir métodos seguros de destrucción, adecuada encripción y fuertes controles en el acceso a los mismos.

F. Visibilidad y transparencia

El sistema de PbD procura asegurar a todos los grupos interesados que, cualquiera que sea la práctica de negocios y la tecnología involucrada, en los hechos todas las operaciones van a ser realizadas de conformidad con las premisas y objetivos fijados, y van a estar sujetas a esquemas de verificación independientes.

Cada parte componente y cada operación van a permanecer visibles y transparentes, tanto para los usuarios como para los proveedores.

Visibilidad y transparencia van de la mano con rendición de cuentas y confianza, y esto nos lleva al concepto de buenas prácticas, que habrá de complementarse con el objetivo de auditar.

En la instancia el énfasis debe ser puesto en:

- Responsabilidad en la rendición de cuentas.
- Apertura y transparencia.
- Cumplimiento de los mecanismos legales para que el titular de los datos pueda evaluar la debida aplicación de las políticas de privacidad y sus consiguientes procedimientos.

G. Respeto por la privacidad del usuario

La idea de PbD es mantener todo el sistema centrado en el usuario. Tanto los arquitectos como los operadores tienen la responsabilidad de proveerle de fuertes esquemas de privacidad por defecto, que recaben el previo consentimiento y fortalezcan las soluciones que son amigables para el usuario.

En general, se entiende que los mejores sistemas son los que han sido conscientemente diseñados con especial atención a las necesidades de los usuarios, que son los primeros interesados en manejar su propia información.

Otorgar al usuario la posibilidad de jugar un rol activo en la manipulación de sus propios datos puede constituir un chequeo muy efectivo contra malos usos y abusos de la protección de datos personales. Para ello, el usuario debe otorgar su consentimiento en forma libre y específica, y poder controlar la veracidad de la información, a cuyos efectos debe proveérsele de acceso a dicha información, así como de los medios de reclamo en casos de verificarse inexactitud en sus datos. Tanto las soluciones técnicas como las operaciones de negocios y las arquitecturas físicas de las redes, en fin, todo el sistema debe proveer al usuario de un grado tal de consideración que lo coloque en el centro de las operaciones de acopio de datos personales.

Se dice que el futuro de la privacidad está en los diseños de PbD. Esto podrá suceder o no, pero de lo que no cabe duda es del crecimiento exponencial que está teniendo la recolección, diseminación, uso y retención de los datos personales. Y tampoco cabe duda de que el sistema de protección de datos generado bajo el concepto de PbD, muy factiblemente vaya a coadyuvar a que sobreviva el concepto de privacidad y protección de datos personales en el decurso del siglo XXI.

La PbD puede aplicarse a las tecnologías de la información, a las prácticas negociales, a la arquitectura del sistema de información, en uno de los tres ámbitos, en dos, o en todos ellos.

Así concebida, la privacidad es esencial para crear un entorno de confianza, de relaciones cliente-proveedor a largo plazo, que hacen, tanto a las organizaciones como a las empresas más atractivas para generar nuevas oportunidades de negocios.

La misma concepción ha venido sufriendo una evolución con el tiempo, y —al día de la fecha— se habla también de *Privacy by Redesign*, tér-

mino que aduce a la aplicación de la PbD sobre sistemas que ya se encuentran en funcionamiento y que se transforman para incorporar esta tecnología a sus operaciones.

IV. EJEMPLOS DE APLICACIÓN PRÁCTICA DEL PbD

A modo de conclusión, a efectos de mostrar cómo funciona la teoría del PbD en casos prácticos, se mencionarán dos ejemplos. En cada uno de ellos puede inferirse su forma de operar y cómo los principios fundacionales forjan nuevas formas de encarar la protección de datos personales, mejorando la relación de las empresas para con el consumidor en forma muy eficiente. Cada ejemplo de por sí amerita uno o más ensayos como el presente. Son casos que funcionan y son efectivos. Su desarrollo extensivo excede el objeto del presente.

A. PbD en el uso de la energía eléctrica

La privacidad integrada en el diseño de la disposición y el suministro de la energía eléctrica fue uno de los casos importantes de aplicación de esta doctrina. Conscientes del riesgo que traía aparejada la recopilación de datos sobre consumo de energía eléctrica, en razón a que puede dar a conocer los horarios en que cada persona comienza su día, toma una ducha, se alimenta, mira televisión, descansa; conscientes asimismo de que el hecho de que existan estos datos los torna apetecibles para ladrones, empresas de mercadeo y piratas informáticos, surge la idea de proteger los datos que refieren al uso de la energía eléctrica. Es así como desde la oficina de la Comisionada de Información y Privacidad de Ontario, conjuntamente con el Ministerio de Energía y con las compañías proveedoras de energía eléctrica, decidieron instalar mecanismos para la protección de los datos relacionados con la red eléctrica, y su vigilancia. En el caso, se integró la privacidad al diseño del sistema de electricidad, de forma tal que la protección de datos funciona por defecto durante todo el periodo en que las compañías suministradoras de energía toman contacto con los datos personales de sus clientes.

B. PbD para encarar los problemas de seguridad y privacidad asociados con los sistemas biométricos

Entre los nuevos enfoques que se dan a los métodos de verificación e identificación, la encriptación biométrica está siendo cada vez más valorada y cabe resaltar que dicho proceso utiliza el PbD para encarar los problemas de seguridad y de privacidad. Se trata de un proceso que extrae en forma segura una clave biométrica de forma tal que ni la clave ni los demás aspectos pueden ser recuperados, ni almacenados por la aplicación. La clave es encriptada biométricamente y puede ser desencriptada solamente si se presenta la muestra biométrica viviente para su verificación. No existe ninguna macro, ni representación de la biometría, que sea objeto de retención. Este sistema fue aplicado con éxito por la Ontario Lottery and Gaming Corporation, con la cooperación del despacho de la comisionada Cavoukian y miembros del Departamento de Sistemas de la Universidad de Toronto, así como por la firma iView Systems, especializada en biometría e incidentes de seguridad.

V. CONCLUSIONES

El concepto de *Privacy by Design* constituye una teoría para implementar los principios de la protección de datos personales de una forma integral, con una visión holística, que los incorpora con la concepción del negocio y de los sistemas de información. Se presenta como una forma novedosa de pensar los datos personales, que viene a mostrar los fundamentos de la privacidad con un enfoque netamente diferenciado de los anteriormente existentes.

Implica un compromiso con estándares universalmente aceptados y requiere de la determinación de actuar en materia de protección de este derecho humano fundamental desde la concepción del sistema de negocios.

Su filosofía viene siendo aplicada desde hace varios lustros, y sus resultados pueden apreciarse en los ejemplos presentados más arriba o en otros referentes a la telefonía celular[2], los drones[3] y otros. Su aplicación ha sido siempre en pos del respeto a una adecuada protección de los datos personales, con una óptica eminentemente práctica, que no descuida aspectos técnicos ni jurídicos.

La trascendencia de esta concepción está en que viene a conciliar la privacidad y, por consiguiente, la protección y la libre autodeterminación de qué se hará con los datos, en los esquemas más actuales de negocios. Ve más allá de los esquemas de negocios que siguen al marketing comportamental, y concibe una forma de convivencia libre y en armonía dentro del sistema, con el conocimiento pleno de que donde terminan los derechos del uno comenzarán los del otro; solo de esta forma podrá concebirse la privacidad en el futuro.

2 García, Víctor, "HP s privacy-enhancing technologies", 2009.

3 Villasenor, John, PH.D., "Beware of Surveillance by Design. The impact of surveillance on… dissent, freedom, and social change", 2012.

Bibliografía consultada

Anderson, Ken y otros, "Operationalizing Privacy by Design. The Ontario Smart Grid Case Study", 2011.

Asu, Information and Privacy Commissioner, Ontario, Canada. "The roadmap for PbD in mobile communications. A practical tool for developrs, service providers, and users", 2010.

Carson, Angelique, "Anne Cavoukian receives industry awards" in *The Privacy Advisor*, the official newsletter of the IAPP, 2011.

Cavoukian, Ann, *Data protection,* 2011.

Privacy by Design Curriculum 2.0, 2011.

Privacy by Design… Take the challenge, 2009.

Privacy by Design. Los 7 principios, 2011.

Privacy by Design. The 7 Foundational Principles, 2009.

Privacy by ReDesign: A transformative process, 2011.

Submission of the Information and Privacy Commissioner, Ontario, Canada. Response to the

FTC Framework for Protection Consumer Privacy in an Era of Rapid Change, 2011.

Cwalina, Christofer. *Building privacy protection into product design,* 2011.

Gallus, Tanya. *Commissioner Cavoukian receives International Privacy Award,* 2011.

HP, Information and Privacy Commissioner, Ontario, Canada, The Centre for Information Policy Leadership Hunton and Williams LL.P. PbD. *Essential for organizational accountability and strong business practices,* 2009.

Information and Privacy Commissioner, Ontario, Canada, "Data Protection", 2009.

IBM. PbD. "From Policy to Practice", 2011.

Information and Privacy Commissioner, Ontario, Canada. "Privacy by Design", 2010.

Information and Privacy Commissioner, Ontario, Canada. "Privacy by Design. The 7 Foundatinal Principles. Implementation and mapping of fair information practices", 2006.

Kashmir, Hill, "Why PbD is the new corporate hotness", 2011.

Moss, David, "FBI techs shy away from facial recognition: spends 40 years losing face", 2009.

Ohlden, Anna, "Landmark Resolution passed to preserve the Future of Privacy", 2010.

Ontario Lottery and Gaming Corporation. Information and Privacy Commissioner, Ontario, Canada. "Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept", 2010.

Pato, J.N. y otros, "Biometrics Recognition: Challenges and Opportunities". http://www.nap.edu. Consulta: 5 de agosto de 2012. Ruffolo, Rafael, "How to start a privacy-focused legacy redesign", 2011.

Ruffolo, Rafael, "How to start a privacy-focused legacy redesign", 2011.

Talaa, Tanya, "Smart grid data must be protected. Privacy czar", 2010.

Tapscott, Don y otro, "Social media s unexpected threat", 2011.