Español

GDPR AND THE PRIVACY SHAKE-UP

Time to Abandon Zero-Sum Models and Shift to Positive-Sum Thinking

April 2018

GLOBAL PRIVACY AND SECURITY BY DESIGN

DATA Catalyst

Shift to Positive-Sum (Not Zero-Sum) Thinking

GDPR and the Privacy Shake-up: Time to Abandon Zero-Sum Models and Shift to Positive-Sum Thinking

Ann Cavoukian, Ph.D., LL.D. (Hon.), M.S.M.
Creator of Global Privacy and Security by Design
Distinguished Expert-in-Residence, Privacy and Data Analytics
Privacy by Design Centre of Excellence, Ryerson University, Ontario, Canada
Email: ann.cavoukian@ryerson.ca

Con la fecha de implementación de la GDPR acercándose rápidamente, está claro que esta nueva regulación europea de privacidad ha estado sacudiendo a los negocios en todo el mundo, sin mencionar, que ha puesto en relieve la desactualización de las leyes de privacidad en otras jurisdicciones. Este documento recomendará considerar las virtudes del enfoque de privacidad de Privacy by Design: reconocer los intereses múltiples además de la privacidad, conduce inevitablemente a una mejor gobernanza de la privacidad.

Agradecimientos: El autor desea agradecer las contribuciones de Michelle Chibba, Ryerson University y Jake Ward, Data Catalyst por su aporte y comentarios sobre las diversas versions de borradores de este documento.

La Tormenta Perfecta

La implementación del Reglamento General de Protección de Datos de la Unión Europea (GDPR) en mayo de 2018 introduce nuevas obligaciones para cualquier organización que maneje datos sobre ciudadanos de la UE, sin importar que esa organización esté ubicada en la UE o no. El nuevo marco de privacidad paneuropeo es ambicioso, a veces complejo y estricto. El ímpetu de los esfuerzos europeos y el efecto dominó en otras jurisdicciones con leyes de privacidad obsoletas, genera la necesidad y la oportunidad de establecer marcos de privacidad innovadores y efectivos que sean sostenibles y positivos para todos.

Esta acción regulatoria es el resultado de las últimas dos décadas en las cuales Internet entró en una nueva fase. Ya no es solo una red de comunicaciones, sino más bien una plataforma para la informática: una gran supercomputadora virtual interconectada. Este nuevo ecosistema digital presenta desafíos complejos de seguridad y privacidad. Las transacciones de datos legítimas generan inquietudes sobre la privacidad, especialmente a medida que los datos de ubicación se vuelven más identificables producto del mayor uso de dispositivos móviles. En esta era de informática móvil, social y en la nube, estamos produciendo puntos de datos sin precedentes, y a la vez, perdiendo el control efectivo sobre nuestra información personal. Así, surge la siguiente pregunta: ¿qué significará la privacidad y cómo sobrevivirá y prosperará, como un derecho humano viable, de valor operacional y factor crítico de confianza habilitante, en un mundo donde el individuo está cada vez menos presente en el medio de transacciones ricas en datos? La privacidad equivale a control: control personal sobre los usos de la información personal.

En este contexto de avances tecnológicos radicales, agreguemos las revelaciones de Snowden sobre la vigilancia masiva, y el desenredo de un régimen de privacidad que se consideró adecuado para respaldar los flujos transfronterizos de datos personales desde Europa a Estados Unidos. En 2015, el Tribunal Europeo de Justicia invalidó el “Safe Harbor Agreement”, declarándolo inadecuado; entonces el Escudo de privacidad UE-Estados Unidos se estableció en 2016.

En Canadá, no hay menos discusiones o preguntas respecto a la capacidad de las empresas para enfrentar el desafío a tiempo para mayo de 2018. Del mismo modo, se están planteando preguntas sobre la adecuación de los regímenes de privacidad canadienses a la nueva realidad europea. De hecho, en una reciente conversación, el Comisionado de privacidad de Canadá, Daniel Therrien advirtió que "Canadá podría enfrentar problemas de idoneidad a la luz de la nueva regulación europea" e indicó que ha estado exhortando al gobierno federal canadiense a actualizar sus leyes de privacidad, [1] y recomendó que se incluya a “Privacy by Design”. El comisionado señaló: "Las organizaciones también deben ser más transparentes y responsables de sus prácticas de privacidad. Como conocen mejor su negocio, es justo que esperemos que encuentren formas efectivas, dentro de su propio contexto específico, de proteger la privacidad de sus clientes, especialmente integrando enfoques como Privacy by Design"[2]. Otros expertos en privacidad y actores claves también han medido el impacto de la GDPR en las leyes de privacidad de Canadá, incluidas las implicacias para el sector de las pequeñas y medianas empresas. [3] [4]

[1] https://iapp.org/news/a/canadian-privacy-commissioner-announces-proactive-approach-to-enforcement/
[2] https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1
[3] http://www.colinbennett.ca/data-protection/is-canada-still-adequate-under-the-new-general-data-protection-regulation/
[4] https://www.itworldcanada.com/article/canadas-privacy-laws-need-to-be-be-updated-but-dont-look-to-europe-or-the-us-for-guidance-canadian-experts-say/385134

La multiplicidad de eventos en las últimas dos décadas han contribuido a la necesidad de que la política de privacidad y la política de datos en general sean adecuadas. La importancia de la privacidad no puede ser exagerada. En un mundo cada vez más interconectado, el gobierno y la industria tienen la responsabilidad compartida de protegerse contra el exceso que pueda cometer cualquiera de los dos partes por sobre la otra.

La Privacidad por Diseño

Privacy by Design (PbD) es un conjunto de siete principios fundamentales que sirven como un marco general para incluir proactivamente la privacidad y protección de datos desde el inicio, de manera efectiva y creíble, en las tecnologías de la información, los procesos organizacionales, las arquitecturas en red y, de hecho, en sistemas completos de gobierno y fiscalización. Los objetivos son garantizar el control del usuario, mejorar la transparencia y generar confianza. Los 7 Principios Fundamentales que forman PbD (ver Figura 3) expresan no solo los principios universales de Prácticas de Información Justa (PIJ) sino que también incorporan un enfoque de pensamiento de diseño. Los principios, vinculados de manera integral, abordan la necesidad de una sólida protección de datos y el deseo de una organización de descubrir el potencial de la innovación impulsada por los datos. Al igual que con el GDPR, el concepto de PbD comenzó a tomar forma en la década de 1990. Como su autora, la necesidad de abordar los efectos sistémicos y en constante crecimiento de las tecnologías de la información y la comunicación, y de los sistemas de datos en red a gran escala, era claro que el futuro de la privacidad no podía garantizarse únicamente mediante el cumplimiento de marcos regulatorios que actuaran después de los actos de violación a la privacidad; más bien, la seguridad de la privacidad tenía que convertirse idealmente en el modo de funcionamiento predeterminado de una organización.

A lo largo de los años, ha prevalecido un paradigma de suma cero, en el que un valor, como la privacidad, compite con otro valor, como la seguridad, en una ecuación de "ganancia-pérdida" de suma cero. Lo anterior sigue la siguiente lógica: para tener la seguridad adecuada y protegernos contra la amenaza del terrorismo, debemos renunciar a nuestra privacidad. Esta noción, sin embargo, se basa en una lógica completamente defectuosa y en una falsa dicotomía: que la privacidad y la seguridad deben considerarse mutuamente opuestas, lo que no es cierto. La privacidad puede y debe coexistir junto con otros requisitos críticos: seguridad, funcionalidad, eficiencia operativa, control organizacional, procesos de negocios y usabilidad en una ecuación de "suma positiva" o "ganancia doble".

Al hacerlo, creo que Privacy by Design ayudará a crear una cultura particular de privacidad que he defendido desde hace muchos años. Esta cultura de la privacidad es lo que surge cuando las organizaciones abordan la privacidad no como un problema de cumplimiento, sino como un problema comercial. Es lo que se sostiene cuando el liderazgo de una organización llega a ver que la implementación de controles de privacidad positivos crea – en lugar de limitar – oportunidades comerciales. En resumen, es una cultura de "ganar-ganar" o suma positiva. Esto no quiere decir que la privacidad por diseño deba aplicarse al vacío. Es una parte crítica, pero solo una parte, de un conjunto de protecciones de privacidad que incluye instrumentos normativos, conciencia y educación del consumidor, responsabilidad y transparencia, auditoría y control, y fuerzas del mercado.

Acercarse a la privacidad desde el nivel de códigos es un cambio significativo de las formas tradicionales de pensar sobre la protección de datos. Así como PbD representa un cambio en la forma en que las organizaciones deben pensar acerca de la privacidad -cambiando de un modo reactivo a uno proactivo-, consagrar el PdD en instrumentos regulatorios, códigos voluntarios y mejores prácticas requiere un cambio en la forma en que los legisladores se acercan a generar regulaciones en esta área. PbD representa la próxima generación de protección de la privacidad: invita al desarrollo de enfoques innovadores para promover y consagrar la privacidad en diversos instrumentos. El objetivo de las leyes relacionadas con su aplicación, la sostenibilidad y la falta de consecuencias imprevistas. incorporando enfoques flexibles / progresistas como PbD. Esto requiere un cambio de paradigma en el pensamiento sobre la privacidad como un asunto de negocios, no simplemente relacionado con una cuestión de cumplimiento regulatorio.

Incorporar el PbD en la legislación de un país no está exenta de desafíos. No solo deben explorar qué tipos de instrumentos son apropiados sino también cómo interpretarlos. Los principios de Privacy by Design pueden informar tanto el estado final (por ejemplo, la privacidad como el valor predeterminado), como el proceso para llegar al estado final (por ejemplo, protección integral de ciclo de vida completo). En el proceso, los gobiernos siempre deben considerar que PbD proporciona una base para integrar las consideraciones de privacidad en la legislación, y que la presencia de PbD en todo el mundo de los negocios se está convirtiendo cada vez más en la norma.

Mientras en Canadá miramos hacia el futuro, queremos dar forma a las estrategias de privacidad y gobierno de datos, y dado que el GDPR también incluye privacidad por diseño y privacidad por defecto, tal vez existan características clave del marco de privacidad por diseño que podamos considerar a medida que avanzamos.

Figura 3: 7 Principios claves de la Privacidad por Diseño

1. Use medidas proactivas en lugar de reactivas, anticipe y prevenga los eventos invasivos de privacidad antes de que sucedan (Proactivo, no reactivo; Preventivo, no correctivo).

2. Los datos personales deben estar protegidos automáticamente en cualquier sistema de TI o práctica comercial. Si un individuo no hace nada, su privacidad permanece intacta (Privacidad como valor predeterminado).

3. La privacidad debe integrarse en el diseño y la arquitectura de los sistemas de TI y las prácticas comerciales. No se integra como un complemento, después de los hechos. (Privacidad integrada en el diseño).

4. Todos los intereses y objetivos legítimos son incorporados. (Funcionalidad completa - Suma positiva, no suma cero).

5. La seguridad se aplica a lo largo de todo el ciclo de vida de los datos involucrados. (Seguridad de extremo a extremo - Protección completa del ciclo de vida).

6. Para la rendición de cuentas, se asegura a todos los interesados que cualquiera que sea la práctica comercial o la tecnología involucrada, se está operando de acuerdo con las promesas y objetivos establecidos, sujeto a verificación independiente. (Visibilidad y transparencia - Mantenerlo abierto).

7. Los arquitectos y operadores deben mantener los intereses de la persona en lo más alto, ofreciendo medidas tales como estrictos valores predeterminados de privacidad, notificación adecuada y opciones de fácil uso para el usuario (Respeto por la privacidad del usuario – Manteniendo el foco en el usuario).

Elementos Básicos de la Privacidad por Diseño: las 3 c'S (Consulta, Cooperación, Colaboración)

Las principales características que hacen que la privacidad por diseño sea relevante cuando consideramos que nuestros regímenes de privacidad (de Canadá) están listos para cumplir con el siglo XXI son:

i) Tomar un enfoque proactivo de resolución de problemas está en el centro del de PbD (Principio 1). PbD hace de la privacidad un requisito fundamental, anticipando y previniendo los eventos invasivos de privacidad antes de que estos mismos sucedan. Un factor crítico de éxito en este enfoque es que el regulador también debe ser adaptativo. De hecho, el comisionado de privacidad de Canadá señaló el año pasado que su oficina planea iniciar un enfoque 'proactivo' centrado en el consumidor donde la Oficina encontraría la manera de trabajar con las compañías para identificar las brechas que pueden abordarse antes de que ocurran problemas serios[5]. Los marcos creados sin el beneficio de los aportes de la industria, particularmente las pequeñas empresas, se niegan a sí mismos una perspectiva única y valiosa, fácilmente disponible y cada vez más esencial.

ii) El principio de funcionalidad completa requiere ir más allá de hacer declaraciones de privacidad y compromisos de protección de datos, para demostrar cómo todos los procesos de datos y otros objetivos han sido y están siendo satisfechos (Principio 4). Al integrar privacidad y protección de datos en una determinada tecnología de información, proceso, sistema o arquitectura, debe hacerse de tal manera que no se deteriore la funcionalidad completa y que se satisfagan todos los intereses legítimos relacionados con la privacidad y la seguridad y se optimicen los requisitos.

La privacidad y la protección de datos a menudo se ubican en una forma de suma cero; es decir, como compitiendo con otros intereses legítimos, objetivos de diseño y capacidades técnicas en un dominio dado. Privacy by Design rechaza adoptar este enfoque: abarca objetivos adicionales legítimos y los acomoda de una manera innovadora y positiva. Todos los intereses y objetivos deben estar claramente documentados, las funciones deseadas articuladas, las métricas acordadas y aplicadas, y las compensaciones innecesarias o las consecuencias involuntarias rechazadas, a favor de encontrar una solución que permita la multifuncionalidad y los múltiples intereses de las partes interesadas.

[5] https://iapp.org/news/a/canadian-privacy-commissioner-announces-proactive-approach-to-enforcement/

Estas virtudes que hacen que Privacy by Design se destaque como un marco de privacidad global – el principio de ser proactivo sobre privacidad y el principio de inclusión de objetivos e intereses o suma positive -, debe llevarse a cabo con tres palabras clave en mente: consulta , cooperación y colaboración (3 C's). El proceso de consulta mantiene abiertas las líneas de comunicación. Se enfatiza la cooperación sobre la confrontación para resolver las diferencias. La colaboración se busca de manera proactiva mediante la búsqueda de alianzas para encontrar soluciones conjuntas a problemas emergentes de privacidad y seguridad. El desarrollo de una comprensión compartida ayuda a facilitar el enfoque en los derechos de privacidad del individuo y el logro de resultados innovadores y centrados en el usuario. Como siempre, el objetivo es comprender y ser receptivo a todas las perspectivas involucradas.

Piensa en la Suma Positiva No en la Suma Cero

Un reconocimiento adicional es obtenido por la creatividad y la innovación en el logro de todos los objetivos y funcionalidades de una manera integradora, de suma positiva (ganar/ganar). Las entidades que logran superar las opciones obsoletas de suma cero (ganar / perder) están demostrando un liderazgo global en temas de privacidad. La privacidad por diseño desafía a los legisladores, ejecutivos, expertos en tecnología y diseñadores, entre otros, a encontrar formas de lograr una mejor privacidad y protección de datos en una tecnología, sistema o dominio determinado de lo que es actualmente el caso, o propuesto, y para poder documentar y demostrar los logros para que otros puedan aprender de ellos, convirtiéndolos en mejores prácticas. ¿Por qué no podría esto aplicarse a esquemas de regulación de la privacidad?

El ambiente de privacidad continúa evolucionando. Entonces, al igual que las tecnologías que dan forma y remodelan el mundo en el que vivimos, la conversación sobre privacidad se debe renovar y enfocar continuamente. Actualmente, lo que está en juego es mucho; quizás más que nunca. La privacidad seguirá bajo la presión creciente de muchas fuerzas diferentes, incluidas las redes sociales en línea, la explosión de redes sociales, los gobiernos y las empresas que prestan servicios altamente individualizados y dependientes de la información.

La errónea visión de que la privacidad, en sí misma, reprime la innovación es un mito. Es una falsa dicotomía, construida sobre innecesarias concesiones. De hecho, es lo opuesto: ¡priorizar la privacidad impulsa la innovación! Obliga a los innovadores a pensar creativamente para encontrar soluciones que sirvan a múltiples intereses y funcionalidades.

Pero ¿cómo sobrevivirá la privacidad, como la base de nuestras libertades, impulsor de la prosperidad, como valor operativo y factor crítico de confianza habilitante, en un mundo donde el individuo rara vez está presente para ejercer control sobre su información personal, en medio de tales transacciones ricas en datos? El futuro de la privacidad digital puede depender del cambio del actual paradigma *online*.

Por algún tiempo, he sostenido que se necesita un nuevo "libro de estrategies". Necesitamos abandonar el pensamiento de suma cero (ganar / perder) y adoptar un paradigma de suma positiva (ganar / ganar) donde se pueda lograr tanto la innovación como la privacidad. Adoptar la privacidad por diseño es una forma poderosa y efectiva de integrar la privacidad en el "ADN" de una organización con el fin de establecer una base sólida para el análisis de datos que respalden la innovación, sin comprometer la privacidad. Me he referido a esto como la "compensación de kaprivacidad": proteger la privacidad del cliente produce grandes retornos, desde una mayor confianza del consumidor y una mayor confianza del cliente, hasta obtener una ventaja competitiva. Aquí es donde la privacidad actúa como un diferenciador significativo. He considerado tan vital la necesidad de este nuevo libro de estrategias, que recientemente formé el Consejo Internacional de Privacidad y Seguridad Global, por Diseño.

Este consejo internacional trata de promover la privacidad por diseño no solo dentro de las grandes empresas, sino de difundir el mensaje para que incluso las organizaciones pequeñas y medianas no solo reconozcan el valor de hacer que la privacidad y la seguridad sean esenciales, sino que también pueden implementar este enfoque en una forma proactiva

Para diseñar una protección de datos y privacidad práctica pero efectiva en una tecnología de información, organización o arquitectura en red determinada, los arquitectos de soluciones de privacidad generalmente deben tener en cuenta múltiples intereses legítimos (y, sí, a veces en competencia), y acomodarlos de manera óptima e innovadora.

Privacidad y Seguridad Globales por Diseño

Así, mientras nos encontramos en la tormenta perfecta y en medio de la reorganización de los regímenes de privacidad a medida que nos acercamos a la implementación de GDPR, estoy adoptando el enfoque de las 3 C's para llegar a una solución 'ganar-ganar' para atraer especial atención y disipar la opinión común de que las organizaciones deben elegir entre privacidad y seguridad pública o intereses comerciales (es decir, análisis de "big data"). El objetivo del consejo, idealmente el objetivo de todos, es educar a las partes interesadas para que las organizaciones públicas y privadas puedan desarrollar políticas y tecnologías donde la privacidad y la seguridad pública, y la privacidad y el análisis de datos, puedan trabajar juntos para lograr resultados positivos y beneficiosos. El Consejo Internacional sobre Privacidad y Seguridad Global por Diseño trabajará con compañías, comisionados nacionales de privacidad y profesionales de la tecnología, incluidas ONGs internacionales como Data Catalyst, para educar al público y crear conciencia sobre la privacidad por diseño. También reconocemos que las pequeñas empresas son grandes en Canadá: son el motor de la economía, su éxito es vital para la prosperidad de Canadá y sus contribuciones esenciales para redactar regulaciones de privacidad de datos eficaces y bien informadas.

El tercer objetivo del consejo es colaborar con los diseñadores de políticas tanto en gobiernos como en el mundo de loos negocios, con la esperanza de derribar el enfoque tradicional de "silo" para desarrollar estrategias de privacidad. Un enfoque más integrado para resolver el desafío de la privacidad, que incluya a las partes interesadas desde la concepción hasta la ejecución, dará lugar a reglas de privacidad nacional e internacional más informadas, efectivas y sostenibles en beneficio de todos.

Conclusión / Recomendaciones

La implementación del GDPR en la Unión Europea (y para todas las empresas que hacen negocios en Europa) se acerca rápidamente. Hay muchos aspectos del GDPR que son relevantes y progresivos. La inclusión de Privacidad por diseño (Protección de datos por diseño) como un pilar central es esencial para su éxito, y es también una lección que deben aprender los países que está creando sus propios marcos de privacidad de datos.

El momento es adecuado para Canadá y otras jurisdicciones que están empezando desde cero o revisando los regímenes legales de privacidad existentes, para no solo incluir Privacidad por Diseño, sino para recordar la Resolución 2010 del Comisionado de Datos Internacionales, aprobada por unanimidad, y que, entre otros compromisos resolvió: "*Fomentar la incorporación de los Principios Fundamentales de la Privacidad por Diseño en la formulación de políticas de privacidad y legislación dentro de sus respectivas jurisdicciones*".

La protección de la privacidad y la regulación de datos no son un ejercicio dual, sino que representan una colaboración esencial entre empresas y gobierno. Para los gobiernos que trabajan buscando soluciones sostenibles para regular las industrias dinámicas sin generar consecuencias no deseadas, es ahora el momento de involucrar a esas industrias. Comiencen por incorporar la Privacidad por Diseño como un principio central, adoptando un enfoque de suma positiva, comunicando a las pequeñas y medianas empresas con los legisladores, y generen un proceso integrado que incorpore a todos los interesados para crear un mejor producto que refleje una estructura de gobierno diseñada para la privacidad.
Abril 2018