Instituto de Transparencia
Acceso a la Información
Pública y Protección de Datos
Personales del Estado de Puebla

PRIVACIDAD POR DISEÑO Y PRIVACIDAD POR DEFECTO

La privacidad por diseño es un concepto desarrollado en la década de 1990 en Canadá, el cual se enfoca en la actualidad al ámbito de las Tecnologías de la Información y de la Comunicación, y busca combatir los efectos nocivos de la tecnología a la privacidad a través de la observancia de una filosofía que busca integrar la garantía de la privacidad en la propia arquitectura de la tecnología que se quiera desarrollar e implementar.

Esta filosofía persigue realizar un cambio de paradigma en el modelo de negocios, así como en la puesta en marcha de políticas públicas que conlleven un tratamiento de datos personales, de manera que los encargados del desarrollo de la tecnología a emplearse, tenga en consideración, desde la fase inicial de su diseño, los parámetros de protección de datos personales. Esto se traduce en que al momento de desarrollar políticas públicas o sistemas, plataformas, programas, aplicaciones y demás tecnología que conlleve un tratamiento de datos personales, los desarrolladores introduzcan los principios y deberes legales, así como los mejores estándares de protección de datos personales.

Asimismo, el cambio de paradigma referido se traduce en la práctica en la sustitución de la idea “Si alguien gana, otro pierde” por el de “Todos ganan”. Esta funcionalidad total consigue un equilibrio entre los intereses en juego, sumando a las partes a la causa de una política de privacidad basada en las ideas de responsabilidad proactiva, transparencia, lealtad y confidencialidad; lo anterior, sin menoscabo o perjuicio al modelo de negocio de que se trate, así como a la obtención de beneficios.

Es por ello que la privacidad por diseño se entiende como una herramienta útil para asegurar y garantizar la privacidad del usuario frente al apetito voraz de las empresas en su afán de recabar información personal, sobre todo cuando no existe una cultura de protección de datos personales y de cumplimiento normativo, responsabilidad y rendición de cuentas (“accountability”).

La privacidad debe concebirse como un elemento esencial y fundamental para el buen funcionamiento y operatividad de la tecnología a desarrollar y debe abarcar todos sus procesos: la incrustación de la privacidad en el diseño de la tecnología no tiene por qué disminuir o frenar su eficiencia, si se hace un buen diseño, configuración y equilibrio.

Los diseñadores, los inversores en el proyecto, y los procesos de negocio deben buscar la fórmula adecuada y equilibrada en base a la cual con el diseño de su tecnología todos ganen. En este sentido, se deben desprender de las ideas en virtud de las cuales el aumento en la calidad de la protección de la privacidad resultará en detrimento del negocio y de la efectividad y funcionalidad de la tecnología. En ese sentido, aquellos esquemas de negocio que implementen efectivas políticas de privacidad, claras y sensatas, tendrán éxito en la medida en que, poco a poco, la población vaya siendo consciente de la importancia en la protección y garantía de su información personal. Se deben

diseñar políticas de privacidad claras, que faciliten su conocimiento por parte de los usuarios: deben permanecer visibles y transparentes tanto para los usuarios como para agentes externos que puedan realizar verificaciones, con todo lo cual se genere confianza.

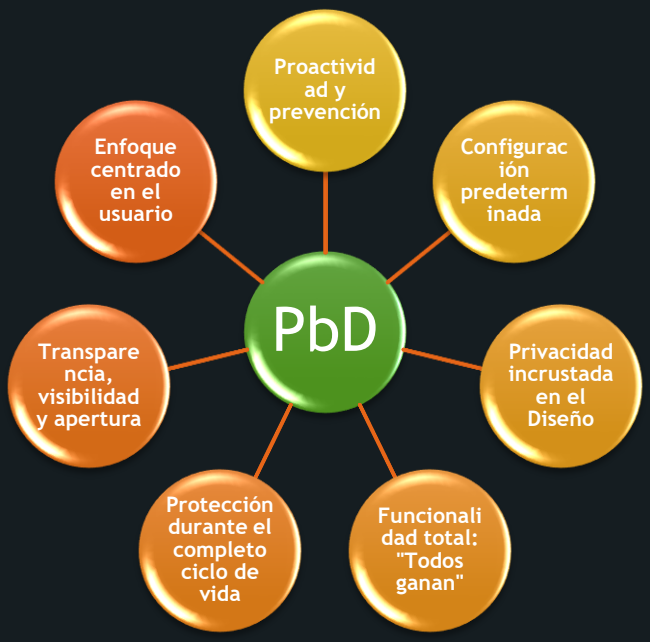
Por otro lado, el diseño debe incluir medidas que aseguren y garanticen la efectiva protección de la información de carácter personal, desde el primer hasta el último minuto en que el usuario es parte activa del sistema, programa, plataforma, o aplicación, e incluso después. Se trata de dotar al sistema de medias que protejan la información recabada desde que el usuario abre una cuenta y empieza a interactuar con la tecnología de que se trate, hasta que solicita su baja. Además, se debe incluir medidas que garanticen la efectiva eliminación de todo dato tratado y el rastro de éste dejado, siempre y cuando la finalidad para la cual dicha información fue recabada haya dejado de existir.

La protección al derecho debe ser de extremo a extremo, durante todo el ciclo de vida de la finalidad del tratamiento.

Respecto de la naturaleza de la información recabada y tratada, se tiene que tener en cuenta que, a mayor sensibilidad de los datos manejados, mayor debe ser el nivel de protección de dicha información. En este sentido, se debe seguir el principio de recabamiento de los datos estrictamente necesarios –principio de pertinencia o proporcionalidad–, evitando a toda cosa recabar información de forma indiscriminada, sobre todo cuando se trata de información delicada y que puede comprometer la esfera más íntima de la privacidad del usuario.

TRADICIONALMENTE, LA JERGA JURÍDICA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES HA IDENTIFICADO SIETE PRINCIPIOS QUE NUTREN LA IDEA DE PRIVACIDAD POR DISEÑO, Y QUE SON LOS SIGUIENTES:

- **Diseño PROACTIVO, no REACTIVO (Preventivo y no correctivo).**
- **Privacidad como configuración por defecto.**
- **Privacidad incrustada en el diseño.**
- **Funcionalidad total: “Suma Positiva” no “Suma Cero”.**
- **Seguridad en todo el ciclo de vida (End to End).**
- **Visibilidad y Transparencia (Keep it Open).**
- **Respeto a la Privacidad Personal (User Centric).**



Proactividad y no reacción, prevención y no corrección: los riesgos e impactos a los derechos y libertades de los titulares deben ser anticipados, ideando de manera proactiva medidas preventivas.

Privacidad integrada en el diseño: la arquitectura de la tecnología que se pretenda desarrollar y poner en uso, debe tomar en consideración desde su fase inicial de diseño los parámetros, principios, deberes y obligaciones de protección de los datos personales.

Privacidad como configuración predeterminada: los parámetros de seguridad y protección a la información de carácter personal que se recopile, deben estar habilitados por defecto.

Funcionalidad plena: en el diseño de la tecnología de que se trate, se debe buscar un equilibrio entre los intereses en juego, de tal forma que sea un ganar – ganar para todos los involucrados.

Protección del dato en todo el ciclo vital: en el diseño, desarrollo e implementación de la tecnología de que se trate, se debe buscar una seguridad de extremo a extremo, es decir, brindar una protección a los datos personales durante todo el ciclo vital de éstos. Esto asegura que todos los datos serán recabados y usados adecuadamente, y que también serán destruidos de manera apropiada al final del proceso, conforme corresponda.

Visibilidad y transparencia: se debe transparentar las condiciones, generales y particulares, de los procesos, fases, etapas y actividades a los cuales quedarán sujetos los datos personales recabados y tratados. Esta apertura no sólo debe realizarse de cara a las autoridades de control, sino también de cara a los usuarios, titulares de los datos personales que se recaban.

Enfoque centrado en el usuario: los diseñadores de la tecnología de que se trate, deben proveer mecanismos, medidas y esquemas de protección a la privacidad de los usuarios, que atiendan sus necesidades, y les posibilite jugar un rol activo en las decisiones en torno a la manipulación de sus datos personales, acceder a dicha información, y plantear dudas, quejas o reclamaciones en relación

a la manipulación de ésta. La arquitectura de la tecnología a desarrollar debe colocar al usuario -como titular de los datos que se recaban- en el centro de la operatividad de la misma.

La privacidad por diseño y por defecto se encuentra regulada en el artículo 25 del **Reglamento General de Protección de Datos Personales**, publicado en el Diario Oficial de la Unión Europea el 27 de abril de 2016, estableciendo lo siguiente:

> ***"1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.***
>
> ***2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.***
>
> ***(...)"***

En el ámbito de la legislación nacional, para el sector privado, ni la **Ley Federal de Protección de Datos Personales en Posesión de Particulares** ni su Reglamento, hacen referencia expresa en su articulado al modelo de privacidad por diseño. Sin embargo, el artículo 14 de dicha ley, establece que "El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por esta Ley, debiendo adoptar las medidas necesarias para su aplicación. Lo anterior aplicará aún y cuando estos datos fueren tratados por un tercero a solicitud del responsable. (…)". Por otro lado, el Reglamento de la citada ley, en su artículo 47, dispone que "En términos de los artículos 6 y 14 de la Ley, el responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquéllos que haya comunicado a un encargado, ya sea que este último se encuentre o no en territorio mexicano. Para cumplir con esta obligación, el responsable podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines." De todo lo cual, se advierte que los preceptos aludidos permiten a los responsables de los tratamientos de datos personales, por un lado, adoptar las medidas necesarias para cumplir con los principios de protección de datos personales, y por otro, recurrir a estándares, mejores prácticas internacionales o cualquier otro recurso para cumplir con dichas obligaciones legales. Es decir, el responsable debe adoptar medidas en cuanto al diseño de la tecnología que vaya a desarrollar e implementar, con la finalidad de garantizar la atención de los principios y deberes en la materia y, por tanto, el derecho fundamental a la protección de datos personales.

Ahora bien, en el ámbito del sector público, esta obligación se encuentra prevista en el artículo 30, fracciones VII y VIII, de la **Ley General de Protección de Datos Personales**, cuyo similar en la **Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla** establece lo siguiente:

> ***"ARTÍCULO 45***
>
> ***Entre los mecanismos que deberá adoptar el Responsable para cumplir con el principio de responsabilidad están, al menos, los siguientes:***
>
> ***(…)***
>
> ***VII. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el Tratamiento de Datos Personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia, y***
>
> ***VIII. Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el Tratamiento de Datos Personales, cumplan por defecto con las obligaciones previstas en la presente Ley y las que resulten aplicables en la materia."***

Asimismo, los artículos 15 y 16 de los **Lineamientos Generales en Materia de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla** refieren a la privacidad por diseño y por defecto, determinando lo siguiente:

> ***"ARTÍCULO 15. Para el cumplimiento de lo dispuesto en el artículo 45, fracción VII, de la Ley Estatal, el responsable deberá contemplar, desde la fase inicial de diseño, los principios y deberes previstos en las Leyes General y Estatal así como las medidas de seguridad y demás garantías en el tratamiento de datos personales, buscándose, en todo momento y de manera proactiva, la protección de los datos personales, la proporcionalidad y minimización de los datos recabados y tratados, así como la prevención a la vulneración de la privacidad de los titulares. En caso de que las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas, o cualquier otra tecnología que implique tratamiento de datos personales, ya se encuentren diseñadas y desarrolladas, el responsable deberá implementar las pertinentes adecuaciones de conformidad con la legislación.***
>
> ***ARTÍCULO 16. Para el cumplimiento de lo dispuesto en el artículo 45, fracción VIII, de la Ley Estatal, el responsable deberá aplicar garantías, medidas y configuraciones de privacidad de mayor protección por encima de las de menor protección, preestableciéndose por defecto las primeras, y buscando, en todo momento, la minimización de datos, el control de accesos, y la indicación de plazos de conservación e información transparente y entendible."***

BIBLIOGRAFÍA:

- Reglamento General de Protección de Datos Personales, publicado en el Diario Oficial de la U.E. el 27 de abril de 2016.

- Ley Federal de Protección de Datos Personales en Posesión de Particulares, publicado en el Diario Oficial de la Federación el 5 de julio de 2010.
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, publicado en el Diario Oficial de la Federación el 21 de diciembre de 2011.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, publicada en el Periódico Oficial del Estado de Puebla el 26 de julio de 2017.
- Lineamientos Generales en Materia de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, publicados en el Periódico Oficial del Estado de Puebla el 19 de junio de 2018.
- Ana Brian Nougrères, “La protección inteligente de los datos personales: Privacy by design (PbD)”, 2012.
- GEV Asesores Internacionales, S.C., “Proyecto: “Privacy by design para fomentar la figura del encargado [Procesos 2013]”, 2014.
- PREVENSYSTEM, “¿Qué es la Privacidad desde el diseño?”, (sin fecha). https://www.prevensystem.com/internacional/prevensystemnoticias.php?id=807#submenuhome