INICIATIVA QUE REFORMA LOS ARTÍCULOS 7, 9 Y 11 DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES, SUSCRITA POR EL DIPUTADO JOSÉ SALVADOR ROSAS QUINTANILLA E INTEGRANTES DEL GRUPO PARLAMENTARIO DEL PAN

El suscrito, José Salvador Rosas Quintanilla, integrante del Grupo Parlamentario del Partido Acción Nacional en la LXIV Legislatura del Congreso de la Unión, con fundamento en los artículos 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos; y 6, numeral 1, fracción I, 77 y 78 del Reglamento de la Cámara de Diputados, somete a consideración de esta asamblea la presente iniciativa con proyecto de decreto, por el que reforman los artículos 7, 9 y 11 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, al tenor de los siguientes

Considerandos

Con el auge de las tecnologías de la información, la manera en que se realizan las actividades cotidianas del día a día en México ha sufrido severos cambios en las últimas dos décadas. El flujo inmediato de información y su uso para elaborar documentos, agilizar trámites y facilitar la comunicación entre personas, son tres de sus principales características, las cuales han reajustado la manera en la cual interactuamos, desarrollamos rutinas y aprendemos o desarrollamos nuestras obligaciones educativas o laborales.

Como consecuencia de esto, la creación de un mundo hiperconectado, donde las actividades cotidianas se llevan a cabo a través de medios electrónicos con la capacidad de registrar una serie inimaginable de la actividad de sus usuarios, se requiere adoptar una postura general acerca del papel y los problemas que plantean esta clase de tecnologías para la población en general y especialmente sobre grupos vulnerables, como adultos mayores y niños.

La conservación de registros de esta clase, la cual tiene un carácter central para la operación de muchas plataformas, deriva en la creación de un "bien" que no solamente es útil para el usuario, sino también para la plataforma y el creciente "mercado de datos".[1] Esto, conjugado con la "brecha" digital (generacional, económica e intelectual), en sus aspectos privados y públicos, es únicamente una suma de ingredientes que puede generar consecuencias catastróficas para el futuro de la ciudadanía, la incidencia efectiva por parte del Estado para la salvaguarda de nuestros connacionales y, por tanto, la generación de confianza hacia grandes organizaciones, ya sean estatales o empresariales, las cuales cumplen funciones orgánicas para el resto de la comunidad.

Sobre esto, plantear el peso que la información personal tiene hoy en día pareciera una obviedad. El trabajo de inteligencia, es decir, el hecho de producir información acerca de algún tema o grupo de personas, ha sido parte intrínseca para el desarrollo de las sociedades contemporáneas. El control sobre el acceso y producción de información es visto como ventajoso al otorgar elementos relevantes para la toma de decisiones y la planificación en el plano de la política pública.

Con la consolidación de la estadística como método y el financiamiento por parte del Estado mexicano para entender a la población, donde como resultado se gestaron el Instituto Nacional de Estadística y Geografía en 1983 y del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI, hoy INAI) en 2002, por dar ejemplos muy concisos, resulta claro que el propio gobierno mexicano ha asumido la relevancia de la producción de información y su valía en la gestión pública. A pesar de ello, la actualidad ha preservado la valía de la información, pero ha encontrado nuevos nichos para su elaboración.

Un escenario de este tipo, donde la legislación nacional e internacional ha mostrado que los fenómenos de la realidad cotidiana superan con creces las regulaciones por parte de los Estados contemporáneos.

Ello se debe a que el marco legal no considera, en gran parte de los casos, situaciones que involucran factores que no existían al momento de la elaboración de las normatividades para su respectiva época.

La implantación de una reforma en ciberseguridad por parte de la Unión Europea en 2017[2] y por el gobierno de Estados Unidos de América en 2013,[3] han mostrado la relevancia del involucramiento estatal en el cuidado y gestión de la información en ambos sectores.

En el caso concreto de México, la situación es similar al estado de cosas en el que se encontraban los países desarrollados hace 5 o 10 años, donde se carece de un cuerpo integral de leyes que puedan hacer frente al fenómeno de las múltiples plataformas que preservan la información personal de los usuarios, hacen uso de ella de manera operativa para el otorgamiento del servicio, pero que a su vez generan prácticas que atentan contra el consentimiento explícito de las personas involucradas, donde agentes propios de las empresas o externos (vulneraciones de seguridad, o *hacking),* como los cibercriminales, obtienen algún tipo de beneficio con dicha información, exponiendo a los usuarios a peligros desconocidos e impensados para ellos. Por usar una analogía, los servidores operan como "bancos de datos", con los cuales se puede obtener un beneficio "invirtiéndolos" de manera correcta. Por ello se vuelven "botines" atractivos para personas involucradas en el crimen, los cuales pueden usar o vender dicha información y que usualmente se emplea para robos de identidad o extorsiones,[4] por ejemplo.

Ambas acciones, las realizadas por los poseedores de los "bancos de datos" y su "inversión", como las realizadas por el acceso a dicha información de manera ilegal por parte de cibercriminales, requieren de una normatividad pertinente. En el caso de las primeras, la generación de beneficios no debe de atentar contra los derechos humanos de la ciudadanía, donde la relación con el propietario del servicio deba de tener suficiente transparencia acerca de la ubicación y uso de dicha información, la cual deba de ser asequible e intuitiva para el usuario, especialmente en grupos vulnerables como niños y adultos mayores. En el caso de las segundas, la colaboración entre instituciones estatales y privadas protege la operación del modelo de negocio y, a su vez, de la información personal de la ciudadanía.

En sus implicaciones sociales, el mayor beneficio pasa para poblaciones vulnerables como niños y adultos mayores. La falta de transparencia en el uso y cuidado de la información personal, al igual que el incremento de actividades relacionadas al cibercrimen (el cual aumentó en México en 32 por ciento en 2018),[5] pueden tener un efecto relevante en grupos vulnerables. Ejemplificando, el proceso de aceptación de términos y condiciones tiende a ser confuso y poco práctico. Los adultos mayores, en muchos casos, no están familiarizados con el uso de dispositivos y requieren de configuraciones especiales, ya sea por la brecha generacional o por problemas físicos o psicológicos, para hacer uso de estas plataformas. Comprometerlos a consensos sin una paridad de condiciones, asumiendo que sí hay una igualdad, es una actividad que requiere ser erradicada en favor de una sociedad democrática y de libre acceso a la información.

El caso de jóvenes y niños es igualmente relevante. El uso cotidiano hace que este grupo se les considere "nativos digitales", pero eso no implica que sean "nativos legales". Los riesgos que tiene la filtración de datos personales de niños mexicanos es algo a considerar para el presente y futuro del país. La posibilidad de que la trayectoria de vida de una persona, de principio hasta el momento que se consulte, pueda ser registrada y vendida al mejor postor es una cosa que es indeseable, atenta contra los derechos de la ciudanía y puede tener consecuencias irreparables en la vida de las personas, por lo que abogar por evitar un futuro, muy cercano, de esta clase debe de ser prioritario para el ejercicio legislativo nacional.

Debido a ello, la posesión de dicha información es un tema sensible, donde lo óptimo sería disponer de los medios para evitar atropellos o abusos por parte de los poseedores, autorizados o no, de dicha información.

La necesidad de mantener reguladas las actividades que impliquen una recolección de datos privados ya tiene un referente existente en México mediante la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

En sus objetivos, plasmados en su artículo 1, se sostiene que "**tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas".** [6]

En favor de ello y al hacer una revisión de la ley, los artículos 7, centrado en la transparencia del proceso de transferencia de datos personales, 9, en la autorización "formal" del uso de datos personales "sensibles", y 11, en el tratamiento de la información con la finalización del uso de los datos personales por parte de los particulares y su relación con el usuario del servicio, están orientados al propósito de la legislación, pero requieren de modificaciones para contemplar situaciones que hoy son visibles y requieren ser consideradas en la actual legislación.

Generar herramientas legales para evitar el uso y abuso de esta clase de información es una cuestión prioritaria para las demandas actuales de la política contemporánea. Igualmente, implementar mecanismos de transparencia colabora en la creación de una "pedagogía digital" y un uso responsable de esta clase de medios. La sensibilidad que conlleva la concentración de la información, el uso de datos personales y su impacto en la realidad cotidiana es algo que puede ser considerado desde la política pública en favor de los actores, públicos y privados, que desean ajustarse al bienestar de la comunidad y el apego a la ley en favor de un mejor futuro para la nación.

A efecto de clarificar los cambios que se proponen se muestra continuación el siguiente cuadro:

Ley Federal de Protección de Datos Personales en Posesión de los Particulares	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
VIGENTE	**MODIFICACIÓN**
Artículo 7.- Los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta Ley y demás normatividad aplicable. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos. En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta Ley. … **Artículo 9.-** Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las	**Artículo 7.-** Los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta Ley y demás normatividad aplicable. La obtención de datos personales no debe hacerse a través de medios engañosos, fraudulentos **o incomprensibles para sectores de población vulnerables.** En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta Ley. … **Artículo 9.-** Tratándose de **cualquier tipo de datos personales**, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca. No podrán crearse bases de datos que contengan datos personales ~~sensibles~~, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

actividades o fines explícitos que persigue el sujeto regulado. … **Artículo 11.**- El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados. Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	… **Artículo 11.**- El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron **consensuados entre los partícipes**. Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, **deberá presentarse un reporte general de la situación de la información, donde se especifique qué datos fueron almacenados, dónde estaban almacenados, su respectivo uso durante el tiempo que fue almacenado y las posibles vulneraciones de seguridad que pudieran afectar al usuario del servicio, el cual deberá de ser entregado en un plazo no mayor a dos meses**. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de **seis meses**, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.

Con esto se ejemplifica de manera explícita el argumento para proponer la siguiente iniciativa con proyecto de

Decreto por el que se reforman los artículos 7, 9 y 11 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Único. Se **reforman** los artículos 7, 9 y 11 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, para quedar de la siguiente manera:

Artículo 7. ...

La obtención de datos personales no debe hacerse a través de medios engañosos, fraudulentos o incomprensibles para sectores de población vulnerables.

...

...

Artículo 9. Tratándose de cualquier tipo de datos personales, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca.

No podrán crearse bases de datos que contengan datos personales, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

...

Artículo 11. El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron consensuados entre los partícipes.

Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberá presentarse un reporte general de la situación de la información, donde se especifique qué datos fueron almacenados, dónde estaban almacenados, su respectivo uso durante el tiempo que fue almacenado y las posibles vulneraciones de seguridad que pudieran afectar al usuario del servicio, el cual deberá de ser entregado en un plazo no mayor de dos meses.

El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de seis meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.

Transitorio

Único. El presente decreto entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.

Notas

1 Editorial El País (2018). "Mercado de datos y miedo digital", 17 de febrero de 2020, de *El País*. Sitio web: https://elpais.com/economia/2018/05/24/actualidad/1527180839_511844.html

2 Consejo de la Unión Europea (2018). *Reforma de la ciberseguridad en Europa,* 17 de febrero de 2020, de Consejo de la Unión Europea. Sitio web: https://www.consilium.europa.eu/es/policies/cyber-security/

3 Office of the Press Secretary (2013). *Executive order on improving critical infrastructure cybersecurity,* 17 de febrero de 2020, de Office of the Press Secretary. Sitio web: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/execut ive-order-improving-critical-infrastructure-cybersecurity-0

4 Notimex (2019). "'Verificar información, clave para evitar robo de identidad': expertos", 17 de febrero de 2020, de *El Economista.* Sitio web: https://www.eleconomista.com.mx/finanzaspersonales/Verificar-informacio n-clave-para-evitar-robo-de-identidad-expertos-20190118-0016.html

5 Forbes Staff (2018). "Ciberataques en México crecieron 35 por ciento en últimos 12 meses", 17 de febrero de 2020, de *Forbes.* Sitio web: https://www.forbes.com.mx/ciberataques-en-mexico-crecieron-35-en-ultimo s-12-meses/

6 Felipe de Jesús Calderón Hinojosa (2010). Ley Federal de Protección de Datos Personales en Posesión de los Particulares. 17 de febrero de 2020, de Diario Oficial de la Federación. Sitio web: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Dado en el Palacio Legislativo de San Lázaro, a 5 de marzo de 2020.

Diputado José Salvador Rosas Quintanilla (rúbrica)