Plataforma para la federalización de la data personal

Heriberto Pérez
Profesionista informático

Resumen

Este artículo presenta una posible solución para gestionar el uso y compartición de datos personales, independientemente de su naturaleza y tipificación, aprovechando los modelos operativos y las tecnologías empleadas en la transformación digital.

PALABRAS CLAVES:
Transformación Digital, Gobierno Digital, Data Personal, MDM, Cliente Único

¿Recuerda usted a quién le ha compartido sus datos personales, sabe cuales datos compartió y con qué propósito los proporcionó? creo que ni usted ni nadie es capaz de responder esto a ciencia cierta, y si bien la privacidad es considerada un derecho humano, al menos en la Unión Europea, su logro es algo que está aún muy lejos de cumplirse en un entorno donde se generan cantidades masivas de información cada segundo y donde nos vemos obligados a proporcionar cada vez más datos personales a fin de consumir más bienes y servicios en un mundo cada vez más digitalizado.

El problema no es sencillo, empezando por la definición de qué son los Datos Personales, al respecto, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LGDPPP) establece en su Artículo 3 las siguientes Fracciones:

> *V. Datos personales: Cualquier información concerniente a una persona física identificada o identificable.*
>
> *VI. Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.*

Así mismo, el Reglamento General de Protección de Datos de la Unión Europea (GDPR por sus siglas en inglés) establece lo siguiente en su Artículo 4, Fracción Primera:

> *A efectos del presente Reglamento se entenderá por:*
> *1) | «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;*

Así pues, mientras que la legislación mexicana considera los datos personales como aquellos que puedan identificar a una persona y aquellos otros que sean "íntimos", la legislación europea sólo se ocupa de los datos comprendidos en el primer rubro, no obstante en ese punto la ley mexicana es más ambigua, y no es la excepción, pues en los Estados Unidos, aún se debate si la dirección IP de un usuario de internet debe considerarse o no, como información personalmente identificante (PII, por sus siglas en inglés). En todo caso es importante recordar que la GDPR es regulación de alcance global y que es ya el referente para todas las regulaciones al respecto.[1]

Dejando fuera de aquellos datos que sirvan para identificarnos individualmente, considero que en todos los demás casos nunca habrá un consenso absoluto, pues el concepto de intimidad o privacidad es algo relativo a cada persona, y además esa opinión puede cambiar con el tiempo. Así pues, la solución ideal debería dejar a criterio de cada individuo la selección y modificación de lo que para él o ella es algo íntimo o privado.

El presente artículo propone una solución práctica para gestionar los datos personales de forma individual y modificable en el tiempo, imitando un poco las estrategias adoptadas en la transformación digital que actualmente se vive en otros ámbitos. Así como Uber y Air B&B modificaron el modelo de negocio de la transportación pública y del alojamiento a través de la creación de plataformas digitales para conectar a prestadores de servicios y usuarios, esta solución buscaría *plataformizar* el uso de los datos personales (cualesquiera que estos sean) con el fin de centralizar su gestión y las solicitudes de acceso.

Grosso modo el caso de uso sería el siguiente, una vez que usted se hubiese identificado biométricamente, obtendría una clave de registro en la plataforma y llenaría un formato predefinido con sus *datos personales*, que para no entrar en polémicas y para los términos de este ejemplo serían aquellos que comprenden los que le solicitan para tramitar su pasaporte o licencia de conducir, hasta los que deja en la escuela de sus hijos o en la tintorería, lo importante es recordar que este universo de datos personales podría crecer o decrecer por usuario y con el tiempo. Esta data se resguardaría en un repositorio de datos en la nube para hacerla accesible a través de una plataforma digital, una *app* para teléfono móvil por ejemplo. Posteriormente, y de la misma forma en que usted concede permisos a las aplicaciones que descarga en su celular, usted concedería privilegios de lectura a las solicitudes de acceso a su información personal que le llegaran a través de esta plataforma. Así pues, cuando fuese a inscribirse a un gimnasio o a contratar una nueva línea de teléfono móvil, estos establecimientos solo les solicitarían su *clave de registro* en la plataforma, y a usted le llegaría una notificación de aprobación de lectura sobre los datos obligatorios y opcionales que el prestador de servicios requiriese y deseara saber.

Es importante notar que estos permisos se otorgarían por dato y por solicitante dado que mientras la tintorería necesitaría conocer su domicilio exacto para hacer entregas, el gimnasio solo desearía conocer opcionalmente su colonia para conducir sus estudios demográficos. La otorgación de permisos sería tan fácil como palomear los grupos de datos requeridos y los opcionales, y en cualquier momento podría revisar con más calma la data que le solicita el prestador y despalomear los datos opcionales en dado caso.

[1] https://expansion.mx/bespoke-ad/2018/06/08/como-cumplir-con-la-gdpr

Si bien el uso obligatorio de esta plataforma conllevaría costos importantes para su implementación por parte de los prestadores de servicios, los beneficios que les acarrearía sobrepasarían por mucho tal inversión pues el primer beneficio y el más obvio, sería la reducción de los riesgos y costos asociados al cumplimiento de la normatividad aplicable, ya que el riesgo de incumplimiento se habría trasladado efectivamente al operador de la plataforma. No obstante, un beneficio aún mayor sería que mediante el uso de esta plataforma los prestadores de servicio estarían adquiriendo un catálogo único de personas, llámense clientes, usuarios, huéspedes, pacientes, etc. y que presumiblemente siempre estaría actualizado y por lo que sería 100% confiable pues distinguiría perfectamente a Juan López Pérez padre de Juan López Pérez hijo (ambos con madre de apellido Pérez) que viven en el mismo domicilio y que comparten la misma cuenta de correo y número de telefonía móvil porque trabajan juntos. Actualmente las inversiones para consolidar los catálogos de personas para así poder conformar una *vista 360° del cliente* son millonarias[2], no son 100% confiables, y fácilmente pueden quedar desactualizadas. Así que los ahorros asociados a mantener unificados y actualizados estos catálogos, aunados al valor de la analítica que se podría derivar de ellos, podrían pagar la inversión de adoptar esta plataforma en muy poco tiempo.

Para nosotros, los dueños de esta data, los beneficios también serían considerables, pues si bien regulaciones como la del GDPR permiten actualizar y exportar nuestros datos personales a otros sitios, seguimos teniendo el problema de tener que recordar todos los lugares donde ingresamos estos datos. Con esta plataforma recordar esto ya no sería necesario, sabríamos exactamente quienes tienen acceso a nuestros datos y hasta cuando, y podríamos revocar estos permisos en los casos que así procediera. Así mismo, la experiencia de registro para adquirir nuevos servicios sería mucho más ágil y estándar, lo cual también sería un beneficio para el prestador de servicios.

Por otro lado, el contar con un repositorio de datos personales presumiblemente confiable y actualizado, sería un botín llamativo para criminales o un instrumento del que la autoridad gubernamental pudiese abusar, por lo tanto dicha plataforma tendría que garantizar que esta data no fuese sujeta a robo, alteración, secuestro o destrucción, y las solicitudes de información por parte de las autoridades tendrían que estar debidamente protocolizadas en la ley. Así mismo, y con la finalidad de que la autoridad no fuese juez y parte, la gestión de esta plataforma debería quedar en manos de un organismo descentralizado (en México, una posibilidad sería asignarla al RENAPO y desvincular este organismo de la Secretaría de Gobernación, nótese que en este caso la clave de registro sería la CURP).

Si bien garantizar la prevención del robo, alteración, secuestro o destrucción de esta data es tecnológicamente posible, evitar el abuso por parte de la autoridad o de prestadores de servicios que ya tengan acceso a ella no lo es tanto, no obstante se podrían instrumentar mecanismos para identificar, prevenir y denunciar estos hechos. Uno de ellos sería que todos los accesos a la data personal serían auditables y generarían una notificación a su tutor. Así pues, en este contexto, habría tres variantes del caso de uso para solicitar información:

1. Solicitudes de prestadores de servicios aprobadas por el tutor de la data.

2. Requerimientos de la autoridad notificadas al, y aprobadas por, el tutor de la data.

3. Requerimientos de la autoridad ejecutiva con anuencia de la autoridad judicial y notificadas al tutor de la data salvo en los casos explícitamente previstos en la ley.

No obstante, en todos los casos el organismo descentralizado a cargo, mantendría una bitácora de estos requerimientos, la cual podría ser consultada en todo momento por la autoridad legislativa a fin de comprobar el buen uso de esta plataforma.

Nótese también que la data personal podría estar bajo la tutela de un tercero en los casos donde la per-

[2] https://www.prnewswire.com/news-releases/the-global-mdm-market-size-is-expected-to-grow-from-usd-281-billion-in-2018-to-usd-786-billion-by-2023-at-a-compound-annual-growth-rate-cagr-of-228-300625203.html

sona en cuestión fuese un menor, haya fallecido, se encontrara desaparecida, o bien careciera de las facultades físicas o mentales para gestionar sus datos personales.

Un beneficio adicional para los consumidores de esta data, y ciertamente una atribución del organismo encargado de esta plataforma, sería la validación de estos datos, y tratándose de un organismo gubernamental esta validación podría llevarse a cabo en conjunto con instituciones como el IMSS, el SAT o la SRE.

En la era digital la data es un activo y por lo tanto es sujeta de ser capitalizable, en este caso, con el fin de solventar la operación de la plataforma misma. Por el ejemplo, parte del presupuesto asignado a organismos como el INEGI o el RENAPO podría trasladarse a este nuevo organismo en virtud de los ahorros o eficiencias asociados a la minería de datos que pudieran haber, además de que esta misma información, debidamente anonimizada o seudonimada, también tendría un valor comercial importante para muchísimas empresas, después de todo estaríamos hablando de un catálogo único de personas, actualizado por ellas mismas y validado contra fuentes legales.

La transformación digital, no solo es una oportunidad para cambiar el status quo de los modelos de negocio, también es una oportunidad para hacer más eficiente al aparato gubernamental, mejorar los servicios que provee, y ¿por qué no? también proveer servicios disruptivos como el que se plantea aquí, el cual no solo beneficiaría a los ciudadanos, sino también a los consumidores de estos datos y además generaría ahorros e ingresos que podrían significar la autosustentabilidad de esta plataforma.

Día con día exponemos nuestros datos personales para la obtención de un sin fin de servicios y productos, y eso no va a cambiar ni en el corto ni el mediano plazo por que en muchos casos el conocimiento de los mismos es legítimo. No obstante, el uso indebido de esos datos vulnera nuestra seguridad y violenta nuestra privacidad, la única forma en que podamos tener un verdadero control de esta data y así saber quienes la consultan y hacen uso de ella, es federándola en una plataforma accesible al ciudadano para así garantizar su uso homologado, transparente y seguro.

La viabilidad técnica de esta plataforma no es tan compleja (bien pudiera ser el tema de un siguiente artículo), y los beneficios tanto para los tutores de la data como para sus consumidores superarían por mucho las inconveniencias de su implementación, no obstante, y como suele ser el caso, la voluntad política para su legislación e instrumentación podría ser minada por los intereses de unos cuantos.

Heriberto Pérez

Es un profesionista informático especializado en desarrollar estrategias y soluciones de integración, análisis y visualización de datos. Tiene una trayectoria profesional de más de veinte años y actualmente ha enfocado su trabajo en la aplicación de tecnologías semánticas en los campos de gobernanza de datos y de arquitectura empresarial.