Síntomas de la ausencia de gobernanza de datos en México

Por: Socialtic. 28/12/2021

La gobernanza de datos es el establecimiento de políticas y mecanismos para mantener el control de calidad, la gestión adecuada y la rendición de cuentas en todo el proceso de obtención, almacenamiento y uso de datos en instituciones públicas y privadas. Las políticas de gobernanza de datos son instrumentos que deben vislumbrar lo que puede afectar tanto la calidad de los datos mismos como a sus fuentes y clientes finales para prevenir y atender posibles problemáticas o impactos. Y ante esos escenarios, muchas veces las comunidades especializadas en datos solemos teorizar sobre políticas públicas, legislaciones y metodologías que puedan prevenir las posibles consecuencias e impactos ante la ausencia de gobernanza de datos.

En ocasiones, identificar estas consecuencias es un ejercicio abstracto puesto que se habla de lo que pudiera suceder. En conferencias, escritos académicos y conversaciones sobre políticas de gobernanza de datos se establecen escenarios de impacto ante la carencia o erraticidad de políticas de gobernanza de datos tanto para el sector público como el privado. Lamentablemente, en México estas historias ya son una realidad pública y conocerlas ayuda a esbozar los retos que enfrenta la gobernanza de datos en contextos similares.

A través de esta colaboración con ILDA, en una serie de publicaciones latinoamericanas, se describe el estado de la gobernanza de datos en la región. Este post narra focos naranjas y rojos de la ausencia y deficiencia de las políticas de gobernanza de datos en México con la finalidad de dejar tomar ejemplos reales para fortalecer o crear políticas realistas, operables y eficaces en otros países

Datos personales como insumo del crimen cotidiano

En México es común que la población sea víctima de extorsiones telefónicas y bancarias, cotidianamente se reciben llamadas con supuestas promociones, ofertas o alertas con la finalidad de engañar a personas usuarias de tarjetas de crédito con tal de recabar información personal que permita a grupos criminales realizar distintas

estafas como acceder a sus cuentas bancarias o utilizar sus tarjetas de crédito. Esta industria criminal está alimentada por múltiples bases de datos que se filtran y venden en un mercado ilegal que habilita que los números telefónicos, nombres completos y hasta números de tarjetas de crédito lleguen a manos de estos grupos delictivos.

Es difícil saber cuáles son los puntos de filtración de las bases de datos con información personal de la población mexicana. Igual pudieron haber surgido de un establecimiento comercial como de un banco o alguna empresa gestora de créditos. Del lado público también se sospecha de filtraciones de datos personales tanto de instituciones locales, estatales o nacionales. Y, a diferencia de lo que se suele leer de casos en países de América del Norte o Europa, en México no es necesario realizar complejos hackeos a la infraestructura tecnológica de una empresa o gobierno cuando ya existen redes de compra-venta de datos personales.

¿Cómo se pueden detener estas redes criminales en un país donde el sistema de investigación criminal y de justicia es deficiente? ¿Cómo se puede dar cuenta una persona de la fuente de filtración de sus datos personales? La ciudadanía mexicana no se preocupa ya por el origen de las filtraciones de sus datos personales, si no de evitar ser víctima de extorsión, estafa o robo de identidad. Esto se ha normalizado a tal grado que el Buró de Crédito, institución dedicada a la evaluación del crédito particular y empresarial, cuenta con un sistema de alerta que notifica al titular cuando otra persona esté solicitando un crédito mediante una suplantación de identidad.

Datos en tiempos de COVID

COVID hizo la obtención de datos personales por parte de empresas e instituciones públicas algo cotidiano. A medida que empezó a haber más pruebas de detección disponibles en el mercado, proliferó la oferta de pruebas tanto en gobiernos municipales y estatales como en centros de salud privados, laboratorios médicos, farmacias y establecimientos comerciales. En todos estos establecimientos se recogen detallados datos personales de quienes solicitan y/o adquieren una prueba. Pero los niveles de apego, por lo menos a lo establecido en la Ley de Protección de Datos, es variado. En el mejor de los casos, se puede encontrar un aviso de privacidad de manera visible en el establecimiento o en los formatos para llenado por los solicitantes de pruebas COVID.

¿Qué pasa con esos datos de identidad, contacto e historial de salud colectados en los formularios en papel, sitios web o apps asociados a pruebas de COVID? ¿Cómo puede una persona saber si esos datos van a ser resguardados de manera segura? ¿Se puede saber si la empresa o institución compartirá para otros fines o venderá esos datos para alimentar las redes ilegales de compraventa de datos personales? No se sabe y será prácticamente imposible evidenciarlo. Además, en ese momento a la ciudadanía no le es prioritario conocer si a quién le está entregando sus datos cuenta con políticas robustas para la protección de estos, pues está ahí para saber si tiene o no COVID.

A nivel nacional, la Secretaría de Salud ha dejado también incertidumbre sobre sus políticas de generación, control de calidad y gestión de los datos de vacunación. El proceso de registro para la vacunación ha sido a través de un formulario web asociado a la CURP (clave única de registro poblacional) pero al recibir la vacuna se debe llevar un formato impreso que se descarga de la plataforma de registro en donde se le escriben a mano datos personales adicionales (ej. sexo y edad) así como los datos del lote y fecha de vacunación. A la persona vacunada le entregan la mitad de la hoja de papel y la otra es resguardada para el registro de vacunación. Estas medias hojas de papel son retenidas por los equipos de vacunación en sitio y eventualmente capturados en el sistema de la Secretaría de Salud.

A medida que la vacunación se expandió, múltiples personas expresaron que alguna de las dosis de vacunación recibida no mostraba en él su certificado de vacunación que se descarga del sistema de la Secretaría de Salud. En el mejor de los casos, simplemente tomó semanas o meses de espera para que esta información se viera reflejada en el certificado de vacunación, pero miles de personas tuvieron que solicitar aclaraciones mediante el canal correspondiente en la plataforma web para que le actualizaran los datos de las vacunación apropiadamente.

En la vida cotidiana, instituciones públicas y privadas se adaptaron a la incertidumbre generada por la inexactitud de los certificados de vacunación. Para ingresar a pruebas o tratamientos médicos, por ejemplo, se volvió común que una persona pudiera llevar copia del “papelito” (media hoja de papel del formato de vacunación) como comprobante de haber recibido la vacuna. No obstante, mayores afectaciones las tienen las personas con certificados de vacunación incompletos o erróneos al acudir a instituciones que solicitan un documento de certificación oficial de vacunación y rechazan el “papelito” puesto que no tiene ningún tipo de sello o

certificación oficial de veracidad y puede ser fácilmente falsificable.

En contradicción a la proactividad mostrada por la Secretaría de Salud al inicio de la pandemia cuando construyó un portal de datos abiertos para dar a conocer los registros de casos de contagios, personas recuperadas y decesos con actualización diaria, los datos de vacunación se presentan totalizados en las diapositivas de las conferencias de prensa de la Secretaría de Salud. No ha habido publicación de datos abiertos y sólo se han podido acceder a datos granulares a través de solicitudes de acceso a la información, y en algunos casos los reportes oficiales no concuerdan con los datos otorgados a la ciudadanía. Este conflicto lo ha documentado en detalle el medio Serendipia.

Cuando una institución pública ejemplifica la apertura de datos en algún ámbito del combate a la pandemia y no en otro, deja más preguntas que respuestas relacionadas a su transparencia así como su gobernanza de datos. ¿Por qué hay distintos criterios de apertura de la información de los aspectos más relevantes en la gestión sanitaria? ¿Existen carencias o fallas relevantes en los procesos de generación de datos o gestión de la información? ¿Qué tan confiables son los procesos de captura manual de datos o los sistemas utilizados para gestionar las bases de datos?

La pandemia ha evidenciado las complejidades que enfrentan instituciones para obtener información relevante de calidad para poder gestionar las diferentes necesidades ciudadanas derivadas de la pandemia. Uno de estos han sido los mecanismos para generar, verificar, resguardar y publicar información clave para la toma de decisiones y la vida de la ciudadanía. La Secretaría de Salud se basó en la Política Nacional de Datos Abiertos para promover su portal de datos abiertos pero la ignoró manteniendo los datos de vacunación cerrados. Pregona su apego a la Ley de Protección de Datos Personales dejando en un acto de confianza ciega que los datos personales de vacunación de millones de personas se transformen y conserven de manera segura en todas sus etapas: los formularios de registro, los “papelitos” entregados en centros de vacunación y el sistema de certificados de vacunación.

Comercio de datos ante la tragedia

La gobernanza de datos debe tener en cuenta siempre la pregunta *¿qué puede salir mal?* para contemplar los controles y mecanismos de rendición de cuentas

necesarios para evitar que afectaciones o mal uso de los datos generen impactos en la institución, fuentes de origen o clientes finales. Lamentablemente, el reportaje Traficantes de ADN documentó una escabrosa historia que evidencia una cara perversa de ausencia de políticas y prácticas efectivas de gobernanza de datos personales.

En un país donde se estima que hay más de 95,000 personas desaparecidas, y" ante la falta de información sobre su paradero por parte de las autoridades, grupos de búsqueda exploran zonas en todos los estados buscando restos humanos, y empresas privadas han tenido acceso a las principales bases de datos genéticas del país para lucrar con el dolor de sus familiares. Es el caso de Central ADN, una empresa con acceso a una copia de la base de datos genéticos de la Procuraduría General de la República (PGR, ahora FGR) así como contactos al interior de instituciones de gobierno que utiliza para ofrecer apoyo a familiares de personas desaparecidas para su búsqueda. El reportaje detalla cómo representantes de la empresa contactan a grupos de búsqueda para ofrecer comparar perfiles genéticos de familiares con aquellos en la base de datos gubernamental y así orientar a familiares y grupos de búsqueda sobre el posible paradero de las personas desaparecidas que buscan.

"Traficantes de ADN" también narra el caso en donde una representante de Central ADN actualiza a una familiar de una persona desaparecida sobre el avance del caso puesto que tienen fuentes dentro del Gobierno. Al investigar a la empresa, describen a los accionistas como profesionistas de diversos perfiles profesionales en donde sobresalen algunos individuos con vínculos políticos, familiares y comerciales con distintos funcionarios (pasados y actuales) del gobierno.

Central ADN, así como otras empresas en el país, venden tecnología y servicios de análisis genéticos a dependencias públicas tanto a nivel nacional como en en los estados y municipios teniendo acceso a datos bajo un amplio abanico de niveles de restricciones en materia de privacidad. A ello se le añade el acceso a datos derivados de los análisis que realizan directamente con familiares y grupos de búsqueda para complementar su esquema comercial. El reportaje estima que el costo de un análisis genético es de entre $40 y $50 dólares americanos, infiriendo que, dado la magnitud de la crisis de personas desaparecidas en México, es una fuente de ingresos considerable.

Esta historia se conoce en parte porque existe una carpeta de investigación en

contra del primer comisionado de búsqueda que actualmente está vinculado a proceso y acusado de ejercicio indebido de la función pública presuntamente por haber entregado a Central ADN una copia de datos genéticos mientras dirigió la Comisión Nacional de Búsqueda (CNB) en 2018. Nadie más está bajo investigación. Se estima que la base de datos de la CNB contiene registros genéticos de más de cincuenta mil personas mientras que la actual base de la FGR supera los 90 mil.

La perversidad de este caso revela no sólo la corrupción que caracteriza a las instituciones públicas mexicanas sino el desarme con el que se llega a lucrar aprovechando la desgracia humana. La falta de controles en el resguardo y gestión de los datos genéticos sumado a contubernios corruptos entre privados y públicos deja preguntas desesperadas: ¿Será posible resguardar datos sensibles en instituciones débiles y corruptas? ¿Qué controles se deben establecer para evitar la transferencia ilegal de datos genéticos especialmente cuando son las empresas privadas quienes tienen la tecnología para proveer análisis especializados? ¿Es posible evitar que más personas en situaciones de desesperación buscando familiares sean clientes de esquemas comerciales basados en acceso ilegal de datos personales?

Los retos de la protección de datos personales en particular y la gobernanza de los datos en lo general, en contextos como el mexicano, supera las propuestas tradicionales de política pública. La complejidad de los contextos institucionales débiles e inmersos en corrupción e ilegalidad, en donde la impunidad es el desenlace común de la justicia, ha superado las leyes de protección de datos personales como principal recurso de defensa ante el abuso. Y tanto en la vida cotidiana como en momentos de angustia, la ciudadanía no tendrá como prioridad defender sus propios datos, más aún cuando carezca de información y herramientas institucionales para hacer frente a abusos y hacer valer su derecho a la privacidad.

En las próximas entregas de esta serie de análisis, reflexionaremos sobre el estado de las políticas públicas responsables para establecer e implementar gobernanza de datos en el ámbito público y privado. Bajo marcos de referencia para la gobernanza de datos analizaremos cuál es la situación de México así como posibles caminos para fortalecer acciones a favor de esquemas de gobernanza de datos más asequibles y realistas.

LEER EL ARTICULO ORIGINAL PULSANDO AQUÍ

Fotografía: socialtic

Fecha de creación
2021/12/28